Α.Τ.Ε.Ι. ΜΕΣΟΛΟΓΓΙΟΥ
ΣΧΟΛΗ:ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ:ΕΦΑΡΜΟΓΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΣΤΗ ΔΙΟΙΚΗΣΗ ΚΑΙ ΣΤΗΝ ΟΙΚΟΝΟΜΙΑ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΣΠΟΥΔΑΣΤΗΣ

ΚΑΤΣΙΜΠΑΣ ΔΗΜΗΤΡΙΟΣ

ΘΕΜΑ

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΑΚΗΣ ΔΙΑΚΙΝΗΣΗΣ ΠΛΗΡΟΦΟΡΙΩΝ ΜΕΣΩ INTERNET ΚΡΥΠΤΟΓΡΑΦΙΑ, ΤΑΥΤΟΤΗΤΕΣ, ΠΙΣΤΟΠΟΙΗΤΙΚΑ (Εφαρμογές με SSL και PGP)

ΕΙΣΗΓΗΤΗΣ: ΜΠΕΛΗΓΙΑΝΝΗΣ ΓΡΗΓΟΡΙΟΣ

ΜΕΣΟΛΟΓΓΙ 2004

ΠΡΟΛΟΓΟΣ

Η ανάπτυξη και επέκταση του διαδικτύου τα τελευταία χρόνια αυξάνεται με εκθετικούς ρυθμούς τόσο σε επίπεδο πλήθους χρηστών, όσο και σε επίπεδο παρεχόμενων υπηρεσιών. Μέσω αυτού διακινείται τεράστιος όγκος και μεγάλη ποικιλία πληροφοριών για κάθε λογής θέμα. Πλήθος ευαίσθητων πληροφοριών, όπως αριθμοί πιστωτικών καρτών και προσωπικών δεδομένων ταξιδεύουν τώρα στο διαδίκτυο και επιβάλλεται να προστατευτούν. Εξάλλου το internet είναι εκ φύσεως ιδιαίτερα ευπρόσβλητο σε επιθέσεις λόγω του σχεδιασμού του να επιτρέπει την κατά το δυνατόν ελεύθερη ανταλλαγή πληροφοριών, δεδομένων και αρχείων. Έτσι η ανοιχτή φύση του έχει επιτρέψει σε ικανούς χρήστες να ερευνήσουν και να ανακαλύψουν τα ευάλωτα σημεία του. Για το λόγο αυτό τα συστήματα ασφάλειας συνεχώς αναπτύσσονται και εξελίσσονται, αναζητώντας νέους τρόπους και τεχνικές που θα καλύψουν τα κενά ασφαλείας που δημιουργούνται. και θα βελτιστοποιήσουν την ασφάλεια των παρεχόμενων υπηρεσιών τους. Στην πτυχιακή αυτή περιγράφονται οι τεχνικές και τα πρωτόκολλα που χρησιμοποιούνται σήμερα για την ασφαλή διαδικτυακή διακίνηση ευαίσθητων πληροφοριών.

Στο 1° Κεφάλαιο γίνεται μια εισαγωγή στην κρυπτογραφία. Περιγράφονται οι βασικές έννοιες της κρυπτογραφίας, τα είδη της, οι αλγόριθμοι κρυπτογράφησης και συγχώνευσης μηνυμάτων, καθώς και οι επιθέσεις στα κρυπτοσυστήματα. Στο 2° Κεφάλαιο παρουσιάζονται τα κρυπτογραφικά συστήματα που χρησιμοποιούνται στο WEB σήμερα και ικανοποιούν τις βασικές απαιτήσεις ασφάλειας.(εμπιστευτικότητα, ακεραιότητα, απόδειξη γνησιότητας και μη απάρνηση). Στο 3° Κεφάλαιο περιγράφεται αναλυτικά το πρωτόκολλο SSL. Στ 4° Κεφάλαιο περιγράφονται οι βασικότερες τεχνικές αναγνώρισης ταυτότητας, οι ψηφιακές υπογραφές και τα πρωτόκολλα πιστοποίησης αυθεντικότητας. Στο 5° Κεφάλαιο γίνεται αναφορά στα ψηφιακά πιστοποιητικά, περιγράφονται οι αρχές και ιεραρχίες πιστοποίησης και η υποδομή δημοσίου κλειδιού (PKI). Στο 6° Κεφάλαιο παρουσιάζονται τα ψηφιακά πιστοποιητικά από τη μεριά του χρήστη και δίνονται παραδείγματα απόκτησης, εισαγωγής και εξαγωγής ψηφιακών πιστοποιητικών από τον Internet Explorer και τον Netscape Navigator. Τέλος στο 7° Κεφάλαιο γίνεται αναλυτική περιγραφή του προγράμματος προστασίας ηλεκτρονικού ταχυδρομείου PGP.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 1
ΚΡΥΠΤΟΓΡΑΦΙΑ

1.1 Εισαγωγή

Η κρυπτογραφία αναφέρεται στην υλοποίηση μεθόδων τροποποίησης των μεταδιδομένων πληροφοριών, έτσι ώστε να γίνονται κατανοητά μόνο από τον προβλεπόμενο παραλήπτη ή παραλήπτες. Είναι μια διαδικασία που μπορεί να εκτελεστεί τόσο σε υλικό (hardware) όσο και σε λογισμικό (software). Η ενσωμάτωση των μεθόδων της κρυπτογραφίας σε υλικό επιταχύνει σε μεγάλο βαθμό την διεκπεραίωση της. Επίσης, οι χρήστες δεν γνωρίζουν, ούτε καν αντιλαμβάνονται την παρουσία της και πραγματοποιούν ανενόχλητοι τις εργασίες τους. Το γεγονός ότι ο χρήστης δεν ανακατεύεται καθόλου στις διαδικασίες της κρυπτογραφίας, αυξάνει την αποτελεσματικότητα του εργαλείου στην παρεχόμενη ασφάλεια. Παρ' όλα αυτά, δεν έχει καθιερωθεί η κρυπτογραφία σε υλικό λόγω του υψηλού κόστους της, που απαγορεύει την αγορά και διατήρηση των ειδικών μηχανημάτων που χρειάζονται για την εφαρμογή της. Τα ειδικά αυτά μηχανήματα βρίσκονται τοποθετημένα σε στρατηγικά σημεία κάθε δικτύου.
Η λογισμική κρυπτογραφία είναι φτηνότερη, πράγμα που την κάνει ευρέως αποδεκτή και εύκολα πραγματοποιήσιμη. Βέβαια, δεν είναι το ίδιο γρήγορη με την εκτέλεση της σε υλικό, αλλά η ολοένα αυξανόμενη ανάγκη για διασφάλιση των επικοινωνιών εδραίωσε την χρήση της. Στην εργασία αυτή θα αναφερθούμε αποκλειστικά στην λογισμική κρυπτογραφία.

1.2 Ορισμοί

Ως *κρυπτογραφία* μπορεί να ορισθεί ο επιστημονικός κλάδος που ασχολείται με τη μετατροπή των πληροφοριών, με σκοπό τη διαφύλαξη του απορρήτου τους. Σκοπός της είναι να διασφαλίσει την ιδιοτικώτητα ενός μηνύματος με το να κρατά την πληροφορία "κρυφή" από οποιοδήποτε άτομο, το οποίο δεν έχει ορισθεί ως αποδέκτης του μηνύματος ακόμα και εάν έχει πρόσβαση στα κρυπτογραφημένα δεδομένα
Στην ορολογία της κρυπτογραφίας, το αρχικό μήνυμα που προορίζεται για κρυπτογράφηση ονομάζεται *απλό κείμενο* (plaintext ή cleartext). Η διαδικασία μετατροπής του περιεχομένου του μηνύματος σε μορφή τέτοια που να είναι μη κατανοητή για μη εξουσιοδοτημένους αποδέκτες ονομάζεται *κρυπτογράφηση*, ενώ το κρυπτογραφημένο μήνυμα ονομάζεται *κρυπτογράφημα* (ciphertext). Η κρυπτογράφηση ενός μηνύματος πραγματοποιείται με τη χρήση μιας μαθηματικής συνάρτησης η οποία ονομάζεται *κλειδί* (key).
Σε ορισμένους κρυπτογραφικούς μηχανισμούς χρησιμοποιείται το ίδιο κλειδί τόσο για τη διαδικασία της κρυπτογράφησης όσο και της αποκρυπτογράφησης, ενώ σε άλλους έχουμε διαφορετικά κλειδιά. Ως *αποκρυπτογράφηση* (decryption) ορίζεται η αντίστροφη διαδικασία κατά την οποία το κρυπτογραφημένο μήνυμα μετατρέπεται στο αρχικό απλό μήνυμα με τη βοήθεια ενός κλειδιού.

Εκτός από την κρυπτογραφία που έχει στόχο τη διατήρηση της μυστικότητας των μηνυμάτων υπάρχει και η *κρυπτανάλυση* (cryptanalysis) η οποία ορίζεται ως η «τεχνική» της παραβίασης του κρυπτογραφημένου μηνύματος, χωρίς να είναι γνωστό το κλειδί της αποκρυπτογράφησης. Η τεχνική της επινόησης κρυπτογραφημάτων και της παραβίασης αυτών είναι συνολικά γνωστή ως *κρυπτολογία*.
Παλαιότερα χρησιμοποιούσαν την κρυπτογράφηση αποκλειστικά για στρατιωτικούς σκοπούς. Στη σημερινή κοινωνία της πληροφορίας, η κρυπτογράφηση είναι ένα από τα βασικά εργαλεία διατήρησης του απορρήτου των μηνυμάτων με όλα τα προφανή πλεονεκτήματα. Ως αποτέλεσμα, η σύγχρονη κρυπτογραφία αποτελεί κάτι περισσότερο από απλή κρυπτογράφηση και αποκρυπτογράφηση δεδομένων. Για παράδειγμα, η πιστοποίηση αποτελεί μια εξίσου θεμελιώδη έννοια που συνδέεται άμεσα με την κρυπτογραφία. Όταν υπογράφεται ένα έγγραφο, είναι απαραίτητο να υπάρχουν μηχανισμοί με τους οποίους να μπορούμε να πιστοποιήσουμε τον κάτοχο του εγγράφου. Η κρυπτογραφία μας παρέχει μηχανισμούς για τέτοιες διαδικασίες. Η ψηφιακή υπογραφή (digital signature) «συνδέει» ένα έγγραφο με τον κάτοχο ενός συγκεκριμένου κλειδιού, ενώ η ψηφιακή χρονοσφραγίδα «συνδέει» ένα έγγραφο με το χρόνο της δημιουργίας του.

Γενικότερα, η κρυπτογράφηση μπορεί να χρησιμοποιηθεί σε μια πληθώρα εφαρμογών όπως:

- Προστασία δεδομένων, αποθηκευμένων στον υπολογιστή, από μη εξουσιοδοτημένη πρόσβαση.
- Προστασία δεδομένων κατά τη μεταφορά τους ανάμεσα σε δύο υπολογιστικά συστήματα.
- Ανίχνευση τυχαίας ή εσκεμμένης αλλαγής σε δεδομένα.
- Πιστοποίηση της ταυτότητας του συντάκτη/ εκδότη ενός κειμένου ή μηνύματος.

Βέβαια, η κρυπτογράφηση έχει και μειονεκτήματα, όπως το γεγονός ότι δε μπορεί να αποτρέψει τη διαγραφή δεδομένων από έναν εισβολέα του συστήματος. Επίσης, κατά τη διάρκεια μιας επίθεσης μπορεί να μεταβληθεί το πρόγραμμα κρυπτογράφησης, ώστε να χρησιμοποιεί διαφορετικό κλειδί από αυτό που έχει καθοριστεί από το νόμιμο χρήστη ή να καταγραφούν όλα τα κλειδιά για μελλοντική χρήση. Επιπλέον, μπορεί να βρεθεί ένας εύκολος και όχι ευρέως γνωστός τρόπος για την αποκωδικοποίηση μηνυμάτων και, τέλος, μπορεί ένα αρχείο να προσπελασθεί πριν την κωδικοποίηση του ή μετά από την αποκωδικοποίηση του. Οι παραπάνω λόγοι συντελούν στο να χρησιμοποιείται η κρυπτογράφηση ως μέρος της "αρχιτεκτονικής ασφάλειας" ενός συστήματος και όχι ως υποκατάστατο όλων των υπαρχόντων μηχανισμών ασφάλειας.

1.3 Ιστορική αναδρομή

1.3.1 Η κρυπτογραφία κατά τους αρχαίους χρόνους

- Κατά το 1900 π.Χ. στην Αίγυπτο για πρώτη φορά χρησιμοποιήθηκε μια παραλλαγή των τυπικών ιερογλυφικών της εποχής για την επικοινωνία.

- Μια από τις παλαιότερες αναφορές στην κρυπτογραφία υπάρχει στην Ιλιάδα του Ομήρου, όπου αναφέρεται η αποστολή ενός κρυπτογραφημένου μηνύματος από τον Βελλερεφόντη.
- Ο δίσκος της Φαιστού, 17ος αιώνας π.Χ. δεν έχει ακόμα αποκρυπτογραφηθεί. Ο Ηρόδοτος περιγράφει πώς μεταφέρονταν κρυπτογραφημένα μηνύματα από τους αγγελιοφόρους. Οι αρχαίοι Εβραίοι κρυπτογραφούσαν κάποιες λέξεις στις περγαμηνές τους.
- Ο Πολύβιος ήταν ο πρώτος που χρησιμοποίησε αριθμούς σε μορφή πίνακα για την κωδικοποίηση γραμμάτων.
- Η πρώτη καταγεγραμμένη χρήση της κρυπτογραφίας για επικοινωνιακούς σκοπούς είναι από τους Σπαρτιάτες το 400 π.Χ. που χρησιμοποιούσαν τον αλγόριθμο της σκυτάλης για την επικοινωνία ανάμεσα στους στρατηγούς τους. Χρησιμοποιούσαν έναν ξύλινο κύλινδρο γύρω από τον οποίο τύλιγαν μια ταινία από δέρμα και έγραφαν το μήνυμα. Όταν η ταινία ξετυλιγόταν τα γράμματα ήταν ανακατεμένα και μη αναγνώσιμα. Για να διαβάσει κάποιος το μήνυμα έπρεπε να τυλίξει την ταινία σε ένα κύλινδρο ίδιων διαστάσεων.
- Οι Φαραώ συνήθιζαν να γράφουν τα μηνύματά τους στο ξυρισμένο κεφάλι κάποιου σκλάβου και να τον στέλνουν στον παραλήπτη όταν τα μαλλιά του είχαν ξαναμεγαλώσει. Αυτός δεν είχε παρά να ξυρίσει το σκλάβο για να διαβάσει το μήνυμα. Μερικές φορές απλοποιούταν η αποστολή στέλνοντας μόνο το κεφάλι. Η μέθοδος αυτή είχε προφανή προβλήματα και η αξιοπιστία της επιβαρυνόταν ακόμα περισσότερο από τη συνήθεια των σκλάβων να προσπαθούν να απελευθερωθούν από τα αφεντικά τους.
- Οι Αιγύπτιοι ιερείς χρησιμοποιούσαν μέθοδο αντίστοιχη με τη σκυτάλη των Σπαρτιατών, την οποία χρησιμοποίησε και ο Ιούλιος Καίσαρας. Επίσης μεθόδους κρυπτογραφίας είχαν αναπτύξει και οι Αριστοτέλης, Πυθαγόρας και Νέρωνας.
- Ο Ιούλιος Καίσαρας (100 – 44 π.Χ.) χρησιμοποίησε μια απλή αντικατάσταση στο κανονικό αλφάβητο (μετακίνηση – shift των γραμμάτων κατά μια προκαθορισμένη ποσότητα – τρία γράμματα) στις "κυβερνητικές" επικοινωνίες (Caesar cipher). Ο Αύγουστος Καίσαρας χρησιμοποίησε την ίδια μέθοδο μετακινώντας κατά ένα γράμμα

1.3.2 Η κρυπτογραφία από το μεσαίωνα μέχρι τον 20ο αιώνα

- Οι πρώτοι που κατάλαβαν καλά τις αρχές της κρυπτογραφίας και της κρυπτανάλυσης ήταν οι Άραβες. Κατασκεύασαν και χρησιμοποίησαν αλγόριθμους αντικατάστασης και μετατόπισης και ανακάλυψαν τη χρήση της συχνότητας των χαρακτήρων και των πιθανοτήτων στην κρυπτανάλυση. Έτσι το 1412 ο Al-Kalka-Shandi συμπεριέλαβε την περιγραφή αρκετών κρυπτογραφικών συστημάτων στην εγκυκλοπαίδεια Subh al-a'sha και έδωσε σαφείς οδηγίες και παραδείγματα για την κρυπτανάλυση κρυπτογραφημένων κειμένων χρησιμοποιώντας τη συχνότητα των χαρακτήρων.
- Η Ευρωπαϊκή κρυπτολογία έχει τις ρίζες της το μεσαίωνα, που αναπτύχθηκε από τους Πάπα και τις Ιταλικές πόλεις κράτη, αλλά τα περισσότερα συστήματα βασίζονταν στην απλή αντικατάσταση γραμμάτων της αλφαβήτου (όπως στον αλγόριθμο του Καίσαρα). Οι πρώτοι αλγόριθμοι βασίζονταν στην αντικατάσταση των φωνηέντων. Το πρώτο Ευρωπαϊκό εγχειρίδιο κρυπτογραφίας (1379) ήταν μια συλλογή αλγορίθμων από τον Gabriele de Lavinde of Parma, για τον Πάπα. Το 1470 ο Leon Battista Alberti εξέδωσε το

"Trattati in cifra", όπου περιγράφεται ο πρώτος δίσκος κρυπτογράφησης (τον οποίο είχε κατασκευάσει το 1460), χρησιμοποιώντας και την έννοια της χρήσης πολλαπλών αλφαβήτων. Επίσης στο βιβλίο αυτό περιέγραφε και τις αρχές της ανάλυσης συχνότητας των γραμμάτων.

- Ο Sir Francis Bacon το 1563 περιέγραψε έναν αλγόριθμο που σήμερα φέρει το όνομά του. Ήταν ένας αλγόριθμος που χρησιμοποιούσε κωδικοποίηση 5 bits. Τον αλγόριθμο αυτό τον εξέλιξε σαν μια μέθοδο στεγανογραφίας, χρησιμοποιώντας μία μεταβολή στη μορφή των χαρακτήρων μετέφερε κάθε bit της κωδικοποίησης. Ο Blaise de Vigenere δημοσίευσε ένα βιβλίο πάνω στην κρυπτολογία το 1585, που περιέγραφε τον αλγόριθμο της πολυαλφαβητικής αντικατάστασης. Ακολούθησαν και άλλα βιβλία πάνω στην κρυπτογραφία με εξελίξεις των αλγορίθμων.
- Τα μυστικά της κρυπτολογίας φυλάσσονταν στα μοναστήρια ή στα μυστικά αρχεία των βασιλιάδων και λίγες μέθοδοι γίνονταν ευρέως γνωστές.
- Κατά την αναγέννηση η κρυπτολογία έγινε χωριστή επιστήμη και ταυτόχρονα οι εφαρμοστές της αναζητούσαν μια γενική γλώσσα.
- Το 1600 ο Καρδινάλιος Ρισελιέ χρησιμοποιούσε μια κάρτα με τρύπες για να γράψει το μήνυμά του. Όταν τελείωνε γέμιζε τα κενά με λέξεις ώστε να μοιάζει με ένα κανονικό γράμμα. Για την αποκωδικοποίηση χρειαζόταν η κάρτα με την οποία είχε γραφεί το γράμμα.
- Το 1776 ο Αμερικάνος Arthur Lee ανέπτυξε ένα κώδικα με βιβλίο τον οποίο σύντομα υιοθέτησε ο στρατός.
- Επίσης ο Thomas Jefferson εφηύρε ένα wheel cipher το 1790 που έμελλε να μετασχηματιστεί στο Strip Cipher, M-138-A, που χρησιμοποιήθηκε από το Αμερικανικό ναυτικό κατά τον 2° Παγκόσμιο Πόλεμο.
- Ένας άλλος διάσημος κώδικας είναι ο κώδικας Μορς, που αναπτύχθηκε από τον Samuel Morse το 1832, και απλώς περιγράφει τον τρόπο κωδικοποίησης του αλφαβήτου σε μακρύς και σύντομους ήχους. Με την ταυτόχρονη ανακάλυψη του τηλέγραφου ο κώδικας Μορς βοήθησε στην επικοινωνία των ανθρώπων σε μεγάλες αποστάσεις.
- Το 1860 οι μεγάλοι κώδικες χρησιμοποιούνταν συχνά στις διπλωματικές επικοινωνίες. Στη διπλωματία και κατά τις περιόδους πολέμου υπήρχε αυξημένη χρήση της κρυπτογραφίας, χαρακτηριστικό παράδειγμα είναι τα one-time pads που χρησιμοποιούνταν ευρέως.
- Στα πρώτα χρόνια της Αμερικάνικης ιστορίας έχουμε την ευρεία χρήση κωδίκων σε βιβλία. Κατά τον εμφύλιο πόλεμο έγινε εκτεταμένη χρήση αλγορίθμων μετάθεσης από το ένα μέρος και του αλγορίθμου Vigenere από το άλλο μέρος. Στην προσπάθεια αποκρυπτογράφησης των εχθρικών μηνυμάτων χρησιμοποιήθηκαν μέχρι και δημοσιεύσεις κωδικοποιημένων μηνυμάτων στις εφημερίδες, ζητώντας τη βοήθεια των αναγνωστών.

1.3.3 Η κρυπτογραφία τον 20° αιώνα

- Αν και η κρυπτογραφία χρησιμοποιήθηκε κατά τον 1° Παγκόσμιο Πόλεμο, δύο από τις πιο αξιοπρόσεκτες μηχανές εμφανίστηκαν κατά τον 2° Παγκόσμιο Πόλεμο: οι Γερμανοί χρησιμοποίησαν την Enigma machine που αναπτύχθηκε από τον Arthur Scherbius και οι Γιαπωνέζοι την Purple Machine που αναπτύχθηκε χρησιμοποιώντας τεχνικές που ανακαλύφτηκαν από τον Herbert O. Yardley.

- Από όλες τις ιστορικές προσωπικότητες που συνέβαλαν στην ανάπτυξη της κρυπτογραφίας ο William Frederick Friedman, ιδρυτής των Riverbank Laboratories, κρυπτολόγος της Αμερικανικής κυβέρνησης και οδηγός του σπασίματος του κώδικα της Ιαπωνικής Purple Machine κατά τον 2° Παγκόσμιο Πόλεμο, θεωρείται ο πατέρας της Αμερικάνικης κρυπτανάλυσης. Το 1918 έγραψε το βιβλίο «The Index of Coincidence and Its Applications in Cryptography» που ακόμα θεωρείται από αρκετούς σαν το σημαντικότερο σύγγραμμα πάνω στην κρυπτογραφία κατά τον 20° αιώνα.
- Κατά το τέλος της δεκαετίας του 1920 και τις αρχές της δεκαετίας του 1930 το FBI ίδρυσε ένα γραφείο με στόχο την αντιμετώπιση της χρήσης της κρυπτογραφίας από τους εγκληματίες. Το πρόβλημα της εποχής ήταν η λαθραία εμπορία οινοπνευματωδών ποτών και σύμφωνα με μια αναφορά η πολυπλοκότητα της κρυπτογραφίας που χρησιμοποιούσαν οι λαθρέμποροι ήταν πιο πολύπλοκη από κάθε άλλη που είχε χρησιμοποιηθεί, ακόμα και από κυβερνήσεις ή κατά τη διάρκεια του 1ου Παγκοσμίου Πολέμου.
- Τη δεκαετία του 1970 ο Dr. Horst Feistel δημιούργησε τον πρόγονο του σημερινού Data Encryption Standard (DES) με την οικογένεια ciphers, που ονομάστηκε 'Feistel ciphers', δουλεύοντας στο Watson Research Laboratory της IBM. Το 1976 η National Security Agency (NSA) σε συνεργασία με τον Feistel δημιούργησε τον αλγόριθμο FIPS PUB-46, γνωστό σήμερα σαν DES. Σήμερα, η εξέλιξή του σε triple-DES είναι το πρότυπο ασφαλείας που χρησιμοποιείται από τους οικονομικούς οργανισμούς των Ηνωμένων Πολιτειών. Επίσης το 1976 δύο συνεργάτες του Feistel, ο Whitfield Diffie και ο Martin Hellman, εισήγαγαν για πρώτη φορά την ιδέα της κρυπτογραφίας δημοσίου κλειδιού στο άρθρο "New Directions in Cryptography". Η κρυπτογραφία δημοσίου κλειδιού είναι αυτό που χρησιμοποιεί το ευρέως χρησιμοποιούμενο σήμερα PGP.
- Το Σεπτέμβριο του 1977 σε άρθρο του περιοδικού «The Scientific American», οι Ronald L. Rivest, Adi Shamir και Leonard M. Adleman εισήγαγαν τον αλγόριθμο RSA για την κρυπτογραφία δημοσίου κλειδιού και τις ψηφιακές υπογραφές. Οι συγγραφείς προσφέρθηκαν να στείλουν τον αλγόριθμο σε όποιον τους έστελνε ένα φάκελο με πληρωμένα τα ταχυδρομικά έξοδα και η διεθνής ανταπόκριση ήταν τεράστια. Παρόλο που αυτό δεν άρεσε στην NSA τελικά ο αλγόριθμος δημοσιεύτηκε τον επόμενο χρόνο στην έκδοση The Communications της ACM.
- Στα μέσα της δεκαετίας του 1980 ο αλγόριθμος ROT13 χρησιμοποιήθηκε από χρήστες του USENET "για να μη βλέπουν τα μηνύματά με επιλήψιμο περιεχόμενο αθώα μάτια" και λίγο αργότερα το 1990 μια ανακάλυψη από τους Xuejia Lai και James Massey οδήγησε σε ένα δυνατότερο, 128-bit key cipher με σκοπό να αντικαταστήσει το γερασμένο DES standard. Ο αλγόριθμος IDEA (International Data Encryption Algorithm) που σχεδιάστηκε από αυτούς είχε σκοπό να είναι πιο αποδοτικός με γενικής χρήσης υπολογιστές όπως αυτούς που χρησιμοποιούνται στις επιχειρήσεις και στα νοικοκυριά.
- Το FBI ανησυχώντας από την εξάπλωση της κρυπτογραφίας ανανέωσε την προσπάθειά του να έχει πρόσβαση στα μηνύματα κειμένου των Αμερικανών πολιτών. Σε απάντηση ο Phil Zimmerman εξέδωσε την πρώτη έκδοση του Pretty Good Privacy (PGP) το 1991 σαν ένα προϊόν ελεύθερα διαθέσιμο, που χρησιμοποιεί τον αλγόριθμο IDEA. Το PGP, ένα δωρεάν πρόγραμμα του παρέχει στρατιωτικού επιπέδου αλγορίθμους ασφαλείας στην κοινότητα του

Internet, έχει εξελιχθεί σε πρότυπο κρυπτογραφίας λόγω της ευρείας διάδοσής του.

- Τελευταία, το 1994, ο καθηγητής Ron Rivest, που βοήθησε στην ανάπτυξη του RSA, δημοσίευσε ένα νέο αλγόριθμο, το RC5.

1.4 Βασικές Απαιτήσεις Ασφάλειας

1.4.1 Έλεγχος αυθεντικότητας (Authentication)

Η αυθεντικοποίηση έχει ως στόχο την απόδειξη της γνησιότητας μιας οντότητας έτσι ώστε να παρεμποδίζεται η εμφάνιση μιας οντότητας ως μια άλλη (impersonation). Επιπλέον, με τη διαδικασία της αυθεντικοποίησης μπορεί να εξασφαλιστεί η γνησιότητα ενός μηνύματος.

Γενικά, η αυθεντικοποίηση είναι η βασικότερη υπηρεσία ασφάλειας που μπορεί να προσφέρει ένα δίκτυο υπολογιστών καθώς αυτή παρέχει προστασία έναντι μη εξουσιοδοτημένων δοσοληψιών, εξασφαλίζοντας τη γνησιότητα ενός μηνύματος, τη νομιμότητα ενός χρήστη ή αποστολέα και την εγκυρότητα ενός τερματικού υπολογιστή.

Η απλούστερη μορφή αυθεντικοποίησης βασίζεται στην τεχνική των συνθηματικών (passwords). Οι ισχυρές τεχνικές αυθεντικοποίησης στηρίζονται σε κρυπτογραφικά συστήματα και διακρίνονται στην απλή αυθεντικοποίηση, κατά την οποία ο χρήστης δικτύου πρέπει να γνωστοποιήσει την ταυτότητά του στον υπολογιστή που πρέπει να χρησιμοποιήσει, ώστε να του επιτραπεί η προσπέλαση σε αυτόν, και στην αμοιβαία αυθεντικοποίηση, κατά την οποία και ο χρήστης και ο υπολογιστής πρέπει να γνωστοποιήσουν ο ένας στον άλλον τις ταυτότητές τους.

Η αυθεντικοποίηση σε ένα περιβάλλον δικτύων υπολογιστών όπου εμπλέκεται μεγάλος αριθμός χρηστών, επιβάλλεται η δημιουργία ενός κέντρου ελέγχου (κέντρο αυθεντικοποίησης) που διευκολύνει τη διαδικασία αυθεντικοποίησης με την παροχή αναγκαίων πληροφοριών για κάθε εμπλεκόμενο χρήστη. Απαραίτητη προϋπόθεση για την ύπαρξη ενός τέτοιου κέντρου είναι η αποδοχή του από όλα τα εμπλεκόμενα μέρη, καθώς το κέντρο κατέχει και διαχειρίζεται πληροφορίες, η αποκάλυψη και τροποποίηση των οποίων συνεπάγεται την υπονόμευση του συστήματος ασφαλείας.

Επειδή η λειτουργία του κέντρου αυθεντικοποίησης εμπλέκεται και ο ανθρώπινος παράγοντας, ο οποίος μπορεί να συντελέσει στην εξασθένιση της ασφάλειας του συστήματος, προτάθηκε τελευταία μερικές από τις αρμοδιότητες του κέντρου να μεταφερθούν στους χρήστες. Η υλοποίηση ενός τέτοιου συστήματος μπορεί να επιτευχθεί με τη βοήθεια έξυπνων καρτών (smart cards) στις οποίες καταχωρούνται μυστικά κλειδιά, αλγόριθμοι και χαρακτηριστικά των χρηστών.

1.4.2 Εμπιστευτικότητα (Confidentiality)

Η υπηρεσία εμπιστευτικότητας εγγυάται ότι οι πληροφορίες δεν είναι διαθέσιμες ούτε αποκαλύπτονται στους μη εξουσιοδοτημένους χρήστες και παρέχει μηχανισμούς οι οποίοι προστατεύουν τα μεταδιδόμενα δεδομένα από τους μη ενεργούς παρεμβολής. Η έννοια της εμπιστευτικότητας μπορεί να εφαρμοστεί σε ολόκληρο το μήνυμα ή σε ένα τμήμα του.

Για την εξασφάλιση της εμπιστευτικότητας μπορεί να χρησιμοποιηθεί, ανάλογα με την περίπτωση, κρυπτογράφηση με *end to end* ή *link to link*. Κατά την πρώτη μέθοδο, τα δεδομένα αποστέλλονται κρυπτογραφημένα και αποκρυπτογραφούνται όταν παραληφθούν από το χρήστη για τον οποίον προορίζονται. Έτσι, τα δεδομένα δεν

είναι αναγνώσιμα από τους ενδιάμεσους κόμβους του δικτύου στο βαθμό που η χρησιμοποιούμενη κρυπτογραφική τεχνική είναι ασφαλής. Κατά τη δεύτερη μέθοδο, τα δεδομένα αποστέλλονται κρυπτογραφημένα και αποκρυπτογραφούνται όχι μόνο από τον τελικό προορισμό αλλά και από τον ενδιάμεσο κόμβο του δικτύου. Έτσι, είναι δυνατή η αποστολή κρυπτογραφημένων δεδομένων από έναν κόμβο στον άλλον και η ταυτόχρονη κοινοποίησή τους σε όλους τους ενδιάμεσους κόμβους.

1.4.3 Ακεραιότητα (Integrity)

Η υπηρεσία ακεραιότητας δεδομένων εξασφαλίζει ότι τα δεδομένα δεν έχουν αλλαχθεί ή καταστραφεί από μη εξουσιοδοτημένους χρήστες και είναι συναφής με την αυθεντικοποίηση των δεδομένων. Ειδικότερα, οι υπηρεσίες ακεραιότητας και αυθεντικοποίησης των δεδομένων είναι συνήθως απαραίτητες και οι δύο στο πλαίσιο της ασφάλειας δικτύων και χρησιμοποιούν τους ίδιους μηχανισμούς οι οποίοι βασίζονται σε κρυπτογραφικές τεχνικές. Επίσης, ακεραιότητα των δεδομένων μπορεί να εφαρμοστεί είτε σε ολόκληρο το μήνυμα είτε σε επιλεγμένα τμήματά του.

1.4.4 Μη αποποίηση ευθύνης (Non-repudiation)

Επιπλέον της αυθεντικοποίησης ενός χρήστη και της ακεραιότητας των δεδομένων που διακινούνται σε ένα δίκτυο υπολογιστών συχνά απαιτείται ο καταλογισμός της ευθύνης για την αποστολή/ παραλαβή ενός μηνύματος. Δηλαδή, είναι απαραίτητο σε ορισμένες περιπτώσεις ο αποστολέας/ παραλήπτης ενός μηνύματος να μη μπορεί να απαρνηθεί τη ευθύνη αποστολής/ παραλαβής του συγκεκριμένου μηνύματος. Ένας μηχανισμός αντιμετώπισης του προβλήματος αυτού του είδους είναι με τη χρήση ψηφιακής υπογραφής (digital signature) που υλοποιείται με τη βοήθεια κρυπτογραφικών συστημάτων. Ένας άλλος μηχανισμός καταλογισμού ευθύνης είναι η ύπαρξη ενός έμπιστου κέντρου ελέγχου (trusted third party).
Αν και πολλές από τις παραπάνω υπηρεσίες μπορούν να παρέχονται στα περισσότερα από τα επτά επίπεδα του μοντέλου αναφοράς OSI, τελευταία υποστηρίζεται ότι οι υπηρεσίες αυτές είναι καλύτερο να παρέχονται στο επίπεδο εφαρμογής.

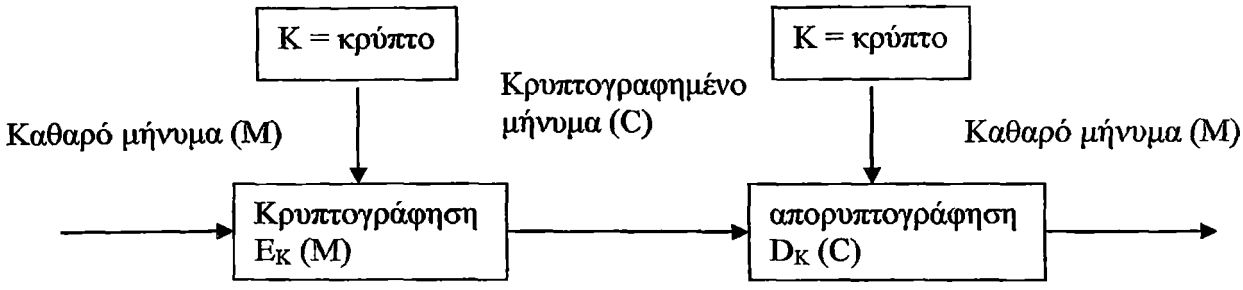
1.5 Κλασική Κρυπτογραφία

1.5.1 Συμβολισμοί

Ας υποθέσουμε ότι ο αποστολέας Α, επιθυμεί να στείλει στον παραλήπτη Β, ένα μήνυμα Μ, σε κρυπτογραφημένη μορφή C, δηλαδή μυστικό κώδικα, με τη βοήθεια ενός κρυπτογραφικού συστήματος μυστικού κλειδιού. Θα χρησιμοποιούμε τους όρους «καθαρό μήνυμα», Μ, και «κρυπτογραφημένο μήνυμα», C, που αντιστοιχούν στους όρους «plaintext» και «ciphertext» της αγγλικής γλώσσας. Συμβολίζουμε τη λειτουργία της κρυπτογράφησης με Εκ(.), από το πρώτο γράμμα της αγγλικής λέξης «encipherment», και της αποκρυπτογράφησης με DK(.), από το πρώτο γράμμα της λέξης «decipherment».
Το Κ είναι το κρυπτογραφικό κλειδί, κάτω από τον έλεγχο του οποίου εκτελείται η κρυπτογράφηση και η αποκρυπτογράφηση. Στο Σχήμα 1.1 μπορούμε να δούμε ένα παράδειγμα κρυπτογράφησης και αποκρυπτογράφησης.
Στην εργασία αυτή θα χρησιμοποιούμε τα ακόλουθα σύμβολα:

$C = E_K(M)$, το καθαρό μήνυμα Μ κρυπτογραφείται με τη συνάρτηση Ε κάτω από τον έλεγχο του κλειδιού Κ. Το αποτέλεσμα είναι το κρυπτογραφημένο μήνυμα C.

$M = D_K (C)$, το κρυπτογραφημένο μήνυμα C αποκρυπτογραφείται με τη συνάρτηση D κάτω από τον έλεγχο του κλειδιού K. Τ ο αποτέλεσμα αυτής είναι το καθαρό μήνυμα M.



Σχήμα 1.1: Κρυπτογράφηση και αποκρυπτογράφηση

1.5.2 Τεχνικές Αντικατάστασης

1.5.2.1 Η μέθοδος του Καίσαρα

Σύμφωνα με τη μέθοδο του Καίσαρα κάθε γράμμα του απλού μηνύματος αντικαθίσταται από το γράμμα που βρίσκεται τρεις θέσεις δεξιά του στο αλφάβητο. Δηλαδή, το 'A' αντικαθίσταται από το 'D', το 'B' από το 'E', το 'C' από το 'F', κτλ. Θεωρούμε πως το αλφάβητο σχηματίζει κύκλο.
Μπορούμε να εκφράσουμε την κρυπτογράφηση και την αποκρυπτογράφηση της μεθόδου του Καίσαρα με τις ακόλουθες σχέσεις

Κρυπτογράφηση: C=(M+3) mod 26

Αποκρυπτογράφηση: M=(C-3) mod 26

Εάν το αποτέλεσμα της αφαίρεσης (C-3) είναι αρνητικός αριθμός, προσθέτουμε σε αυτόν το 26, και έτσι παίρνουμε τον επιθυμητό μη αρνητικό αριθμό.

1.5.2.2 Μονοαλφαβητικη αντικατάσταση

Η μέθοδος του Καίσαρα μπορεί να γενικευτεί εάν στη θέση του 3 (κλειδιού) χρησιμοποιήσουμε έναν οποιονδήποτε αριθμό k μικρότερο του 26 και μεγαλύτερο του μηδενός. Ωστόσο, και η γενικευμένη μέθοδος του Καίσαρα δεν είναι ασφαλής, αφού υπάρχουν μόνο 25 δυνατά κλειδιά. Έτσι, η εξέταση όλων αυτών οδηγεί με βεβαιότητα στην παραβίαση (κρυπτανάλυση) του κώδικα, αν και είναι δυνατό να υποτεθεί η τιμή του k από την εξέταση της συχνότητας εμφάνισης των γραμμάτων στον κώδικα
Η μονοαλφαβητική αντικατάσταση μπορεί να βελτιωθεί αν χρησιμοποιούνται περισσότεροι του ενός κώδικες για κάθε γράμμα του αλφαβήτου. Η επιλογή του κώδικα που θα αντικαταστήσει ένα συγκεκριμένο γράμμα του μηνύματος γίνεται είτε

τυχαία είτε με τη σειρά από το σύνολο των κωδίκων που χρησιμοποιούνται γι' αυτό το γράμμα. Η τεχνική αυτή ονομάζεται ομοφωνική αντικατάσταση
Ωστόσο, αν και οι διαφορετικές σχετικές συχνότητες των γραμμάτων μπορεί να συγκαλυφθούν με την ομοφωνική αντικατάσταση, οι συχνότητες διγραμμάτων και τριγραμμάτων διατηρούνται ως ένα βαθμό. Για την αντιμετώπιση αυτού του προβλήματος μπορεί να χρησιμοποιηθεί η κρυπτογράφηση πολλαπλών γραμμάτων ή η πολυαλφαβητική αντικατάσταση. Σύμφωνα με την κρυπτογράφηση πολλαπλών γραμμάτων, διγράμματα ή τριγράμματα του μηνύματος αντιμετωπίζονται ως μονάδες που αντικαθίστανται από ίσου μήκους κώδικες για να προκύψει το κρυπτογραφημένο μήνυμα.

1.5.2.3 Πολυαλφαβητική αντικατάσταση

Επιτρέποντας το κλειδί να έχει περισσότερες της μιας τιμής, δηλαδή κρυπτογραφώντας το πρώτο γράμμα του μηνύματος με την πρώτη τιμή του κλειδιού, το δεύτερο γράμμα του μηνύματος με τη δεύτερη τιμή του κλειδιού κτλ., επιτυγχάνουμε κάποια βελτίωση της ασφάλειας της τεχνικής της αντικατάστασης.
Συνδυάζουμε, λοιπόν, πολλές μονοαλφαβητικές αντικαταστάσεις. Έτσι, στη γενική περίπτωση, με κλειδί μήκους k, το πρώτο γράμμα του απλού κειμένου κωδικοποιείται σύμφωνα με την πρώτη μονοαλφαβητική αντικατάσταση, το δεύτερο γράμμα σύμφωνα με τη δεύτερη κτλ., έως το κ-οστό γράμμα του απλού κειμένου. Το (κ+1)-οστό γράμμα χρησιμοποιεί, και πάλι, την πρώτη μονοαλφαβητική αντικατάσταση, το (κ+2)-οστό γράμμα τη δεύτερη κτλ

1.5.3 Τεχνικές μετάθεσης

Σε έναν **κωδικοποιητή μετάθεσης** (transposition cipher) οι χαρακτήρες παραμένουν ως έχουν, μόνο που αλλάζει η σειρά τους. Σε έναν απλό κωδικοποιητή μετάθεσης με στήλες το απλό κείμενο γράφεται κάθετα σε στήλες και το κρυπτογραφημένο κείμενο διαβάζεται οριζόντια, η μια γραμμή μετά την άλλη. Ο αριθμός των γραμμών είναι το κλειδί που συμφωνούν εκ των προτέρων ο αποστολέας και ο παραλήπτης. Η αποκρυπτογράφηση γίνεται χωρίζοντας το κωδικοποιημένο κείμενο σε τμήματα που αντιστοιχούν στις γραμμές, θέτοντας το ένα τμήμα κάτω από το άλλο και διαβάζοντας κατά στήλη, τη μία μετά την άλλη

1.5.3.1 Απλή και πολλαπλή μετάθεση

Η προηγούμενη μέθοδος μπορεί να γίνει πιο σύνθετη με τον ακόλουθο τρόπο. Αφού γράψουμε το καθαρό κείμενο κατά στήλες, όπως προηγουμένως, αναδιατάσσουμε αυτές κατά τρόπο που περιγράφεται από το κλειδί. Στη συνέχεια σχηματίζουμε τον κώδικα.
Η απλή κωδικοποίηση μετάθεσης μπορεί εύκολα να παραβιαστεί. Από .τη συχνότητα εμφάνισης των γραμμάτων που διατηρείται, μπορεί να αναγνωριστεί αν η μέθοδος κρυπτογράφησης βασίζεται στην τεχνική της μετάθεσης. Σε αυτή την περίπτωση ο κρυπταναλυτής χωρίζει το κρυπτογραφημένο κείμενο σε γραμμές, δημιουργεί εξ αυτών έναν πίνακα και επιχειρεί αναδιάταξη των στηλών, λαμβάνοντας υπόψη τη συχνότητα εμφάνισης διγραμμάτων και τριγραμμάτων. Αυτό το δοκιμάζει για διαφορετικούς αριθμούς γραμμών, έως ότου μπορέσει να εξαγάγει ένα κατανοητό μήνυμα. Μπορούμε να δυσχεράνουμε την προσπάθεια του κρυπταναλυτή αν μεταθέσουμε τις στήλες περισσότερες φορές. Τότε μιλάμε για πολλαπλή μετάθεση.

Και σ' αυτή την περίπτωση ο κρυπταναλυτής μπορεί σχετικά εύκολα, να συναγάγει ότι πρόκειται για την τεχνική της μετάθεσης, όμως πιο δύσκολα να δημιουργήσει τον πίνακα που θα του επιτρέψει να αποκρυπτογραφήσει το κείμενο

1.6 Μηχανικοί αλγόριθμοι κρυπτογράφησης

1.6.1 Ο κύλινδρος του Jefferson

Ο Thomas Jefferson, που διετέλεσε και πρόεδρος των ΗΠΑ, ανέπτυξε, στη δεκαετία του 1790, μια συσκευή για την εφαρμογή πολυαλφαβητικής αντικατάστασης. Η συσκευή αυτή αποτελούνταν από 36 δίσκους, καθένας από τους οποίους έφερε ένα αλφάβητο, με διαφορετική διάταξη των γραμμάτων, στην περιφέρειά του. Οι δίσκοι μπορούσαν να τεθούν στον άξονά τους σε οποιαδήποτε σειρά από τις 36 δυνατές διατάξεις (περίπου 10^{41}). Ο κάθε δίσκος έφερε έναν αριθμό, η δε σειρά αυτών αποτελούσε κάθε φορά το κλειδί που συμφωνούσαν ο αποστολέας και ο παραλήπτης του μηνύματος.

Κατά την κρυπτογράφηση ενός μηνύματος, οι δίσκοι περιστρέφονταν κατάλληλα ώστε να σχηματιστούν τα γράμματα αυτού *σε* μια σειρά (γραμμή) κατά μήκος του άξονα. Το κρυπτόγραμμα του μηνύματος αποτελούσε οποιαδήποτε από τις υπόλοιπες 25 γραμμές της συσκευής. (Το σύνολο των γραμμών είναι 26, όσα και τα γράμματα του αγγλικού αλφαβήτου.) Από την πλευρά του, ο παραλήπτης, αφού διατάξει τους δίσκους στη σειρά που υπαγορεύεται από το κλειδί περιστρέφει αυτούς κατάλληλα ώστε να σχηματίσει σε μία από τις γραμμές το κρυπτόγραμμα που έχει λάβει. Τότε, *σε* κάποια από τις υπόλοιπες γραμμές έχει σχηματιστεί το καθαρό μήνυμα.

Ο μηχανισμός αυτός χρησιμοποιήθηκε συστηματικά από το 1920 περίπου και για μερικές δεκαετίες από το Αμερικανικό Πολεμικό Ναυτικό.

1.6.2 Ο δίσκος Wheatstone

Ο μηχανισμός αυτός επινοήθηκε αρχικά από τον Wadsworth, το 1817, αλλά αναπτύχθηκε από τον Wheatstone, τη δεκαετία του 1860. Πρόκειται, ουσιαστικά, για έναν κωδικόποιητή πολυαλφαβητικής αντικατάστασης. Δύο ομόκεντροι δίσκοι φέρουν τα γράμματα του αλφαβήτου στις περιφέρειές τους. *Ο* εξωτερικός δίσκος Wheatstone είχε τα 26 γράμματα σε αλφαβητική σειρά και ένα κενό, ενώ ο εσωτερικός δίσκος είχε απλώς τα 26 γράμματα σε τυχαία σειρά. Επίσης, υπήρχαν δύο δείκτες. Όταν ο εξωτερικός δείκτης περνούσε από τα 26 γράμματα και το κενό, ο εσωτερικός έκανε το ίδιο για τα 26 γράμματα της περιφέρειας του δίσκου του. Κατά την κρυπτογράφηση, ο εξωτερικός δείκτης μετακινούνταν διαδοχικά *στα* γράμματα του καθαρού κειμένου, πάντα κατά τη φορά των δεικτών του ρολογιού και συμπεριλαμβάνοντας το κενό ως χαρακτήρα, ενώ τα γράμματα του κρυπτογράμματος προσδιορίζονταν από τον εσωτερικό δείκτη. Αντίστοιχα προέβαινε *ο* παραλήπτης κατά την αποκρυπτογράφηση.

Σε κάθε λέξη αντιστοιχούσε και ένα διαφορετικό αλφάβητο, λόγω του κενού, αλλά και η ίδια λέξη μπορούσε να κωδικοποιηθεί με διαφορετικά αλφάβητα, αν υπήρχαν διαδοχικά γράμματα με αντίστροφη αλφαβητική σειρά ή επαναλαμβανόμενα. Ιδιαίτερο ενδιαφέρον παρουσιάζει η ιδιότητα του κωδικοποιητή αυτού που επιτρέπει να επηρεάζεται η κωδικοποίηση μιας λέξης από το προηγούμενο καθαρό μήνυμα.

1.6.3 Η μηχανή του Hagelin

Τη δεκαετία του 1930, ο Σουηδός Bopis Hagelin επινόησε μια μηχανή κρυπτογράφησης βασισμένη στην τεχνική της πολυαλφαβητικής αντικατάστασης. Η μηχανή αυτή έκανε χρήση ενός συνόλου αλφαβήτων, του ονομαζόμενου τετραγώνου του Beaufort, συγκρίσιμου με τον Πίνακα του Vigenere, αλλά. με τα γράμματα των αλφαβήτων σε αντίστροφη σειρά. Το κρυπτόγραμμα υπολογίζονταν ως εξής y=b+1-x (mod 26), όπου x είναι η αλφαβητική θέση του γράμματος του καθαρού κειμένου, παραδείγματος χάρη του 'a' το 1, του 'b' το '2' κτλ.. Το b είναι η γραμμή του τετραγώνου του Beaufort που υπαγορεύεται από το κλειδί και το Y η αλφαβητική θέση του κώδικα. Αυτό επαναλαμβανόταν για όλα τα γράμματα του μηνύματος.

1.6.4 Μηχανές Ροτορα

Οι μηχανές αυτές αποτελούνται από πολλούς περιστρεφόμενους κυλίνδρους. Κάθε κύλινδρος έχει 26 εισόδους και εξόδους και κάθε είσοδος συνδέεται με μία έξοδο. Κάθε γράμμα του μηνύματος κωδικοποιείται στον πρώτο κύλινδρο, στη συνέχεια στο δεύτερο κτλ. Ο πιο απόμακρος από το χειριστή κύλινδρος περιστρέφεται με την εισαγωγή κάθε γράμματος του μηνύματος, με αποτέλεσμα μια διαφορετική σύνδεση μεταξύ εισόδων και εξόδων αυτού, δηλαδή διαφορετικό αλφάβητο αντικατάστασης. Όταν αυτός συμπληρώνει 26 περιστροφές και επανέρχεται στην αρχική κατάσταση, τότε ο γειτονικός του περιστρέφεται κατά μία θέση, με αποτέλεσμα ένα άλλο αλφάβητο. Όταν συμπληρώσει και αυτός 26 περιστροφές και επανέλθει στην αρχική κατάσταση, από άποψη συνδέσεων εισόδων και εξόδων, περιστρέφεται ο τρίτος κατά μία θέση κτλ. Έτσι, σε μια συσκευή με τρεις κυλίνδρους έχουμε 26 x 26 x 26 συνδυασμούς αλφαβήτων. Επομένως, σε ένα μήνυμα με λιγότερα από 26 x 26 x 26 γράμματα κάθε γράμμα θα κωδικοποιείται από: διαφορετικό συνδυασμό αλφαβήτων.
Πολύ γνωστά παραδείγματα κρυπτογραφικών συσκευών βασισμένων σε μηχανές ρότορα ήταν η Enigma, με καταρχήν τρεις και αργότερα τέσσερις κυλίνδρους, και η Purple, που χρησιμοποιήθηκαν από τους Γερμανούς και τους Ιάπωνες, αντίστοιχα, κατά το Β' Παγκόσμιο πόλεμο. Η παραβίαση και των δύο αυτών κρυπτογραφικών συσκευών συνετέλεσε, επίσης, στην επιτυχή για τους Συμμάχους έκβαση του πολέμου.

1.7 Επιθέσεις στα κρυπτοσυστήματα

1.7.1 Επίθεση κρυπτογραφημένου κειμένου (Ciphertext-only attack).

Η επίθεση βασίζεται μόνο σε κρυπτογραφημένο κείμενο. Ο κρυπταναλυτής έχει στη διάθεσή του αρκετά κρυπτογραφημένα, με τον ίδιο αλγόριθμο και το ίδιο κλειδί, μηνύματα. Ο κρυπταναλυτής επιδιώκει να αποκρυπτογραφήσει όσο πιο πολλά μηνύματα μπορεί ή και να προσδιορίσει το κρυπτογραφικό κλειδί που χρησιμοποιήθηκε ή ακόμα και να επινοήσει έναν αλγόριθμο που θα του επιτρέπει να υπολογίζει το καθαρό από το κρυπτογραφημένο μήνυμα.

1.7.2 Επίθεση γνωστού μη κρυπτογραφημένου (καθαρού) κειμένου (Known-plaintext attack).

Ο κρυπταναλυτής έχει στη διάθεσή του όχι μόνο κρυπτογραφημένα μηνύματα αλλά και τα αντίστοιχα καθαρά μηνύματα. Επιδιώκει να προσδιορίσει το κλειδί που

χρησιμοποιήθηκε για την κρυπτογράφηση των μηνυμάτων. Εναλλακτικά, επιδιώκει να επινοήσει έναν αλγόριθμο που θα του επιτρέπει να υπολογίζει από το κρυπτογραφημένο μήνυμα το αντίστοιχο καθαρό, που πλέον δε γνωρίζει.

1.7.3 Επίθεση επιλεγμένων μη κρυπτογραφημένων (καθαρών) κειμένων (Chosen plaintext attack).

Οι κρυπταναλυτές έχουν στη διάθεσή τους τα κρυπτογράμματα επιλεγμένων από τους ίδιους καθαρών μηνυμάτων. Η επίθεση αυτή είναι πιο ισχυρή από την προηγούμενη, αφού οι κρυπταναλυτές έχουν τη δυνατότητα να επιλέξουν τέτοια καθαρά μηνύματα προς κρυπτογράφηση, που δίνουν περισσότερες πληροφορίες για το κλειδί. Ο στόχος είναι να βρεθεί το κλειδί που χρησιμοποιείται για την κρυπτογράφηση των μηνυμάτων ή να επινοηθεί ένας αλγόριθμος για την αποκρυπτογράφηση των νέων μηνυμάτων, τα οποία κρυπτογραφούνται με το ίδιο κλειδί.
Μια ειδική περίπτωση αυτού του τύπου επιθέσεων είναι να μπορούν οι κρυπταναλυτές όχι μόνο να επιλέγουν το καθαρό μήνυμα που κρυπτογραφείται, αλλά και να τροποποιούν την επιλογή, βασιζόμενοι στα αποτελέσματα της προηγούμενης κρυπτογράφησης. Δηλαδή, αφού επιλέξουν ένα τμήμα από το καθαρό κείμενο, στη συνέχεια να επιλέξουν ένα άλλο τμήμα με βάση τα αποτελέσματα της κρυπτογράφησης του πρώτου κ.τ.λ.

1.7.4 Επίθεση επιλεγμένων κρυπτογραφημένων κειμένων (Chosen-ciphertext attack).

Οι κρυπταναλυτές μπορούν να επιλέξουν διάφορα κρυπτογραφημένα μηνύματα και διαθέτουν ακόμα τα αντίστοιχα καθαρά μηνύματα, επιδιώκουν δε τον προσδιορισμό του κλειδιού που μπορεί να χρησιμοποιηθεί για την αποκρυπτογράφηση. Αυτή η επίθεση λαμβάνει χώρα κυρίως σε ασύμμετρα κρυπτογραφικά συστήματα. Επίσης, είναι σχετική και αποτελεσματική και ενάντια συμμετρικών αλγόριθμων, αλλά τότε είναι μάλλον ισοδύναμη με μια επίθεση του τρίτου τύπου, αφού στα συμμετρικά συστήματα έχουμε το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση, σε αντίθεση με τα ασύμμετρα, όπου το μυστικό κλειδί χρησιμοποιείται για την αποκρυπτογράφηση και αποτελεί ζητούμενο της επίθεσης και το δημόσιο (είναι γνωστό σε όλους) για την κρυπτογράφηση.

1.7.5 Man-in-the-middle attack

Αυτή η επίθεση είναι σχετική με την κρυπτογραφημένη επικοινωνία και με τα πρωτόκολλα ανταλλαγής κλειδιών. Η βασική ιδέα είναι πως, όταν δύο άτομα ανταλλάσσουν κλειδιά, τότε ο επιτιθέμενος "εγκαθίσταται" στη γραμμή επικοινωνίας μεταξύ των δύο ατόμων. Στη συνέχεια, ο επιτιθέμενος ανταλλάσσει με τον καθένα από τα δύο άτομα διαφορετικό κλειδί. Έτσι, τα δύο ενδιαφερόμενα άτομα καταλήγουν να επικοινωνούν μεταξύ τους χρησιμοποιώντας ο καθένας διαφορετικό κλειδί (K1, K2) τα οποία όμως είναι γνωστά στον επιτιθέμενο.
Συνεπώς, ένα κρυπτογραφημένο με το κλειδί K1 μήνυμα που ξεκινάει από το ένα από τα δύο ενδιαφερόμενα άτομα αποκρυπτογραφείται από τον επιτιθέμενο ο οποίος στη συνέχεια κρυπτογραφεί το μήνυμα με το κλειδί K2 και το αποστέλλει στο δεύτερο άτομο (και αντίστροφα). Με τον τρόπο αυτό, τα δύο ενδιαφερόμενα άτομα νομίζουν ότι επικοινωνούν μεταξύ τους με ασφάλεια, αλλά στην πραγματικότητα ο επιτιθέμενος παρεμβάλλεται και γνωρίζει τα πάντα.

1.8 Κρυπτογραφία μυστικού κλειδιού (Συμμετρική)

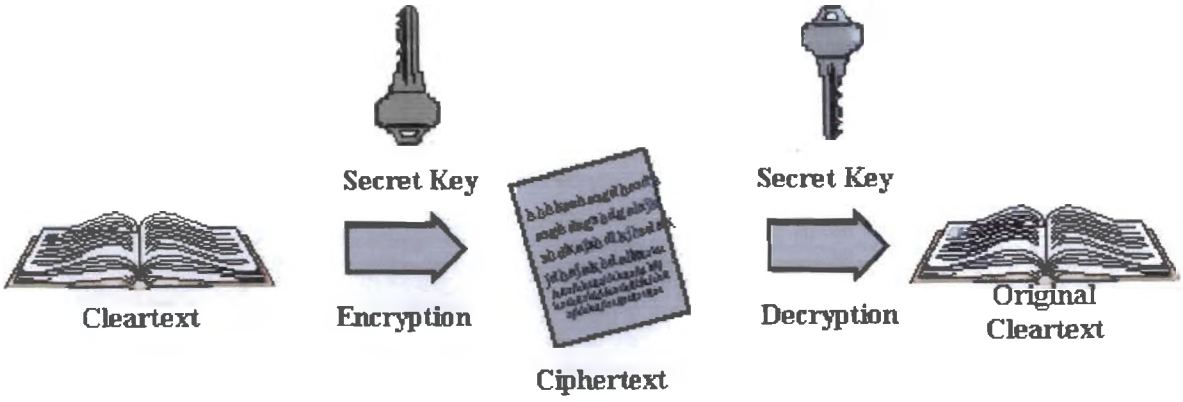
Οι συμμετρικοί αλγόριθμοι είναι αλγόριθμοι όπου το κλειδί κρυπτογράφησης μπορεί να υπολογιστεί από το κλειδί αποκρυπτογράφησης και αντίστροφα. Στους περισσότερους συμμετρικούς αλγορίθμους, το κλειδί κρυπτογράφησης και το κλειδί αποκρυπτογράφησης είναι ίδιο. Αυτοί οι αλγόριθμοι, αποκαλούμενοι και ως αλγόριθμοι μυστικού κλειδιού, μονού κλειδιού ή ενός κλειδιού, απαιτούν ο αποστολέας και ο παραλήπτης να συμφωνήσουν σε ένα κρυφό κλειδί προτού ξεκινήσουν να επικοινωνούν ασφαλώς. Η ασφάλεια ενός συμμετρικού αλγορίθμου στηρίζεται στο κλειδί. Η αποκάλυψη του κλειδιού σημαίνει ότι καθένας θα μπορούσε να κρυπτογραφήσει και να αποκρυπτογραφήσει τα μηνύματα. Εφ' όσον πρέπει να παραμείνει η επικοινωνία μυστική, το κλειδί πρέπει να παραμείνει μυστικό.

Ένα σχήμα συμμετρικής κρυπτογράφησης έχει πέντε συστατικά.

Καθαρό κείμενο: Αυτό είναι το αρχικό μήνυμα ή δεδομένα που τροφοδοτούνται ως είσοδος στον αλγόριθμο.
Αλγόριθμος κρυπτογράφησης:
Ο αλγόριθμος κρυπτογράφησης εκτελεί διάφορες αντικαταστάσεις και μετασχηματισμούς στο καθαρό κείμενο.
Μυστικό κλειδί: Το μυστικό κλειδί είναι επίσης μία είσοδος στον αλγόριθμο κρυπτογράφησης. Οι ακριβείς αντικαταστάσεις και οι μετασχηματισμοί που εκτελούνται από τον αλγόριθμο εξαρτώνται από το κλειδί..
Κρυπτογραφημένο κείμενο: Αυτό είναι το περιπλεγμένο κείμενο που παράγεται ως έξοδος. Εξαρτάται από το καθαρό κείμενο και το μυστικό κλειδί. Για ένα συγκεκριμένο μήνυμα, δύο διαφορετικά κλειδιά θα παράγουν δύο διαφορετικά κρυπτογραφημένα κείμενα.
Αλγόριθμος αποκρυπτογράφησης: Αυτός είναι απαραίτητα ο αλγόριθμος κρυπτογράφησης εκτελεσμένος αντίστροφα. Παίρνει το κρυπτογραφημένο κείμενο και το μυστικό κλειδί και παράγει το αρχικό καθαρό κείμενο.

Υπάρχουν δύο απαιτήσεις για την ασφαλή χρήση της συμβατικής κρυπτογράφησης:

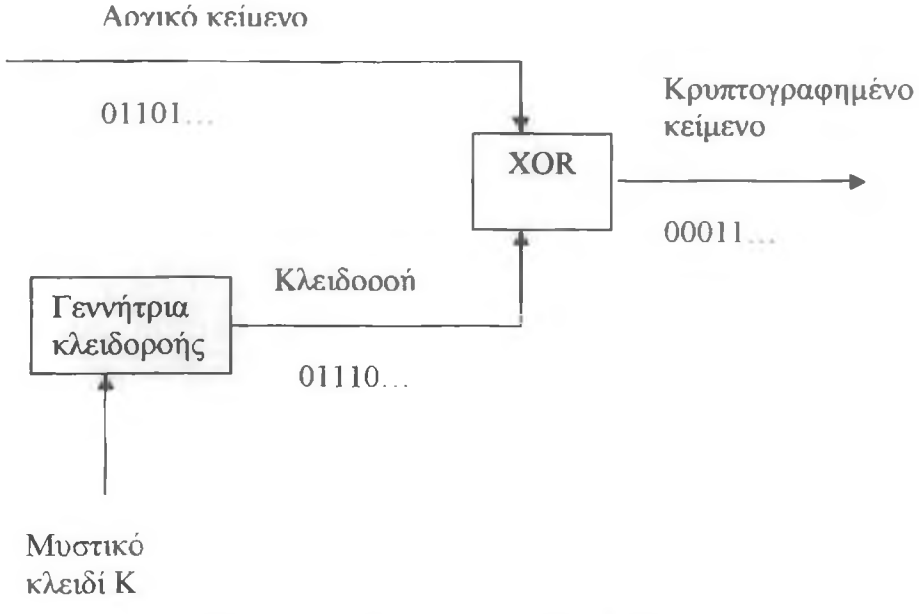
- Χρειαζόμαστε έναν ισχυρό αλγόριθμο κρυπτογράφησης. Κατ' ελάχιστο, θα θέλαμε ο αλγόριθμος να είναι τέτοιος ώστε ένας αντίπαλος, ο οποίος γνωρίζει τον αλγόριθμο και έχει πρόσβαση σε ένα ή περισσότερα κρυπτογραφημένα κείμενα, να μην είναι ικανός να αποκρυπτογραφήσει το κρυπτογραφημένο κείμενο ή να ανακαλύψει το κλειδί Αυτή η απαίτηση συνήθως διατυπώνεται με έναν πιο ισχυρό τρόπο: Ο αντίπαλος δε θα πρέπει να είναι ικανός να αποκρυπτογραφήσει ή να ανακαλύψει το κλειδί ακόμη και εάν κατέχει έναν αριθμό από κρυπτογραφημένα κείμενα μαζί με το καθαρό κείμενο που παρήγαγε το κάθε κρυπτογραφημένο κείμενο.
- Ο αποστολέας και ο παραλήπτης πρέπει να έχουν προμηθευτεί αντίγραφα του μυστικού κλειδιού με ασφαλή τρόπο και πρέπει να κρατούν το κλειδί ασφαλές. Εάν κάποιος μπορεί να ανακαλύψει το κλειδί και γνωρίζει τον αλγόριθμο, κάθε επικοινωνία που χρησιμοποιεί αυτό το κλειδί είναι αναγνώσιμη.



Σχήμα 1.2: Κρυπτογραφία μυστικού κλειδιού

1.8.1 Κρυπτογραφικοί Αλγόριθμοι Ροής

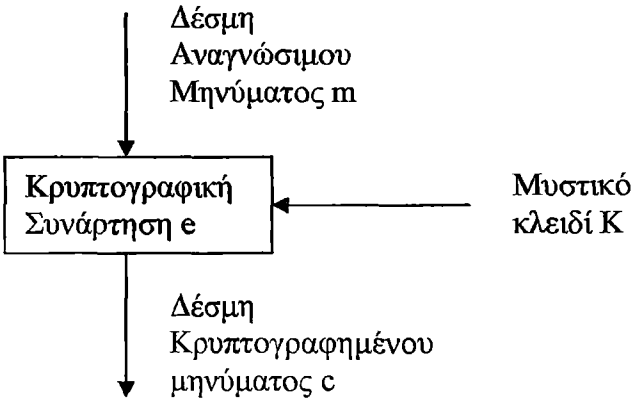
Ένας *κρυπτογραφικός αλγόριθμος ροής* (stream cipher) λειτουργεί ως εξής:
Τα δεδομένα που πρόκειται να κρυπτογραφηθούν (plaintext) παριστάνονται ως μια ακολουθία από δυαδικά ψηφία (bits). Κατόπιν, επιλέγεται *γεννήτρια κλειδοροής* (keystream generator) που δέχεται ως είσοδο μυστικό κλειδί k και παράγει στην έξοδό της μια ψευδοτυχαία. Ακολουθία από bits που ονομάζεται *κλειδοροή* (keystream). Η γεννήτρια κλειδοροής είναι ένας ειδικός τύπος γεννήτριας ψευδοτυχαίων αριθμών.
Στη συνέχεια, το αρχικό κείμενο κρυπτογραφείται με modulo 2 (XOR) , δηλαδή προσθέτοντας την κλειδοροή στο αρχικό κείμενο. Η ακολουθία από bits που παράγεται με αυτό τον τρόπο αποτελεί το κρυπτογραφημένο κείμενο (ciphertext).



Σχήμα 1.3: Κρυπτογραφικός αλγόριθμος ροής

1.8.2 Κρυπτογραφικοί Αλγόριθμοι Δέσμης

Οι κρυπτογραφικοί αλγόριθμοι δέσμης (Block Ciphers) λειτουργούν ως εξής:
Τα δεδομένα που πρόκειται να κρυπτογραφηθούν (αρχικό κείμενο) πρέπει να έχουν την μορφή μιας σειράς από m δέσμες (blocks) δυαδικών ψηφίων (bits). Το μήκος μιας δέσμης συνήθως συμβολίζεται με n. Τυπικές τιμές για το n είναι 64 ή 128 bits.
Το αρχικό κείμενο κατόπιν κρυπτογραφείται με εφαρμογή της κρυπτογραφικής συνάρτησης e και του μυστικού κλειδιού k. Το αποτέλεσμα είναι μια δέσμη του κρυπτογραφημένου κειμένου c, που συνήθως έχει το ίδιο μήκος με την αντίστοιχη δέσμη του αρχικού κειμένου.



Σχήμα 1.4: Κρυπτογραφικός αλγόριθμος δέσμης

1.8.2.1 Τρόποι Λειτουργίας

Ένας αλγόριθμος τύπου block cipher έχει διάφορους τρόπους λειτουργίας. Κάθε τρόπος λειτουργίας μπορεί να έχει τις δικές του ιδιότητες εκτός από αυτές που κληρονομεί από τον βασικό cipher.
Οι βασικοί τρόποι λειτουργίας είναι οι:

- Electronic Code Book (ECB)
- Cipher Block Chaining (CBC)
- Cipher Feedback (CFB)
- Output Feedback (OFB).

1.8.2.1.1 Electronic Code Book (ECB)

Σε ECB mode, το κείμενο χωρίζεται σε ισομήκη block. Κάθε μη κρυπτογραφημένο block κρυπτογραφείται ανεξάρτητα από την συνάρτηση του βασικού block cipher. Μειονέκτημα αυτού του τρόπου είναι ότι ομοιότητες του plaintext δεν καλύπτονται. Τα plaintext block που είναι ταυτόσημα, δίνουν ταυτόσημα ciphertext block και το κείμενο μπορεί εύκολα να τροποποιηθεί με την αφαίρεση, πρόσθεση ή και ανακατάταξη των όμοιων ciphertext block. Η ταχύτητα της κρυπτογράφησης κάθε plaintext block είναι ίδια με την ταχύτητα του block cipher. Ο ECB επιτρέπει την παράλληλη παραγωγή των ciphertext blocks για καλύτερη απόδοση.

1.8.2.1.2 Cipher Block Chaining (CBC)

Σε CBC mode, κάθε μη κρυπτογραφημένο block συνδυάζεται μέσω της λογικής πράξης X-OR με το πρωτύτερα κρυπτογραφημένο block. Το αποτέλεσμα κρυπτογραφείται. Απαιτείται μια αρχική τιμή για την πρώτη X-OR πράξη που καλείται Initialization Vector, c_0. Τα όμοια plaintext blocks καλύπτονται με την χρήση της λογικής πράξης και αυξάνεται η ασφάλεια του αλγόριθμου. Η ταχύτητα της κρυπτογράφησης είναι ίδια με αυτή του block cipher, αλλά η διαδικασία δεν μπορεί να πραγματοποιηθεί παράλληλα παρ' όλο που η αποκρυπτογράφηση μπορεί.

1.8.2.1.3 Cipher Feedback (CFB)

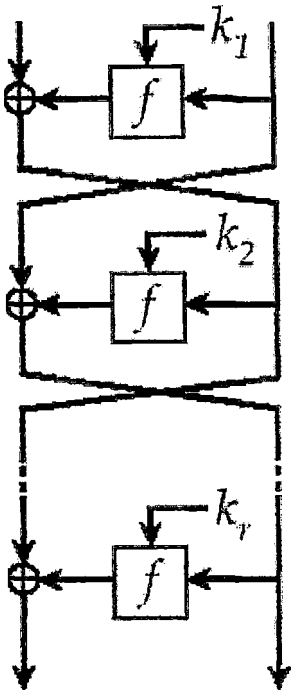
Με αυτόν τον τρόπο καλύπτονται πιθανές ομοιότητες στα plaintext blocks μέσω της X-OR. Γίνεται, όμως, στην πλήρη ανάδραση τα c_i και c_{i-1} να είναι ταυτόσημα. Σαν συνέπεια και το επόμενο ζεύγος κρυπτογραφημένων block θα είναι ταυτόσημα μεταξύ τους. Αυτό το πρόβλημα λύνεται με την χρήση μερικής ανάδρασης. Η ταχύτητα της κρυπτογράφησης είναι ίδια με αυτή του block cipher και δεν επιτρέπεται παράλληλη επεξεργασία.
Σε CFB mode, το προηγούμενο ciphertext block κρυπτογραφείται και το αποτέλεσμα που παράγεται συνδυάζεται με το επόμενο plaintext block με χρήση μιας X-OR. Η έξοδος της X-OR αποτελεί το νέο ciphertext block που θα κρυπτογραφηθεί, συνεχίζοντας την διαδικασία. Γίνεται η ποσότητα που χρησιμοποιείται για ανάδραση (feedback) να μην είναι ένα πλήρες block.Απαιτείται ένας Initialization Vector c_0 για την πρώτη X-OR πράξη.

1.8.2.1.4 Output Feedback (OFB)

Σε OFB mode, η διαδικασία είναι παρόμοια με αυτήν του CFB mode, με την διαφορά ότι η ποσότητα που συνδυάζεται με X-OR με κάθε plaintext block παράγεται ανεξάρτητα από τα plaintext και ciphertext. Ένας Initialization Vector s_0 χρειάζεται για να ξεκινήσει την διαδικασία και κάθε block s_i προκύπτει από την κρυπτογράφηση του προηγούμενου s_{i-1}. Η κρυπτογράφηση plaintext block γίνεται με τον συνδυασμό κάθε plaintext block μέσω μιας X-OR, με το κρυπτογραφημένο s.

1.8.2.2 Κρυπτογραφικός Αλγόριθμος Feistel

Ο κρυπτογραφικός αλγόριθμος Feistel αποτελεί έναν ειδικό τύπο επαναληπτικού κρυπτογραφικού αλγορίθμου δέσμης. Η δέσμη m του αρχικού κειμένου που πρόκειται να κρυπτογραφηθεί διαιρείται αρχικά σε δυο υποδέσμες Lo και Ro (ίδιου μήκους). Για παράδειγμα, αν το μήκος της δέσμης είναι n, τότε οι υποδέσμες L_0 και Ro θα έχουν και οι δυο ίδιο μήκος n/2. Το κλειδί k πρέπει να χρησιμοποιείται για τον υπολογισμό ενός συνόλου από r μέρη κλειδιού k_1, k_2, ..., k_r (ένα για κάθε ανακύκλωση).



Σχήμα 1.5: Κρυπτογραφικός αλγόριθμος Feistel

1.9 Αλγόριθμοι κρυπτογραφίας μυστικού κλειδιού

1.9.1 DES

Ο αλγόριθμος DES (Data Encryption Standard) αναπτύχθηκε από την IBM το 1970 και υιοθετήθηκε από την κυβέρνηση των ΗΠΑ το 1977. Χρησιμοποιεί το ίδιο κλειδί τόσο για τη κρυπτογράφηση όσο και για την αποκρυπτογράφηση. Χρησιμοποιείται κυρίως στις εμπορικές εφαρμογές.

Ο κρυπτογραφικός αλγόριθμος DES είναι ένας αλγόριθμος τύπου Feistel με δεκαέξι (16) ανακυκλώσεις (r=16). Το μήκος δέσμης αρχικού και κρυπτογραφημένου κειμένου είναι 64 και το μήκος του κλειδιού k είναι 56 bits. Αξίζει να σημειώσουμε εδώ ότι τα κλειδιά του DES συνήθως αναπαρίστανται ως σειρές χαρακτήρων των 64-bit, όπου 8 από τα bits παράγονται ως ψηφία ισοτιμίας (parity bits) των υπολοίπων 56. Ως αποτέλεσμα, μπορούν να υπάρξουν μόνο 256 διαφορετικά κλειδιά για τον αλγόριθμο DES και για αυτό πρέπει να θεωρείται ότι το μήκος κλειδιού του αλγορίθμου DES είναι 56-bits. Για κάθε κλειδί των 56-bit του αλγορίθμου DES, παράγονται 16 μέρη κλειδιού k1, k2, ..., kl6 που το καθένα έχει μήκος48 bits.

1.9.2 Triple-DES

Είναι μια παραλλαγή του DES όπου το μήνυμα κρυπτογραφείται και αποκρυπτογραφείται διαδοχικά με διαφορετικά κλειδιά για την ενίσχυση του βασικού αλγόριθμου. Υπάρχουν τέσσερις διαφορετικοί τρόποι για να επιτευχθεί αυτό:

DES-EEE3 (Encrypt-Encrypt-Encrypt): πραγματοποιούνται τρεις συνεχόμενες κρυπτογραφήσεις με το τρία διαφορετικά κλειδιά.

DES-EDE3 (Encrypt-Decrypt-Encrypt): το μήνυμα διαδοχικά κρυπτογραφείται, αποκρυπτογραφείται και τέλος κρυπτογραφείται με χρήση τριών διαφορετικών κλειδιών.

Το πιο σημαντικό κρυπταναλυτικό αποτέλεσμα οφείλεται στον Daemen. Αυτός βρήκε μια μεγάλη τάξη από 2^{51} αδύνατα κλειδιά για τα οποία η χρήση ενός από αυτά κατά την διάρκεια της κρυπτογράφησης μπορούσε να ανιχνευθεί και το κλειδί να βρεθεί. Ωστόσο, επειδή υπάρχουν 2^{128} πιθανά κλειδιά το προηγούμενο αποτέλεσμα δεν έχει επιπτώσεις στην ασφάλεια του αλγορίθμου. Ο IDEA γενικά θεωρείται ασφαλής και τόσο η ανάπτυξη του αλγορίθμου όσο και η θεωρητική του βάση έχουν ευρέως συζητηθεί.
Η πιο σπουδαία χρήση του IDEA είναι η εφαρμογή του στο δωρεάν παρεχόμενο πακέτο κρυπτογράφησης, το Pretty Good Privacy (PGP).

1.9.6 AES

Ο κρυπτογραφικός αλγόριθμος AES (Advanced Encryption Standard) αναπτύχθηκε με πρωτοβουλία των ΗΠΑ από το NIST (National Institute of Standards and Technology) με σκοπό την αντικατάσταση του DES και αναμένεται να αποτελέσει το νέο πρότυπο κρυπτογραφικού αλγόριθμου δέσμης.
Το 1998 ανακοινώθηκε από το NIST η αποδοχή 15 αλγόριθμων από αυτούς που είχαν υποβληθεί ως υποψήφιοι να αποτελέσουν το υπό ανάπτυξη πρότυπο. Επίσης, το NIST προσκάλεσε τη συνδρομή της ερευνητικής κοινότητας στην αξιολόγηση των υποψήφιων αλγόριθμων. Η αξιολόγηση των αλγόριθμων, κυρίως από τη σκοπιά της ασφάλειας και της αποτελεσματικότητας, οδήγησε το NIST στην επιλογή 5 αλγόριθμων για περαιτέρω ανάλυση και στον αποκλεισμό των υπόλοιπων 10.
Μετά από συγκριτική ανάλυση των 5 αλγόριθμων της τελικής φάσης αξιολόγησης, το NIST αποφάσισε να εισηγηθεί τον αλγόριθμο Rijndael ως το Advanced Encryption Standard (AES). Ο αλγόριθμος Rijndael είχε υποβληθεί από τους Βέλγους Κρυπτογράφους Joan Daemen και Vincent Rijmen.

1.10 Επιθέσεις στους αλγορίθμους μυστικού κλειδιού

1.10.1 Διαφορική κρυπτανάλυση

Αποτελεί το είδος της επίθεσης που μπορεί να προσαρτηθεί σε επαναληπτικά κρυπτογραφήματα ομάδας. Αυτές οι τεχνικές αρχικά παρουσιάστηκαν από τον Murphy σε μια επίθεση στον αλγόριθμο κρυπτογράφησης FEAL-4. Στη συνέχεια, υπήρξε "βελτίωση" των επιθέσεων από τους Biham και Shamir, οι οποίοι τους χρησιμοποίησαν για να επιτεθούν στον DES. Η διαφορική κρυπτανάλυση είναι βασικά μια επίθεση τύπου "επιλεγμένου κειμένου" (chosen plaintext). Βασίζεται στην ανάλυση της εξέλιξης των διαφορών ανάμεσα σε δύο σχετιζόμενα μη κωδικοποιημένα κείμενα καθώς αυτά κωδικοποιούνται χρησιμοποιώντας το ίδιο κλειδί. Με προσεκτική ανάλυση των διαθέσιμων δεδομένων, πιθανότητες μπορούν να προσαρτηθούν σε κάθε ένα από τα πιθανά κλειδιά και στο τέλος το πιο πιθανό από αυτά αναγνωρίζεται ως το σωστό.
Η διαφορική κρυπτανάλυση έχει χρησιμοποιηθεί για την προσβολή πολλών σημαντικών κρυπτογραφημάτων με κυμαινόμενο όμως βαθμό επιτυχίας. Σε επιθέσεις απέναντι στον DES, η αποτελεσματικότητα του περιορίστηκε με τον πολύ προσεκτικό σχεδιασμό των S-boxes κατά την περίοδο σχεδιασμού του DES στα μέσα της δεκαετίας του 1970. Μελέτες για την προστασία των κρυπτογραφημάτων απέναντι στις επιθέσεις διαφορικής κρυπτανάλυσης έγιναν από τους Nyberk και Knudsen καθώς και από τους Lai, Massey και Murphy.

1.10.2 Γραμμική Κρυπτανάλυση (Linear Cryptanalysis)

Η γραμμική κρυπτανάλυση επινοήθηκε από τους Matsui και Yamagishi σε μια επίθεση στον FEAL. Στη συνέχεια επεκτάθηκε από τον Matsui σε μια προσπάθεια επίθεσης στον DES. Η γραμμική κρυπτανάλυση είναι μια επίθεση τύπου "γνωστού κειμένου" (known plaintext) η οποία χρησιμοποιεί μια γραμμική διαδικασία προσέγγισης για να περιγράψει τη συμπεριφορά του κρυπτογραφήματος ομάδας. Έχοντας επαρκή ζεύγη κωδικοποιημένων και μη μηνυμάτων, είναι δυνατό να βρεθούν κάποια κομμάτια του κλειδιού. Λόγω της σχεδιαστικής προσέγγισης, όσο μεγαλύτερος είναι ο αριθμός των δεδομένων, τόσο μεγαλύτερη είναι και η πιθανότητα επιτυχίας.

Αξίζει να σημειωθεί ότι στις παραπάνω μεθόδους κρυπτανάλυσης έγιναν προσθήκες και βελτιώσεις. Οι Langford και Hellman παρουσίασαν μια επίθεση με την επωνυμία διαφορική-γραμμική κρυπτανάλυση η οποία ενσωματώνει και συνδυάζει στοιχεία τόσο της διαφορικής όσο και της γραμμικής κρυπτανάλυσης. Επιπλέον, οι Kaliski και Robshaw έδειξαν ότι, χρησιμοποιώντας γραμμική κρυπτανάλυση με πολλαπλές προσεγγίσεις, μπορούν να ελαττώσουν τον όγκο των δεδομένων που χρειάζονται για μια επιτυχή επίθεση. Η λεπτομερής παρουσίαση των προσεγγίσεων αυτών είναι εκτός του σκοπού του παρόντος συγγράμματος.

1.10.3 Επίθεση στα αδύναμα κλειδιά

Τα λεγόμενα "αδύναμα κλειδιά" είναι μυστικά κλειδιά με συγκεκριμένη τιμή γιο την οποία το κρυπτογράφημα που εξετάζεται θα παρουσιάσει συμμετρικότητα στην κρυπτογράφηση ή σε άλλες περιπτώσεις χαμηλό επίπεδο κρυπτογράφησης. Για παράδειγμα, για τον DES υπάρχουν τέσσερα κλειδιά για τα οποία η διαδικασία της κρυπτογράφησης είναι ίδια με αυτή της αποκρυπτογράφησης. Αυτό σημαίνει ότι αν κάποιος κρυπτογραφούσε τα δεδομένα δύο φορές με το ίδιο αδύναμο κλειδί, τότε το αρχικό μη κωδικοποιημένο μήνυμα θα αποκαλυπτόταν. Για τον IDEA υπάρχει μια κατηγορία κλειδιών για τα οποία η κρυπτανάλυση διευκολύνεται ιδιαίτερα κα το κλειδί μπορεί να ανακτηθεί. Ωστόσο και για τις δύο αυτές περιπτώσεις, ο αριθμός των αδύναμων κλειδιών αποτελεί μόνο ένα μικρό ποσοστό όλων των πιθανών κλειδιών και η πιθανότητα να επιλεχθεί ένα τέτοιο είναι εξαιρετικά μικρή. Φυσικα για άλλους αλγορίθμους κρυπτογράφησης ο αριθμός των πιθανών αδύναμων κλειδιών μπορεί να είναι αρκετά μεγάλος, τόσος που να αποτελεί απειλή για την ικανότητα αντίστασης του αλγορίθμου.

1.10.4 Αλγεβρικές επιθέσεις

Οι *αλγεβρικές επιθέσεις* αποτελούν μια κατηγορία τεχνικών των οποίων η επιτυχία εξαρτάται *από* τα κρυπτογραφήματα ομάδας που παρουσιάζουν υψηλό βαθμό μαθηματικής δομής. Για παράδειγμα, είναι εύκολα αντιληπτό ότι ένα κρυπτογράφημα ομάδας μπορεί να παρουσιάζει μια ομαδοποιημένη δομή. Στην περίπτωση αυτή, α κρυπτογραφούσαμε ένα κείμενο με τη βοήθεια ενός κλειδιού και στη συνέχεια κρυπτογραφούσαμε *το* παραγόμενο κρυπτογράφημα με ένα δεύτερο κλειδί, το αποτέλεσμα θα ήταν ισοδύναμο με την κρυπτογράφηση του αρχικού κειμένου με τη βοή θεια ενός τρίτου κλειδιού. Σε μια τέτοια περίπτωση *το* κρυπτογράφημα ομάδας α και κρυπτογραφήθηκε δύο φορές, δεν έγινε περισσότερο πολύπλοκο ούτε περισσότερο ασφαλές, αφού *το* ίδιο αποτέλεσμα θα μπορούσε να παραχθεί με την

κρυπτογράφηση του αρχικού κειμένου με κάποιο άλλο κλειδί. Για τα περισσότερα κρυπτογραφήματα ομάδας, παραμένει ακόμα ανοικτό το ερώτημα αν αυτά συνθέτουν ομάδα. Ωστόσο, για τον DES είναι γνωστό ότι δεν ανήκει σε ομάδα.

1.11Ασύμμετρη κρυπτογραφία

Η κρυπτογράφηση δημόσιου κλειδιού, που για πρώτη φορά προτάθηκε δημόσια από τους Diffie και Hellman το 1976, αποτελεί την πρώτη πραγματική επαναστατική πρόοδο στην κρυπτογράφηση κυριολεκτικά εδώ και χιλιάδες χρόνια. Αν μη τι άλλο, οι αλγόριθμοι δημόσιου κλειδιού βασίζονται σε μαθηματικές συναρτήσεις παρά σε απλές πράξεις πάνω σε ακολουθίες από bit.
Ένα σχήμα κρυπτογράφησης δημοσίου κλειδιού έχει έξι συστατικά:

Καθαρό κείμενο: αυτό είναι το αναγνώσιμο μήνυμα ή δεδομένα που τροφοδοτούνται ως είσοδος στον αλγόριθμο
Αλγόριθμος κρυπτογράφησης: Ο αλγόριθμος κρυπτογράφησης εκτελεί διάφορους μετασχηματισμούς στο καθαρό κείμενο.
Δημόσιο και ιδιωτικό κλειδί: αυτό είναι ένα ζεύγος κλειδιών που έχουν επιλεγεί έτσι ώστε, αν το ένα χρησιμοποιείται για κρυπτογράφηση το άλλο χρησιμοποιείται για αποκρυπτογράφηση. Οι ακριβείς μετασχηματισμοί που εκτελούνται από τον αλγόριθμο κρυπτογράφησης εξαρτώνται από το δημόσιο ή ιδιωτικό κλειδί που παρέχεται ως είσοδος.
Κρυπτογραφημένο κείμενο: Αυτό είναι το περιπλεγμένο μήνυμα που παράγεται ως έξοδος. Εξαρτάται από το καθαρό κείμενο και το κλειδί. Για ένα συγκεκριμένο μήνυμα, δύο διαφορετικά κλειδιά θα παράγουν δύο διαφορετικά κωδικοποιημένα κείμενα.
Αλγόριθμος αποκρυπτογράφησης: Αυτός ο αλγόριθμος δέχεται το κωδικοποιημένο κείμενο και το ταιριαστό κλειδί και παράγει το αρχικό καθαρό κείμενο.

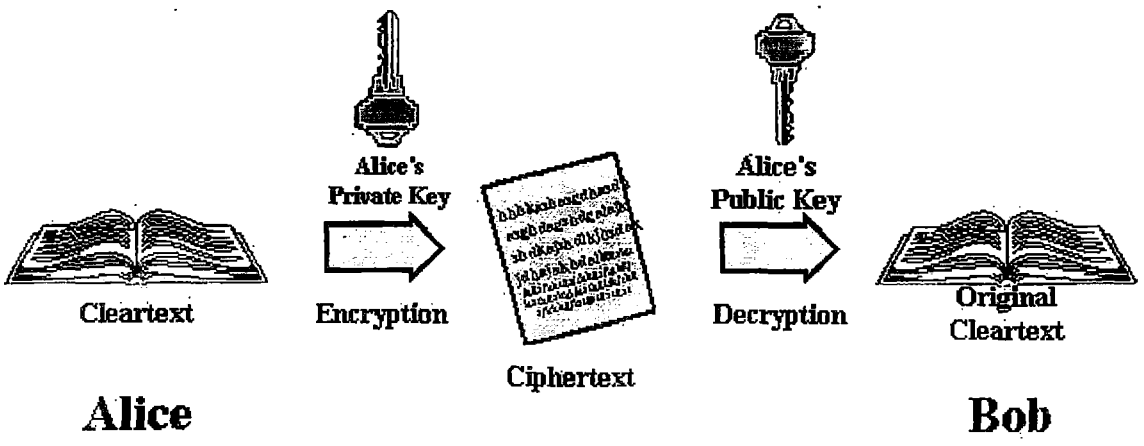
Όπως υποδηλώνουν τα ονόματα, το δημόσιο κλειδί από το ζεύγος κοινοποιείται για χρήση από άλλους, ενώ το ιδιωτικό κλειδί είναι γνωστό μόνο στον ιδιοκτήτη του. ένας γενικού σκοπού κρυπτογραφικός αλγόριθμος δημόσιου κλειδιού βασίζεται σε ένα κλειδί για κρυπτογράφηση και ένα διαφορετικό, αλλά σχετικό κλειδί για αποκρυπτογράφηση. Επιπλέον, αυτοί οι αλγόριθμοι έχουν τα ακόλουθα σημαντικά χαρακτηριστικά:

- Είναι υπολογιστικά ανέφικτο να προσδιοριστεί το κλειδί αποκρυπτογράφησης με δεδομένη μόνο τη γνώση του κρυπτογραφικού αλγορίθμου και του κλειδιού κρυπτογράφησης.
- Για τα περισσότερα σχήματα δημόσιου κλειδιού, μπορεί να χρησιμοποιηθεί για κρυπτογράφηση οποιοδήποτε από τα δύο σχετικά κλειδιά, με το άλλο να χρησιμοποιείται για αποκρυπτογράφηση.

Τα βασικά βήματα είναι τα παρακάτω:

1. Κάθε χρήστης παράγει ένα ζεύγος κλειδιών για να χρησιμοποιηθούν για κρυπτογράφηση και αποκρυπτογράφηση μηνυμάτων.

2. Κάθε χρήστης τοποθετεί το ένα από τα δύο κλειδιά σε ένα δημόσιο κατάλογο ή άλλο προσβάσιμο αρχείο. Αυτό είναι το δημόσιο κλειδί. Το αντίστοιχο δεύτερο κλειδί κρατιέται μυστικό. Κάθε χρήστης διατηρεί μία συλλογή από δημόσια κλειδιά προμηθευμένα από άλλους.
3. Εάν ο Bob επιθυμεί να στείλει ένα ιδιωτικό μήνυμα στην Alice, ο Bob κρυπτογραφεί το μήνυμα χρησιμοποιώντας το δημόσιο κλειδί της Alice.
4. Όταν η Alice λάβει το μήνυμα, το αποκρυπτογραφεί χρησιμοποιώντας το ιδιωτικό της κλειδί. Κανένας άλλος παραλήπτης δε μπορεί να αποκρυπτογραφήσει το μήνυμα επειδή μόνον η Alice γνωρίζει το ιδιωτικό κλειδί της Alice.



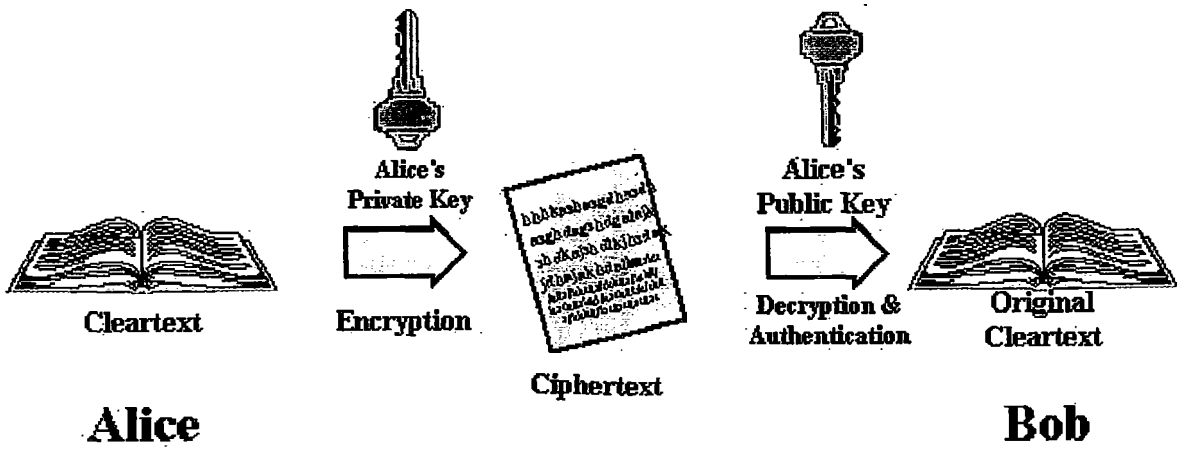
Σχήμα 1.6 : Αλγόριθμος δημόσιου κλειδιού

Με αυτήν την προσέγγιση, όλοι οι συμμετέχοντες έχουν πρόσβαση στα δημόσια κλειδιά και τα ιδιωτικά κλειδιά παράγονται τοπικά από κάθε συμμετέχοντα και για το λόγο αυτό δε χρειάζεται ποτέ να διανεμηθούν. Όσον ένας χρήστης προστατεύει το ιδιωτικό του κλειδί, η εισερχόμενη επικοινωνία είναι ασφαλής. Οποιαδήποτε στιγμή, ένας χρήστης μπορεί να αλλάξει το ιδιωτικό του κλειδί και να δημοσιοποιήσει το αντίστοιχο δημόσιο κλειδί για να αντικαταστήσει το παλιό δημόσιο κλειδί.

Οι αλγόριθμοι δημοσίου κλειδιού δεν χρησιμοποιούνται μόνο για κρυπτογράφηση αλλά και για εξακρίβωση γνησιότητας (ηλεκτρονικές υπογραφές).

Ψηφιακή υπογραφή

Για την υπογραφή ενός μηνύματος, η Alice κάνει έναν υπολογισμό εμπεριέχοντας το ιδιωτικό της κλειδί και το μήνυμα το ίδιο. Το αποτέλεσμα λέγεται ηλεκτρονική υπογραφή και επικολλάται στο μήνυμα, το οποίο και στέλνεται. Ο Bob για να επιβεβαιώσει την υπογραφή, κάνει έναν υπολογισμό χρησιμοποιώντας το μήνυμα, την υπογραφή της Alice και το δημόσιο κλειδί της Alice. Αν το αποτέλεσμα δείξει ότι το μήνυμα υπολογισμένο με το δημόσιο κλειδί της Alice είναι ίδιο με την υπογραφή της, τότε το μήνυμα είναι αυθεντικό, διαφορετικά υπάρχει περίπτωση αλλοίωσης του μηνύματος.



Σχήμα 1.7: ψηφιακή υπογραφή

1.12 Αλγόριθμοι κρυπτογραφίας δημοσίου κλειδιού

1.12.1 RSA

Το σύστημα RSA είναι ένα σύστημα ασύμμετρης κρυπτογραφίας που προσφέρει Τεχνικές κρυπτογράφηση και ψηφιακές υπογραφές. Αναπτύχθηκε το 1977 από τους Ron Rivest, Adi Shamir και Leonard Adleman. Από τα αρχικά των επιθέτων τους προέρχεται το ακρωνύμιο RSA.

Το RSA λειτουργεί ως εξής: παίρνουμε δύο μεγάλους πρώτους αριθμούς *p, q* και υπολογίζουμε το γινόμενο τους $n = pq$. Το *n* καλείται *modulus*. Διαλέγουμε ένα αριθμό *e* μικρότερο του *n* και τέτοιο, ώστε *e* και *(p-1)(q-1)* να μην έχουν κοινούς διαιρέτες εκτός του 1. Βρίσκουμε έναν άλλο αριθμό *d*, ώστε *(ed-1)* να διαιρείται από το *(p-1)(q-1)*. Τα ζευγάρια *(n,e)* και *(n,d)* καλούνται δημόσια κλείδα και ιδιωτική κλείδα, αντίστοιχα.

Είναι δύσκολο να βρεθεί η ιδιωτική κλείδα *d* από την δημόσια κλείδα *e*. Αυτό θα απαιτούσε την εύρεση των διαιρετέων του πρώτου αριθμού *n*, δηλαδή των αριθμών *p* και *q*. Ο *n* είναι πολύ μεγάλος και επειδή είναι πρώτος, θα έχει μόνο δύο πρώτους διαιρέτες. Άρα η εύρεση των διαιρετέων είναι πολύ δύσκολη έως και αδύνατη. Στο άλυτο αυτού του προβλήματος βασίζεται το σύστημα RSA. Η ανακάλυψη μιας εύκολης μεθόδου επίλυσης του προβλήματος θα αχρήστευε το RSA.

Με το RSA η κρυπτογράφηση και η πιστοποίηση ταυτότητας πραγματοποιούνται χωρίς των κοινή χρήση ιδιωτικών κλείδων. Ο καθένας χρησιμοποιεί μόνο την δικιά του ιδιωτική κλείδα ή την δημόσια κλείδα οποιουδήποτε άλλου. Όλοι μπορούν να στείλουν ένα κρυπτογραφημένο μήνυμα ή να επαληθεύσουν μια υπογραφή, αλλά μόνο ο κάτοχος της σωστής ιδιωτικής κλείδας μπορεί να αποκρυπτογραφήσει ή να υπογράψει ένα μήνυμα.

1.12.1.1 Κρυπτογράφηση με το RSA

Έστω ο χρήστης Α που θέλει να στείλει κρυπτογραφημένο στον χρήστη Β ένα έγγραφο. Ο Α κρυπτογραφεί το έγγραφο με την εξής εξίσωση: $c = m^e \bmod n$, όπου (n,e) είναι η δημόσια κλείδα του Β. Ο Β, όταν παραλάβει το μήνυμα θα εφαρμόσει την εξής εξίσωση: $m = c^d \bmod n$, όπου *(n,d)* η ιδιωτική κλείδα του Β. Η μαθηματική

σχέση που το *e* και το *d* εξασφαλίζει το γεγονός ότι ο Β αποκρυπτογραφεί το μήνυμα. Αφού μόνο ο Β ξέρει το *d*, μόνο αυτός μπορεί να αποκρυπτογραφήσει το μήνυμα.

1.12.1.2 Ψηφιακές Υπογραφές με το RSA

Ας υποθέσουμε, τώρα, ότι ο Α θέλει να στείλει μήνυμα στον Β με τέτοιον τρόπο ώστε ο Β να είναι σίγουρος ότι το μήνυμα είναι αυθεντικό και δεν έχει μεταβληθεί. Ο Α υπογράφει το έγγραφο με ως εξής: $s = m^d \bmod n$, όπου d και n είναι η ιδιωτική κλείδα του Α. Για να επαληθεύσει την υπογραφή ο Β εκτελεί την πράξη: $m = s^e \bmod n$, όπου e και n η δημόσια κλείδα του Α.

1.12.2 El Gamal

Το σύστημα El Gamal είναι ένα δημοσίου κλειδιού κρυπτογραφικό σύστημα βασισμένο στο πρόβλημα διακριτικού λογαρίθμου. Αποτελείται τόσο από αλγορίθμους κρυπτογράφησης όσο και ψηφιακών υπογραφών. Ο αλγόριθμος κρυπτογράφησης είναι παρόμοιας φύσης με τον αλγόριθμο Diffie-Hellman .
Οι παράμετροι του συστήματος αποτελούνται από έναν πρώτο αριθμό p και έναν integer g, του οποίου g οι δυνάμεις modulo p παράγουν ένα μεγάλο αριθμό στοιχείων, όπως στον αλγόριθμο Diffie-Hellman.

Ο Α έχει ένα ιδιωτικό κλειδί a και ένα δημόσιο κλειδί y, όπου $y=g^a \pmod p$.
Ας υποθέσουμε ότι ο Β επιθυμεί να σταλεί ένα μήνυμα m στον Α.
Ο Β παράγει αρχικά έναν τυχαίο αριθμό k, μικρότερο του p. Στη συνέχεια υπολογίζει:

$y_1=g^k \pmod p$ and $y_2 = m \oplus y^k$ (1.1)

Ο Β στέλνει (y_1 , y_2) στον Α.
Ο Alice υπολογίζει:

$M = (y_1^a \bmod p) \oplus y_2$ (1.2)

Η ανάλυση βασισμένη στους καλύτερους διαθέσιμους αλγορίθμους δείχνει ότι RSA και El Gamal έχουν παρόμοια ασφάλεια για αντίστοιχου μήκους κλειδιά. Το κύριο μειονέκτημα του El Gamal είναι η ανάγκη για τυχαιότητα, και η αργή ταχύτητά του (ειδικά για την υπογραφή). Ένα άλλο πιθανό μειονέκτημα του συστήματος El Gamal είναι ότι η επέκταση μηνυμάτων από έναν παράγοντα δύο πραγματοποιείται κατά τη διάρκεια της κρυπτογράφησης. Εντούτοις, τέτοια επέκταση μηνυμάτων είναι αμελητέα εάν το κρυπτογραφικό σύστημα χρησιμοποιείται μόνο για την ανταλλαγή των μυστικών κλειδιών.

1.12.3 Diffie-Hellman

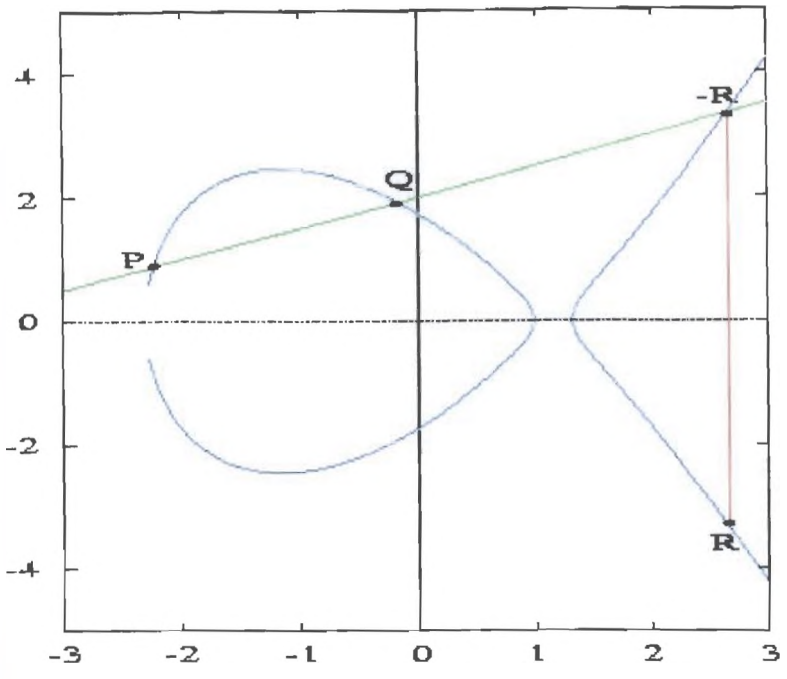
Ο αλγόριθμος δημόσιου κλειδιού Diffie-Hellman αναπτύχθηκε το 1976 από τους Diffie και Hellman. Ο αλγόριθμος χρησιμοποιείται ευρέως για ανταλλαγή μυστικών κλειδιών που μεταδίδονται χρησιμοποιώντας μη ασφαλή μέσα. Η ασφάλεια του Diffie-Hellman βασίζεται στη δυσκολία που παρουσιάζει το πρόβλημα του υπολογισμού διακριτών λογαρίθμων. Στον αλγόριθμο Diffie-Hellman θα αναφερθούμε αναλυτικότερα στο 4° κεφάλαιο

1.12.4 DSS (Digital Signature Algorithm)

Το National Institute of Standards and Technology (NIST) δημοσιοποίησε το *Digital Signature Algorithm (DSS)*, που είναι μέρος του *Capstone Project* της κυβέρνησης των Ηνωμένων Πολιτειών, τον Μάιο του 1994. Έχει καθιερωθεί σαν το επίσημο αλγόριθμο παραγωγής ψηφιακών υπογραφών της κυβέρνησης των Η.Π.Α.
Βασίζεται στο πρόβλημα του διακριτού λογαρίθμου και χρησιμοποιείται μόνο για παραγωγή ψηφιακών υπογραφών. Η διαφορά από τις υπογραφές του RSA είναι ότι ενώ στο DSA η παραγωγή των υπογραφών είναι πιο γρήγορη από την επιβεβαίωση τους, στο RSA συμβαίνει το αντίθετο: η επιβεβαίωση είναι ταχύτερη από την υπογραφή. Παρ' όλο που μπορεί να υποστηριχθεί ότι η γρήγορη παραγωγή υπογραφών αποτελεί πλεονέκτημα, επειδή ένα μήνυμα υπογράφεται μία φορά αλλά η υπογραφή του μπορεί να επαληθευτεί πολλές φορές, κάτι τέτοιο δεν ανταποκρίνεται στην πραγματικότητα.
Το DSS έχει ολοκληρωθεί σε πολλά συστήματα ασφαλείας, αν και έχει λάβει πολλές άσχημες κριτικές. Τα κυριότερα θέματα κριτικής είναι η έλλειψη ευελιξίας, η αργή επαλήθευση των υπογραφών, η αδυναμία συνεργασίας με άλλο πρωτόκολλο πιστοποίησης ταυτότητας και τέλος ότι ο αλγόριθμος δεν είχε αποκαλυφθεί.

1.12.5 Ελλειπτικές καμπύλες

Οι *ελλειπτικές καμπύλες* είναι μαθηματικά κατασκευάσματα από τη θεωρία αριθμών και την αλγεβρική γεωμετρία που βρήκαν πρόσφατα πολυάριθμες εφαρμογές στην κρυπτογραφία:
Μια ελλειπτική καμπύλη μπορεί *να* ορισθεί σε ένα οποιοδήποτε πεδίο (π.χ. πραγματικό, λογικό, μιγαδικό), αν και οι ελλειπτικές καμπύλες που χρησιμοποιούνται στην κρυπτογραφία ορίζονται κυρίως σε πεπερασμένα πεδία. Μια ελλειπτική *καμπύλη* αποτελείται *από* όλα τα στοιχεία *(X, Y)* που ικανοποιούν την εξίσωση:
$y^2 = x^3 + ax + b$ μαζί με ένα μοναδικό στοιχείο που συμβολίζεται με 0 και ονομάζεται "σημείο στο άπειρο", το οποίο μπορεί *να* αναπαρασταθεί *σαν* σημείο στην κορυφή και στη βάση κάθε κατακόρυφης γραμμής.
Το σύνολο των σημείων σε μια ελλειπτική καμπύλη σχηματίζει μία ομάδα υπό άθροιση, όπου η άθροιση δύο σημείων σε μια ελλειπτική καμπύλη προσδιορίζεται σύμφωνα με *ένα* σύνολο απλών κανόνων. Για παράδειγμα, έστω δύο σημεία ρ1 και *p2* στο Σχήμα 1. Το σημείο ρ1 και το σημείο p2 είναι ίσο με το σημείο *p4 = (x,-y),* όπου *(x, y) = p3* είναι το τρίτο σημείο στην τομή της ελλειπτικής καμπύλης και της γραμμής *L* που ενώνει το ρι και το *p2.* Η πράξη της πρόσθεσης σε μια ελλειπτική καμπύλη είναι το ισοδύναμο του πολλαπλασιαστικού διαιρέτη στα κοινά κρυπτοσυστήματα δημοσίου κλειδιού και η πολλαπλή άθροιση είναι το ισοδύναμο της εκθετοποίησης του διαιρέτη.



Σχήμα 1.8: Ελλειπτική καμπύλη

1.13 Επιθέσεις στους αλγόριθμους δημόσιου κλειδιού

Οι αλγόριθμοι δημόσιου κλειδιού είναι θεωρητικά ποιο ευάλωτοι στις επιθέσεις από αυτούς συμμετρικού κλειδιού γιατί ο επιτιθέμενος έχει (ίσως) ένα αντίγραφο του δημόσιου κλειδιού που χρησιμοποιήθηκε για την κρυπτογράφηση του μηνύματος. Η δουλειά του επιτιθέμενου είναι ακόμα ευκολότερη γιατί το ίδιο το μήνυμα πιθανώς να υποδηλώνει με ποιόν αλγόριθμο έχει κρυπτογραφηθεί.
Οι επιθέσεις στους αλγόριθμου ς δημόσιου κλειδιού χωρίζονται σε δυο κατηγορίες:

1.13.1 Επιθέσεις παραγοντοποίησης (factoring attacks)

Αυτού του είδους οι επιθέσεις είναι πολύ δημοφιλείς στα συστήματα δημόσιου κλειδιού γιατί είναι πολύ εύκολες να κατανοηθούν. Αυτή η επίθεση αποσκοπεί να αντλήσει το προσωπικό κλειδί από το αντίστοιχο δημόσιο κλειδί. Στην επίθεση αυτή χρειάζεται να επιλύσουμε διάφορα είδη μαθηματικών προβλημάτων.
Στην περίπτωση του RSA αλγόριθμου για να πετύχουμε την επίθεση αυτή, χρειάζεται να παραγοντοποιήσουμε έναν αριθμό που σχετίζεται με το δημόσιο κλειδί. Το μαθηματικό πρόβλημα της παραγοντοποίησης απασχολεί αιώνες του μαθηματικούς και είναι ακόμα δυσκολότερο όταν πρόκειται για μεγάλους αριθμούς. Έχουν βρεθεί μερικοί εύκολοι μέθοδοι για κάποια κατηγορία αριθμών, αλλά παραμένει δύσκολή δουλειά. Μια γνωστή τέτοια επίθεση είναι η παραγοντοποίηση του RSA-129 αριθμού το 1994. Η RSA Data Security δημοσιεύει λίστες από τέτοιούς αριθμούς και προκαλεί να παραγοντοποιηθούν έναντι χρηματικής αμοιβής.

1.13.2 Επίθεση αλγοριθμική

Ένας άλλος τρόπος επίθεσης είναι να βρούμε ένα βασικό ελάττωμα ή αδυναμία του μαθηματικού προβλήματος στο οποίο είναι βασισμένο το σύστημα κρυπτογράφησης. Αυτό έχει γίνει περισσότερες από μια φορές στο παρελθόν. Το πρώτο κρυπτογραφικό σύστημα που εφαρμόστηκε ήταν βασισμένο σε ένα μαθηματικό πρόβλημα που ονομαζόταν Superincreasing Knapsack Problem. Μερικά χρόνια μετά βρέθηκε ένας μαθηματικός τρόπος για να αποκτάται το μυστικό κλειδί από το δημόσιο μέσα σε πολύ λίγο χρόνο.

Όταν μια σημαντική μαθηματική καινοτομία βρίσκεται, ίσως να μην δημοσιευτεί σε όλους αλλά να φυλαχτεί από μια κυβερνητική αρχή για να χρησιμοποιηθεί εναντίον κρυπτογραφημένων μηνυμάτων που ανταλλάσσουν άλλες χώρες. Αλλιώς εάν μια μέθοδος βρεθεί από κάποιον με εγκληματικές προθέσεις, ίσως να κρατηθεί μυστική για να χρησιμοποιηθεί σε μελλοντικά οικονομικά εγκλήματα.

1.14 Σύγκριση Αλγόριθμων συμμετρικής και ασύμμετρης κρυπτογραφίας

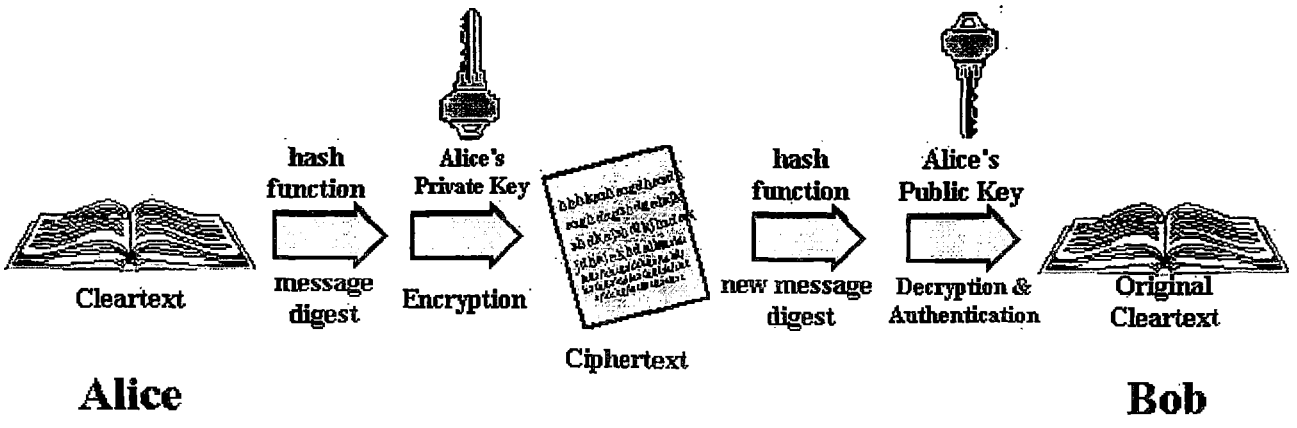
Το βασικό πλεονέκτημα της κρυπτογραφίας δημόσιου κλειδιού είναι η αυξημένη ασφάλεια που παρέχει. Το πλεονέκτημα αυτό απορρέει από το γεγονός ότι το ιδιωτικό κλειδί, στην ασύμμετρη κρυπτογραφία, δε χρειάζεται ποτέ να μεταδοθεί ή να αποκαλυφθεί σε οποιονδήποτε. Αντίθετα, στα συστήματα κρυπτογράφησης ιδιωτικού κλειδιού, το ιδιωτικό κλειδί πρέπει είτε να μεταδοθεί με κάποιο συμβατικό τρόπο, είτε να μεταδοθεί ηλεκτρονικά μέσω ενός καναλιού μετάδοσης. Κατά τη μετάδοση του ιδιωτικού κλειδιού, υπάρχει πάντα ο κίνδυνος να ανακαλυφθεί το κλειδί από μη εξουσιοδοτημένα άτομα και κατά συνέπεια να «σπάσει» (όπως λέγεται) η κρυπτογράφηση. Για το λόγο αυτό, η μετάδοση του ιδιωτικού κλειδιού στα συμμετρικά συστήματα αποτελεί βασικό μειονέκτημά τους.

Ένα άλλο σημαντικό πλεονέκτημα των συστημάτων δημόσιου κλειδιού είναι ότι παρέχουν επιπρόσθετα μια μέθοδο για ψηφιακές υπογραφές. Η πιστοποίηση μέσω των συστημάτων ιδιωτικού κλειδιού προϋποθέτει το "μοίρασμα κάποιου μυστικού" και μερικές φορές απαιτείται και η εμπιστοσύνη από κάποιο τρίτο πρόσωπο. Αυτό δίνει εν δυνάμει τη δυνατότητα στον αποδέκτη να "αρνείται" προηγούμενες πιστοποιήσεις μηνυμάτων, ισχυριζόμενος ότι το "κοινό μυστικό" διέρρευσε από ένα από τα πρόσωπα που το γνώριζαν. Για παράδειγμα, το σύστημα πιστοποίησης ταυτότητας Κέρβερος (KAS-Kerberos Authentication System) χρησιμοποιεί μια κεντρική Βάση Δεδομένων στην οποία κρατάει αντίγραφα των ιδιωτικών κλειδιών όλων των χρηστών της. Είναι προφανές πως μια πιθανή προσβολή της βάσης δεδομένων θα προκαλέσει αστοχία του συστήματος. Από την άλλη πλευρά, στα συστήματα δημόσιου κλειδιού, ο κάθε χρήστης έχει ο ίδιος την ευθύνη προστασίας του προσωπικού του ιδιωτικού κλειδιού.

Ως βασικό μειονέκτημα της χρήσης της ασύμμετρη ς κρυπτογραφίας θεωρείται η ταχύτητα. Υπάρχουν δημοφιλείς μέθοδοι ασύμμετρης κρυπτογράφησης που είναι σημαντικά πιο γρήγορες από οποιαδήποτε μέθοδο συμμετρικής κρυπτογράφησης. Ωστόσο, η κρυπτογραφία δημόσιου κλειδιού μπορεί να συνδυαστεί με την κρυπτογραφία ιδιωτικού κλειδιού, ώστε να καταστεί δυνατή η αξιοποίηση των συγκριτικών πλεονεκτημάτων και των δύο μεθόδων. Τα συστήματα που λειτουργούν με αυτόν τον τρόπο ονομάζονται *υβριδικά συστήματα κρυπτογραφίας*.

1.15 Συναρτήσεις κατακερματισμού

Οι hash functions είναι θεμελιώδεις στην κρυπτογραφία. Μια hash function είναι μια συνάρτηση η οποία παίρνει μεταβλητού μήκους δεδομένα εισόδου και παράγει σταθερού μήκους δεδομένα εξόδου, τα οποία μπορούν να θεωρηθούν ως αποτύπωμα της εισόδου. Αυτό σημαίνει ότι αν οι τιμές κατακερματισμού (hash values) δύο μηνυμάτων ταιριάζουν, τότε υπάρχει μια μεγάλη πιθανότητα ότι τα μηνύματα είναι τα ίδια.
Κρυπτογραφικά χρήσιμες συναρτήσεις κατακερματισμού πρέπει να είναι αυτές που είναι μη αντιστρέψιμες (one way), που σημαίνει ότι είναι εύκολες να υπολογιστούν, αλλά πρακτικώς αδύνατον να αντιστραφούν. Μια καλή συνάρτηση κατακερματισμού πρέπει να είναι ανθεκτική στις συγκρούσεις. Πρέπει δηλαδή να είναι δύσκολο να βρεθούν δύο διαφορετικές τιμές που η τιμή κατακερματισμού να είναι η ίδια. Όπως κάθε hash function αντιστοιχεί set εισόδων σε set εξόδων με μικρότερο μήκος από τις εξόδους, θεωρητικά είναι δυνατόν να βρεθούν συγκρούσεις. Ο στόχος είναι να παρέχεται σε ένα μήνυμα ένα μοναδικό ψηφιακό αποτύπωμά του, το οποίο να το προσδιορίζει με μεγάλη σιγουριά, όπως ένα δακτυλικό αποτύπωμα προσδιορίζει ένα πρόσωπο.



Σχήμα 1.9: Ψηφιακή υπογραφή με χρήση συναρτήσεων κατακερματισμού

Οι βασικές απαιτήσεις για μια κρυπτογραφική συνάρτηση κατακερματισμού είναι:

1. Η συνάρτηση Η μπορεί να εφαρμοστεί σε ένα τμήμα δεδομένων οποιουδήποτε μεγέθους.
2. Η συνάρτηση Η παράγει μία έξοδο σταθερού μήκους.
3. Η συνάρτηση *H(x)* είναι σχετικά εύκολο να υπολογιστεί για οποιοδήποτε δοσμένο x, κάνοντας πρακτικές τις υλοποιήσεις υλικού και λογισμικού.
4. Για οποιονδήποτε δοσμένο κώδικα *h*, είναι υπολογιστικά ανέφικτο να βρεθεί *x* τέτοιο ώστε *H(x) = h.*
5. Για οποιοδήποτε δοσμένο τμήμα *X*, είναι υπολογιστικά ανέφικτο να βρεθεί y $\neq$ x με *H(y) = H(x).*
6. Είναι υπολογιστικά ανέφικτο να βρεθεί ένα ζεύγος *(y,x)* τέτοιο ώστε *H(y) = H(x).*

Επειδή οι συναρτήσεις κατακερματισμού είναι πιο γρήγορες από τους αλγόριθμους κρυπτογράφησης και ψηφιακών υπογραφών, συνηθίζεται να παράγεται η υπογραφή των μηνυμάτων με την εφαρμογή κρυπτογραφικών διαδικασιών στο συγχωνευμένο

μήνυμα, το οποίο είναι πιο μικρό και εύκολο στη διαχείριση. Επιπλέον ένασυγχωνευμένο μήνυμα μπορεί να δημοσιοποιηθεί χωρίς να αποκαλύπτει τα περιεχόμενα του αυθεντικού κειμένου. Το παραπάνω είναι σημαντικό στις ψηφιακές χρονοσφραγίδες, όπου χρησιμοποιώντας συναρτήσεις κατακερματισμού, μπορούν να αποδοθούν χρονοσφραγίδες σε έγγραφα χωρίς να αποκαλυφθεί το περιεχόμενο τους στην υπηρεσία που εκδίδει τις χρονοσφραγίδες.
Οι Damgard και Merkle επηρέασαν σημαντικά το σχεδιασμό κρυπτογραφικών συναρτήσεων κατακερματισμού εισάγοντας την έννοια της *συμπίεσης*. Μία συνάρτηση συμπίεσης δέχεται ως είσοδο ένα μήνυμα σταθερού μεγέθους και παράγει στην έξοδο ένα μήνυμα επίσης σταθερού μεγέθους αλλά μικρότερο. Σύμφωνα με τους Damgard και Merkle, δοσμένης μιας συνάρτησης συμπίεσης, μια συνάρτηση κατακερματισμού μπορεί να οριστεί μέσα από επαναληπτικές εφαρμογές της συνάρτησης συμπίεσης έως ότου να επεξεργαστεί ολόκληρο το μήνυμα. Σύμφωνα με αυτή τη διαδικασία, ένα μήνυμα αυθαίρετου μεγέθους χωρίζεται σε ομάδες, των οποίων το μέγεθος εξαρτάται από τις προδιαγραφές της συνάρτησης συμπίεσης που χρησιμοποιείται και συμπληρώνεται (για λόγους ασφάλειας), έτσι ώστε το μέγεθος του μηνύματος να γίνει πολλαπλάσιο του μεγέθους ομάδας. Στη συνέχεια, οι ομάδες επεξεργάζονται σειριακά δίνοντας ως έξοδο την τιμή κατακερματισμού για το συγκεκριμένο μήνυμα.

1.16 Αλγόριθμοι συγχώνευσης μηνύματος

1.16.1 SHA και SHA-1 (Secure Hash Algorithm)

Ο SHA, όπως και SHA-1, αναπτύχθηκαν από την Εθνική Υπηρεσία Ασφάλειας των Η.Π.Α (NIST). Ο SHA-1 αποτελεί επανέκδοση του SHA με διόρθωση μιας ατέλειας του τελευταίου. Η σχεδίαση του είναι παρόμοια με αυτή του MD5. Ο αλγόριθμος δέχεται ένα μήνυμα μικρότερο των 264 bits σε μέγεθος το οποίο και επεξεργάζεται σε μπλοκ των 512 bits, παράγοντας ένα συγχωνευμένο μήνυμα των 160 bit.
Όσον αφορά τη λειτουργία του, ο αλγόριθμος ξεκινάει και σε αυτήν την περίπτωση διαμορφώνοντας το αρχικό μήνυμα και στη συνέχεια προσθέτει 64 bits για να πάρουμε πολλαπλά μπλοκ των 512 bits. Έπειτα, τοποθετεί μια αρχική τιμή στον καταχωρητή των 160 bits.
Για κάθε μπλοκ εισόδου, ο καταχωρητής εξόδου ενημερώνεται χρησιμοποιώντας το μπλοκ των 512 bits εισόδου. Επειδή το message digest του SHA είναι μεγαλύτερο, κατά 32 bits, από αυτό του MD5, η μέθοδος αυτή είναι ασφαλέστερη κατά 232 φορές από την MD5. Ωστόσο, είναι ελαφρά πιο αργή από την MD5 και, επειδή το μήκος του message digest δεν αποτελεί δύναμη του 2, συνήθως η χρήση του είναι μη πρακτική. Κατά τα άλλα, οι δύο μέθοδοι είναι τεχνικά παρόμοιες.

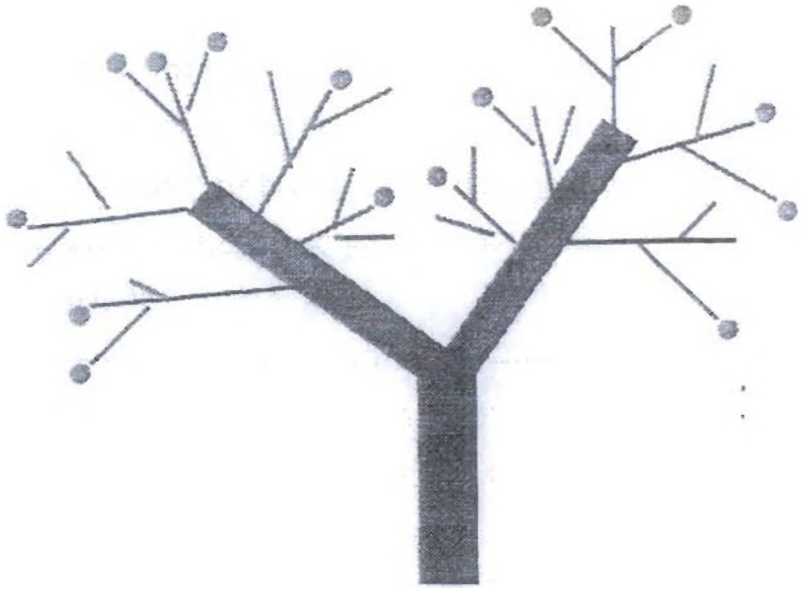
1.16.2 MD2, MD4, MD5 (Message Digest)

Όλοι αυτοί οι αλγόριθμοι είναι hash functions που έχουν αναπτυχθεί από τον Ron Rivest. Προορίζονται, κυρίως, για την παραγωγή ψηφιακών υπογραφών. Το μήνυμα πρώτα σμικρύνεται με έναν από αυτούς τους αλγόριθμους και έπειτα, το message digest του μηνύματος κρυπτογραφείται με την ιδιωτική κλείδα του αποστολέα. Και οι τρεις παίρνουν στην είσοδο μήνυμα αυθαίρετου μήκους και δίνουν στην έξοδο ένα message digest 128 bits. Παρ' όλο που η κατασκευή τους μοιάζει αρκετά, ο MD2 είχε σχεδιαστεί για μηχανές 8 bit, σε αντίθεση με τους MD4 και MD5 που προορίζονται για μηχανές 32 bits.

Ο MD2 αναπτύχθηκε το 1989. Το μήνυμα αρχικά συμπληρώνεται με κατάλληλο αριθμό bytes, ώστε το μήκος του σε bytes να είναι διαιρέσιμο από το 16. Ένα αρχικό checksum των 16 bits προστίθεται στο τέλος του μηνύματος και το τελικό message digest παράγεται από το αποτέλεσμα της προηγούμενης ενέργειας. Η κρυπτανάλυση του MD2 έδειξε ότι είναι δυνατόν να υπάρχουν μηνύματα που παράγουν το ίδιο message digest αν και μόνο αν παραλείπεται το βήμα πρόσθεσης του 16-byte checksum.
Ο MD4 αναπτύχθηκε το 1990. Το μήκος του μηνύματος συμπληρώνεται με κατάλληλο αριθμό bits, ώστε να το μήκος του σε bits συν 448 να είναι διαιρέσιμο από το 512. Μια δυαδική αναπαράσταση του μηνύματος των 64 bits προστίθεται στο μήνυμα και το αποτέλεσμα επεξεργάζεται με compression function. Τα blocks που διαχειρίζεται ο compression function έχουν μήκος 512 bits και κάθε block επεξεργάζεται πλήρως σε τρεις διακριτούς επαναληπτικούς γύρους. Ο MD4 έχει επανειλημμένα αναλυθεί με διάφορους τρόπους και δεν πρέπει να θεωρείται πλέον ασφαλής. Συγκεκριμένα, έχει αποδειχθεί ότι μπορεί να αντιστραφεί η διαδικασία και ότι υπό ορισμένες συνθήκες δεν είναι αμφιμονοσήμαντος.
Ο MD5 αναπτύχθηκε το 1991. Είναι μια κατά πολύ βελτιωμένη έκδοση του MD4, γι' αυτό είναι και λίγο πιο αργός. Η μόνη διάφορα είναι η χρήση τεσσάρων επαναλήψεων κατά την επεξεργασία του κάθε block. Οι απαιτήσεις σε μέγεθος block και μήκος μηνύματος παραμένουν οι ίδιες. Η κρυπτανάλυση του MD5 συνεχίζεται ακόμα, αλλά οι πρώτες εκτιμήσεις δείχνουν ότι έχει αρκετές αδυναμίες.

1.17 Στεγανογραφία

Η στεγανογραφία είναι η απόκρυψη της ύπαρξης του ίδιου του μηνύματος. Παρόλο που η διάκρισή της από τη κρυπτογραφία είναι πολύ λεπτή, υπάρχουν σημαντικές τεχνικές διαφοροποιήσεις ανάμεσά τους.
Κατά καιρούς έχουν αναφερθεί διάφορες στεγανογραφικές μέθοδοι. Από την αρχαιότητα αναφέρεται και η ακόλουθη μέθοδος.: Εάν κάποιος ήθελε να στείλει ένα μήνυμα, έπαιρνε έναν αγγελιοφόρο, ξύριζε το κεφάλι του, έγραφε το μήνυμα που ήθελε στο ξυρισμένο κεφάλι του, περίμενε μέχρι να μεγαλώσουν τα μαλλιά του και τον έστελνε εκεί που ήθελε. Ο παραλήπτης, από την άλλη, μόλις έφτανε ο αγγελιοφόρος, του ξύριζε και πάλι το κεφάλι και διάβαζε το μήνυμα!
Μια άλλη μέθοδος χρησιμοποιούσε εικόνες για τη μεταφορά κρυμμένων μηνυμάτων
Στο Σχήμα (1.10) βλέπουμε ένα οπωροφόρο δέντρο. Όμως, στη συγκεκριμένη εικόνα υπάρχει ένα κρυμμένο μήνυμα. Ακολουθώντας το περίγραμμα του δέντρου με τη φορά των δεικτών του ρολογιού και σημειώνοντας με '1' τα κλαδιά που φέρουν φρούτα και 'Ο' τα υπόλοιπα, μπορούμε να σχηματίσουμε την ακολουθία των δυαδικών ψηφίων η οποία αποτελεί το μήνυμα.



Σχήμα 1.10: Μια εικόνα που περιέχει το κρυμμένο μήνυμα (110, 010, 111, 010, 010, 010, 100,101,011,001)

Το γράψιμο ενός μηνύματος με αόρατο μελάνι θεωρείται στεγανογραφική μέθοδος. Οι μέθοδοι στεγανογραφίας είναι ατέλειωτες. Μεταξύ άλλων, έχει προταθεί και η χρησιμοποίηση του λιγότερου σημαντικού bit ενός πλαισίου (frame) σε ένα CD. Η στεγανογραφία απαιτεί όμως την αποστολή και «μη χρήσιμης» πληροφορίας (overhead) και, από αυτή την άποψη, υστερεί σημαντικά σε σύγκριση με την κρυπτογράφηση. Ωστόσο, αξίζει η εφαρμογή της όταν ακόμα το γεγονός και μόνο της εξακρίβωσης της ανταλλαγής μηνυμάτων (και όχι απαραίτητα το περιεχόμενο) οδηγεί σε σημαντική απώλεια εμπιστευτικής πληροφορίας. Αξίζει να σημειωθεί ότι η απόκρυψη ύπαρξης επικοινωνιακής σχέσης είναι δυνατή και με την εφαρμογή κρυπτογραφικών πρωτοκόλλων, αλλά είναι ιδιαίτερα πολυέξοδη.

ΚΕΦΑΛΑΙΟ 2
ΚΡΥΠΤΟΓΡΑΦΙΑ ΣΤΟ WEB

Στο κεφάλαιο αυτό παρουσιάζονται τα κρυπτογραφικά συστήματα που χρησιμοποιούνται στο WEB σήμερα και ικανοποιούν τις βασικές απαιτήσεις ασφάλειας.(εμπιστευτικότητα, ακεραιότητα, απόδειξη γνησιότητας και μη απάρνηση)

2.1 PEM (Privacy Enhanced Mail)

2.1.1 Εισαγωγή

Ένα ηλεκτρονικό μήνυμα του Internet, κατά την πορεία του από τον αποστολέα στον τελικό παραλήπτη, διανύει πολλά ενδιάμεσα συστήματα και δίκτυα. Δεν είναι δυνατόν να βασιστούμε στην αξιοπιστία όλων αυτών των οντοτήτων. Ένας εισβολέας μπορεί να κρύβεται οπουδήποτε και τα μηνύματα μπορούν εύκολα να διαβαστούν, να τροποποιηθούν και ακόμα να εμποδιστούν από το να φθάσουν στον τελικό τους προορισμό.
Το πρωτόκολλο Privacy-Enhanced Mail (PEM) προβλέπει για αυτή την αδυναμία του ηλεκτρονικού ταχυδρομείου του Internet, προσθέτοντας την εφαρμογή των υπηρεσιών της απόρρητης συναλλαγής, της πιστοποίησης ταυτότητας, της ακεραιότητας των μηνυμάτων και την εξασφάλιση της μη αποκήρυξης της πηγής. Οι υπηρεσίες αυτές προσφέρονται μέσω της χρήσης απ' άκρη σ' άκρη κρυπτογράφησης μεταξύ του αποστολέα και του παραλήπτη. Δεν απαιτούνται ειδικές ικανότητες επεξεργασίας στα συστήματα MTS (Message Transfer System) και υποστηρίζεται η συνεργασία με άλλα ταχυδρομικά συστήματα μεταφοράς.
Προς το παρών το PEM χρησιμοποιείται με μηνύματα RFC822, ενώ επέκταση του πρωτοκόλλου ώστε να εφαρμόζεται και σε περιβάλλοντα MIME αναμένεται.

2.1.2 Αρχές του PEM

Σημαντικότατο γεγονός είναι ότι, που έρχεται σε αντίθεση με το S/MIME, η εφαρμογή των υπηρεσιών ασφαλείας που παρέχει το PEM γίνεται στο σώμα του μήνυμα στο σύνολο του. Δεν επιτρέπεται ούτε υποστηρίζεται η επιλεκτική χρήση των υπηρεσιών του PEM σε κομμάτια του μηνύματος.

Η ανάπτυξη του PEM στηρίχθηκε στις εξής βασικές αρχές:

- Όλες προσθήκες ασφάλειας εφαρμόζονται στο Application Layer του OSI και είναι ανεξάρτητες από οποιαδήποτε χαρακτηριστικά ασφαλείας χαμηλότερων επιπέδων.
- Οι προσθήκες ασφαλείας εφαρμόζονται μόνο από τους αποστολείς και τους Τελικούς αποδέκτες των μηνυμάτων. Η λειτουργία των ενδιάμεσων συστημάτων που δεν υποστηρίζουν τις δυνατότητες του PEM δεν επηρεάζεται από αυτή την συνθήκη. Παρ' όλα αυτά είναι απαραίτητο ο αποστολέας να γνωρίζει κατά πόσο ο προοριζόμενος παραλήπτης του μηνύματος εφαρμόζει

τις υπηρεσίες ασφάλειας του PEM, ώστε να αποφευχθεί η άσκοπη κρυπτογράφηση και κωδικοποίηση του μηνύματος.

- Οι καθορισμένοι μηχανισμοί είναι συμβατοί με μία μεγάλη ποικιλία ταχυδρομικών συστημάτων μεταφοράς (MTAs) και πρέπει να μπορούν να λειτουργούν πρωτόκολλα μεταφορά εκτός του SMTP (USENET, CSNET, BITNET).
- Οι καθορισμένοι μηχανισμοί είναι συμβατοί με μεγάλη ποικιλία προγραμμάτων ηλεκτρονικού ταχυδρομείου (Mail User Agents – UAs). Επιπλέον οι μηχανισμοί του PEM διαλέγονται έτσι ώστε να μπορούν να χρησιμοποιηθούν με στα περισσότερα προγράμματα χρηστών.
- Υποστηρίζεται μεγάλη ποικιλία τεχνικών διαχείρισης κλειδιών και διαφορετικές τεχνικές χρησιμοποιούνται με διαφορετικούς παραλήπτες. Διαφορετικές τεχνικές μπορούν να οριστούν ακόμα και με τους διαφορετικούς παραλήπτες ενός multicast μηνύματος. Για δυο PEM εφαρμογές να συνεργαστούν, πρέπει να μοιράζονται ένα τουλάχιστον κοινό μηχανισμό διαχείριση κλειδιών.

2.1.3 Παραγωγή PEM Μηνυμάτων

2.1.3.1 Είδη Κλειδιών και Διαχείριση τους

Η περιγραφή του πρωτοκόλλου στο RFC1421 καθορίζει δύο τύπους κλειδιών:
Data Encrypting Keys (DEKs): Είναι κλειδιά που χρησιμοποιούνται για την κρυπτογράφηση των κειμένων των μηνυμάτων. Στην ασύμμετρη διαχείριση κλειδιών (asymmetric key management), στα PEM μηνύματα που εφαρμόζεται η υπηρεσία της διαφύλαξης του απόρρητου (ENCRYPTED μηνύματα – βλέπε παρακάτω) τα DEKs χρησιμοποιούνται στην επιπλέον κρυπτογράφηση των Message Integrity Checks (MICs). Λέμε επιπλέον γιατί τα MICs, για την παραγωγή της υπογραφής του μηνύματος, κρυπτογραφούνται από το IK. Λέγοντας MICs εννοούμε το αποτέλεσμα που δίνει στην έξοδο του ένας digest ή hash algorithm όταν στην είσοδο εισάγουμε το μήνυμα. Τα κλειδιά DEKs παράγονται εκ νέου για κάθε μήνυμα προς μετάδοση.
Interchange Keys (IKs): Χρησιμοποιούνται για την κρυπτογράφηση των DEKs και MICs τα οποία μεταφέρονται μέσα στο μήνυμα. Κανονικά, το ίδιο IK θα χρησιμοποιηθεί για όλα τα μηνύματα από έναν συγκεκριμένο αποστολέα σε έναν συγκεκριμένο παραλήπτη, για περιορισμένο χρονικό διάστημα. Η κρυπτογράφηση των DEKs και MICs μπορεί να γίνει είτε με συμμετρική κρυπτογραφία (συμμετρική διαχείριση κλειδιών), οπότε το IK είναι το ίδιο για αποστολέα και παραλήπτη, είτε με ασύμμετρη κρυπτογραφία (ασύμμετρη διαχείριση κλειδιών), οπότε η κρυπτογράφηση γίνεται με την δημόσια κλείδα του παραλήπτη. Στην ασύμμετρη κρυπτογράφηση των MICs χρησιμοποιείται η ιδιωτική κλείδα του αποστολέα.
Όταν ένα μήνυμα πρόκειται να επεξεργαστεί από το PEM, παράγεται ένα DEK για την κρυπτογράφηση του μηνύματος καθώς και απαραίτητοι παράμετροι (π.χ. Initialization Vectors) που εξαρτώνται από τους επιλεγμένους αλγόριθμους. Στην περίπτωση συμμετρικών IKs, χρησιμοποιούνται διαφορετικά κλειδιά για κάθε παραλήπτη του μηνύματος, για την προετοιμασία των κρυπτογραφημένων DEKs και MICs. Αντίθετα, στην περίπτωση των ασύμμετρων IKs, επειδή ο αποστολέας κατέχει ένα ζευγάρι δημόσιας – ιδιωτικής κλείδας, η κρυπτογράφηση των DEKs και MICs γίνεται για όλους τους παραλήπτες με την ίδια κλείδα.

Είναι δυνατόν ένα αφιερωμένο σύστημα (Key Distribution System) να δημιουργεί τα τυχαία DEKs. Τέτοια συστήματα μπορούν να εφαρμόζουν πιο ισχυρούς αλγόριθμους στην παραγωγή των τυχαίων DEKs, παρ' αυτά όμως η αποκέντρωση της παραγωγής επιτρέπει στα συστήματα των χρηστών να είναι αυτοσυντηρούμενα και απαλείφει την εμπιστοσύνη σε τρίτες οντότητες.
Η ασύμμετρη διαχείριση κλειδιών μπορεί να συνδυαστεί με την χρήση πιστοποιητικών για την επαλήθευσης της ταυτότητας του αποστολέα. Το πιστοποιητικό περιέχει, εκτός των πληροφοριών που σχετίζονται με τον εκδότη του (Certificate Authority – CA) και την δημόσια κλείδα του αποστολέα.

2.1.3.2 Περιληπτική Παρουσίαση της Επεξεργασίας

Με σκοπό τα κρυπτογραφημένα μηνύματα να είναι παγκοσμίως αναγνωρίσιμα και να μπορούν να μεταφερθούν σε όλα τα περιβάλλοντα, απαιτείται ένας μετασχηματισμός τεσσάρων φάσεων. Αρχικά τα μηνύματα συντάσσονται σύμφωνα με τους τοπικούς κανόνες, χρησιμοποιώντας το σύνολο χαρακτήρων (character set) και τους χαρακτήρες ελέγχου του τοπικού συστήματος. Η αρχική αυτή μορφή μετατρέπεται σε κανονική μορφή (canonical form), η οποία αποτελεί είσοδο στις διαδικασίες της κρυπτογράφησης και της παραγωγής MIC. Τέλος, το αποτέλεσμα της κρυπτογράφησης και / ή της παραγωγής του MIC κωδικοποιείται βάσει κατάλληλου μηχανισμού. Το σύνολο χαρακτήρων που χρησιμοποιεί ο μηχανισμός αυτός είναι παγκόσμια παρουσιάσιμο. Παρακάτω θα αναλύσουμε περισσότερο τα βήματα επεξεργασίας.
Η έξοδος του τέταρτου βήματος συνδυάζεται με κατάλληλες επικεφαλίδες που μεταφέρουν πληροφορίες ελέγχου της κρυπτογράφησης. Το PEM μήνυμα που προκύπτει περιλαμβάνεται στα περιεχόμενα ενός μηνύματος προς μετάδοση. Στα περιεχόμενα είναι δυνατόν να υπάρχει και απλό, μη προστατευμένο κείμενο.
Ο παραλήπτης του μηνύματος, αφού αφαιρέσει την κωδικοποίηση, εξετάζει τις πεδία ελέγχου της κρυπτογράφησης που του παρέχουν τις απαραίτητες πληροφορίες για να επαλήθευση την εγκυρότητα του MIC και για να αποκρυπτογραφήσει το κείμενο. Τέλος, το μήνυμα μετατρέπεται από την κανονική μορφή στην μορφή που αντιστοιχεί στα χαρακτηριστικά του τοπικού συστήματος του παραλήπτη.
Συντακτικά άκυρα PEM μηνύματα θα πρέπει να αναφερθούν μαζί με συλλογή διαγνωστικών πληροφοριών για να αντιμετωπιστούν προβλήματα ασυμβατότητας ή άλλων αιτιών. Τα PEM μηνύματα, όμως, που είναι συντακτικά έγκυρα αλλά παρουσιάζουν αποτυχημένη επαλήθευση του MIC πρέπει να αντιμετωπίζονται με προσοχή. Οι χρήστες θα πρέπει να ειδοποιούνται ότι το δεν μπορεί να εγγυηθεί η αυθεντικότητα και η ακεραιότητα των περιεχομένων του εν λόγω μηνύματος.

2.1.3.3 Τύποι Μηνυμάτων

Ανάλογα με το είδος της παρεχόμενης προστασίας και τις εφαρμοζόμενες υπηρεσίες, τα PEM μηνύματα διακρίνονται σε τέσσερα είδη:

- **ENCRYPTED:** Αναπαριστά ένα PEM μήνυμα στο οποίο έχουν εφαρμοστεί οι υπηρεσίες της διαφύλαξης του απόρρητου της συναλλαγής, της εξασφάλισης της ακεραιότητας των δεδομένων, της πιστοποίησης ταυτότητας και της εξασφάλισης της μη αποκήρυξης της πηγής.
- **MIC-ONLY:** Αναπαριστά ένα PEM μήνυμα στο οποίο παρέχονται όλες οι προηγούμενες υπηρεσίες εκτός της διαφύλαξης του απόρρητου. Μόνο οι UAs

που ενσωματώνουν το PEM μπορούν να παρουσιάσουν το μήνυμα για ανάγνωση.

- **MIC-CLEAR:** Το μήνυμα είναι το ίδιο με προηγουμένως με την διαφορά ότι όλοι η UAs μπορούν να παρουσιάσουν το μήνυμα, αλλά μόνο οι συμβατοί με το PEM μπορούν να επαληθεύσουν την αυθεντικότητα και την ακεραιότητα του μηνύματος.
- **CERTIFICATE REVOCATION:** Μήνυμα που περιέχει μία ή περισσότερες λίστες ανάκλησης πιστοποιητικών (CRL).

2.1.4 Μηχανισμός Ενθυλάκωσης

Το τελικό αποτέλεσμα του τέταρτου βήματος της προηγούμενης διαδικασίας συνδυάζεται με πληροφορίες που σχετίζονται με την προστασία του εγγράφου και ενθυλακώνονται στο σώμα (text portion – body) ενός κανονικού μηνύματος και μεταδίδεται. Τα πεδία που αναφέρονται στην κρυπτογράφηση και στα MIC (πληροφορίες προστασίας) τοποθετούνται σε τμήμα επικεφαλίδων πριν τα προστατευμένα δεδομένα, ενώ όλο το PEM μήνυμα περικλείεται από κατάλληλες διαχωριστικές γραμμές.

```
Encapsulated Message

    Pre-Encapsulation Boundary (Pre-EB)
        -----BEGIN PRIVACY-ENHANCED MESSAGE-----

    Encapsulated Header Portion
        (Contains encryption control fields inserted in plaintext.
        Examples include "DEK-Info:" and "Key-Info:".)

    Blank Line
        (Separates Encapsulated Header from subsequent
        Encapsulated Text Portion)

    Encapsulated Text Portion
        (Contains protected message data)

    Post-Encapsulation Boundary (Post-EB)
        -----END PRIVACY-ENHANCED MESSAGE-----
```

Σχήμα 2.1: Μορφή Ενθυλακωμένου PEM μηνύματος

Η ενθυλάκωση παρέχει γενίκευση του τρόπου επεξεργασίας του παραληφθέντος μηνύματος και διαχωρίζει τα πεδία που είναι χρήσιμα για την αποκρυπτογράφηση και επαλήθευση του μηνύματος από αυτά που αλλάζουν κατά την μεταφορά.
Η τεχνική ενθυλάκωσης μπορεί να χρησιμοποιηθεί για την ενθυλάκωση πολλαπλών PEM μηνυμάτων ή ακόμα για την συνοδεία του PEM μηνύματος από απλό κείμενο. Οι διαχωριστικές γραμμές (encapsulation boundaries) χρησιμεύουν στον διαχωρισμό των PEM μηνυμάτων και για την διάκριση των μη κρυπτογραφημένων δεδομένων από τα PEM μηνύματα. Η αρχή ενός PEM μηνύματος υποδηλώνεται με την γραμμή

-----BEGIN PRIVACY-ENHANCED MESSAGE-----
ενώ το τέλος υποδηλώνεται είτε με την ίδια γραμμή είτε με την
-----END PRIVACY-ENHANCED MESSAGE-----

υποδηλώνοντας ότι ακολουθεί άλλο PEM μήνυμα.

2.1.5 Ταχυδρομικές Λίστες

Όταν ένα μήνυμα απευθύνεται σε ταχυδρομικές λίστες, δύο διαφορετικές μέθοδοι μπορούν να εφαρμοστούν όσον αναφορά τα κλειδιά ΙΚ:

- **ΙΚ ανά λίστα (ΙΚ-per-list)**
  Στην περίπτωση των ΙΚ ανά παραλήπτη, το κλειδί κρυπτογράφησης των δεδομένων του μηνύματος, DEK, κρυπτογραφείται με κάθε κλειδί ΙΚ για κάθε παραλήπτη και όλες αυτές οι κρυπτογραφημένες παρουσιάσεις των DEK μεταφέρονται με το μήνυμα. Αξίζει να επισημάνουμε ότι η ανά χρήστη κρυπτογράφηση δεν γίνεται στο προστατευμένο κείμενο παρά μόνο στα DEK και στα MIC. Το μειονέκτημα είναι η χρήση πολλών ΙΚ που περιπλέκουν την επεξεργασία του μηνύματος και την διαχείριση των κλειδιών. Παρ' όλα αυτά, όμως, η υποκλοπή ενός κλειδιού που δεν μοιράζεται μεταξύ πολλών χρηστών είναι πιο δύσκολη και η ανάκληση ενός ζεύγους ΙΚ δεν προκαλεί προβλήματα σε όλα τα μέλη της ταχυδρομική λίστας.

- **ΙΚ *ανά παραλήπτη* (ΙΚ-per-recipient)**
  Όταν ο αποστολέας επιλέξει να μην αναλύσει την ταχυδρομική λίστα στα μέλη της και χρησιμοποιήσει κοινό ΙΚ κλειδί για όλους του παραλήπτες της ταχυδρομική λίστας, τότε έχουμε την περίπτωση των ΙΚ ανά λίστα. Το ίδιο ΙΚ κλειδί πρέπει να είναι διαθέσιμο σε όλα τα μέλη της ταχυδρομικής λίστας, πράγμα που κάνει εύκολη την επεξεργασία του μηνύματος. Δυστυχώς, η μέθοδος αυτή συνεπάγεται σημαντικό βαθμό έκθεσης του ΙΚ και η ανάκλήση του δημιουργεί προβλήματα μεταξύ των μελών. Επιπλέον, επειδή, μιλάμε για συμμετρικά κλειδιά, οποιοσδήποτε κατέχει το ΙΚ μπορεί να προσποιηθεί ότι είναι ο αυθεντικός αποστολέας. Ακόμα και στη ασύμμετρη διαχείριση κλειδιών (με κοινή ιδιωτική κλείδα μεταξύ των μελών) μειονεκτεί καθ' ότι δεν είναι δυνατόν να εφαρμοστούν όλες οι υπηρεσίες ασφαλείας.

Καταλαβαίνουμε ότι είναι προτιμότερη μία υβριδική προσέγγιση, όπου στο μονοπάτι από τον αποστολέα προς τον Mail List Agent (MLA) εφαρμόζεται η ΙΚ ανά λίστα προστασία, ενώ στο μονοπάτι από τον MLA προς τους τελικούς αποδέκτες εφαρμόζεται ΙΚ ανά παραλήπτη προστασία.

2.1.6 Περίληψη Ενθυλακωμένων Επικεφαλίδων

Παρακάτω θα αναφερθούμε περιληπτικά στις σημαντικότερες επικεφαλίδες που ενθυλακώνονται στο PEM μήνυμα και περιέχουν απαραίτητες πληροφορίες για το είδος της παρεχόμενης προστασίας τους αλγόριθμους κρυπτογράφησης και παραγωγής MIC και επιπλέον στοιχεία για την πιστοποίηση της ταυτότητας της πηγής. Οι επικεφαλίδες παρουσιάζονται με την σειρά που δίνονται εδώ.

- **Proc-Type:** Απαιτείται σε όλα τα PEM μηνύματα, απαντάται μόνο μια φορά και είναι η πρώτη ενθυλακωμένη επικεφαλίδα. Υποδηλώνει τον τύπο του PEM μηνύματος και οι τιμές που μπορεί να πάρει είναι ENCRYPTED, MIC-ONLY, MIC-CLEAR και CRL.

- **Content-Domain:** Περιγράφει το είδος των περιεχομένων που μεταφέρονται ενθυλακωμένα και στα οποία εφαρμόζονται οι υπηρεσίες ασφαλείας του PEM. Η μόνη προκαθορισμένη τιμή είναι η "RFC822", ενώ αναμένονται και άλλες.
- **DEK-Info:** Περιγράφει τον αλγόριθμο κρυπτογράφησης των περιεχομένων και μεταφέρει κατάλληλους παραμέτρους για συγκεκριμένους αλγόριθμους (Initialization Vectors). Υπάρχει μόνο μια DEK-Info ανά μήνυμα και απαιτείται για όλα τα ENCRYPTED μηνύματα.
- **Originator-ID:** Προσδιορίζει την ταυτότητα του αποστολέα και καθορίζει το ΙΚ κλειδί που χρησιμοποιείται. Η επικεφαλίδα αυτή έχει δύο διαφορετικές μορφές, ανάλογα με την τεχνική διαχείρισης κλειδιών, την "Originator-ID-Asymmetric" και την "Originator-ID-Symmetric". Η επικεφαλίδα "Originator-ID-Asymmetric" απαιτείται για όλα τα PEM μηνύματα με ασύμμετρη διαχείριση κλειδιών και αντίστοιχα η "Originator-ID-Symmetric" για τα PEM μηνύματα με συμμετρική διαχείριση κλειδιών. Η "Originator-ID-Asymmetric" υπάρχει μόνο εν απουσία της "Originator-Certificate".Στις περισσότερες περιπτώσεις υπάρχει μόνο μία "Originator-ID" Η" Originator-Certificate". Για την συμμετρική περίπτωση, το ΙΚ που περιγράφεται συνδυάζεται με όλες τις "Recipient-ID-Symmetric" επικεφαλίδες που ακολουθούν μέχρι να βρεθεί άλλη "Originator-ID-Symmetric". Για την περίπτωση ασύμμετρων κλειδιών, η επεξεργασία των "Originator-ID-Asymmetric" και "Recipient-ID-Asymmetric" είναι ανεξάρτητη.Πολλαπλές επικεφαλίδες "Originator-ID" μπορούν να υπάρχουν μόνο όταν ένα μήνυμα προορίζεται για μετάδοση σε διαφορετικούς παραλήπτες.
- **Originator-Certificate:** Η επικεφαλίδα αυτή χρησιμοποιείται μόνο στην ασύμμετρη διαχείριση κλειδιών. Μεταφέρει το πιστοποιητικό του αποστολέα (που περιέχει την δημόσια κλείδα του) κωδικοποιημένο σύμφωνα με τον μηχανισμό Base64.
- **MIC-Info:** Χρησιμοποιείται μόνο με την ασύμμετρη διαχείριση κλειδιών και περιέχει στοιχεία που υποδηλώνουν τον αλγόριθμο που παρήγαγε το MIC, τον αλγόριθμο που κρυπτογράφησε το MIC και τέλος περιέχει την υπογραφή του μηνύματος (δηλαδή το κρυπτογραφημένο MIC) από την ιδιωτική κλείδα του αποστολέα. Για την περίπτωση ENCRYPTED PEM μηνυμάτων, το κρυπτογραφημένο MIC ξανά κρυπτογραφείται με το ίδιο DEK και το ίδιο αλγόριθμο που χρησιμοποιήθηκε στα προστατευόμενα περιεχόμενα.
- **Recipient-ID:** Η επικεφαλίδα αυτή προσδιορίζει την ταυτότητα του παραλήπτη ή και παραληπτών. Συγχρόνως, παρέχει το ΙΚ κλειδί. Παρουσιάζεται με δύο διαφορετικές μορφές, την Recipient-ID-Asymmetric και την Recipient-ID-Symmetric, ανάλογα με την τεχνική διαχείρισης των κλειδιών.
- **Key-Info:** Οι πληροφορίες που περιέχει εξαρτώνται από την διαχείριση των κλειδιών. Στην συμμετρική διαχείριση των κλειδιών περιλαμβάνεται ο αλγόριθμος που χρησιμοποιήθηκε για την κρυπτογράφηση των DEK και MIC από το ΙΚ καθώς και τα ίδια τα DEK και MIC κρυπτογραφημένα από το ΙΚ. Στην ασύμμετρη διαχείριση κλειδιών περιλαμβάνονται ο αλγόριθμος κρυπτογράφησης του DEK από την δημόσια κλείδα του αποστολέα και επίσης το κρυπτογραφημένο DEK από την δημόσια κλείδα.

Ακολουθούν μερικά παραδείγματα PEM μηνυμάτων.

```
-----BEGIN PRIVACY-ENHANCED MESSAGE-----
   Proc-Type: 4,ENCRYPTED
   Content-Domain: RFC822
   DEK-Info: DES-CBC,F8143EDE5960C597
   Originator-ID-Symmetric: linn@zendia.enet.dec.com,,
   Recipient-ID-Symmetric: linn@zendia.enet.dec.com,ptf-kmc,3
   Key-Info: DES-ECB,RSA-MD2,9FD3AAD2F2691B9A,
             B70665BB9BF7CBCDA60195DB94F727D3
   Recipient-ID-Symmetric: pem-dev@tis.com,ptf-kmc,4
   Key-Info: DES-ECB,RSA-MD2,161A3F75DC82EF26,
             E2EF532C65CBCFF79F83A2658132DB47

   LLrHB0eJzyhP+/fSStdW8okeEnv47jxe7SJ/iN72ohNcUk2jHEUSoH1nvNSIWL9M
   8tEjmF/zxB+bATMtPjCUWbz8Lr9w1oXIkjHU1BLpvXR0UrUzYbkNpk0agV2IzUpk
   J6UiRRGcDSvzrsoK+oNvqu6z7Xs5Xfz5rDqUcM1K1Z6720dcBWGGsDLpTpSCnpot
   dXd/H5LMDWnonNvPCwQUHt==
   -----END PRIVACY-ENHANCED MESSAGE-----
```

Σχήμα 2.2: Παράδειγμα Encapsulated Message (Symmetric Key Management)

```
-----BEGIN PRIVACY-ENHANCED MESSAGE-----
   Proc-Type: 4,ENCRYPTED
   Content-Domain: RFC822
   DEK-Info: DES-CBC,BFF968AA74691AC1
   Originator-Certificate:
    MIIB1TCCAScCAWUwDQYJKoZIhvcNAQECBQAwUTELMAkGA1UEBhMCVVMxIDAeBgNV
    BAoTF1JTQSBEYXRhIFN1Y3VyaXR5LCBJbmMuMQ8wDQYDVQQLEwZCZXRhIDExDzAN
    BgNVBAsTBk5PVEFSWTAeFw05MTA5MDQxODM4MTdaFw05MzA5MDMxODM4MTZaMEUx
    CzAJBgNVBAYTA1VTMSAwHgYDVQQKExdSUOEgRGFOYSBTZWN1cml0eSwgSW5jLjEU
    MBIGA1UEAxMLVGVzdCBVc2VyIDEwWTAKBgRVCAEBAgICAANLADBIAkEAwHZHl7i+
    yJcqDtjJCowzTdBJrdAiLAnSC+CnnjOJELyuQiBgkGrgIh3j8/xOfM+YrsyF1u3F
    LZPVtzlndhYFJQIDAQABMA0GCSqGSIb3DQEBAgUAA1kACKrOPqphJYw1j+YPtcIq
    iW1FPuN5jJ79Khfg7ASFxskYkEMjRNZV/HZDZQEhtVaU7Jxfzs2wfX5byMp2X3U/
    5XUXGx7qusDgHQGs7Jk9W8CW1fuSWUgN4w==
   Key-Info: RSA,
    I3rRIGXUGWAF8js5wCzRTkdhO34PTHdRZY9TuvmO3M+NM7fx6qc5udixps2LngD+
    wGrtiUm/ovtKdinz6ZQ/aQ==
   Issuer-Certificate:
    MIIB3DCCAUgCAQowDQYJKoZIhvcNAQECBQAwTzELMAkGA1UEBhMCVVMxIDAeBgNV
    BAoTF1JTQSBEYXRhIFN1Y3VyaXR5LCBJbmMuMQ8wDQYDVQQLEwZCZXRhIDExDTAL
    BgNVBAsTBFRMQOEwHhcNOTEwOTAxMDgwMDAwWhcNOTIwOTAxMDc1OTU5WjBRMQsw
    CQYDVQQGEwJVUzEgMB4GA1UEChMXU1NBIERhdGEgU2VjdXJpdHksIE1uYy4xDzAN
    BgNVBAsTBkJ1dGEgMTEPMA0GA1UECxMGTk9UQVJZMHAwCgYEVQgBAQICArwDYgAw
    XwJYCsnp61QCxYykN1ODwutF/jMJ3kL+3PjYyHOwk+/9rLg6X65B/LD4bJHtO5XW
    cqAz/7R7XhjYCmOPcqbdzoACZtIlETrKrcJiDYoP+DkZ8k1gCk7hQHpbIwIDAQAB
    MA0GCSqGSIb3DQEBAgUAA38AAICPv4f9Gx/tY4+p+4DB7MV+tKZnvBoy8zgoMGOx
    dD2jMZ/3HsyWKWgSFOeH/AJB3qr9zosG47pyMnTf3aSy2nBO7CMxpUWRBcXUpE+x
    EREZd9++32ofGBIXaialnOgVUn0OzSYgugiQ077nJLDUj0hQehCizEs5wUJ35a5h
   MIC-Info: RSA-MD5,RSA,
    UdFJR8u/TIGhfH65ieewe2lOW4tooa3vZCvVNGBZirf/7nrgzWDABz8w9NsXSexv
    AjRFbHoNPzBuxwmOAFeAOHJszL4yBvhG
   Recipient-ID-Asymmetric:
    MFExCzAJBgNVBAYTA1VTMSAwHgYDVQQKExdSUOEgRGFOYSBTZWN1cml0eSwgSW5j
    LjEPMA0GA1UECxMGQmV0YSAxMQ8wDQYDVQQLEwZOT1RBU1k=,
    66
   Key-Info: RSA,
    O6BS1ww9CTyHPtS3bMLD+L0hejdvX6Qv1HK2ds2sQPEaXhX8EhvVphHYTjwekdWv
    7xOZ3Jx2vTAhOYHMcqqCjA==

   qeW1j/YJ2Uf5ng9yznPbtDOmY1oSwIuV9FRYx+gzY+8iXd/NQrXHfi6/MhPfPF3d
   jIqCJAxv1d2xgqQimUzoS1a4r7kQO5c/lua4LqKeq3ciFzEv/MbZhA==
   -----END PRIVACY-ENHANCED MESSAGE-----
```

Σχήμα 2.2: Παράδειγμα Encapsulated ENCRYPTED Message (Asymmetric Key Management)

2.1.7 Υποστηριζόμενοι Αλγόριθμοι

2.1.7.1 Αλγόριθμοι Κρυπτογράφησης

Ο μοναδικός αλγόριθμος που χρησιμοποιείται για την κρυπτογράφηση των περιεχομένων είναι ο DES σε CBC (Cipher Bloch Chaining) mode. Η είσοδος στον αλγόριθμο πολύ πιθανών να απαιτεί κατάλληλο συμπλήρωμα, ώστε το μήκος να είναι πολλαπλάσιο των 8 bytes. Επίσης απαιτεί έναν 64-bit Initialization Vector, ο οποίος είναι διαφορετικός για κάθε ENCRYPTED PEM μήνυμα.
Ο DES CBC απαιτεί ένα κλειδί κρυπτογράφησης των 64 bits. Από τα 64 bits, τα 56 χρησιμοποιούνται απευθείας για από τον DES CBC, ενώ τα υπόλοιπα 8 bits είναι bits περιττής ισοτιμίας. Για κάθε ENCRYPTED PEM μήνυμα παράγεται νέο τυχαίο κλειδί.

2.1.7.2 Αλγόριθμοι Παραγωγής MICs

Υπάρχουν δύο αλγόριθμοι σε αυτήν την κατηγορία, ο MD2 και ο MD5. Και οι δύο αλγόριθμοι δέχονται σαν είσοδο μήνυμα οποιουδήποτε μήκους και παράγουν στην έξοδο μια ακολουθία 16 bytes. Όταν χρησιμοποιείται συμμετρική διαχείριση κλειδιών, το αποτέλεσμα των αλγορίθμων διασπάται στα δύο μισά των 8 bytes, τα οποία κρυπτογραφούνται ξεχωριστά και έπειτα συνενώνονται.

2.1.7.3 Αλγόριθμοι Συμμετρικής Διαχείρισης Κλειδιών

Οι αλγόριθμοι που χρησιμοποιούνται για την κρυπτογράφηση των DEKs και MICs είναι δύο παραλλαγές του DES: ο DES σε ECB (Electronic-Codebook) mode και ο DES σε EDE (Encrypt-Decrypt-Encrypt) mode. Και οι δύο απαιτούν IK κλειδιά μήκους 64 bits.

2.1.7.4 Αλγόριθμοι Ασύμμετρης Διαχείρισης Κλειδιών

Το ασύμμετρο ζευγάρι IK κλειδιών (δημόσια κλείδα – ιδιωτική κλείδα) είναι της μορφής που καθορίζεται από το RSA μηχανισμό. Ομοίως, για την κρυπτογράφηση των DEKs και MICs ο μηχανισμός RSA εφαρμόζεται, κατά τον οποίο η ιδιωτική κλείδα κρυπτογραφεί το MICs παράγοντας έτσι ψηφιακές υπογραφές των μηνυμάτων και η δημόσια κλείδα κρυπτογραφεί το DEK.
Χρησιμοποιείται, επίσης, και ο MD2 σε συνδυασμό με τον RSA για την υπογραφή των πιστοποιητικών και των λιστών ανάκλησης πιστοποιητικών (CRL).

2.2 PGP (Pretty Good Privacy)

Το PGP (Pretty Good Privacy) είναι ένα σύστημα κρυπτογράφησης δημόσιου κλειδιού, το οποίο αναπτύχθηκε το 1991 στις ΗΠΑ από τον τότε μηχανικό λογισμικού, Φιλ Τσίμερμαν. Μέχρι το 1999, η εξαγωγή κρυπτογραφικού υλικού σε ηλεκτρονική μορφή εκτός της χώρας απαγορευόταν, αφού οι τεχνολογίες του είδους είχαν χαρακτηριστεί «πυρομαχικά». Ωστόσο, χάρη στην εθελοντική πρωτοβουλία PGP International (εν συντομία PGPi, www.pgpi.org), το πρόγραμμα διαδόθηκε ευρέως σε ολόκληρο τον κόσμο, ήδη από το 1997. Κάθε φορά που κυκλοφορούσε στις ΗΠΑ μια νέα έκδοση του PGP, οι άνθρωποι που συμμετείχαν στην πρωτοβουλία αγόραζαν από την Αμερική βιβλία με τον πηγαίο κώδικα του προγράμματος και τα

έστελναν στην Ευρώπη. Στη συνέχεια, τα βιβλία σαρώνονταν σελίδα προς σελίδα, περνούσαν από πρόγραμμα OCR, και όταν ο πηγαίος κώδικας είχε μεταφερθεί ολόκληρος στον υπολογιστή, μεταγλωττίζονταν. Σήμερα στις ΗΠΑ έχουν χαλαρώσει οι περιορισμοί εξαγωγών κρυπτογραφικού υλικού, γεγονός που μεταξύ άλλων σημαίνει ότι το PGP μπορεί πλέον να εξάγεται και σε ηλεκτρονική μορφή. Ωστόσο, το πρότζεκτ PGPi συνεχίζει να έχει τον έλεγχο της διανομής των εκδόσεων του προγράμματος στον υπόλοιπο κόσμο, μαζί με τον πηγαίο κώδικα.
Το PGP διατίθεται δωρεάν για προσωπική χρήση, όμως απαιτείται άδεια για τη χρησιμοποίησή του σε εμπορικές εφαρμογές. Το Ινστιτούτο Τεχνολογίας της Μασσαχουσέτης (MIT) λειτουργεί ως κέντρο προώθησης του λογισμικού που προορίζεται για προσωπική χρήση σε συνεργασία με τον Τσίμερμαν ο οποίος ίδρυσε και μια ομώνυμη με το λογισμικό, εταιρία (Pretty Good Privacy, Inc.) για να προωθήσει την εμπορική έκδοση του λογισμικού.
Σκοπός του PGP ήταν η χρήση του σε συνδυασμό με το σύστημα ηλεκτρονικού ταχυδρομείου που προϋπήρχε και είναι συμβατό με σχεδόν κάθε πλατφόρμα. Η βασική ιδέα του PGP ήταν ότι είναι ανώφελο να επιχειρήσει κάποιος να εμποδίσει την εξέταση πληροφοριών που διακινούνται σε δίκτυα μέσω του ηλεκτρονικού ταχυδρομείου ή κάποιου άλλου μέσου επικοινωνίας. Έτσι, η μοναδική μορφή προστασίας είναι η εξασφάλιση ότι τα δεδομένα που παρακολουθούνται είναι ακατανόητα σε όλους τους άλλους εκτός από τους νόμιμους παραλήπτες τους. Αυτό επιτυγχάνεται με ισχυρή κρυπτογράφηση.(Για περισσότερη ανάλυση κοιτάξτε το 7° Κεφάλαιο).

2.3 S/MIME (SECURE – MIME)

2.3.1 Το MIME (Multipurpose Internet Mail Extensions)

Το ηλεκτρονικό ταχυδρομείο του Διαδικτύου επιτρέπει σε χρήστες από όλο τον κόσμο να ανταλλάσσουν μηνύματα. Τον Ιούνιο του 1992, ένα νέο πρωτόκολλο του Διαδικτύου καθιερώθηκε, το MIME, το οποίο είναι το ακρωνύμιο της αγγλικής φράσης *Multipurpose Internet Mail Extensions.* Το MIME και προσφέρει έναν τρόπο για την ανταλλαγή κειμένου σε γλώσσες εκτός της αγγλικής και μηνυμάτων πολυμέσων μεταξύ διαφορετικών υπολογιστικών συστημάτων. Συγκεκριμένα, ένα μήνυμα συμβατό του MIME μπορεί να περιέχει:

- Πολλαπλά αντικείμενα.
- Κείμενο με απεριόριστο μήκος και απεριόριστο μήκος γραμμών.
- Σύνολα χαρακτήρων πέρα από το US - ASCII, επιτρέποντας τη σύνταξη μηνυμάτων σε διάφορες γλώσσες.
- Εμπλουτισμένο κείμενο, χρήση δηλαδή διάφορων τυπογραφικών στοιχείων *(fonts)*
- Εικόνα, κινούμενη εικόνα, ήχο.
- Δυαδικά αρχεία ή αρχεία εφαρμογών (tar files, postscriptfiles).
- Δείκτες σε αρχεία αποθηκευμένα σε άλλους υπολογιστές.

Το MIME υποστηρίζει αρκετούς προκαθορισμένους τύπους περιεχομένων, όπως 8 bit μ-LAW *audio* με δειγματοληψία 8 kHz, αρχεία εικόνων OIP, προγράμματα postscript και επιπλέον επιτρέπει στους χρήστες να καθορίζουν τους δικούς τους τύπους δεδομένων. Λογισμικό που ενσωματώνει το MIME παράγει μηνύματα ηλεκτρονικού ταχυδρομείου με περιεχόμενα που μπορούν αναμφίβολα να αναγνωριστούν, ενώ,

όταν το ίδιο λογισμικό επεξεργάζεται ένα εισερχόμενο μήνυμα, είναι σε θέση να διαχειριστεί όλη την πληροφορία που δεν προορίζεται για το χρήστη και να τον προστατέψει από την μη ερμηνεύσιμη απόδοση της.
Ένα μήνυμα MIME αποτελείται από πολλά κομμάτια (body parts) και κάθε κομμάτι αντιπροσωπεύει ένα ξεχωριστό αντικείμενο (ηχητικό μήνυμα, κείμενο, αρχείο κτλ.). Κάθε τέτοιο κομμάτι με τη σειρά του αποτελείται από τον κορμό *(body)* και από τις επικεφαλίδες *(headers)*. Στον κορμό υπάρχουν τα δεδομένα που προορίζονται για το χρήστη, ενώ στις επικεφαλίδες περιλαμβάνονται πληροφορίες που χρησιμοποιεί το πρόγραμμα του χρήστη.
Όπως έχει αποδειχθεί, το λογισμικό που εφαρμόζει το MIME πρωτόκολλο μπορεί να προκαλέσει πολλά προβλήματα. Τα πιο σημαντικά από αυτά έχουν να κάνουμε τα *postscript* προγράμματα. Γνωστά παραδείγματα είναι η-χρήση τους για την αλλαγή των κωδικών σε εκτυπωτές postscript με αποτέλεσμα την άρνηση εξυπηρέτησης και την αυθαίρετη διαχείριση αρχείων.

Επικεφαλίδες		*Περιγραφή*
1.	MIME-Version	Αριθμός έκδοσης του MIME.
2.	Content-Type	Καθορίζει το είδος των δεδομένων.
3.	Content-Transfer-Encoding	Η κωδικοποίηση των δεδομένων.
4.	Content- ID	Επιπλέον περιγραφή και ταυτοποίηση των δεδομένων.
5.	Content-Description	

Σχήμα 2.4: Περιληπτικός πίνακας επικεφαλίδων του PEM

Πρέπει επίσης να τονιστεί ότι τα ηλεκτρονικά μηνύματα του Διαδικτύου και τα μηνύματα UUCP (unix to unix Copy Protocol) δεν είναι ασφαλή, αφού υπηρεσίες όπως η πιστοποίηση ταυτότητας και η ακεραιότητα δεδομένων δεν παρέχονται από τα πρωτόκολλα SMTP, RFC822 και MIME. Για να αντιμετωπιστούν τα προαναφερόμενα προβλήματα ασφαλείας αναπτύχθηκε ένα νέο πρωτόκολλο με επεκτάσεις ασφαλείας. Το νέο αυτό πρωτόκολλο ονομάζεται S/MIME (Secure-MIME) και αποτελεί εξειδίκευση του πρωτοκόλλου MIME.

2.3.2 Το S/MIME

Το S/MIME είναι ένα πρωτόκολλο που χρησιμοποιείται από προγράμματα ηλεκτρονικού ταχυδρομείου για την εφαρμογή κρυπτογραφικών υπηρεσιών σε αποστέλλονται μηνύματα και για την επεξεργασία προστατευμένων παραληφθέντων. Η δεύτερη έκδοση του S/MIME είναι επί του παρόντος ενσωματωμένη σε πολλά δημοφιλή προϊόντα, όπως τα *Lotus Domino, Netscape Communicator, Novell GroupWise* και *Microsoft Exchange*. Το S/MIME δίνει την δυνατότητα σε εταιρίες

που σχεδιάζουν λογισμικό να αναπτύσσουν προγράμματα τέτοια ώστε ένα μήνυμα που κρυπτογραφήθηκε με ένα συγκεκριμένο πρόγραμμα να μπορεί να αποκρυπτογραφηθεί από ένα άλλο.
Η ομάδα *Internet Engineering Task Force (IETF)* αναπτύσσει την 3η έκδοση του S/MIME που περιλαμβάνει την εξειδίκευση *Cryptographic Message Syntax (CMS)* που ορίζει μια τυποποιημένη σύνταξη για την επικοινωνία των κρυπτογραφικών πληροφοριών που είναι ανεξάρτητες από την μορφή των ενθυλακωμένων περιεχομένων ή από τον μηχανισμό μεταφοράς. Κάθε τύπος δεδομένων μπορεί να προστατευθεί από το CMS. Εκτός από τις εφαρμογές S/MIME, το CMS μπορεί να χρησιμοποιηθεί με τα πρωτόκολλα HTTP, X.400, FTP, SSL και SET. Η στρατηγική ανάπτυξης της τρίτης έκδοσης είναι τέτοια ώστε να διατηρείται η συμβατότητα με την προηγούμενη έκδοση (version 2). Αυτό επιτυγχάνεται με την πρόσθεση νέων, προαιρετικών στοιχείων στην νέα έκδοση, των οποίων η απουσία στις επικεφαλίδες επιτρέπει την συνεργασία των δύο εκδόσεων.
Επίσης, η έκδοση 3 του S/MIME απαιτεί την ύπαρξη ενός ελάχιστου συνόλου κρυπτογραφικών αλγορίθμων που διασφαλίζουν την συνεργασίας μεταξύ διαφορετικών εφαρμογών.
Η περιγραφή του S/MIME v3, που αναπτύχθηκε από την ομάδα IETF περιλαμβάνει τα εξής έγγραφα:

- *Cryptographic Message Syntax (CMS)*: Όπως προείπαμε, το CMS ορίζει ένα τυποποιημένο τρόπο σύνταξης για την ανταλλαγή κρυπτογραφικών πληροφοριών που σχετίζονται με τα προστατευμένα περιεχόμενα. Το CMS βασίζεται στο PKCS#7 Version 1.5 που χρησιμοποιείται στα τρέχοντα προϊόντα S/MIME. στο τελευταίο έχουν ενσωματωθεί προαιρετικά χαρακτηριστικά ασφάλειας όπως η ακεραιότητα δεδομένων (integrity), η πιστοποίηση ταυτότητας (authentication), η εξασφάλιση της μη αποκήρυξης της προέλευσης (non-repudiation of origin) και της διασφάλισης του απόρρητου (privacy).

- *S/MIME Version 3 Message Specification*: Ορίζει την MIME κωδικοποίηση που χρησιμοποιείται για την μεταφορά περιεχομένων προστατευμένων από το CMS. Συγκεκριμένα, καθορίζει τις διάφορες επιλογές για την ενθυλάκωση αυτών των περιεχομένων στα MIME μηνύματα και προστίθενται οι νέοι τύποι περιεχομένων multipart/signed και application/pkcs7-siganture. Όλα τα προγράμματα με εφαρμοσμένο το S/MIME πρέπει να συμμορφώνονται με αυτό το έγγραφο.
- *S/MIME Version 3 Certificate Handling System*: Υποχρεώνει την υποστήριξη των πιστοποιητικών X.509, που μαζί με τις Λίστες Ανάκλησης Πιστοποιητικών (Certificate Revocation Lists) χρησιμοποιούνται για την πιστοποίηση ταυτότητας και την διαχείριση κλείδων.
- *Enhanced Security Services*: Το έγγραφο αυτό περιγράφει προαιρετικές υπηρεσίες ασφάλειας που μπορούν να παρέχονται σε συνδυασμό με την CMS προστασία.

Οι προβλεπόμενες προαιρετικές υπηρεσίας είναι:

- **Υπογεγραμμένες αποδείξεις *(Signed Receipts)*:**

Η επιστροφή μιας υπογεγραμμένης απόδειξης παραλαβής παρέχει στον αποστολέα εξασφάλιση της παραλαβής του μηνύματος και του επιτρέπει να

αποδείξει σε τρίτο ότι ο παραλήπτης ήταν σε θέση να επαληθεύσει την υπογραφή του αρχικού μηνύματος. Η αίτηση επιστροφής απόδειξης επιτυγχάνεται με την τοποθέτηση της ιδιότητας receipt Request στο πεδίο SignerInfo. Φυσικά, η ιδιότητα receiptRequest μπορεί να ζητηθεί μόνον εφόσον το μήνυμα είναι ψηφιακά υπογεγραμμένο.

- **Ετικέτες Ασφαλείας *(Security Labels)*:**

Ετικέτα ασφαλείας είναι ένα σύνολο πληροφοριών ασφαλείας που αφορούν στο βαθμό ασφαλείας των περιεχομένων. Μπορούν να περιγράφουν επίπεδα ασφάλειας ("μυστικό", "απόρρητο", "περιορισμένη πρόσβαση" κτλ.) ή να περιγράφουν ομάδες ανθρώπων που μπορούν να έχουν πρόσβαση στην πληροφορία (π.χ. "γιατροί", "ασφαλιστικές εταιρίες", "ασθενείς", "όλοι").

- **Ταχυδρομικές Λίστες *(Mail Lists)*:**

Τα προγράμματα ηλεκτρονικού ταχυδρομείου πρέπει να δημιουργούν κρυπτογραφημένα μηνύματα με διαφορετική δομή για κάθε παραλήπτη και συνεπώς ο φόρτος εργασίας αυξάνεται σημαντικά για μεγάλο αριθμό παραληπτών που ανήκουν στην ίδια ταχυδρομική λίστα. Για το λόγο αυτό, συστήματα που καλούνται Mail List Agents (MLAs) αναλαμβάνουν την ανά χρήστη διαχείριση του μηνύματος. Με τον τρόπο αυτό διευκολύνεται η αποστολή μηνυμάτων σε μεγάλες ταχυδρομικές λίστες. Ένας MLA παρουσιάζεται στον αποστολέα ως ένας τυπικός αποδέκτης, ενώ στην πραγματικότητα λειτουργεί ως ένα σημείο περαιτέρω επεξεργασίας του μηνύματος που διανέμει το μήνυμα σε όλα τα μέλη της ταχυδρομικής λίστας. Επίσης, ένας MLA πρέπει να αντιμετωπίζει τους λεγόμενους «βρόχους ηλεκτρονικού ταχυδρομείου» (mailloops). Βρόχος Ηλεκτρονικού Ταχυδρομείου είναι μια κατάσταση που εμφανίζεται όταν μια ταχυδρομική λίστα είναι μέλος μιας δεύτερης που και αυτή με τη σειρά της είναι μέλος της πρώτης.

- **Υπογεγραμμένα Πιστοποιητικά *(Signing Certificates)*:**

Σημαντικά προβλήματα έχουν παρουσιαστεί λόγω του γεγονότος ότι τα πιστοποιητικά του υπογράφοντος δεν ασφαλίζονται μαζί με τις υπογεγραμμένες ιδιότητες ενός μηνύματος. Η εκμετάλλευση αυτού του ελαττώματος έχει οδηγήσει στην ανάπτύξη τεχνικών «επίθεσης» που έχουν ως στόχο την αντικατάσταση του πιστοποιητικού. Η ιδιότητα υπογεγραμμένου πιστοποιητικού έχει σκοπό να αποτρέψει τις επιθέσεις αυτές. Η ιδιότητα αυτή προστίθεται στις υπογεγραμμένες ιδιότητες και περιλαμβάνει στοιχεία που ταυτοποιούν το σωστό πιστοποιητικό. Συγκεκριμένα, η συνάρτηση κατακερματισμού (hash) του πιστοποιητικού περιλαμβάνεται στις υπογεγραμμένες ιδιότητες παρέχοντας επιπλέον ασφάλεια. Εάν η συνάρτηση κατακερματισμού στις υπογεγραμμένες ιδιότητες δεν ταιριάζει με τη συνάρτηση κατακερματισμού του λαμβανόμενου πιστοποιητικού, τότε η υπογραφή θεωρείται άκυρη.

2.4 SSL (SECURE SOCKET LAYER)

Το SSL είναι ένα γενικού σκοπού πρωτόκολλο για την αποστολή κρυπτογραφημένης πληροφορίας μέσω internet.Είναι ένα «στρώμα» που τοποθετείται ανάμεσα στο

internet και στον web browser (π.χ. Netscape). Κρυπτογραφεί τις πληροφορίες που φεύγουν από τον client και ταξιδεύουν μέσω του internet στον server. Εκεί αποκρυπτογραφούνται και πάλι όλα τα δεδομένα. Το στρώμα αυτό θα πρέπει να υποστηρίζεται από την εκάστοτε εφαρμογή (π.χ. Netscape, Internet Explorer) για να ενεργοποιηθεί και να αξιοποιηθεί. Έχει σχεδιαστεί να παρέχει απόρρητη επικοινωνία μεταξύ δύο συστημάτων, εκ των οποίων το ένα λειτουργεί σαν client και το άλλο σαν server, προσφέροντας αξιόπιστη από άκρο σε άκρο (end to end) ασφαλή υπηρεσία. Για παράδειγμα κάνοντας κανείς χρήση του SSL μπορεί να εισάγει τον αριθμό της πιστωτικής του κάρτας σε μία ασφαλή φόρμα μέσω του web browser και να την μεταδώσει μέσω του internet σε έναν ασφαλή server χωρίς τον κίνδυνο μιας ενδιάμεσης αποκάλυψης της μεταφερόμενης πληροφορίας.
Το Transmission Control Protocol / Internet Protocol (TCP/IP)είναι υπεύθυνο για τον τρόπο μεταφοράς των δεδομένων στο internet. Άλλα πρωτόκολλα όπως το HTTP, IMAP, LDAP τρέχουν πάνω από το TCP/IP και φροντίζουν για τυπικές διαδικασίες, όπως η σωστή απεικόνιση web pages ή εφαρμογές e-mail. Ακριβώς με τον ίδιο τρόπο τρέχει και το πρωτόκολλο SSL.για την ακρίβεια τρέχει πάνω από το TCP/IP πρωτόκολλο και κάτω από άλλα πρωτόκολλα όπως HTTP, IMAP, TELNET. Χρησιμοποιεί το TCP/IP εκ μέρους άλλων πρωτοκόλλων και επιτρέπει σε έναν SSL server να κάνει σωστό authentication σε έναν client και φυσικά το αντίστροφο.
Το SSL είναι ένα επεκτάσιμο και εύκολα προσαρμόσιμο πρωτόκολλο. Αν τα δύο μέρη της επικοινωνίας δεν χρησιμοποιούν τους ίδιους αλγορίθμους, τα κρυπτογραφικά πρωτόκολλα δεν δουλεύουν. Γι αυτό όταν ένα πρόγραμμα που χρησιμοποιεί SSL προσπαθεί να επικοινωνήσει με ένα άλλο, τότε τα δύο προγράμματα συγκρίνουν ηλεκτρονικά τα στοιχεία και καθορίζουν ποιος είναι ο δυνατότερος κρυπτογραφικός αλγόριθμος που διαθέτουν από κοινού.(Για περισσότερη ανάλυση κοιτάξτε το 3° κεφάλαιο).

2.5 S-HTTP (Secure Hyper-Text Transfer Protocol)

2.5.1 Εισαγωγή

Το WWW είναι ένα διανεμημένο σύστημα πολυμέσων το οποίο χαίρει μεγάλης αποδοχής από πολλούς χρήστες. Το βασικό και περισσότερο χρησιμοποιούμενο πρωτόκολλο μεταξύ WWW clients και WWW servers είναι το Hyper Text Transfer Protocol. Η ευκολία της χρήσης του WWW έχει προκαλέσει το παγκόσμιο ενδιαφέρον και χρησιμοποιείται σαν η υποδομή client / server για πολλές δικτυακές εφαρμογές. Τέτοιες εφαρμογές απαιτούν την αμοιβαία πιστοποίηση της ταυτότητας των δύο επικοινωνούντων υπολογιστών και την ικανότητα ανταλλαγής ευαίσθητων πληροφοριών. Οι τρέχοντες, όμως, HTTP εφαρμογές έχουν μέτρια έως και μηδαμινή υποστήριξη για τους κρυπτογραφικούς μηχανισμούς που είναι απαραίτητοι για τέτοιες συναλλαγές.
Το πρωτόκολλο Secure HTTP παρέχει ασφαλής μηχανισμούς επικοινωνίας μεταξύ ένα ζευγάρι HTTP server – client με σκοπό να επιτρέψει αυθόρμητες εμπορικές συναλλαγές. Στόχος της σχεδίασης ήταν ένα ευέλικτο πρωτόκολλο που διαθέτει πολλαπλούς μηχανισμούς και αλγόριθμους, και την δυνατότητα διαπραγμάτευσης αυτών. Σχεδιάστηκε από τους E. Rescorla και A. Schiffman του EIT και αποτελεί υπερσύνολο του HTTP.

2.5.2 Χαρακτηριστικά του S/HTTP

1. Το S/HTTP υποστηρίζει μία ποικιλία μηχανισμών ασφαλείας στους HTTP clients και servers. Το πρωτόκολλο παρέχει συμμετρικές δυνατότητες στον client και server που σημαίνει ότι τα μηνύματα και οι προτιμήσεις και των δύο πλευρών μεταχειρίζονται με τον ίδιο τρόπο, ενώ παράλληλα διατηρούνται το μοντέλο συναλλαγής και τα χαρακτηριστικά επικοινωνίας του HTTP.
2. Αρκετά κρυπτογραφικά στάνταρντς ενσωματώνονται στους S/HTTP clients και servers συμπεριλαμβανομένων των PEM, PGP, Kerberos και PKCS-7 (ο πρόγονος του CMS). Είναι συμβατό με το HTTP.
3. Το S/HTTP δεν απαιτεί πιστοποιητικά δημοσίων κλείδων από την μεριά του client, καθ' ότι υποστηρίζει και τα συμμετρικά κλειδιά. Αυτό είναι σημαντικό γιατί αυθόρμητες ιδιωτικές συναλλαγές μπορούν να λάβουν χώρα, χωρίς την απαίτηση από τους χρήστες να έχουν ένα έγκυρο ζεύγος δημόσιας – ιδιωτικής κλείδας. Βέβαια, είναι σε θέση να εκμεταλλευτεί την υπάρχουσα υποδομή πιστοποιητικών και ασύμμετρων κλειδιών.
4. Το S/HTTP υποστηρίζει απ' άκρη σ' άκρη ασφαλής συναλλαγές, σε αντίθεση με το HTTP που προϋποθέτει μία αποτυχημένη προσπάθεια πρόσβασης του χρήστη πριν την εφαρμογή οποιωνδήποτε μηχανισμών ασφαλείας. Με το S/HTTP, σε καμία περίπτωση ευαίσθητα δεδομένα θα μεταδοθούν στο δίκτυο απροστάτευτα.
5. Επιτρέπει πλήρη ευελιξία όσον αναφορά τους κρυπτογραφικούς αλγόριθμούς και τις παραμέτρους αυτών. Το είδος της παρεχόμενης προστασίας (κρυπτογράφηση, ψηφιακή υπογραφή, και τα δύο), οι αλγόριθμοι και τα πιστοποιητικά μπορούν να διαπραγματευτούν.
6. Οι χρήστες αναμένονται να έχουν (αν και δεν συνιστάται) πολλαπλά πιστοποιητικά.

2.5.3 Είδη Προστασίας

Η προστασία ενός μηνύματος εφαρμόζεται με τρεις διαφορετικούς τρόπους: με υπογραφή, με κρυπτογράφηση και με παραγωγή MACs. Κάθε μήνυμα μπορεί να υπογραφεί, να κρυπτογραφηθεί ή οποιοσδήποτε συνδυασμός αυτών, συμπεριλαμβανομένων της παραγωγής και της παροχής καμίας προστασίας.
Υποστηρίζονται αρκετές τεχνικές διαχείρισης κλειδιών όπως συμμετρικά μυστικά κλειδιά, ασύμμετρη διαχείριση και το σύστημα Key Distribution Center (KDC) του Kerberos. Επιπλέον, ένας μηχανισμός challenge-response παρέχει στους επικοινωνούντες υπολογιστές την δυνατότητα να αναγνωρίζουν τις επιθέσεις επανάληψης (replay attacks).

2.5.3.1 Υπογραφές

Όταν υπογράφεται ψηφιακά, ένα κατάλληλο πιστοποιητικό μεταφέρεται με το μήνυμα ή ο αποστολέας μπορεί να αφήσει τον παραλήπτη να αποκτήσει το απαιτούμενο πιστοποιητικό από μόνος του.

2.5.3.2 Κρυπτογράφηση

Εκτός από την βασική κρυπτογράφηση, το S/HTTP καθορίζει δύο μηχανισμούς ανταλλαγής κλειδιών: (α) χρήση ασύμμετρης διαχείρισης κλειδιών και (β) χρήση ενός προκαθορισμένου κλειδιού.
Στην πρώτη περίπτωση, οι παράμετροι και το κλειδί του συμμετρικού κρυπτοσυστήματος κρυπτογραφούνται με την δημόσια κλείδα του παραλήπτη.
Στην δεύτερη περίπτωση, τα ίδια στοιχεία κρυπτογραφούνται με κλειδί που έχει προαποφασιστεί νωρίτερα. Τα κλειδιά αυτά μπορούν να προέλθουν και από τα tickets του Kerberos.

2.5.3.3 Παραγωγή Message Authentication Codes (MACs)

Το S/HTTP παρέχει επιπλέον μέσα για την επαλήθευση της ακεραιότητας των δεδομένων και την πιστοποίηση της ταυτότητας του αποστολέα. Χρησιμοποιεί το MAC του μηνύματος, το οποίο υπολογίζεται από hash αλγόριθμο σε συνδυασμό με ένα κοινό μυστικό κλειδί (π.χ. MD5). Αυτή η τεχνική δεν απαιτεί την χρήση ασύμμετρης διαχείρισης ούτε την χρήση κρυπτογράφησης.

2.5.4 Μοντέλο Επεξεργασίας

2.5.4.1 Προετοιμασία Μηνύματος

Η δημιουργία ενός S/HTTP μηνύματος μπορεί να θεωρηθεί σαν μια συνάρτηση με τρεις εισόδους:

- Το μήνυμα που πρόκειται να προστατευτεί. Μπορεί να είναι ένα HTTP μήνυμα ή κάποιο άλλο αντικείμενο. Το HTTP μήνυμα μπορεί να είναι οποιασδήποτε έκδοσης του HTTP πρωτοκόλλου.
- Οι κρυπτογραφικές προτιμήσεις του παραλήπτη. Αυτές είτε έχουν καθοριστεί σε προηγούμενη επικοινωνία, είτε βασίζονται σε προρυθμίσεις.
- Οι κρυπτογραφικές προτιμήσεις του αποστολέα.

Ο αποστολέας συνδυάζει τις προτιμήσεις και των δύο πλευρών και αποφαίνεται για τους αλγόριθμους και μηχανισμούς που θα χρησιμοποιηθούν καθώς και για την μορφή των κλειδιών. Ίσως χρειαστεί η επέμβαση του χρήστη σε περίπτωση πολλών επιλογών. Στο προστατευμένο HTTP μήνυμα, έπειτα, προστίθονται κατάλληλες S/HTTP επικεφαλίδες και παράγεται το τελικό S/HTTP μήνυμα.

Παραλαβή του Μηνύματος

Η επεξεργασία του παραληφθέντος S/HTTP μηνύματος, με την σειρά της, μπορεί να θεωρηθεί σαν συνάρτηση με τέσσερις διακριτές εισόδους:

- Το S/HTTP μήνυμα.
- Οι πρωτύτερα δηλωμένες κρυπτογραφικές προτιμήσεις του παραλήπτη.
- Οι τρέχοντες κρυπτογραφικές προτιμήσεις του παραλήπτη.
- Οι πρωτύτερα δηλωμένες κρυπτογραφικές προτιμήσεις του αποστολέα. Ο αποστολέας μπορεί να έχει δηλώσει το είδος των κρυπτογραφικών διαδικασιών που θα εφήρμοζε στο μήνυμα.

Για να μπορέσει να επεξεργαστεί το S/HTTP μήνυμα, ο παραλήπτης διαβάζει τις S/HTTP επικεφαλίδες για να ανακαλύψει τι κρυπτογραφικοί μετασχηματισμοί

εφαρμόστηκαν στο μήνυμα και με την βοήθεια των προσυμφωνημένων κλειδιών τις αφαιρεί. Το αποτέλεσμα είναι το HTTP μήνυμα (ή κάποιο άλλο αντικείμενο).
Ο παραλήπτης μπορεί να επιλέξει να επαληθεύσει ότι οι εφαρμοσμένοι μηχανισμοί ταιριάζουν με αυτούς που είχε δηλώσει ο αποστολέας (είσοδος 4), με αυτούς που είχε ζητήσει ο παραλήπτης (είσοδος 2) καθώς και με τις τρέχοντες προτιμήσεις του τελευταίου (είσοδος 3), με σκοπό να αποφανθεί εάν το μήνυμα είχε μετασχηματιστεί κατάλληλα.

2.5.4.2 Οι Επικεφαλίδες του S/HTTP

Το πρωτόκολλο καθορίζει μία σειρά από νέες επικεφαλίδες που πηγαίνουν στο πεδίο των επικεφαλίδων του S/HTTP μηνύματος. Από αυτές, όλες εκτός των "Content-Type" και "Content-Privacy-Domain" είναι προαιρετικές. Τα κυρίως περιεχόμενα του μηνύματος διαχωρίζονται από τις επικεφαλίδες με δύο συνεχόμενες ακολουθίες των χαρακτήρων ελέγχου <CR><LF>.

Content-Privacy-Domain
Αυτή η επικεφαλίδα υπάρχει για να παρέχει συμβατότητα με τα S/HTTP εφαρμογές που βασίζονται στο PEM. Οι τιμές της είναι "PEM", "PKCS-7" και "PGP".
Όταν χρησιμοποιείται η επικεφαλίδα "Content-Privacy-Domain: PKCS-7", η προστασία του μηνύματος γίνεται με τους εξής τρόπους, βάσει του PKCS-7: με υπογραφή και με κρυπτογράφηση. Κάθε HTTP μήνυμα μπορεί να κρυπτογραφηθεί, να υπογραφεί ή και τα δύο. Το μήνυμα που υπογράφεται συνήθως συνοδεύεται από πιστοποιητικό ή από αλυσίδα πιστοποιητικών. Οι επικεφαλίδες "Content-Privacy-Domain: PGP" και "Content-Privacy-Domain: PEM" υποδηλώνουν εφαρμογή των κανόνων του PGP ή του PEM, αντίστοιχα.

Content-Transfer-Encoding
Εδώ καθορίζεται η κωδικοποίηση των περιεχομένων και οι τιμές που μπορεί να πάρει η επικεφαλίδα είναι "8-bit", "7-bit" και "BASE64". Η τιμή εξαρτάται από την επικεφαλίδας "Content-Privacy-Domain ".
Για την περίπτωση που είναι "Content-Privacy-Domain: PKCS-7", οι μόνες επιτρεπτές τιμές της "Content-Transfer-Encoding" είναι "BASE64" ή "8-bit".
Για την περίπτωση που είναι "Content-Privacy-Domain: PEM", η μόνη επιτρεπτή τιμή είναι η "7-bit".
Για την περίπτωση που είναι "Content-Privacy-Domain: PGP" , όλες οι παραπάνω τιμές επιτρέπονται ανάλογα με την μορφή του PGP μηνύματος.

Content-Type
Υπό κανονικές συνθήκες, τα ενθυλακωμένα περιεχόμενα μετά την αφαίρεση όλων κρυπτογραφικών μέτρων ασφαλείας, θα είναι ένα HTTP μήνυμα. Σε αυτήν την περίπτωση η επικεφαλίδα θα είναι:
Content-Type: application/http
Δεν αποκλείεται, όμως, τα ενθυλακωμένα περιεχόμενα να είναι κάποιου άλλου τύπου με την προϋπόθεση ότι αυτός ο τύπος δηλωθεί σωστά με την χρήση κατάλληλης επικεφαλίδας "Content-Type".

Prearranged-Key-Info
Η επικεφαλίδα αυτή έχει σαν σκοπό να συνοδεύσει πληροφορίες σχετικά με κλειδί που έχει προκανονιστεί με κάποιον τρόπο έκτος της εσωτερικής κρυπτογράφησης.

Μία χρήση της επικεφαλίδας είναι η in-band επικοινωνία ενός session key στην περίπτωση που κάποια από τις δύο πλευρές δεν κατέχει ένα.
Ορίζονται τρεις μέθοδοι για την ανταλλαγή session keys: (α) Inband, (β) Kerberos και (γ) Outband. Οι δύο πρώτες μέθοδοι, Inband και Kerberos, υποδηλώνουν ότι το κλειδί έχει ανταλλαγεί πρωτύτερα, με χρήση μιας HTTP επικεφαλίδας "Key-Assign". Η Outband μέθοδος υπονοεί ότι ο client και ο server έχουν πρόσβαση σε κλειδιά που σχετίζονται με ονόματα χρηστών, είτε μέσω μιας βάσης δεδομένων, είτε από την εισαγωγή ενός κωδικού από τον χρήστη μέσω του πληκτρολόγιου.

MAC-Info
Μεταφέρει ένα Message Authentication Code (MAC), παρέχοντας πιστοποίηση ταυτότητας και ακεραιότητας. Το MAC υπολογίζεται από τα ενθυλακωμένα περιεχόμενα, την ώρα (προαιρετικό – αποτρέπει τις επιθέσεις replay attacks) και κάποιού κοινού μυστικού που μοιράζονται ο client και ο server. Έστω ότι χρησιμοποιείται hash αλγόριθμος Η, τότε η εξίσωση που περιγράφει την διαδικασία είναι (οι δύο κάθετες παύλες || σημαίνουν συνένωση):
MAC = hex(H(Message||<time>||<shared key>))

2.5.4.3 Διαπραγματεύσεις

Και δύο πλευρές πρέπει να είναι σε θέση να εκφράσουν τις προτιμήσεις και τις απαιτήσεις τους σχετικά με ποίες κρυπτογραφικές ενισχύσεις επιτρέπουν ή απαιτούν. Το σύνολο των πληροφοριών που διαπραγματεύονται, χωρίζεται σε τέσσερα μέρη:

Property: Το είδος της προστασίας (κρυπτογράφηση, υπογραφές, κτλ.).
Value: Ο αλγόριθμος που προσφέρει την παραπάνω προστασία.
Direction: Η κατεύθυνση για την οποία αναφέρονται οι συγκεκριμένες προτιμήσεις (*reception, origination*).
Strength: Πόσο ισχυρή είναι η επιλογή (*required, optional, refused*).

Η τιμή optional του τελευταίου πεδίου φανερώνει ότι οι αλγόριθμοι και το είδος της προστασίας που αναφέρονται στο Value και στο Property είναι προαιρετικές. Κατά την παραλαβή (reception) μηνύματος ασφαλισμένου με προαιρετικούς μηχανισμούς, ο παραλήπτης θα επιλέξει να το επεξεργαστεί αλλά δεν περιορίζεται στην επεξεργασία μόνο τέτοιων μηνυμάτων. Ο αποστολέας (origination) ο οποίος ορίζει κάποιες προτιμήσεις προαιρετικές, μπορεί να τις χρησιμοποιήσει όταν βρίσκονται σε συμφωνία με τις προτιμήσεις του παραλήπτη και δεν μπορεί όταν δεν είναι αποδεκτές.
Η τιμή required υποδηλώνει ότι ο παραλήπτης (reception) θα δέχεται S/HTTP μηνύματα μόνο με αυτές τις κρυπτογραφικές ενισχύσεις, ενώ ο αποστολέας (origination) θα χρησιμοποιεί μόνο αυτές ανεξάρτητα με τις προτιμήσεις του παραλήπτη.
Τέλος, η τιμή refused υποδηλώνει ότι ο παραλήπτης (reception) δεν θα δέχεται S/HTTP μηνύματα με τέτοιες κρυπτογραφικές ενισχύσεις, ενώ ο αποστολέας (origination) δεν θα παράγει ποτέ τέτοια μηνύματα.

Επικεφαλίδες Διαπραγμάτευσης

Η τιμή του πεδίου Property συμπληρώνεται με κατάλληλες επικεφαλίδες που προσδιορίζουν ποια κρυπτογραφική ιδιότητα βρίσκεται υπό συζήτηση.

1. **SHTTP-Privacy-Domains:** Καθορίζει την διαδικασία που θα ασφαλίσει το HTTP μήνυμα (ή οποιουδήποτε άλλου τύπου δεδομένα). Οι δεκτές τιμές είναι "PEM", "PGP" και "PKCS-7". Οι υπόλοιπες επικεφαλίδες μπορούν είτε να αναφέρονται σε ένα από τα PEM", "PGP", "PKCS-7" οπότε ακολουθούν την SHTTP-Privacy-Domains, είτε να αναφέρονται και στις τρεις τιμές οπότε βρίσκονται πριν από την SHTTP-Privacy-Domains. Επιτρέπονται πολλαπλές τέτοιες επικεφαλίδες με σκοπό την υποστήριξη πολλαπλών συνδυασμό παραμέτρων.
2. **SHTTP-Certificate-Types:** Υποδηλώνει τον τύπο των πιστοποιητικών που θα γίνονται ή δεν θα γίνονται δεκτά (ανάλογα με το πεδίο *Strength*).
3. **SHTTP-Key-Exchange-Algorithms:** Υποδηλώνει τους αλγόριθμους που μπορεί να χρησιμοποιηθούν για την διαχείριση και ανταλλαγή κλειδιών.
4. **SHTTP-Signature-Algorithms:** Υποδηλώνει τους αλγόριθμους ψηφιακών υπογραφών που μπορεί να χρησιμοποιηθούν.
5. **SHTTP-Message-Digest-Algorithms:** Υποδηλώνει τους αλγόριθμους παραγωγής message digest.
6. **SHTTP-Symmetric-Contents-Algorithms:** Εδώ καθορίζονται οι αλγόριθμοι συμμετρικής κρυπτογράφησης του HTTP μηνύματος (ή οποιουδήποτε άλλου τύπου δεδομένα).
7. **SHTTP-Symmetric-Header-Algorithms:** Οι επικεφαλίδες ενός HTTP μηνύματος ασφαλίζονται ξεχωριστά από το υπόλοιπο μήνυμα. Οι αλγόριθμοι συμμετρικής κρυπτογράφησης που μπορεί να χρησιμοποιηθούν καθορίζονται με αυτήν την επικεφαλίδα.
8. **SHTTP-Privacy-Enhancement:** Υποδηλώνει εάν θα εφαρμοστεί κρυπτογράφηση ("encrypt"), ψηφιακή υπογραφή ("sign") ή MAC ("auth").

2.5.4.4 Νέες Επικεφαλίδες HTTP

Το πρωτόκολλο S/HTTP καθορίζει μία συλλογή νέων επικεφαλίδων που τοποθετούνται στις επικεφαλίδες του HTTP μηνύματος. Με τον τρόπο αυτό οι νέες επικεφαλίδες μοιράζονται την κρυπτογραφική προστασία που παρέχεται στις υπάρχουσες. Οι νέες επικεφαλίδες παρουσιάζονται παρακάτω.

1. Security-Scheme: Είναι απαραίτητη επικεφαλίδα που καθορίζει την έκδοση του S/HTTP πρωτοκόλλου. Η τρέχουσα έκδοση είναι η 1.4.
2. Encryption-Identity: Προσδιορίζει την ταυτότητα μιας οντότητας για την οποία το μήνυμα θα μπορούσε να κρυπτογραφηθεί.
3. Certificate-Info: Περιέχει πληροφορίες για τα πιστοποιητικά της οντότητας που προσδιορίζεται στην "Encryption-Identity".
4. Key-Assign: Αυτή η επικεφαλίδα υποδηλώνει ότι το σύστημα επιθυμεί να συνδέσει ένα κλειδί με ένα συμβολικό όνομα, για μελλοντική του χρήση. Στην επικεφαλίδα περιέχεται το συμβολικό όνομα, το κλειδί, η μέθοδος σύμφωνα με την οποία θα αποκτηθεί το κλειδί (Inband και Kerberos), η διάρκεια ζωής του και τέλος τους αλγόριθμους με τους οποίους προορίζεται για χρήση το κλειδί. Στην περίπτωση Inband ανταλλαγής, το κλειδί μεταφέρεται σαν

παράμετρος της επικεφαλίδας, ενώ στην περίπτωση Kerberos ανταλλαγής, το κλειδί μεταφέρεται στο εσωτερικό ενός ticket.

5. Nonce: Περιέχει τιμή που χρησιμοποιείται για το ταίριασμα αίτησης και απάντησης. Σκοπός της είναι η διατήρηση της επικαιρότητας της σύνδεσης (freshness) και η αποφυγή replay attacks.

2.5.4.5 Υποστηριζόμενοι Αλγόριθμοι

Οι αλγόριθμοι που υποστηρίζει το S/HTTP χωρίζονται σε κατηγορίες, ανάλογα με είδος της παρεχόμενης προστασίας με την οποία χρησιμοποιούνται.

Αλγόριθμοι Διαχείριση Κλειδιών

Οι μηχανισμοί που καθορίζονται για την διαχείριση και ανταλλαγή κλειδιών (key management, key exchange) είναι οι RSA, Inband, Outband και Kerberos. Οι δύο ς μέθοδοι Inband και Kerberos, υποδηλώνουν ότι το κλειδί έχει ανταλλαγεί πρωτύτερα, με χρήση μιας HTTP επικεφαλίδας "Key-Assign". Η Outband μέθοδος υπονοεί ότι ο client και ο server έχουν πρόσβαση σε κλειδιά που σχετίζονται με ονόματα χρηστών, είτε μέσω μιας βάσης δεδομένων, είτε από την εισαγωγή ενός κωδικού από τον χρήστη μέσω του πληκτρολόγιου. Η RSA χρησιμοποιεί την ιδιωτική κλείδα του αποστολέα για την κρυπτογράφηση του κλειδιού κρυπτογράφησης των ενθυλακωμένων περιεχομένων που συνοδεύεται από πιστοποιητικό τύπου X.509 με την δημόσια κλείδα του αποστολέα.

Αλγόριθμοι Ψηφιακής Υπογραφής και Παραγωγής Message Digest

Το S/HTTP υποστηρίζει δύο αλγόριθμους για την παραγωγή ψηφιακών υπογραφών: RSA και DSS. Για την παραγωγή message digest υποστηρίζονται οι MD2, MD5 και SHS.

Αλγόριθμοι Συμμετρικής Κρυπτογράφησης

Οι αλγόριθμοι αυτοί διαχωρίζονται σε αυτούς που χρησιμοποιούνται στην κρυπτογράφηση των ενθυλακωμένων περιεχομένων και σε αυτούς που χρησιμοποιούνται στην κρυπτογράφηση των ενθυλακωμένων HTTP επικεφαλίδων.

2.6 SET (Secure Electronic Transactions)

Το SET (Secure Electronic Transactions) είναι ένα πρωτόκολλο κρυπτογράφησης που αναπτύχθηκε από κοινού από τη Visa, τη Mastercard, τη Netscape και τη Microsoft. Αντίθετα με το SSL το οποίο είναι ένα σύστημα γενικού σκοπού για κρυπτογραφημένη επικοινωνία, το SET είναι πολύ εξειδικευμένο. Χρησιμοποιείται *μόνο* για την ασφαλή συναλλαγή μέσω πιστωτικών καρτών και επιταγών ανάμεσα στους πελάτες και τους εμπόρους.

2.6.1 Προδιαγραφές

Το SET έχει δημιουργηθεί βάση συγκεκριμένων προδιαγραφών που προήλθαν από τις απαιτήσεις των επιχειρήσεων και αφορούσαν τις συναλλαγές τους. Αυτές οι προδιαγραφές είναι:

1. Παροχή προστασίας των οικονομικών δεδομένων ή και άλλων που διακινούνται μαζί τους από υποκλοπή.
2. Διασφάλιση της ακεραιότητας των δεδομένων.
3. Παροχή διαδικασιών πιστοποίησης ταυτότητας του κατόχου κάρτας.
4. Παροχή υπηρεσιών πιστοποίησης των εμπόρων που μπορούν να δεχθούν την πληρωμή με τη χρήση τέτοιας μεθόδου, που προκύπτει από τη σχέση τους με κάποιο οικονομικό ίδρυμα παροχής καρτών.
5. Διασφάλιση της χρήσης των καλύτερων τεχνικών ασφάλειας και σχεδίασης συστημάτων για την προστασία όλων των νόμιμα εμπλεκομένων πλευρών.
6. Η δημιουργία ενός πρωτοκόλλου το οποίο να είναι ανεξάρτητο από τους μηχανισμούς ασφάλειας του επιπέδου μεταφοράς χωρίς όμως και να αποτρέπει τη χρήση τους.
7. Να είναι διαλειτουργικό (όλοι οι κύριοι browsers δουλεύουν με όλους τους κύριους servers και οι τελευταίοι με τη σειρά τους δεν θα έχουν πρόβλημα συμβατότητας με τους Payment Gateway Servers).

Σε χαμηλό επίπεδο, το πρωτόκολλο SET παρέχει τις ακόλουθες βασικές υπηρεσίες:

- Πιστοποίηση: Όλα τα μέλη που συμμετέχουν σε μία συναλλαγή μέσω πιστωτικής κάρτας πιστοποιούνται χρησιμοποιώντας ψηφιακές υπογραφές. Αυτό περιλαμβάνει τους πελάτες, τον έμπορο, την τράπεζα που εκδίδει την πιστωτική κάρτα του πελάτη και την τράπεζα που διαχειρίζεται το λογαριασμό του εμπόρου.

- Εμπιστευτικότητα: Η συναλλαγή είναι κρυπτογραφημένη έτσι ώστε να μη μπορεί να υποκλαπεί.

- Ακεραιότητα του μηνύματος: Κανένας δε μπορεί να επέμβει στη συναλλαγή με σκοπό να μεταβάλλει τον αριθμό λογαριασμού ή το ποσό της συναλλαγής.

- Διασύνδεση: Το SET επιτρέπει σε ένα μήνυμα που στέλνεται σε ένα μέλος να περιέχει μια προσάρτηση (attachment) που μπορεί να διαβαστεί μόνο από ένα άλλο μέλος. Η διασύνδεση επιτρέπει στο πρώτο μέλος να επιβεβαιώσει ότι η προσάρτηση είναι σωστή χωρίς να είναι σε θέση να διαβάσει τα περιεχόμενα αυτής.

Σε υψηλό επίπεδο, το πρωτόκολλο SET υποστηρίζει σε πραγματικό χρόνο όλες τις δυνατότητες του υπάρχοντος συστήματος πιστωτικών καρτών, συμπεριλαμβανομένων των ακολούθων:

- Εγγραφή κατόχου πιστωτικής κάρτας.
- Εγγραφή εμπόρου.
- Αιτήσεις αγοράς.
- Πιστοποιήσεις πληρωμής.
- Μεταφορά διαθέσιμων χρηματικών πόρων. Επιστροφές αμφισβητούμενων χρεώσεων.
- Πιστώσεις.

- Συναλλαγές μέσω επιταγών.

2.6.2 Οι συμμετέχοντες του SET

Οι βασικοί συμμετέχοντες στο περιβάλλον του SET είναι:

- **Ο εκδότης:** Ένας οικονομικός οργανισμός που εκδίδει τραπεζικές κάρτες (πιστωτικές ή ανάληψης χρημάτων).

- **Ο κάτοχος:** Ένας εξουσιοδοτημένος κάτοχος μιας τραπεζικής κάρτας ο οποίος είναι σε θέση, με την άδεια του εκδότη, να εκτελεί αγορές ηλεκτρονικού εμπορίου.

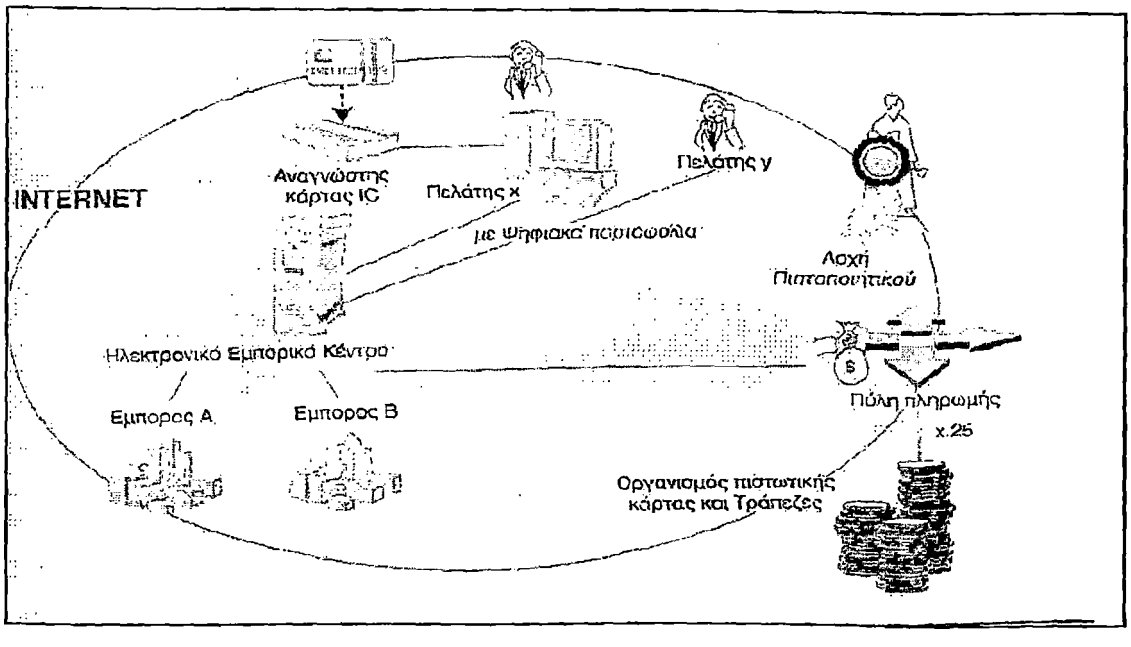
- **Ο πωλητής:** Κάποιος που πουλάει αγαθά, υπηρεσίες ή πληροφορίες και δέχεται πληρωμές ηλεκτρονικά.

- **Ο οργανισμός:** Κάποιο οικονομικό-πιστωτικό ίδρυμα που υποστηρίζει τους πωλητές παρέχοντας υπηρεσίες για την επεξεργασία συναλλαγών με τραπεζικές κάρτες.

Δευτερεύοντες συμμετέχοντες που όμως αποτελούν μέρος της όλης δομής του πρωτοκόλλου SET είναι:

- **Η πύλη πληρωμής:** Ένα σύστημα που παρέχει ηλεκτρονικές υπηρεσίες εμπορίου σε πραγματικό χρόνο (online) στους πωλητές. Ένα τέτοιο σύστημα το διαχειρίζεται κάποιος οργανισμός.

- **Οι αρχές πιστοποίησης:** Συστατικά της όλης δομής που πιστοποιούν τα δημόσια κλειδιά των κατόχων, των πωλητών και των οργανισμών (με τις αντίστοιχες πύλες τους).



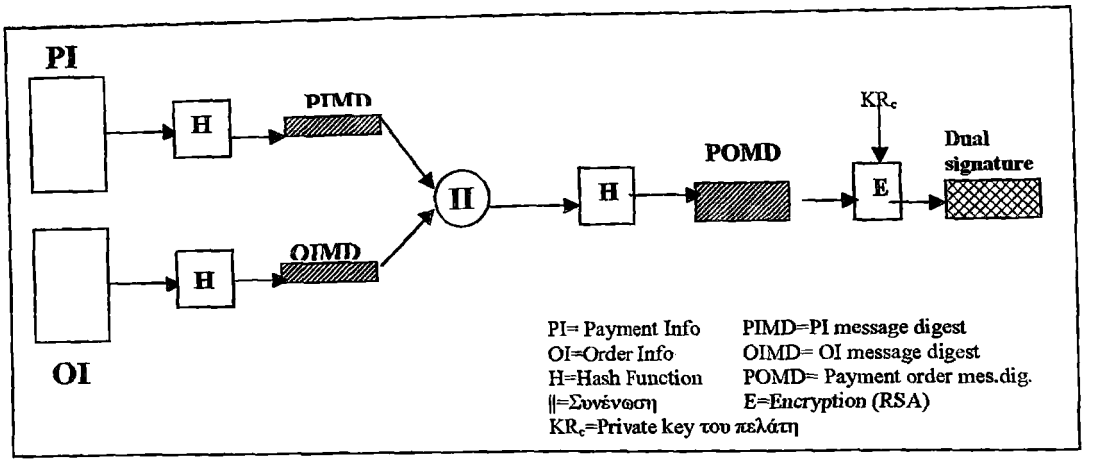
Σχήμα 2.5: Οι συμμετέχοντες στο SET

2.6.3 Η συναλλαγή στο SET

1. Ο πελάτης αποκτά το ηλεκτρονικό πορτοφόλι (digital wallet), το software που επικοινωνεί με το SET software του εμπόρου αυτόματα για να επιβεβαιώσει το πιστοποιητικό του εμπόρου και τη σχέση του με ένα έμπιστο οικονομικό οργανισμό.
2. Ο πελάτης ανοίγει ένα λογαριασμό, από μια τράπεζα που υποστηρίζει ηλεκτρονική πληρωμή και SET.
3. Ο πελάτης λαμβάνει ένα X.509v3 ηλεκτρονικό πιστοποιητικό, το οποίο επιβεβαιώνει το δημόσιο-κλειδί RSA του πελάτη και την ημερομηνία λήξης του πιστοποιητικού.
4. Οι έμποροι έχουν τα δικά τους πιστοποιητικά: ένα πιστοποιητικό δημοσίου-κλειδιού για την υπογραφή μηνυμάτων και ένα άλλο για την ανταλλαγή κλειδιού.
5. Ο πελάτης κάνει μια παραγγελία.
6. Ο έμπορος επιβεβαιώνεται, δηλαδή στέλνει ένα αντίγραφο του πιστοποιητικού του στον πελάτη.
7. Η παραγγελία και η πληρωμή στέλνονται στον έμπορο, μαζί με το πιστοποιητικό του πελάτη.
8. Ο έμπορος ζητά εξουσιοδότηση πληρωμής από το payment gateway, δηλαδή ότι η πίστωση του πελάτη είναι επαρκής για την αγορά.
9. Ο έμπορος επιβεβαιώνει την παραγγελία στον πελάτη.
10. Ο έμπορος παρέχει τα αγαθά ή την υπηρεσία.
11. Ο έμπορος απαιτεί την πληρωμή από το payment gateway, που χειρίζεται την επεξεργασία πληρωμών.

2.6.3.1 Η διπλή υπογραφή

Μια σημαντική καινοτομία που εισάγεται στο SET είναι η διπλή υπογραφή (dual signature). Ο σκοπός της είναι να συνδέσει δύο μηνύματα που απευθύνονται σε δύο διαφορετικούς παραλήπτες. Ο πελάτης θέλει να στείλει την *πληροφορία παραγγελίας* (**Order Information - OI**) στον έμπορο και την *πληροφορία πληρωμής* (**Payment Information - PI**) στην τράπεζα, και του παρέχεται επιπλέον προστασία σε μυστικότητα για να κρατήσει ξεχωριστά αυτά τα δύο αντικείμενα. Ο σύνδεσμος χρειάζεται έτσι ώστε ο πελάτης να μπορεί να αποδείξει ότι αυτή η πληρωμή προορίζεται για τη συγκεκριμένη παραγγελία και όχι για άλλα αγαθά ή υπηρεσία.
Ας υποθέσουμε ότι ο πελάτης στέλνει δύο μηνύματα στον έμπορο- ένα υπογεγραμμένο OI και ένα υπογεγραμμένο PI - και ότι ο έμπορος δίνει το PI στην τράπεζα. Αν ο έμπορος μπορεί να αποκτήσει άλλο OI από τον πελάτη θα μπορούσε να ισχυριστεί ότι το δεύτερο OI πηγαίνει με το PI αντί για το γνήσιο OI.
Η παρακάτω εικόνα δείχνει την κατασκευή της διπλής υπογραφής. Ο πελάτης παίρνει το hash του PI και το hash του OI. Αυτά τα δύο hashes συνενώνονται και το αποτέλεσμα το κάνουμε hash. Ο πελάτης κρυπτογραφεί το τελικό hash με το ιδιωτικό του κλειδί, δημιουργώντας έτσι την διπλή υπογραφή.



Σχήμα2.6: κατασκευή διπλής υπογραφής

Έτσι, ο έμπορος όταν λάβει το OI και τη διπλή υπογραφή (DS) μπορεί να την επιβεβαιώσει. Η τράπεζα όταν λάβει το PI και το DS μπορεί να επιβεβαιώσει την υπογραφή. Ο πελάτης έχει συνδέσει το OI και το PI και μπορεί να αποδείξει το σύνδεσμο.

2.6.4 Βασικοί τύποι συναλλαγών

Από τους τύπους συναλλαγών του SET οι πιο σημαντικοί είναι οι παρακάτω:

2.6.4.1 Αίτηση Αγοράς (Purchase Request)

Η ανταλλαγή αίτησης αγοράς αποτελείται από τέσσερα μηνύματα: Initiate Request, Initiate Response, Purchase Request, και Purchase Response. Ο κάτοχος της κάρτας πρέπει να έχει αντίγραφα των πιστοποιητικών του εμπόρου και του payment gateway, οπότε και ζητά τα πιστοποιητικά αυτά στο μήνυμα **Initiate Request** προς τον έμπορο. Ο έμπορος αποκρίνεται και υπογράφει με το ιδιωτικό του κλειδί. Το **Initiate Response** μήνυμα περιλαμβάνει τα πιστοποιητικά του εμπόρου και του payment gateway. Ο κάτοχος της κάρτας επιβεβαιώνει τα πιστοποιητικά μέσω των αντίστοιχων CA υπογραφών τους, και στη συνέχεια δημιουργεί το OI και το PI. Μετά, ετοιμάζει το **Purchase Request** μήνυμα, και για αυτό το σκοπό παράγει ένα one-time συμμετρικό κλειδί κρυπτογράφησης, το K_s. Το μήνυμα περιλαμβάνει τα ακόλουθα:

- Πληροφορία σχετική με την αγορά. Αυτή η πληροφορία θα προωθηθεί στο payment gateway από τον έμπορο.
- Πληροφορία σχετικά με την παραγγελία. Αυτή η πληροφορία χρειάζεται από τον έμπορο.
- Πιστοποιητικό του κατόχου της κάρτας. Αυτό περιέχει το δημόσιο κλειδί του κατόχου, και χρειάζεται από τον έμπορο και το payment gateway.

Όταν ο έμπορος λάβει το μήνυμα Purchase Request, εκτελεί τις παρακάτω ενέργειες:

- Επιβεβαιώνει τα πιστοποιητικά του κατόχου της κάρτας.
- Επιβεβαιώνει τη διπλή υπογραφή, χρησιμοποιώντας το δημόσιο κλειδί του πελάτη.
- Επεξεργάζεται την παραγγελία και προωθεί την πληροφορία πληρωμής στο payment gateway.

- Στέλνει μήνυμα purchase response στον κάτοχο της κάρτας.

2.6.4.2 Μήνυμα Απόκρισης Αγοράς (Purchase Response)

Αποτελείται από ένα block απόκρισης που αναγνωρίζει την παραγγελία και αναφέρει τον κατάλληλο αριθμό συναλλαγής. Όταν το software του κατόχου της κάρτας λάβει το μήνυμα, επιβεβαιώνει το πιστοποιητικό του εμπόρου και την υπογραφή στο block απόκρισης.

2.6.4.3 Εξουσιοδότηση πληρωμής (Payment Authorization)

Η εξουσιοδότηση πληρωμής εγγυάται ότι η συναλλαγή έγινε δεκτή από τον issuer, δηλαδή ότι ο έμπορος θα πληρωθεί. Στη συνέχεια ο έμπορος μπορεί να παρέχει τις υπηρεσίες ή τα αγαθά στον πελάτη.
Ο έμπορος στέλνει ένα μήνυμα **Authorization Request** στο payment gateway που αποτελείται από

- Πληροφορίες σχετικές με την αγορά
- Πληροφορίες σχετικές με την εξουσιοδότηση
- Πιστοποιητικά

Το payment gateway έχοντας αποκτήσει την εξουσιοδότηση από τον issuer, επιστρέφει μήνυμα Authorization Response στον έμπορο, που περιλαμβάνει τα ακόλουθα:

- Πληροφορίες σχετικές με την εξουσιοδότηση
- Capture token πληροφορία. Αυτή η πληροφορία θα χρησιμοποιηθεί για να πραγματοποιηθεί η πληρωμή αργότερα.
- Πιστοποιητικό του gateway

2.6.4.4 Απόκτηση Πληρωμής (Payment Capture)

Για να πληρωθεί ο έμπορος, ανταλλάσσει με το payment gateway ένα μήνυμα capture request και ένα μήνυμα capture response. Το **Capture Request** μήνυμα περιλαμβάνει το ποσό πληρωμής, το id της συναλλαγής και το capture token από το Authorization Response. Όταν το payment gateway λάβει το μήνυμα αφού ελέγξει για τη συνέπεια μεταξύ του capture request και του capture token, δημιουργεί ένα αίτημα συμψηφισμού που στέλνεται στον issuer, και έτσι μεταφέρονται τα χρήματα στο λογαριασμό του εμπόρου. Εν συνεχεία, το gateway ειδοποιεί τον έμπορο για την πληρωμή με ένα μήνυμα **Capture Response**.

2.7 Άλλα συστήματα ψηφιακής πληρωμής

2.7.1 First Virtual

Η First Virtual (FV) ( ) υλοποίησε και ανέπτυξε ένα από τα πρώτα ηλεκτρονικά συστήματα πληρωμών, το First Virtual Internet Payment System, τον Οκτώβριο του 1994. Όλως περιέργως, το FV δεν χρησιμοποιεί κρυπτογραφία ή ασφαλή μέσα επικοινωνίας. Αντίθετα μάλιστα, το σύστημα της πληρωμής βασίζεται στην ανταλλαγή e-mail μηνυμάτων και στην εντιμότητα των καταναλωτών. Το First Virtual παίζει το ρόλο του μεσολαβητή στις συναλλαγές πιστωτικών καρτών μεταξύ καταναλωτών και εμπόρων. Ένας καταναλωτής πρέπει πρώτα να εγκαταστήσει έναν

λογαριασμό με FV. Ο λογαριασμός ασφαλίζεται με πιστωτικές κάρτες Visa ή MasterCard. Μετά την υπογραφή με FV, παρέχεται ο καταναλωτής με ένα ψηφιακό κωδικό πρόσβασης(Virtual PIN). Το Virtual PIN παίζει το ρόλο του πληρεξούσιο για το νούμερο της πιστωτικής κάρτας, το οποίο κρατιέται από την FV. Ένα ετήσιο ποσό 2$ χρεώνεται στους καταναλωτές με πιστωτική κάρτα.
Τα πλεονεκτήματα της First Virtual και τα οποία παρέχουν ασφάλεια ενάντια σε απάτες βασίζονται σε τρεις επιχειρηματικές πρακτικές:

- Τα νούμερα της πιστωτικής κάρτας δεν μεταφέρονται ποτέ μέσω Internet
- Επανειλημμένες επιθέσεις δεν είναι πιθανές
- Ένα έμπορος που είναι απλήρωτος για online παράδοση πληροφοριών για αγαθά παθαίνει αμελητέες ζημιές.

Παρ' όλα αυτά αν ένας πελάτης που έχει δώσει την ηλεκτρονική του διεύθυνση δεν θα ζητήσει να αποκλειστεί(excluded) η αθετημένη (default) αξία θα ξαναεπανέλθει για επανάληψη πληρωμής.

2.7.2 CyberCash

Το CyberCash είναι ένα προϊόν της CyberCash Corporation το οποίο χρησιμοποιεί εξειδικευμένο λογισμικό από την πλευρά του πελάτη και του πωλητή για να εξασφαλίσει ασφαλείς ηλεκτρονικές συναλλαγές μέσω Διαδικτύου. Το CyberCash υποστηρίζει πληρωμές τόσο με πιστωτικές κάρτες όσο και με ηλεκτρονικά εμβάσματα ("checks"). Η υπηρεσία πιστωτικών καρτών δίνει τη δυνατότητα σε καταστήματα πραγματικού χρόνου (online shops) να δέχονται πληρωμές για αγαθά και υπηρεσίες, ενώ η υπηρεσία «PayNow» δίνει τη δυνατότητα ηλεκτρονικής πληρωμής μέσω του Διαδικτύου. Ένας καταναλωτής που κάνει πληρωμές μέσω του CyberCash στέλνει τον αριθμό της πιστωτικής του κάρτας χρησιμοποιώντας μία φόρμα SSL που του παρέχει ο πωλητής. Εναλλακτικά, μπορεί ο καταναλωτής να χρησιμοποιήσει ένα«πορτοφόλι» InstaBuy για την απλοποίηση της διαδικασίας αγοράς. Το InstaBuy αποθηκεύει τον αριθμό πιστωτικής κάρτας σε 128-bit κρυπτογραφημένη μορφή στους InstaBuy servers.
Όταν κάποιος χρήστης αγοράζει ένα προϊόν από κάποιον πωλητή ο οποίος υποστηρίζει το περιβάλλον CyberCash, τότε συμπληρώνει μια παραδοσιακή φόρμα πληρωμής η οποία θα υποβληθεί μέσω SSL (Secure Socket Layer). Οι CyberCash πωλητές μπορούν να διαλέξουν κατά πόσο θα υλοποιήσουν το InstaBuy, που είναι μια καινούρια υπηρεσία της CyberCash. Η πληροφορία που αφορά την πληρωμή στέλνεται στη συνέχεια στο Web server του πωλητή που με τη σειρά του την προωθεί στους CyberCash Gateway servers που είναι συνδεδεμένοι με τα οικονομικά ιδρύματα (τράπεζες κ.α.).
Ένα βασικό πλεονέκτημα του CyberCash είναι η χρήση κρυπτογράφησης «τριπλού DES» κατά τη μετάδοση της πληροφορίας που αφορά στην πληρωμή. Επίσης, επειδή η διαδικασία της πληρωμής επεξεργάζεται αποκλειστικά στο CyberCash, δεν είναι απαραίτητο οι πωλητές να αποθηκεύουν στη βάση δεδομένων ή σε οποιαδήποτε άλλη μορφή στατικής μνήμης τους αριθμούς των πιστωτικών καρτών των πελατών τους. Αυτό ελαχιστοποιεί τον κίνδυνο να κλαπεί σημαντική πληροφορία που αφορά στην ηλεκτρονική συναλλαγή από άτομα που μπορεί να παραβιάσουν τα συστήματα ασφαλείας στους υπολογιστές του πωλητή. Το βάρος για το χειρισμό των θεμάτων ασφαλείας πέφτει αποκλειστικά στη CyberCash.
Για να μπορούν οι πωλητές να δεχτούν πληρωμές με CyberCash, θα πρέπει πρώτα να

«ανοίξουν» ένα λογαριασμό μέσω ενός χρηματοπιστωτικού οργανισμού. Περισσότερο από το 95% των χρηματοπιστωτικών οργανισμών στις Η.Π.Α. παρέχουν αυτή τη δυνατότητα. Το κόστος για το άνοιγμα ενός τέτοιου λογαριασμού ποικίλει, καθώς αυτό εξαρτάται αποκλειστικά από τις κατά τόπους τράπεζες. Ένα τυπικό σενάριο περιλαμβάνει: Μια χρέωση περίπου 120 ευρώ για το άνοιγμα του λογαριασμού, μια χρέωση περίπου 18 ευρώ το μήνα για να διατηρείται ο λογαριασμός και ένα κόστος για κάθε συναλλαγή που κυμαίνεται στο 2% με 3% της αξίας της συναλλαγής. Εκτός από τη χρέωση στην τράπεζα, οι πωλητές θα πρέπει να γνωρίζουν ότι θα πρέπει να περιμένουν και ένα κόστος 585 έως 1170 ευρώ προς την CyberCash, καθώς επίσης και μηνιαία χρέωση για τις υπηρεσίες της τάξης των 45 με 90 ευρώ όπως και χρέωση 3 Ο με 90 λεπτών για κάθε συναλλαγή.
Αφού ανοιχθεί ένας λογαριασμός για τον πωλητή, στη συνέχεια αυτός οφείλει να εγκαταστήσει το λογισμικό γνωστό με το όνομα "Merchant Connection Kit" (MCK) στον Web server του. Αυτό το λογισμικό ενεργοποιείται όταν ο χρήστης -αγοραστής - κάτοχος κάρτας πατήσει το «κουμπί» PAY κατά την ολοκλήρωση της διαδικασίας αγοράς κάποιου προϊόντος από τον υπολογιστή του. Το MCK τότε προωθεί τη συναλλαγή στην αντίστοιχη εφαρμογή που τρέχει στους servers τηςCyberCash. Το MCK είναι διαθέσιμο δωρεάν και υπάρχουν αρκετές εκδόσεις για διαφορετικές πλατφόρμες, συμπεριλαμβανομένων των Windows 2000 και UNIX. Απαιτούνται μόνο 100k ελεύθερου χώρου στο σκληρό δίσκο και αποτελείται από βιβλιοθήκες κρυπτογράφησης και επικοινωνίας, HTML φόρμες και CGI scripts για τη διαχείριση των πληρωμών στο online κατάστημα.
Η αποστολή του MCK είναι να μεταδίδει όλη την πληροφορία που αφορά την πληρωμή στους CyberCash Gateway server οι οποίοι είναι υπεύθυνοι για την εκτέλεση της συναλλαγής. Αυτοί είναι server πληρωμής που επικοινωνούν με οικονομικούς οργανισμούς με τέτοιο τρόπο ώστε για τον οργανισμό αυτές οι συναλλαγές φαίνονται ως «κλασσικές» συναλλαγές και όχι συναλλαγές μέσω Διαδικτύου. Η CyberCash προσφέρει και ένα «περιβάλλον διαχείρισης» το οποίο είναι ένας δικτυακός τόπος απ' όπου μπορούν να εκτελεστούν λειτουργίες διαχείρισης όπως αναζητήσεις σχετικά με τις συναλλαγές, στατιστικά στοιχεία σχετικά με τις συναλλαγές ανά ημέρα ή μήνα, ή επιστροφή χρημάτων από επιστρεφόμενα αντικείμενα.
Το κυριότερο πλεονέκτημα από την πλευρά του πωλητή είναι ότι του παρέχεται ένα πλήρως λειτουργικό και εξωτερικώς διαχειριζόμενο σύστημα διαχείρισης πληρωμών. Ο πωλητής το μόνο που χρειάζεται να κάνει είναι να ανοίξει ένα λογαριασμό και να εγκαταστήσει το MCK για να ξεκινήσει. Στα μειονεκτήματα περιλαμβάνεται ο κίνδυνος που απορρέει από τη μεγάλη συγκέντρωση οικονομικής πληροφορίας σε έναν και μόνο server (της CyberCash) και την αντίστοιχη εξάρτηση από τους server της CyberCash και τα χαρακτηριστικά τους (απόδοση κ.α.). Επιπλέον η χρέωση προς τους πωλητές για την επεξεργασία ηλεκτρονικών συναλλαγών με πιστωτικές κάρτες δεν ευνοούν τη χρήση του συστήματος σε μικρομεσαία online καταστήματα ή μικρές αγορές όπως τα «pay per play» και τα online video παιχνίδια.

2.7.3 Digicash

Στην Digicash (Chaum 1985), οι καταναλωτές κρατάνε τη νομισματική αξία μέσα σε μία φόρμα ηλεκτρονικών εμβλημάτων(tokens). Καταναλωτές και έμποροι ανταλλάσσουν εμβλήματα(tokens) και αυτά τα εμβλήματα επιβεβαιώνονται από μία τράπεζα. Η τράπεζα επιβεβαιώνει ότι οι υπογραφές πάνω στα εμβλήματα(token) είναι έγκυρες και ότι αυτά τα εμβλήματα(token) δεν έχουν ήδη ξοδευτεί.

Η Digicash παρέχει μόνο ένα μηχανισμό για ηλεκτρονική πληρωμή. Τα πρωτόκολλα της Digicash δεν παρέχουν μηχανισμούς για ανακάλυψη, διαπραγμάτευση, παράδοση ή ανάλυση σύγκρουσης(conflict resolution). Ο σκοπός της Digicash είναι μαζί η δύναμη και η αδυναμία της. Το πλεονέκτημά της είναι ότι παρέχει ένα κομψό και απλό πρωτόκολλο. Το μειονέκτημα της είναι ότι δεν μπορεί να προσφέρει μείωση τους κόστους που σχετίζεται με την συλλογή και αμφισβήτηση ανάλυσης.
Η Digicash είναι ένα υψηλά-ασφαλές σύστημα. Ο έμπορος που σε μια συναλλαγή χρησιμοποιεί Digicash έχει την απαραίτητη πληροφόρηση μόνο για να διασφαλίσει την πληρωμή ενώ η τράπεζα σε μια συναλλαγή έχει την απαραίτητη πληροφόρηση μόνο για να πιστώσει και να χρεώσει ένα λογαριασμό.

2.7.4 Millicent

Το σύστημα Millicent παρουσιάστηκε από την DEC (Digital Equipment Corporation) και χρησιμοποιείται για την εξυπηρέτηση μικρών ηλεκτρονικών αγορών. Η καινοτομία του είναι η χρήση των «brokers» (χρηματομεσίτες) και των «scrips» (χαρτονομίσματα). Ένα scrip έχει μία μικρή ονομαστική αξία και μπορεί να εξαργυρωθεί μόνο σε ένα συγκεκριμένο εμπορικό κατάστημα. Εάν η τιμή του scrip είναι μεγαλύτερη από την αξία του προϊόντος, ο έμπορος επιστρέφει τη διαφορά στον πελάτη με τη μορφή ενός νέου scrip.
Το scrip αριθμείται σειριακά και υπογράφεται ψηφιακά, έτσι ώστε ο έμπορος να μπορεί να επαληθεύσει γρήγορα ότι είναι έγκυρο και ότι δεν έχει ήδη χρησιμοποιηθεί. Τα scrips αγοράζονται σε μεγάλους αριθμούς σε χοντρική τιμή από τους brokers (χρηματομεσίτες) οι οποίοι στη συνέχεια τα μεταπωλούν σε διαφόρους πελάτες. Επειδή τα scrips δημιουργούνται και υπογράφονται από τους εμπόρους, δεν απαιτείται η ύπαρξη κεντρικών εξυπηρετών που θα ελέγχουν την εγκυρότητά τους και το ότι δεν έχουν ήδη χρησιμοποιηθεί. Αυτό έχει ως αποτέλεσμα την ταχύτητα και το ιδιαίτερα χαμηλό κόστος του συστήματος. Τέλος, επειδή το σύστημα Millicent διαχειρίζεται μικρά ποσά, δε χρειάζεται ούτε πολύ ισχυρή κρυπτογραφία ούτε και μία υποδομή δημόσιου κλειδιού για πιστοποίηση αυθεντικότητας.

2.8 IPSec

2.8.1 Εισαγωγή

Ο όρος IPSec (IP Security Protocol) αναφέρεται σε ένα σετ από μηχανισμούς που είναι σχεδιασμένοι να προστατεύουν την κίνηση στο επίπεδο IP. Οι υπηρεσίες που προσφέρει το πρωτόκολλο IPSec είναι η χωρίς σύνδεση (connectionless) ακεραιότητα (integrity) των δεδομένων, η εξακρίβωση γνησιότητας της προέλευσης των δεδομένων, η προστασία απέναντι στις επαναλήψεις και η εμπιστευτικότητα. Αυτές οι υπηρεσίες εξασφαλίζονται στο επίπεδο IP γι' αυτό το λόγο προσφέρεται προστασία και στο επίπεδο IP και σε όλα τα επίπεδα που βρίσκονται πάνω από αυτό.
Το IPSec αποτελείται από τρεις συνιστώσες: Το **Authentication Header (AH)**, το **Encapsulating Security Payload (ESP)** και το **Internet Key Exchange (IKE)**.
Το IPSec σχεδιάστηκε για να χρησιμοποιηθεί σε μεγάλο εύρος εφαρμογών. Όταν εφαρμοστεί σωστά, δεν επηρεάζει τα δίκτυα και τους υπολογιστές που δεν το υποστηρίζουν. Το IPSec είναι ανεξάρτητο από τους τρέχοντες κρυπτογραφικούς αλγορίθμους και μπορεί να χρησιμοποιήσει καινούργιους όταν γίνουν διαθέσιμοι. Το

πρωτόκολλο IPSec δουλεύει και με τα δύο τα πρωτόκολλα IPv4 και IPv6 Συγκεκριμένα, είναι υποχρεωτικό μέρος του IPv6.

2.8.2 Συσχετίσεις Ασφάλειας και Tunneling

Το IPSec χρησιμοποιεί δύο βασικές ιδέες για την υλοποίησή του: τις Συσχετίσεις Ασφάλειας (Security Associations-SA) και το Tunneling. Αυτά περιγράφονται στις επόμενες παραγράφους.

2.8.2.1 Συσχετίσεις Ασφάλειας (Security Associations)

Οι συνιστώσες που αναφέρθηκαν παραπάνω χρησιμοποιούν κρυπτογραφία που σημαίνει χρησιμοποίηση ενός συγκεκριμένου αριθμού από παραμέτρους (όπως κλειδιά, αλγορίθμους κ.ά.) πάνω στις οποίες αυτοί που πρόκειται να επικοινωνήσουν πρέπει να συμφωνήσουν. Για είναι εφικτή η διαχείριση αυτών των παραμέτρων, το IPSec η χρησιμοποιεί την ιδέα των *συσχετίσεων ασφάλειας* (Security Associations-SA).

Μια SA είναι μία μιας κατεύθυνσης σύνδεση η οποία παρέχει υπηρεσίες ασφάλειας στην κίνηση που μεταφέρεται πάνω απ' αυτή. Επίσης μπορεί κάποιος να την δει σαν ένα σετ από παραμέτρους που περιγράφουν πώς μια επικοινωνία θα είναι ασφαλής.

Επειδή μια SA είναι μιας κατεύθυνσης για να προστατευτεί μια διπλής κατεύθυνσης επικοινωνία απαιτούνται δύο SA, μία για κάθε κατεύθυνση.

Μια SA χαρακτηρίζεται από τρία μέρη: το **Security Parameter Index (SPI)** το οποίο χρησιμοποιείται για να ξεχωρίσει διαφορετικές SAs προς τον ίδιο προορισμό, την **IP Destination Address** και το **Security Protocol** το οποίο δηλώνει αν ο μηχανισμός που θα χρησιμοποιηθεί θα είναι ο AH ή ο ESP.

Μια SA παρέχει υπηρεσίες ασφαλείας στην κίνηση που μεταφέρεται χρησιμοποιώντας είτε το AH είτε το ESP αλλά όχι και τα δύο μαζί. Με άλλα λόγια για μια σύνδεση που να προστατεύεται και από τα δύο θα πρέπει να οριστούν δύο SAs για κάθε κατεύθυνση. Σ' αυτήν την περίπτωση το σετ των SAs που ορίζει την σύνδεση αυτή αναφέρεται σαν *SA δέμα (bundle)*.

Η εφαρμογή του IPSec διατηρεί δύο βάσεις δεδομένων που σχετίζονται με τα SA, η μία ονομάζεται **Security Policy Database (SPD)** και καθορίζει τι υπηρεσίες ασφαλείας θα προσφέρονται στην IP κίνηση, δηλαδή σε ποια από τα πακέτα θα χρησιμοποιηθεί το IPSec, και η άλλη είναι η **Security Association Database (SAD)** η οποία περιέχει πληροφορίες σχετικά με τις παραμέτρους για κάθε SA, όπως οι αλγόριθμοι και τα κλειδιά για τα AH και ESP, οι αριθμοί διαδοχής (sequence numbers), η κατάσταση του πρωτοκόλλου (transport ή tunnel) και ο χρόνος διάρκειας μιας SA.

2.8.2.2 Tunneling

Το tunneling είναι μια κοινή τεχνική στα packet-switched δίκτυα. Η ιδέα του είναι η κάλυψη ενός πακέτου πάνω σε ένα άλλο. Αυτό σημαίνει να προστεθεί μια νέα επικεφαλίδα στο αρχικό πακέτο έτσι το αρχικό πακέτο γίνεται το φορτίο ενός άλλου καινούργιου.

Γενικότερα, το tunneling χρησιμοποιείται για την μεταφορά της κίνησης ενός πρωτοκόλλου πάνω από ένα δίκτυο που δεν υποστηρίζει αυτό το πρωτόκολλο άμεσα. Στην περίπτωση του IPSec το πακέτο IP επικαλύπτεται πάνω σε ένα άλλο πακέτο IP για διαφορετικό σκοπό, για να προσφέρει ολική προστασία στο πακέτο, συμπεριλαμβάνοντας και την επικεφαλίδα του πακέτου.

Η τεχνική του tunneling απαιτεί ενδιάμεση επεξεργασία του αρχικού πακέτου στην διαδρομή του. Ο προορισμός που καθορίζεται στην εξωτερική επικεφαλίδα, συνήθως είναι ένας router ή ένα firewall, παίρνει το αρχικό πακέτο και το παραδίδει στον τελικό του προορισμό. Το κόστος της επεξεργασίας του πακέτου αντισταθμίζεται από την παραπάνω ασφάλεια.
Ένα από τα πλεονεκτήματα του tunneling είναι η δυνατότητα μεταφοράς πακέτων με ιδιωτικές Internet διευθύνσεις μεταξύ δύο intranet πάνω από το δημόσιο Internet, το οποίο απαιτεί μοναδικές καθολικές διευθύνσεις.

2.8.3 Authentication Header (AH)

Ο μηχανισμός AH χρησιμοποιείται για την παροχή ακεραιότητας και αυθεντικότητας στα πακέτα IP. Επίσης είναι δυνατή, προαιρετικά, η προστασία από επαναλαμβανόμενα πακέτα.
Ο AH προσδιορίζεται από τον αριθμό πρωτοκόλλου 51 που έχει ανατεθεί από τον IANA.
Ο AH πιστοποιεί όσον το δυνατόν περισσότερα IP πακέτα. Ορισμένα πεδία στην επικεφαλίδα IP αλλάζουν κατά την διαδρομή και οι τιμές τους δεν μπορούν να προβλεφθούν από τον παραλήπτη. Αυτά τα πεδία ονομάζονται ευμετάβλητα (mutable) και δεν προστατεύονται από τον AH. Τα ευμετάβλητα πεδία είναι:

- Type of Service (TOS)
- Flags
- Fragment Offset
- Time to Live (TTL)
- Header Checksum

Όταν χρειάζεται η προστασία αυτών των πεδίων, τότε πρέπει να γίνει χρήση του tunneling. Το φορτίο (payload) του καινούργιου IP πακέτου θεωρείται αμετάβλητο και προστατεύεται από τον AH.
Η επεξεργασία AH εφαρμόζεται μόνο σε μη τεμαχισμένα IP πακέτα. Ωστόσο, ένα IP πακέτο στο οποίο έχει εφαρμοστεί ο AH μπορεί να τεμαχιστεί στους ενδιάμεσους routers. Σ' αυτήν την περίπτωση ο προορισμός πρώτα συνθέτει το πακέτο και ύστερα το επεξεργάζεται με τον AH. Αν ένα πακέτο φανεί να είναι τεμάχιο ενός άλλου τότε απορρίπτεται από την επεξεργασία AH. Αυτό γίνεται για την αποφυγή της επίθεσης η οποία χρησιμοποιεί τον αλγόριθμο σύνθεσης τεμαχισμένων πακέτων για να δημιουργήσει πλαστά πακέτα και να τα περάσει σε ένα firewall.
Τα πακέτα που απορρίπτονται από τον AH δεν πρόκειται ποτέ να ανεβούν στα παραπάνω επίπεδα. Αυτή η κατάσταση λειτουργίας μειώνει στο ελάχιστο την πιθανότητα μιας επιτυχούς *άρνησης υπηρεσίας (denial of service)*, που έχει ως σκοπό να μπλοκάρει τις επικοινωνίες ενός υπολογιστή ή ενός gateway με το να τον κατακλύζει με πλαστά πακέτα.

2.8.3.1 Μορφή της επικεφαλίδας AH

Παρακάτω παρουσιάζεται η μορφή της επικεφαλίδας AH.

Next Header	Length	Reserved
Security Parameter Index (SPI)		
Replay Prevention		
Δεδομένα Αυθεντικοποίησης (n*32 bit)		
32 bit		

Σχήμα 2.7: Η AH επικεφαλίδα

2.8.3.2 Τρόποι χρησιμοποίησης του AH

Ο AH μπορεί να χρησιμοποιηθεί με δύο τρόπους: σε *κατάσταση μεταφοράς* (transport) και σε *κατάσταση tunnel*.

Σε κατάσταση μεταφοράς:

Σ' αυτήν την κατάσταση το αρχικό πακέτο χρησιμοποιείται και η επικεφαλίδα του AH εισχωρεί αμέσως μετά από την επικεφαλίδα του πακέτου IP. Αν το πακέτο έχει ήδη επικεφαλίδες του IPSec τότε η επικεφαλίδα AH εισέρχεται πριν από αυτές.
Η κατάσταση μεταφοράς χρησιμοποιείται μόνο από τους hosts και όχι από τους gateways. Τα πακέτα στέλνονται από host σε host, χωρίς να παρεμβάλλεται κάποιος άλλος κόμβος, έχοντας πιστοποιηθεί.
Το πλεονέκτημα της κατάστασης μεταφοράς είναι ότι έχει χαμηλό επεξεργαστικό φόρτο. Το μειονέκτημα είναι ότι τα ευμετάβλητα πεδία του πακέτου δεν αυθεντικοποιούνται.

Σε κατάσταση tunnel:

Σ' αυτήν την κατάσταση εφαρμόζεται ότι αναφέρθηκε παραπάνω σχετικά με το tunneling: ένα νέο IP πακέτο κατασκευάζεται και το αρχικό IP πακέτο γίνεται φορτίο του. Έπειτα εφαρμόζεται ο μηχανισμός AH σε κατάσταση μεταφοράς στο καινούργιο πακέτο, όπως φαίνεται στην εικόνα.
Η κατάσταση tunnel χρησιμοποιείται όποτε το τελικό άκρο μιας SA είναι ένας gateway ή firewall. Έτσι, μεταξύ δύο firewall χρησιμοποιείται πάντα η κατάσταση tunnel.
Παρόλο που οι gateway υποτίθεται ότι υποστηρίζουν μόνο την κατάσταση tunnel, συχνά μπορούν να δουλεύουν και με την κατάσταση μεταφοράς. Αυτή η κατάσταση επιτρέπεται όταν ο gateway ενεργεί ως host.
Τα πλεονεκτήματα της κατάστασης tunnel είναι η ολική προστασία του αρχικού πακέτου και η πιθανότητα χρησιμοποίησης ιδιωτικών IP διευθύνσεων. Ωστόσο, υπάρχει ένας αυξημένος υπολογιστικός φόρτος συσχετισμένος με αυτήν την κατάσταση.

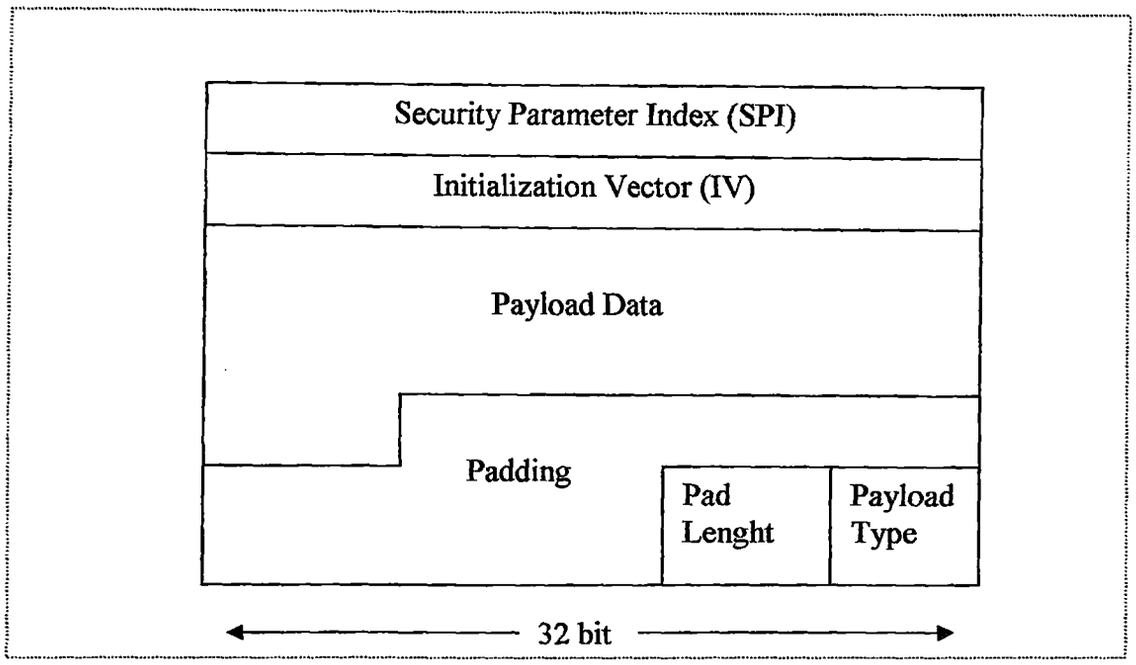
2.8.4 Encapsulating Security Payload (ESP)

Ο μηχανισμός **ESP** χρησιμοποιείται για να παρέχει έλεγχο ακεραιότητας, εξακρίβωση γνησιότητας και κρυπτογράφηση στα IP πακέτα. Επίσης είναι δυνατόν η

προαιρετική προστασία από επαναλήψεις πακέτων. Οι παραπάνω υπηρεσίες είναι χωρίς σύνδεση, όπως είναι και στον μηχανισμό AH.
Ο ESP προσδιορίζεται από τον αριθμό πρωτοκόλλου 50 που έχει ανατεθεί από τον IANA.
Όπως και στον AH και στον ESP η επεξεργασία του εφαρμόζεται μόνο στα μη τεμαχισμένα (non-fragmented) IP πακέτα. Ωστόσο επιτρέπεται ο τεμαχισμός του πακέτου αργότερα στους ενδιάμεσους, κατά την διαδρομή του, δρομολογητές. Η διαδικασία ύστερα για επανασυναρμολόγηση του πακέτου είναι η ίδια με αυτή του AH. Ένα τεμαχισμένο πακέτο απορρίπτεται από την επεξεργασία ESP και αυτό γίνεται για τους λόγους που αναφέρθηκαν παραπάνω στον AH.
Εάν έχει επιλεγεί και η κρυπτογράφηση και η εξακρίβωση γνησιότητας με έλεγχο της ακεραιότητας του πακέτου, τότε ο παραλήπτης του πρέπει να πιστοποιήσει το πακέτο και ύστερα, αν η εξακρίβωση γνησιότητας είναι επιτυχής, να προχωρήσει στην αποκρυπτογράφηση. Αυτή η λειτουργία εξοικονομεί υπολογιστικούς πόρους και μειώνει την ευπάθεια σε επιθέσεις αρνήσεως υπηρεσίας (denial of service).

2.8.4.1 Μορφή του πακέτου ESP

Η μορφή του πακέτου ESP είναι πιο πολύπλοκη από αυτή του AH. Εκτός από την επικεφαλίδα το πακέτο περιέχει και αλλά δύο πεδία το ESP trailer και το ESP authentication data. Το παρακάτω σχήμα δείχνει την μορφή του πακέτου που έχει επεξεργασθεί με το ESP.



Σχήμα 2.8: Η μορφή ESP

2.8.4.2Τρόποι χρησιμοποίησης του ESP

Όπως και ο AH, ο ESP μπορεί να χρησιμοποιηθεί με δύο τρόπους: σε *κατάσταση μεταφοράς* και σε *κατάσταση tunnel*.

Σε κατάσταση μεταφοράς:
Σε αυτήν την κατάσταση το αρχικό πακέτο επεξεργάζεται και ύστερα εισέρχεται η ESP επικεφαλίδα μετά από την IP επικεφαλίδα. Εάν το πακέτο έχει και άλλες IPSec

επικεφαλίδες, τότε η ESP επικεφαλίδα προστίθεται πριν από αυτές. Στο τέλος του πακέτου εισέρχονται άλλα δύο πεδία το ESP *trailer* και τα προαιρετικά δεδομένα εξακρίβωσης γνησιότητας. Στο επόμενο σχήμα φαίνεται πως είναι τα πακέτα.
Ο ESP στην κατάσταση μεταφοράς δεν παρέχει κρυπτογράφηση και εξακρίβωση γνησιότητας στην επικεφαλίδα IP. Το πλεονέκτημα είναι το χαμηλό υπολογιστικό φορτίο.

Σε κατάσταση Tunnel:
Όπως αναμενόταν στην κατάσταση αυτή εφαρμόζεται η αρχή του tunneling. Ένα νέο IP πακέτο κατασκευάζεται με νέα IP επικεφαλίδα και στην συνέχεια εφαρμόζεται στο φορτίο του, που είναι το αρχικό πακέτο, ο μηχανισμός ESP στην κατάσταση μεταφοράς.

2.8.5 Το πρωτόκολλο ανταλλαγής κλειδιών (Internet Key Exchange)

Το **IKE** (πρώην ISAKMP) που σημαίνει **Internet Key Exchange** είναι ένα πρωτόκολλο που σχεδιάστηκε για την υποστήριξη αυτοματοποιημένων διαπραγματεύσεων των SA και αυτοματοποιημένης δημιουργίας και ανανέωσης κρυπτογραφικών κλειδιών.
Το πρωτόκολλο αυτό χρησιμοποιεί πολύπλοκες διαδικασίες κρυπτογράφησης και εξακρίβωσης γνησιότητας, διότι μέσω αυτού γίνονται ανταλλαγές πληροφοριών, όπως κλειδιών, που χρειάζονται για την ασφάλεια των επικοινωνιών.
Οι μέθοδοι που χρησιμοποιεί το πρωτόκολλο IKE για εξακρίβωση γνησιότητας είναι οι παρακάτω:

1. Προ-διαμοιρασμένο κλειδί (Pre-Shared Key)
2. Ηλεκτρονικές Υπογραφές (Digital Signatures – με DSS και RSA)
3. Κρυπτογράφηση δημόσιου κλειδιού (Public key encryption με RSA και revised RSA)

Η αποτελεσματικότητα μιας κρυπτογραφικής λύσης εξαρτάται περισσότερο από την ασφαλή μετάδοση του κλειδιού παρά από την επιλογή του αλγορίθμου. Έτσι, το IETF IPSec Working Group έχει περιγράψει μια σειρά από ιδιαίτερα ανθεκτικά πρωτόκολλα ανταλλαγής Oakley που χρησιμοποιούνται στο IKE. Αυτά χρησιμοποιούν μια προσέγγιση *δύο φάσεων*: Στην *πρώτη φάση* μετά από μια σειρά από διαπραγματεύσεις εγκαθίσταται ένα master κλειδί από το οποίο θα παράγονται όλα τα υπόλοιπα κρυπτογραφικά κλειδιά. Στην γενικότερη περίπτωση αυτό το κλειδί θα πραγματοποιήσει μια ασφαλή σύνδεση πάνω στην οποία θα μεταδίδονται τα μηνύματα του IKE. Η *δεύτερη φάση* είναι η ανταλλαγή των μηνυμάτων, αφού πρώτα γίνει η ασφαλής σύνδεση από την πρώτη φάση, για την παραγωγή των κλειδιών με τα οποία θα εξασφαλιστεί η ασφαλής επικοινωνία των δεδομένων.

2.9 Kerberos

2.9.1 Τι είναι ο Kerberos

Ο Κέρβερος είναι μια έμπιστη «τριμερής» υπηρεσία πιστοποίησης βασισμένη στο μοντέλο που παρουσιάστηκε από τους Needham και Schroeder. Είναι έμπιστη με την έννοια ότι κάθε εξυπηρετούμενος εμπιστεύεται την κρίση του Κέρβερου για την ταυτότητα των άλλων.

Ο χρήστης αναπαρίσταται από μία τριάδα *(primaryname, instance, realm)*, όπου το πρώτο αποτελεί το αναγνωριστικό του κάθε χρήστη, το δεύτερο έχει την τιμή Ο είτε δηλώνει κάποια δικαιώματα του εκάστοτε χρήστη, Π.χ. root, ενώ το τρίτο, *realm*, χρησιμοποιείται για τη διάκριση μεταξύ διαφόρων περιοχών πιστοποίησης.

Αντίθετα με τις πρότυπες διαδικασίες πιστοποίησης του λειτουργικού συστήματος UNIX, ο Kerberos βασίζεται στην απόκτηση κουπονιών (tokens) από έμπιστους ασφαλείς servers, από την πλευρά του χρήστη. Αυτά τα κουπόνια ισχύουν για συγκεκριμένα χρονικά διαστήματα και είναι απαραίτητα για την παροχή άδειας προσπέλασης σε αρχεία ή υπηρεσίες. Γενικά, η διαδικασία της απόκτησης και της καταστροφής των κουπονιών γίνεται αυτόματα για το χρήστη όταν γίνεται η σύνδεση και η αποσύνδεση του στο σύστημα. Χρονοσφραγίδες (timestamps - μεγάλοι αριθμοί που αναπαριστούν την τρέχουσα ημερομηνία και ώρα) προστέθηκαν στο αρχικό μοντέλο για να βοηθήσουν στην ανίχνευση της *επαναμετάδοσης*. Η επαναμετάδοση εμφανίζεται όταν ένα μήνυμα υποκλέπτεται από το δίκτυο και παρουσιάζεται σε μελλοντικό χρόνο.

Ο Κέρβερος κρατάει μια βάση δεδομένων από όλους τους πελάτες (clients), μαζί με τα κλειδιά τους. Το ιδιωτικό κλειδί είναι ένας μεγάλος αριθμός που είναι γνωστός μόνο στον Κέρβερο και στον εξυπηρετούμενο στον οποίο ανήκει. Στην περίπτωση που ο εξυπηρετούμενος είναι χρήστης, το ιδιωτικό κλειδί είναι ένας κρυπτογραφημένος κωδικός πρόσβασης. Οι δικτυακές υπηρεσίες που απαιτούν πιστοποίηση καταχωρούνται στον Κέρβερο, όπως και οι εξυπηρετούμενοι που θέλουν να χρησιμοποιήσουν τις υπηρεσίες αυτές. Τα ιδιωτικά κλειδιά διαπραγματεύονται κατά την καταχώριση.

Αφού ο Κέρβερος γνωρίζει τα ιδιωτικά κλειδιά, μπορεί να δημιουργήσει μηνύματα που να πείσουν έναν εξυπηρετούμενο ότι ο άλλος είναι αυτός που ισχυρίζεται ότι είναι. Ο Κέρβερος επίσης δίνει προσωρινά *κλειδιά συνόδου* σε δύο εξυπηρετούμενους και μόνο σ' αυτούς. Ένα κλειδί συνόδου χρησιμοποιείται για να κρυπτογραφήσει μηνύματα ανάμεσα σε δύο μέρη.

Ο Κέρβερος παρέχει τρία διαφορετικά επίπεδα προστασίας. Ο προγραμματιστής της εφαρμογής αποφασίζει ποιο είναι το πιο κατάλληλο, σύμφωνα με τις απαιτήσεις της εφαρμογής. Για παράδειγμα, κάποιες εφαρμογές απαιτούν πιστοποίηση μόνο κατά την έναρξη της σύνδεσης και υποθέτουν πως αιτήσεις από τη συγκεκριμένη διεύθυνση έρχονται από το πιστοποιημένο μέρος. Το δικτυακό σύστημα αρχείων λειτουργεί μ' αυτόν τον τρόπο.

Άλλες εφαρμογές απαιτούν ταυτοποίηση του κάθε μηνύματος, αλλά δεν ενδιαφέρονται για το αν το μήνυμα θα αποκαλυφθεί ή όχι. Για τις εφαρμογές αυτές ο Κέρβερος παρέχει *ασφαλή μηνύματα*. Ακόμα υψηλότερο επίπεδο ασφαλείας επιτυγχάνεται με τη χρήση *ιδιωτικών κλειδιών*, όπου το κάθε μήνυμα όχι μόνο πιστοποιείται αλλά και κρυπτογραφείται. Τα ιδιωτικά μηνύματα χρησιμοποιούνται από τους servers π.χ. για να στέλνει κωδικούς πρόσβασης μέσα από το δίκτυο.

2.9.2 Πως λειτουργεί ο Κέρβερος

Το Kerberos επιτρέπει στις δικτυακές εφαρμογές να αναγνωρίζουν με ασφάλεια την ταυτότητα του χρήστη που ζητά εξυπηρέτηση, χωρίς να στέλνει στο δίκτυο δεδομένα που μπορούν να επιτρέψουν σε ένα πιθανό εισβολέα να προσποιηθεί ότι είναι ο χρήστης και χωρίς να βασίζεται στις διευθύνσεις των μηχανών του δικτύου. Επίσης, η πιστοποίηση ταυτότητας γίνεται από τον application server και η επικοινωνία γίνεται εν γνώση της πιθανότητας ότι η διακινούμενη πληροφορία μπορεί να τροποποιηθεί και να αναγνωστεί κατά βούληση. Το Kerberos προαιρετικά προσφέρει ακεραιότητα και απόρρητη συναλλαγή για τα δεδομένα που στέλνονται μεταξύ του client και του application server. Σαν *application server* εννοούμε τον server που προσφέρει υπηρεσίες όπως mail, ftp, http, telnet.

Το σύστημα χρησιμοποιεί μια σειρά από κρυπτογραφημένα μηνύματα για να αποδείξει σε έναν application server ότι ο client λειτουργεί εκ μέρους ενός συγκεκριμένου χρήστη. Για την ανταλλαγή των μηνυμάτων ο Kerberos εκμεταλλεύεται το IP επίπεδο σε συνδυασμό με το UDP πρωτόκολλο. Ο client αποδεικνύει την ταυτότητα του χρήστη παρουσιάζοντας στον application server την απόδειξη – *ticket*, η οποία περιέχει ένα προσωρινό κλειδί κρυπτογράφησης που θα χρησιμοποιηθεί για την επικοινωνία μεταξύ του application server και του χρήστη, και το πιστοποιητικό – *authenticator*, το οποίο αποδεικνύει ότι ο client έχει στην κατοχή του το *session key* που έχει εκδοθεί για τον χρήστη που ορίζεται στο ticket. Οι αποδείξεις εκδίδονται από ένα αφιερωμένο υπολογιστή που καλείται *authentication server (AS)*. Ο authentication server έχει αποθηκευμένα μυστικά κλειδιά, που καλούνται server keys και τα μοιράζεται με τους application servers. Εγκαθίστανται μέσα από κρυπτογραφημένο κανάλι ή με *out-of-band* επικοινωνία. Το server key πιστοποιεί την αυθεντικότητα των αποδείξεων – tickets που λαμβάνει ο client και ο server. Επιπλέον, ο AS έχει αποθηκευμένα κλειδιά που αναφέρονται σε κάθε χρήστη και καλούνται *user keys*. Όλα τα κλειδιά εμπεριέχονται σε βάση δεδομένων. Τέλος να πούμε ότι κάθε ticket έχει περιορισμένη διάρκεια ζωής και όταν το χρονικό αυτό διάστημα περάσει τότε είναι άχρηστο. Περαιτέρω ανταλλαγή μηνυμάτων απαιτεί την έκδοση νέου ticket.

2.9.3 Απόκτηση Διαπιστευτηρίων

Οποτεδήποτε ο χρήστης θέλει να έρθει σε επαφή με κάποιον application server, ο client αναλαμβάνει να ξεκινήσει την διαδικασία απόκτησης κατάλληλων διαπιστευτηρίων *(credentials)* για τον θα χρησιμοποιηθούν με τον συγκεκριμένο application server.

Αίτηση Πιστοποίησης Ταυτότητας

Ο client επικοινωνεί με τον AS στέλνοντας κατάλληλη αίτηση και αυτός απαντά με τα διαπιστευτήρια. Τα διαπιστευτήρια αποτελούνται από (α) ένα session key που χρησιμοποιείται σαν κλειδί κρυπτογράφησης και (β) ενός ticket για τον application server. Το session key και το ticket διαφέρουν για κάθε application server με τον οποίο επικοινωνεί ο χρήστης. Η αίτηση που στέλνει ο client στον AS καλείται authentication request και περιέχει τα στοιχεία της ταυτότητας του client, το όνομα του application server, την ζητούμενη διάρκεια ζωής του ticket και ένα τυχαίο αριθμό που θα χρησιμοποιηθεί για το ταίριασμα της authentication request με την authentication response. Επίσης, ο client μπορεί να καθορίσει συγκεκριμένες επιλογές σχετικές με την φύση τού ticket (renewable, proxiable, forwardable κτλ).

Απάντηση στην Αίτηση Πιστοποίησης Ταυτότητας
Ο AS ψάχνει στην βάση δεδομένων του για να ανακτήσει τα κλειδιά του χρήστη (user key) και του application server (server key). Παράγει με τυχαίο τρόπο το session key και ελέγχει τα πεδία με τις επιλογές του client όσον αναφορά το ticket. Σε απάντηση, ο AS επιστρέφει το session key, την διάρκεια ζωής του ticket και του session key, τον τυχαίο αριθμό από την αίτηση και το όνομα του application server, όλα αυτά κρυπτογραφημένα με το μυστικό κλειδί – κωδικό του χρήστη (user key). Μαζί αποστέλλει και το ticket που περιέχει τις ίδιες πληροφορίες που αναφέρθηκαν πριν, κρυπτογραφημένες με το server key. Το ticket θα προωθηθεί από τον client στον server σαν μέρος της αίτησης εξυπηρέτησης. Το ticket έχει ρυθμιστεί σύμφωνα με τις επιλογές του client.
Πολλά λάθη μπορούν να προκύψουν και η απάντηση στην αίτηση του client να είναι ένα μήνυμα λάθους. Στο μήνυμα λάθους θα περιέχεται κατάλληλος κωδικοποιημένος αριθμός που θα υποδεικνύει το είδος του λάθους.
Όταν ο client παραλάβει την authentication response, κατ' αρχή ελέγχει κατά πόσο ο τυχαίος αριθμός που είχε συμπεριλάβει στην αίτηση ταιριάζει με αυτόν που περιέχεται στο παραληφθέν μήνυμα. Γι' αυτό το σκοπό χρησιμοποιεί το κλειδί του χρήστη (user key) για να ανακτήσει το session key και το ticket. Αφού επιβεβαιώσει ότι η απάντηση ανταποκρίνεται στην αυθεντική αίτηση, αποκλείονται έτσι την πιθανότητα επίθεσης replay attack, συνεχίζει με την επεξεργασία του υπόλοιπου μηνύματος. Το γεγονός ότι τα περιεχόμενα της authentication response ήταν κρυπτογραφημένα με το κλειδί του χρήστη, αποδεικνύει ότι η απάντηση προέρχεται από τον αληθινό AS, ενώ το γεγονός ότι ο client μπορεί να αποκρυπτογραφήσει τα περιεχόμενα της απάντησης σημαίνει ότι αντιπροσωπεύει τον έγκυρο χρήστη.
Εάν το μήνυμα που λάβει ο client είναι μήνυμα λάθους, τότε ερμηνεύει τα περιεχόμενα του και αποφαίνεται για το τι πρέπει να πράξει ώστε να μην επαναληφθεί.

Χρήση Διαπιστευτηρίων
Η ανταλλαγή μηνυμάτων αυτού του σταδίου χρησιμοποιείται από application servers του δικτύου για να πιστοποιήσουν την ταυτότητα του client και κατ' επέκταση την ταυτότητα του χρήστη, και αντιστρόφως. Ο client πρέπει πρώτα να έχει στην κατοχή του τα διαπιστευτήρια για την συγκεκριμένο application server.

Η παροχή μόνο του ticket στην αίτηση εξυπηρέτησης δεν αποτελεί ικανοποιητικό στοιχείο για την απόδειξη της ταυτότητας του client. Το ticket μπορεί να χρησιμοποιηθεί από εισβολέα που έχει καταγράψει την διακινούμενη πληροφορία. Η συνοδεία του ticket με επιπλέον πληροφορία (authenticator) που είναι δεμένη με την ταυτότητα του client, εξασφαλίζει ολοκληρωμένη επαλήθευση. Στο authenticator περιλαμβάνεται ένα checksum. Checksum είναι η hash ή digest value του μηνύματος κρυπτογραφημένη με το session key ή άλλο κλειδί.

Αίτηση Εξυπηρέτησης
Μία αίτηση εξυπηρέτησης αποτελείται από δύο μέρη: την απόδειξη – ticket και το πιστοποιητικό – authenticator. Το authenticator περιλαμβάνει την τρέχουσα ώρα, ένα checksum, ένα προαιρετικό κλειδί κρυπτογράφησης και στοιχεία της ταυτότητας του χρήστη όλα κρυπτογραφημένα με το session key. Το προαιρετικό κλειδί κρυπτογράφησης μπορεί να χρησιμοποιηθεί για κρυπτογράφηση των μελλοντικών μηνυμάτων μεταξύ application server και client.

Τα authenticators δεν μπορούν να ξανά χρησιμοποιηθούν και για κάθε αίτηση εξυπηρέτηση, ακόμα και αν είναι για τον ίδιο application server, ετοιμάζεται καινούργιο. Authenticators που επαναλαμβάνονται θα απορριφθούν από τον application server.

Επεξεργασία και Απάντηση στην Αίτηση Εξυπηρέτησης
Η πιστοποίησης της ταυτότητας του client βασίζεται στο πεδίο της τρέχουσας ώρας, στο authenticator και στο ticket.
Όταν ο application server παραλάβει την application request, αποκρυπτογραφεί το ticket με το server key και παίρνει το session key που περιέχεται στο ticket. Με το session key αποκρυπτογραφεί το autheticator και ανακτά τις πληροφορίες για την ταυτότητα του χρήστη και την ώρα αποστολής της αίτησης. Έπειτα ελέγχει το checksum, παράγοντας το δικό του hash value και συγκρίνοντας το με αυτό που προκύπτει από την αποκρυπτογράφηση του checksum. Τέλος ελέγχει το πεδίο της ώρας συγκρίνοντας την τρέχουσα ώρα με την ώρα που περικλείεται στο authenticator. Εάν διαφέρουν περισσότερο από πέντε λεπτά, το μήνυμα απορρίπτεται και θεωρείται προϊόν επίθεσης επανάληψης *(replay attack)*.
Το ότι ο server μπορεί να ανακτήσει το session key επιβεβαιώνει ότι έχει στην κατοχή το server key και άρα αποτελεί τον πραγματικό server. Η κρυπτογράφηση του authenticator με το session key και ο έλεγχος της ώρας αποστολής του authenticator, επαληθεύει ότι την ταυτότητα του χρήστη που αναγράφεται στο ticket.
Προαιρετικά, εάν υποστηρίζεται αμοιβαία πιστοποίησης ταυτότητας, ο application server πιστοποιεί την ταυτότητα του στον client. Για να το επιτύχει αυτό, ετοιμάζει την application response, όπου τοποθετεί την ώρα αποστολής που περιεχόταν στην αίτηση και την κρυπτογραφεί με το session key. Ο client όταν θα παραλάβει την απάντηση, θα την αποκρυπτογραφήσει με το session key και θα επιβεβαιώσει ότι περιέχει την σωστή ώρα αποστολής της αιτήσεως. Η ενέργεια αυτή θα πιστοποιήσει στον client ότι επικοινώνησε με τον αυθεντικό server.
Είναι δυνατόν να προκύψει κάποιο λάθος κατά την επιβεβαίωση της ταυτότητας του client οπότε ο application server ανταποκρίνεται με μήνυμα λάθους που περιλαμβάνει τον είδος του λάθους.

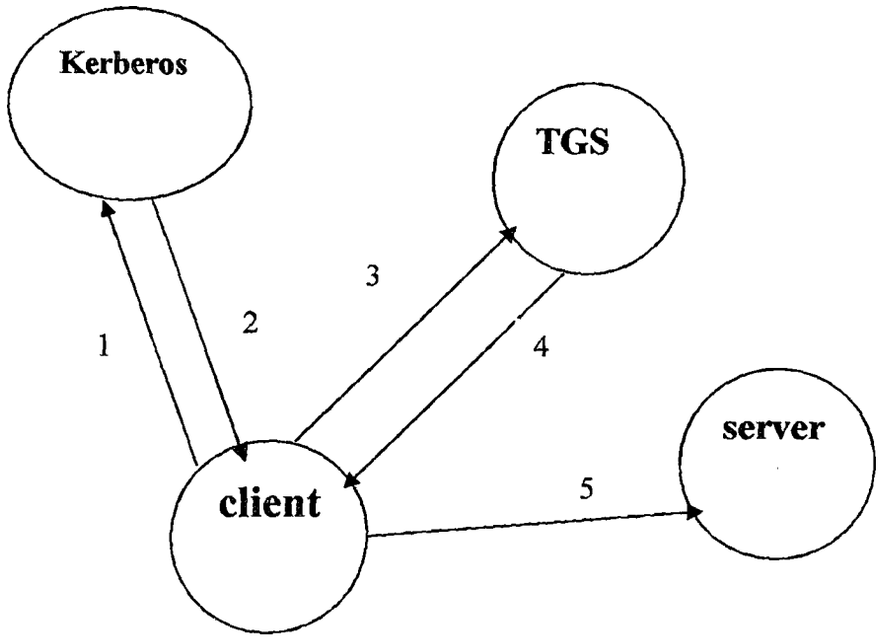
2.9.4 Ticket Granting Server (TGS)

Η παραπάνω συναλλαγή μηνυμάτων παρουσιάζει το εξής πρόβλημα: χρησιμοποιείται κάθε φορά που ο χρήστης θέλει να επικοινωνήσει με κάποιον application server και πρέπει να εισάγει το κλειδί – κωδικό του κάθε φορά που θέλει να αποκρυπτογραφήσει τα διαπιστευτήρια που στέλνονται από τον AS. Μία προφανής λύση του προβλήματος είναι η αποθήκευση του κλειδιού στον client. Αλλά κάτι τέτοιο μπορεί να προσθέσει επιπλέον κινδύνους. Ο εισβολέας που αποκτήσει αντίγραφο του κλειδιού μπορεί να προσποιηθεί ότι είναι ο αυθεντικός χρήστης.
Η επίλυση του προβλήματος γίνεται με την εισαγωγή ενός νέου server, του *Ticket Granting Server (TGS)*. Ο TGS και ο AS είναι ξεχωριστοί server, παρ' όλο που μπορούν να βρίσκονται στο ίδιο μηχάνημα. Ο συνδυασμός τους αποτελεί το *Key Distribution Center (KDC)*. Ο ρόλος του TGS είναι ο εξής: πριν να επικοινωνήσει με κάποιον application server ο client ζητά από τον AS, όπως θα έκανε για οποιοδήποτε application server, για τα απαραίτητα διαπιστευτήρια, ώστε να επικοινωνήσει πρώτα με τον TGS. Το ticket που παίρνει λέγεται *ticket-granting ticket (TGT)*. Μετά την παραλαβή του TGT, ζητά κανονικό ticket για τον application server όχι από τον AS, αλλά από τον TGS. Εξάλλου, η απάντηση του TGS δεν κρυπτογραφείται με το user

key αλλά με το session key που περιεχόταν στο TGT. Μέσα στην απάντηση από τον TGS περιέχεται καινούργιο session key που θα χρησιμοποιηθεί για την κρυπτογράφηση της υπόλοιπης ανταλλαγής μηνυμάτων.
Το πλεονέκτημα αυτής της μεθόδου είναι ότι ενώ οι κωδικοί – κλειδιά των χρηστών δεν αλλάζουν για μεγάλες χρονικές περιόδους (συνήθως μήνες), ένα session key από το TGT είναι έγκυρο μόνο για λίγες ώρες (τυπικά 8 ώρες). Σαν συνέπεια, η αποθήκευση των TGT δεν δημιουργεί σημαντικό ρίσκο και ο χρήστης χρησιμοποιεί τον κωδικό του μόνο κατά την διάρκεια του login.
Αφού ο client αποκτήσει το νέο session key, η διαδικασία συνεχίζεται όπως πριν, με την αποστολή των διαπιστευτηρίων στον application server.

2.9.4.1 Ticket Granting Service

Η μορφή του μηνύματος για αίτηση TGT είναι σχεδόν παρόμοια με την μορφή της αίτησης σε έναν AS. Η κυριότερη διαφορά είναι ότι η κρυπτογράφηση της απάντησης του TGS γίνεται με το session key, ενώ της απάντησης του AS γίνεται με το user key.
Η αίτηση στον TGS αποτελείται από πληροφορίες που πιστοποιούν την ταυτότητα του client στον TGS, την ταυτότητα του application server, την ζητούμενη ώρα λήξης του ticket και το TGT κρυπτογραφημένο με το server key του TGS.
Η απάντηση περιέχει τα διαπιστευτήρια για τον application server, κρυπτογραφημένα με το session key που ανέκτησε ο TGS από το TGT. Περιέχεται το καινούργιο session key που θα χρησιμοποιηθεί για την επικοινωνία με τον application server.
Σε περίπτωση λάθους, ο TGS ανταποκρίνεται με μήνυμα λάθους που περιέχει τον κατάλληλο κώδικά λάθους.
Το σχήμα 2.10 αναπαριστά την ολοκληρωμένη διαδικασία



1. αίτηση για TGT
2. λήψη TGT
3. αίτηση για server ticket
4. λήψη server ticket
5. αίτηση υπηρεσίας

Σχήμα 2.9: Πρωτόκολλα ταυτοποίησης του Κέρβερου

2.9.5 Προστασία Δεδομένων

Υπάρχουν δύο τρόποι για την προστασία των δεδομένων. Με την εφαρμογή κρυπτογράφησης προστατεύεται το απόρρητο της επικοινωνίας, ενώ με την εφαρμογή hash αλγόριθμων διαφυλάσσεται η ακεραιότητα της πληροφορίας. Ο πρώτος τρόπος προστασίας παράγει τα μηνύματα τύπου KRB_SAFE και ο δεύτερος τρόπος παράγει τα μηνύματα τύπου KRB_PRIV.

2.9.5.1 Δημιουργία Αδιάβλητων Μηνυμάτων (KRB_SAFE)

Όταν ο χρήστης επιθυμεί να μπορεί να ανιχνεύει τυχών τροποποιήσεις των μηνυμάτων που λαμβάνουν χρησιμοποιεί τα μηνύματα τύπου KRP_SAFE. Παράγεται το checksum των δεδομένων του χρήστη μαζί με πληροφορίες ελέγχου, με hash αλγόριθμο, μη αντιστρέψιμο. Το αποτέλεσμα του hash αλγόριθμου κρυπτογραφείται με το session key ή άλλο προσυμφωνημένο κλειδί. Οι πληροφορίες ελέγχου περιλαμβάνουν ένα timestamp και έναν ακέραιο αριθμό ακολουθίας, που χρησιμοποιούνται για προσδιορισμό του μηνύματος και καταπολέμηση του φαινομένου της επίθεσης επανάληψης (replay attack).
Η εφαρμογή που λαμβάνει τέτοιο μήνυμα πρώτα ελέγχει την ώρα στο πεδίο timestamp και τον ακέραιο αριθμό ακολουθίας. Αν ο έλεγχος έχει θετικό αποτέλεσμα, υπολογίζεται το checksum των δεδομένων και της πληροφορίας ελέγχου και συγκρίνεται με το παραληφθέν checksum. Σε περίπτωση που η σύγκριση δεν πετύχει, επιστρέφεται στην πηγή του μηνύματος, μήνυμα που προειδοποιεί για την τροποποίηση του μηνύματος.

2.9.5.2 Δημιουργία Απόρρητων Μηνυμάτων (KRB_PRIV)

Χρησιμοποιείται από χρήστες που θέλουν εξασφαλίσουν την ακεραιότητα των ανταλλασσωμένων δεδομένων. Η εφαρμογή του χρήστη συλλέγει τα δεδομένα μαζί με την πληροφορία ελέγχου και τα κρυπτογραφεί με το sub-session key ή με το session key. Η πληροφορία ελέγχου περιλαμβάνει ένα timestamp και έναν ακέραιο αριθμό ακολουθίας, που χρησιμοποιούνται για προσδιορισμό του μηνύματος και καταπολέμηση του φαινομένου της επίθεσης επανάληψης (replay attack).
Όταν μία εφαρμογή λαμβάνει ένα κρυπτογραφημένο μήνυμα πρώτα αποκρυπτογραφεί τα δεδομένα και μετά από επεξεργασίας του αποφαίνεται εάν είναι τροποποιημένα. Έπειτα ελέγχει την ώρα στο πεδίο timestamp και τον ακέραιο αριθμό ακολουθίας. Δεδομένου ότι και οι δύο έλεγχοι είναι επιτυχής, το μήνυμα θεωρείται ότι έχει μεταδοθεί με ασφάλεια.

2.9.6 Αλγόριθμοι Προστασίας

2.9.6.1 Αλγόριθμοι Κρυπτογράφησης

Τα κρυπτογραφημένα περιεχόμενα παράγονται με την εφαρμογή του καθορισμένου αλγόριθμου στα δεδομένα και σε βοηθητικές πληροφορίες που σχετίζονται με το αλγόριθμο. Οι μηχανισμοί κρυπτογράφησης που χρησιμοποιεί ο Kerberos πρέπει να μπορούν να εγγυηθούν την ακεραιότητα των δεδομένων και συνίστανται μέτρα για την προστασία από επιθέσεις λεξικού *(dictionary attacks)*. Γι' αυτό το σκοπό προστίθονται τα βοηθητικά πεδία και checksum αλγόριθμοι. Οι checksum αλγόριθμοι εφαρμόζονται στα περιεχόμενα προς κρυπτογράφηση και στις βοηθητικές

πληροφορίες. Το αποτέλεσμα τους συνοδεύει τα πραγματικά δεδομένα και κρυπτογραφείται μαζί με αυτά.
Σε κατάλληλο πεδίο στην αρχή του μηνύματος και εκτός των κρυπτογραφημένων περιεχομένων, δηλώνεται ο μηχανισμός που χρησιμοποιείται. Εδώ πρέπει να πούμε ότι στις αιτήσεις πιστοποίησης ταυτότητας περιλαμβάνεται πεδίο που ανακοινώνει την προτίμηση του client όσον αναφορά τον μηχανισμό κρυπτογράφησης.
Το Kerberos υποστηρίζει τους εξής μηχανισμούς:

- DES in CBC mode σε συνδυασμό με τον CRC-32 checksum αλγόριθμο.
- DES in CBC mode σε συνδυασμό με τον MD4 checksum αλγόριθμο.
- DES in CBC mode σε συνδυασμό με τον MD5 checksum αλγόριθμο.

2.9.6.2 Αλγόριθμοι Παραγωγής Checksum

Οι μηχανισμοί παραγωγής checksum μπορούν να διακριθούν σε αυτούς που το αποτέλεσμα των hash αλγόριθμων δεν κρυπτογραφείται και σε αυτούς που χρησιμοποιούνται μαζί με αλγόριθμους κρυπτογράφησης για την παραγωγή κρυπτογραφημένων hash values. Συνιστάται το πρώτο είδος μηχανισμών να εφαρμόζεται μόνο σε περιπτώσεις που ακολουθεί κρυπτογράφηση. Το δεύτερο είδος θεωρείται πιο ασφαλές.
Το Kerberos υποστηρίζει τους εξής μηχανισμούς παραγωγής checksum:

- MD4 checksum algorithm.
- MD4 σε συνδυασμό με τον DES.
- MD5 checksum algorithm.
- MD5 σε συνδυασμό με τον DES.

2.9.7 Cross-Realm Authentication

Μέχρι τώρα θεωρήσαμε ότι το δίκτυο ήταν αρκετά μικρό ώστε ένα Key Distribution Center, αποτελούμενο από έναν Ticket Granting Server και έναν Authentication Server, να είναι αρκετό για να εξυπηρετήσει τις ανάγκες όλων των μηχανών – client. Όσο μεγαλώνει το δίκτυο όμως, ο αριθμός των αιτήσεων αυξάνεται και η εξυπηρέτηση γίνεται αργή. Είναι πολλές φορές, λοιπόν, προτιμότερο έως και απαραίτητο να διαχωρίζουμε το δίκτυο σε μικρότερα κομμάτια που καλούνται realms, που το καθένα έχει το δικό του TGS και AS. Συνήθως τα όρια των realms ταυτίζονται με τα όρια των εταιριών, αν και αυτό δεν υποχρεωτικό.
Η διαδικασία *cross-realm authentication* επιτρέπει σε ένα χρήστη να αποδείξει την ταυτότητα του σε έναν application server διαφορετικού realm. Για να επιτευχθεί αυτό ο client ζήτα ένα TGT για τον απομακρυσμένο application server από τον τοπικό AS. Μία τέτοια ενέργεια απαιτεί ο τοπικός AS και ο απομακρυσμένος AS στον οποίο είναι εγγεγραμμένος ο απομακρυσμένος application server να μοιράζονται ένα κλειδί γνωστό ως cross-realm key. Ο client χρησιμοποιεί το αποκτηθέν TGT για να κάνει αίτηση για ticket από τον απομακρυσμένο AS για τον application server του άλλου realm. Ο απομακρυσμένος AS ανιχνεύει ότι το TGT έχει εκδοθεί σε διαφορετικό realm, βρίσκει το cross-realm key που μοιράζεται με τον AS του άλλου realm, επαληθεύει την εγκυρότητα του TGT και τέλος εκδίδει ticket και session key για τον client. Μέσα στο ticket περιέχεται έκτος από το όνομα του client αλλά και το όνομα του απομακρυσμένου realm.

Στην 4η έκδοση του Kerberos, ήταν απαραίτητο για έναν AS να μοιράζεται cross-realm κλειδιά με όλους του απομακρυσμένους AS, γεγονός που δυσχέραινε αφάνταστα την επικοινωνία. Αρκεί να πούμε ότι για πλήρη διασύνδεση απαιτούνταν ανταλλαγή n^2 κλειδιών όπου n ο αριθμός των realms.
Σε αντίθεση, η 5η έκδοση του Kerberos υποστηρίζει την ιεραρχική διανομή των κλειδιών. Τα realms κατανέμονται ιεραρχικά και κάθε realm μοιράζεται κλειδιά με τα θυγατρικά του realms και με το γονικό του. Για παράδειγμα το realm ISI.EDU μοιράζεται κλειδί με το realm EDU, το οποίο με την σειρά του μοιράζεται κλειδιά με τα MIT.EDU, USC.EDU και WASHINGTON.EDU. Η πιστοποίηση της ταυτότητας ενός client στο realm ISI.EDU σε ένα application server στο realm MIT.EDU γίνεται με την απόκτηση ενός TGT από τον AS στο ISI.EDU για το EDU, με χρήση αυτού του TGT για την απόκτηση νέου TGT από τον AS του EDU για τον AS του MIT.EDU και τέλος με αποστολή αίτησης στον AS του MIT.EDU ζητώντας ticket για επικοινωνία με τον application server.
Η λίστα όλων των realms τα οποία έχει διασχίσει αίτηση του client καταγράφονται στο τελικό ticket και ο authentication server του απομακρυσμένου realm πραγματοποιεί την τελική απόφαση για το κατά πόσο μπορεί να εμπιστευτεί το μονοπάτι που ακολουθήθηκε. Η επιλογή μικρότερων διαδρομών υποστηρίζεται από το μοντέλο, καθ' ότι μπορούν να βελτιώσουν την απόδοση της διαδικασίας.

2.9.8 Αδυναμίες του Kerberos

Το Kerberos δεν έχει την δυνατότητα να προστατέψει ένα δίκτυο από κάθε είδους απειλή. Λειτουργεί βάσει συγκεκριμένων υποθέσεων όσον αναφορά την υποκείμενη δικτυακή δομή.

- Επιθέσεις του τύπου άρνησης εξυπηρέτησης (denial of service attack) δεν μπορούν να αντιμετωπιστούν με το Kerberos. Ένας εισβολέας μπορεί εκμεταλλευόμενος τις αδυναμίες του συστήματος να αποτρέψει έναν server από το να συμμετέχει στα κανονικά βήματα πιστοποίησης. Η ανίχνευση και η επιδιόρθωση τέτοιων καταστάσεων αφήνεται στα χέρια των διαχειριστών και των χρηστών.
- Οι χρήστες πρέπει να κρατούν τους κωδικούς τους μυστικούς. Το Kerberos δεν είναι σε θέση να προστατέψει το δίκτυο από ασυνείδητους χρήστες που μοιράζουν τους κωδικούς τους ή που δεν είναι αρκετά προσεκτικοί για να τον κρατήσουν κρυφό.
- Επιθέσεις που βασίζονται στην πρόβλεψη εύκολων κωδικών (password guessing attack) δεν αντιμετωπίζονται από τον Kerberos. Ένας εισβολέας με χρήση ενός λεξικού, μπορεί εύκολα να "σπάσει" μικρούς και εύκολους κωδικούς που αποτελούνται από λέξεις που μπορούν να βρεθούν σε λεξικό.
- Κάθε μηχανή του δικτύου πρέπει να έχει ένα καλά ρυθμισμένο ρολόι. Μηχανές με ρυθμίσεις ώρας που διαφέρουν σημαντικά (πάνω από 5 λεπτά) μπορεί να δημιουργήσουν πρόβλημα στην πιστοποίηση των timestamps που εμπεριέχονται στα μηνύματα. Έτσι, ένας εισβολέας εκμεταλλευόμενος αυτή την αδυναμία μπορεί να πραγματοποιήσει επίθεση επανάληψης (replay attack). Ή ακόμα βρίσκοντας τον απαραίτητο χρόνο, να σπάσει αδύναμους κωδικούς χρηστών.

2.10 SSH (Secure Shell)

2.10.1 Εισαγωγή

Τα εργαλεία απομακρυσμένης επικοινωνίας *(rsh, rcp, rlogin)* είναι γνωστά για την ευκολία χρήσης τους και την παροχή γρήγορης πρόσβασης σε άλλες μηχανές. Το πρόβλημα, όμως, είναι ότι βασίζονται σε IP διευθύνσεις ή host names για την πιστοποίηση της ταυτότητας των μηχανών, γεγονός που τα καθιστά ανασφαλή καθ' ότι οι υπηρεσίες του DNS δεν είναι άξιες εμπιστοσύνης. Επίσης, η μετάδοση των κωδικών χωρίς κανένα είδος προστασίας οξύνει τις τρύπες ασφαλείας. Για να μπορούν, λοιπόν, να χρησιμοποιούνται σε ασφαλή περιβάλλοντα πρέπει να διαθέτουν πιο καλύτερους μηχανισμούς πιστοποίησης ταυτότητας. Η εισαγωγή της έννοιας της κρυπτογράφησης και των ψηφιακών υπογραφών στα εργαλεία rsh, rcp και rlogin, δημιούργησε το *Secure Shell (SSH)*.
Το SSH σχεδιάστηκε για να αντικαταστήσει τα εργαλεία rsh, rcp και rlogin με τα αντίστοιχα ssh, scp και slogin, με επιπλέον χαρακτηριστικά αυτά της ισχυρής από άκρη σε άκρη κρυπτογράφηση, της βελτιωμένης πιστοποίησης ταυτότητας χρήστη και μηχανής και την προώθηση TCP πορτών και X11 συνδέσεων.

2.10.2 Περιγραφή του SSH πρωτοκόλλου

Το SSH είναι ένα πρωτόκολλο που παρέχει ασφαλή απομακρυσμένη σύνδεση σε υπολογιστές πάνω από μη ασφαλές δίκτυο. Αποτελείται από τρία βασικά στοιχεία:

- **Transport layer protocol**
  Το Transport Layer Protocol είναι ένα ασφαλές χαμηλού επιπέδου πρωτόκολλο μεταφοράς, που παρέχει ισχυρή κρυπτογράφηση, πιστοποίηση του server και ακεραιότητα των δεδομένων. Σε αυτό το επίπεδο γίνεται η διαπραγμάτευση των αλγόριθμων ανταλλαγής κλειδιών, συμμετρικής κρυπτογράφησης, ασύμμετρης κρυπτογράφησης, hash και MAC. Συνήθως τρέχει πάνω από TCP/IP. Η πιστοποίηση ταυτότητας σε αυτό το επίπεδο αναφέρεται μόνο σε πιστοποίηση υπολογιστικών μηχανών και όχι χρηστών. Το User Authentication Protocol αναλαμβάνει την επιβεβαίωση της ταυτότητας των χρηστών.
  Έχει σχεδιαστεί για να είναι απλό, ευέλικτο, να επιτρέπει την διαπραγμάτευση παραμέτρων και να χρησιμοποιεί ένα ελάχιστο αριθμό απαραίτητων μηνυμάτων για την εγκαθίδρυση της σύνδεσης. Για τα περισσότερα περιβάλλοντα, έχει υπολογιστεί ότι ένας αριθμός 2 ανταλλαγών *(round-trips)* είναι αρκετός για πλήρη επικοινωνία όλων των απαραίτητων πληροφοριών. Η χειρότερη περίπτωση είναι 3 round-trips.

- **User Authentication protocol**
  Σε αυτό το πρωτόκολλο γίνεται η πιστοποίηση της ταυτότητας του χρήστη που χειρίζεται το μηχανή του client. Προορίζεται να τρέχει πάνω από το SSH Transport Layer Protocol, το οποίο παρέχει ακεραιτότητα δεδομένων και απόρρητη επικοινωνία. Η πρώτη αίτηση εξυπηρέτησης από τον client μετά την διαπραγμάτευση των αλγορίθμων και πιστοποίηση της ταυτότητας του server, είναι για την υπηρεσία με το όνομα "ssh-userauth"και αναφέρεται σε αυτό το πρωτόκολλο.

Όταν το πρωτόκολλο ξεκινά, λαμβάνει από το Transport Layer Protocol το session identifier που χρησιμοποιείται για να προσδιορίζει την σύνδεση με μοναδικό τρόπο. Ο server οδηγεί την διαδικασία της επαλήθευσης της ταυτότητας του χρήστη, λέγοντας στον client ποιες μέθοδοι μπορούν να εφαρμοστούν. Ο server έχει τον απόλυτο έλεγχο της διαδικασίας, αλλά παράλληλα παρέχει στον client την ευελιξία να επιλέξει τον αλγόριθμο που υποστηρίζει περισσότερο ή που είναι πιο βολική στον χρήστη. Οι υποστηριζόμενες μέθοδοι είναι τρεις: (α) με χρήση των δημοσίων κλείδων των χρηστών, (β) με χρήση μυστικών κωδικών και (γ) με χρήση των δημοσίων κλείδων των μηχανών που εργάζονται οι χρήστες. Θα αναλυθούν και οι τρεις παρακάτω.

- **Connection protocol**
  Το Connection Protocol έχει σχεδιαστεί για να τρέχει πάνω από το SSH Transport Layer Protocol και το User Authentication Protocol. Παρέχει interactive login session, απομακρυσμένη εκτέλεση εντολών, προώθηση TCP/IP και X11 συνδέσεων. Οι υπηρεσίες του έπονται των υπηρεσιών του User Authentication Protocol και αναγνωρίζονται από το όνομα "ssh-connection".

2.10.3 Δομή του SSH

2.10.3.1 Ιδιωτικά και Δημόσια Κλειδιά

Κάθε server και client πρέπει να έχει ένα ζευγάρι ιδιωτικού – δημόσιου κλείδιού για να μπορεί να επαλήθευση την ταυτότητα του στο άλλο άκρο. Επιτρέπεται η κατοχή περισσότερων του ενός ζευγάρια κλειδιών, όταν χρησιμοποιούνται με διαφορετικούς αλγόριθμους, ενώ η από κοινού χρήση ενός ζεύγους από πολλούς server δεν απαγορεύεται.

Για να μπορεί ο client με ευκολία να επαληθεύει την ταυτότητα του server είναι απαραίτητο να γνωρίζει το δημόσιο κλειδί που αντιστοιχεί στον server που θέλει να συνδεθεί. Υπάρχουν δυο διαφορετικά μοντέλα που εξασφαλίζουν την προηγούμενη προϋπόθεση:

- Πρώτον, ο client έχει αποθηκευμένα σε μια τοπική βάση δεδομένων τα ονόματα των server και τις σχετιζόμενες με αυτά δημόσιες κλείδες. Αυτή η μέθοδος δεν απαιτεί μια κεντρική διαχείριση των κλειδιών από τρίτους. Το μειονέκτημα είναι ότι το μέγεθος μιας τέτοιας βάσης δεδομένων μπορεί να εξελιχθεί σημαντικά και συνεπώς η συντήρηση της να γίνει δύσκολη.
- Στην δεύτερη περίπτωση, σχέση μεταξύ του ονόματος του server και του κλειδιού του πιστοποιείται από μια άξια εμπιστοσύνης Certification Authority. Το πρόγραμμα του πελάτη γνωρίζει μόνο την δημόσια κλείδα της Certification Authority και μπορεί να επιβεβαιώσει την εγκυρότητα των κλείδων που έχουν πιστοποιηθεί από την CA. Εδώ δεν υπάρχει το πρόβλημα της διατήρησης μεγάλων βάσεων δεδομένων από τα τοπικά συστήματα, αφού μόνο ένα κλειδί χρειάζεται να αποθηκεύει ο client. Από την άλλη μεριά, όμως, δεν είναι δυνατή η απόλυτη εμπιστοσύνη στις διαδικασίες της Certification Authority. Επίσης, πιστοποίηση κάθε κλειδιού μπορεί να είναι μια χρονοβόρα και περίπλοκή διαδικασία.

Οι εφαρμογές του SSH μπορούν να παρέχουν επιπρόσθετες μεθόδους επικύρωσης των δημόσιων κλειδιών, όπως για παράδειγμα την παραγωγή ενός δεκαεξαδικού "αποτυπώματος" της κλείδας και από τα δύο άκρα και την σύγκριση τους μέσω εξωτερικών καναλιών επικοινωνίας (π.χ. τηλέφωνο). Κλείδες που δεν επαληθεύονται, κανονικά δεν πρέπει να γίνονται δεκτές.

2.10.3.2 Επεκτασιμότητα

Βασικός στόχος της σχεδίασης είναι η διατήρηση του πρωτοκόλλου όσο το δυνατόν απλό γίνεται, με όσο το δυνατόν λιγότερους αλγόριθμους. Όλες οι εφαρμογές πρέπει να υποστηρίζουν ένα ελάχιστο σύνολο αλγόριθμων για να εξασφαλιστεί η δια – λειτουργικότητα. Στο μέλλον αναμένεται η πρόσθεση και άλλων αλγορίθμων.

2.10.3.3 Θέματα Πολιτικής

Το πρωτόκολλο επιτρέπει την διαπραγμάτευση όλων των χρησιμοποιούμενων αλγορίθμων. Έτσι, οι αλγόριθμοι κρυπτογράφησης, ανταλλαγή κλειδιών και συμπίεσης καθώς επίσης και οι μηχανισμοί ασύμμετρων κλειδιών και παροχής ακεραιότητας, μπορούν να επιλεγούν από λίστες που παρέχουν ο client και ο server ο ένας στον άλλο και μάλιστα διαφορετικοί για κάθε κατεύθυνση. Η πολιτική ασφαλείας κάθε συστήματος καθορίζει ποιοι προτιμούνται.
Τα παρακάτω θέματα πολιτικής θα πρέπει υπολογίζονται κατά την ρύθμιση SSH εφαρμογών:

- Οι αλγόριθμοι και οι μηχανισμοί που πρόκειται να χρησιμοποιηθούν για κάθε κατεύθυνση. Πρέπει να ορίζεται ποιος προτιμάται.
- Η μέθοδοι πιστοποίησης της ταυτότητας, ξεχωριστοί για κάθε χρήστη που θα εφαρμόζει ο server. Η πολιτική του server μπορεί να ζητά πολλαπλές διαδικασίες πιστοποίησης για μερικού ή όλους τους χρήστες, ενώ οι απαιτούμενοι αλγόριθμοι μπορούν να εξαρτώνται από την τοποθεσία από όπου προσπαθεί να συνδεθεί ο χρήστης.
- Οι ενέργειες που επιτρέπονται σε κάθε χρήστη και στον server. Η πολιτική ασφαλείας δεν θα πρέπει να επιτρέπει στον server να εκτελεί εντολές στην μηχανή του χρήστη ούτε στον χρήστη να συνδέεται στον authentication server.

2.10.3.4 Ιδιότητες Ασφάλειας

Ο πρωταρχικός στόχος του SSH πρωτοκόλλου είναι η βελτίωση της ασφάλειας στο Internet και ο τρόπος με τον οποίο προσπαθεί να το επιτύχει αυτό βασίζεται στο εξής σκεπτικό:

- Όλοι οι αλγόριθμοι κρυπτογράφησης, παροχής ακεραιότητας και ανταλλαγής κλειδιών έχουν δοκιμαστεί και
- Οι αλγόριθμοι χρησιμοποιούν κλειδιά μεγέθους ικανού να παρέχει προστασία απέναντι στις ισχυρότερες επιθέσεις κρυπτοανάλυσης.
- Στην περίπτωση που κάποιος αλγόριθμος "σπάσει", είναι εύκολη η αντικατάσταση του από κάποιον άλλο χωρίς αλλαγές στις βάσεις του SSH.

Για την ταχεία ανάπτυξη και υιοθέτηση του πρωτοκόλλου, κάποιες έχουν γίνει παραχωρήσεις. Σημαντικότερη από αυτές είναι η καθιέρωση της επαλήθευσης των κλείδων με υποχρεωτική, γεγονός όμως που δεν συνιστάται.

ΚΕΦΑΛΑΙΟ 3
SSL (SECURE SOCKET LAYER)

Το πρωτόκολλο SSL αναπτύχθηκε από την Netscape Communications με σκοπό την ασφαλή επικοινωνία στο internet ευαίσθητων πληροφοριών όπως, προσωπικών δεδομένων και πιστωτικών καρτών.
Σήμερα έχει γίνει πλέον αποδεκτό από την παγκόσμια κοινότητα του internet σαν το καλύτερο standard για κωδικοποιημένη επικοινωνία και σωστό authentication μεταξύ clients και servers.

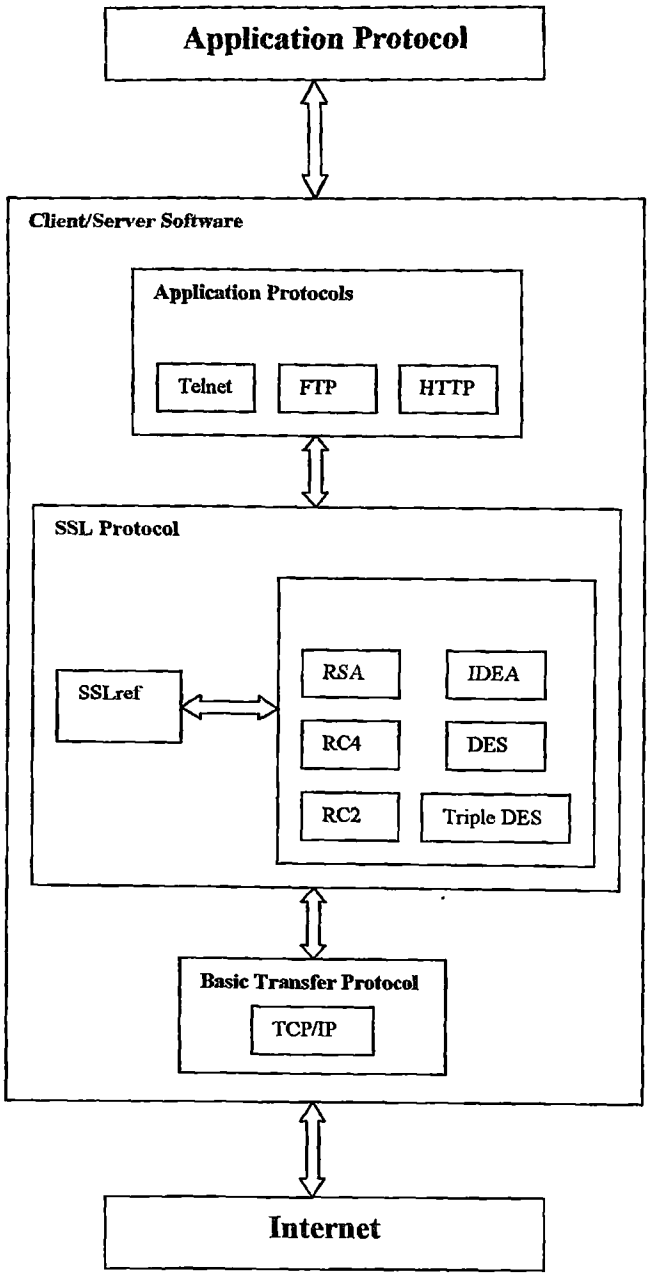
3.1 Τι είναι το SSL

Το SSL είναι ένα γενικού σκοπού πρωτόκολλο για την αποστολή κρυπτογραφημένης πληροφορίας μέσω internet. Είναι ένα «στρώμα» που τοποθετείται ανάμεσα στο internet και στον web browser (π.χ. Netscape). Κρυπτογραφεί τις πληροφορίες που φεύγουν από τον client και ταξιδεύουν μέσω του internet στον server. Εκεί αποκρυπτογραφούνται και πάλι όλα τα δεδομένα. Το στρώμα αυτό θα πρέπει να υποστηρίζεται από την εκάστοτε εφαρμογή (π.χ. Netscape, Internet Explorer) για να ενεργοποιηθεί και να αξιοποιηθεί. Έχει σχεδιαστεί να παρέχει απόρρητη επικοινωνία μεταξύ δύο συστημάτων, εκ των οποίων το ένα λειτουργεί σαν client και το άλλο σαν server, προσφέροντας αξιόπιστη από άκρο σε άκρο (end to end) ασφαλή υπηρεσία. Για παράδειγμα κάνοντας κανείς χρήση του SSL μπορεί να εισάγει τον αριθμό της πιστωτικής του κάρτας σε μία ασφαλή φόρμα μέσω του web browser και να την μεταδώσει μέσω του internet σε έναν ασφαλή server χωρίς τον κίνδυνο μιας ενδιάμεσης αποκάλυψης της μεταφερόμενης πληροφορίας.
Το Transmission Control Protocol / Internet Protocol (TCP/IP)είναι υπεύθυνο για τον τρόπο μεταφοράς των δεδομένων στο internet. Άλλα πρωτόκολλα όπως το HTTP, IMAP, LDAP τρέχουν πάνω από το TCP/IP και φροντίζουν για τυπικές διαδικασίες, όπως η σωστή απεικόνιση web pages ή εφαρμογές e-mail. Ακριβώς με τον ίδιο τρόπο τρέχει και το πρωτόκολλο SSL. Για την ακρίβεια τρέχει πάνω από το TCP/IP πρωτόκολλο και κάτω από άλλα πρωτόκολλα όπως HTTP, IMAP, TELNET. Χρησιμοποιεί το TCP/IP εκ μέρους άλλων πρωτοκόλλων και επιτρέπει σε έναν SSL server να κάνει σωστό authentication σε έναν client και φυσικά το αντίστροφο.
Το SSL είναι ένα επεκτάσιμο και εύκολα προσαρμόσιμο πρωτόκολλο. Αν τα δύο μέρη της επικοινωνίας δεν χρησιμοποιούν τους ίδιους αλγορίθμους, τα κρυπτογραφικά πρωτόκολλα δεν δουλεύουν. Γι αυτό όταν ένα πρόγραμμα που χρησιμοποιεί SSL προσπαθεί να επικοινωνήσει με ένα άλλο, τότε τα δύο προγράμματα συγκρίνουν ηλεκτρονικά τα στοιχεία και καθορίζουν ποιος είναι ο δυνατότερος κρυπτογραφικός αλγόριθμος που διαθέτουν από κοινού.
Οι υπηρεσίες που παρέχει το SSL είναι:

- Παρέχει εμπιστευτικότητα με την κρυπτογράφηση των δεδομένων
- Παρέχει ακεραιότητα των δεδομένων εφαρμόζοντας την τεχνική Massage Authentication Codes (MACs)
- Παρέχει επικύρωση της ταυτότητας του server ή και του client(προαιρετικά) με υπογεγραμμένα ψηφιακά πιστοποιητικά, τα οποία εκδίδονται από

έμπιστους τρίτους, οι οποίοι αποτελούν πηγές πιστοποιητικών. (certificate authorities)

Στο Σχήμα 3.1 βλέπουμε τη σχέση μεταξύ του SSL, των εφαρμογών και του δικτύου.



Σχήμα 3.1: Σχέση μεταξύ SSL, εφαρμογών και δικτύου

Μεγάλη εφαρμογή του συγκεκριμένου πρωτοκόλλου συναντάμε σε εφαρμογές που απαιτούν υψηλή ασφάλεια, όπως για παράδειγμα web-banking, web-shopping όπου ο χρήστης πιθανότατα καταφεύγει στην αποστολή προσωπικών δεδομένων και αριθμών πιστωτικών καρτών. Η υποκλοπή τέτοιων πληροφοριών είναι ότι χειρότερο και τις περισσότερες φορές έχει άσχημες συνέπειες. Το SSL έρχεται λοιπόν να

κρυπτογραφήσει τα δεδομένα με τέτοιο (αξιόπιστο) τρόπο, έτσι ώστε να μην μπορεί κανείς να τα υποκλέψει.

3.2 Χαρακτηριστικά του SSL

Το SSL 3.0 προσφέρει πολλά χαρακτηριστικά θεωρητικού αλλά και πρακτικού ενδιαφέροντος:

3.2.1 Διαχωρισμός των καθηκόντων

Το SSL χρησιμοποιεί ξεχωριστούς αλγόριθμους για την κρυπτογράφηση, την απόδειξη γνησιότητας και την ακεραιότητα των δεδομένων με διαφορετικά κλειδιά (που ονομάζονται "μυστικά", secrets) για κάθε λειτουργία. Το βασικό πλεονέκτημα αυτού του διαχωρισμού των καθηκόντων είναι ότι τα μεγαλύτερα κλειδιά μπορούν να χρησιμοποιηθούν για την απόδειξη γνησιότητας και για την ακεραιότητα των δεδομένων, ενώ τα μικρότερα κλειδιά να χρησιμοποιούνται για την μυστικότητα. Αυτό είναι χρήσιμο για τα προϊόντα που σχεδιάζονται με σκοπό την εξαγωγή τους από τις Ηνωμένες Πολιτείες, επειδή ομοσπονδιακές ρυθμίσεις τοποθετούν περιορισμούς στο θέμα του μήκους των κλειδιών που χρησιμοποιούνται για την εμπιστευτικότητα ενώ δεν χρησιμοποιούνται περιορισμοί για την περίπτωση της ακεραιότητας των δεδομένων και της απόδειξης γνησιότητας.

3.2.2 Αποτελεσματικότητα

Η κρυπτογράφηση και αποκρυπτογράφηση δημόσιου κλειδιού είναι μια χρονοβόρα διαδικασία. Πόσο μάλλον όταν επαναλαμβάνεται αυτή η επεξεργασία για κάθε επικοινωνία ανάμεσα στον client και σε έναν server. Οι SSL εφαρμογές μπορούν να αποθηκεύουν κρυφά ένα μυστικό "master secret" που διατηρείται
αναλλοίωτο μεταξύ των SSL συνδέσεων. Αυτό επιτρέπει στις καινούργιες SSL συνδέσεις να ξεκινήσουν αμέσως την ασφαλή επικοινωνία, χωρίς να χρειάζεται να εκτελεστούν περισσότερες λειτουργίες δημόσιου κλειδιού.

3.2.3 Πιστοποιητικό βασισμένο στην απόδειξη γνησιότητας

Το SSL παρέχετε για την απόδειξη γνησιότητας και των δύο, του client και του server, μέσω της χρήσης των ψηφιακών πιστοποιητικών και των ψηφιακά υπογεγραμμένων προκλήσεων αναγνώρισης.
Το SSLv3 χρησιμοποιεί τα X.509 v3 πιστοποιητικά, μολονότι η IETF (Internet Engineering Task Force) τυποποίηση του SSL (ονομάζεται TLS) ίσως χρησιμοποιεί διαφορετικά είδη πιστοποιητικών καθώς είναι τυποποιημένα. Η απόδειξη γνησιότητας είναι ένα προαιρετικό μέρος του πρωτοκόλλου, μολονότι τα πιστοποιητικά του server είναι αποτελεσματικά εξουσιοδοτημένα από τις σημερινές SSL εφαρμογές.

3.2.4 Αγνωστικό πρωτόκολλο (Protocol Agnostic)

Αν και το SSL σχεδιάστηκε για να τρέχει στην κορυφή του TCP/IP, στην πραγματικότητα μπορεί να τρέξει στην κορυφή κάθε αξιόπιστου connection-oriented πρωτοκόλλου, όπως είναι το x.25. Το SSL πρωτόκολλο *δεν μπορεί* να "τρέξει" στην κορυφή ενός μη αξιόπιστου πρωτοκόλλου όπως είναι το IP User Datagram Protocol (UDP).

Όλη η SSL επικοινωνία παίρνει μέρος πάνω σε ένα απλό διπλής κατεύθυνσης ρεύμα. Στην περίπτωση του TCP/IP, οι πόρτες που χρησιμοποιούνται συνήθως είναι αυτές του παρακάτω πίνακα.

Λέξη κλειδί	Θύρα	Περιγραφή
https	443/tcp	HTTP με υποστήριξη SSL
ssmtp	465/tcp	SMTP (mail sending) με υποστήριξη SSL
snews	563/tcp	Usenet News με υποστήριξη SSL
ssl-ldap	636/tcp	LDAP με υποστήριξη SSL
spop3	995/tcp	POP3 (mail retrieving) με υποστήριξη SSL

3.2.5 Υποστήριξη για συμπίεση

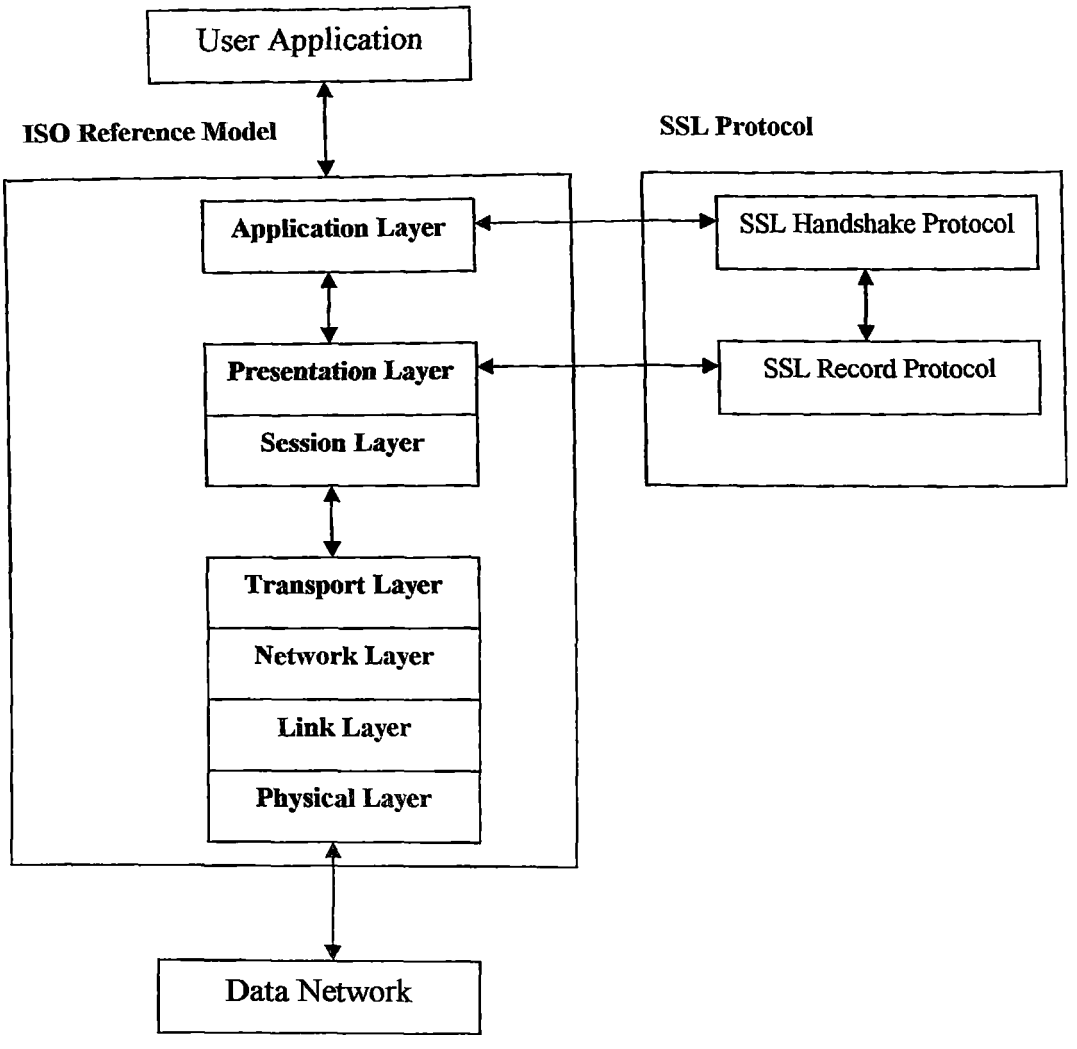
Επειδή τα κρυπτογραφημένα δεδομένα δεν μπορούν να συμπιεστούν, το SSL εξασφαλίζει για το μέλλον την ικανότητα να συμπιέζει τα δεδομένα του χρήστη πριν αυτά κρυπτογραφηθούν. Το SSL υποστηρίζει πολλούς αλγόριθμους συμπίεσης. Ωστόσο δεν υπάρχει σήμερα κάποια SSL εφαρμογή που να ενσωματώνει την συμπίεση. (Σημείωση: Τα κρυπτογραφημένα δεδομένα δεν μπορούν να συμπιεστούν επειδή η καλή κρυπτογράφηση μετακινεί δραστικά κάθε επανάληψη ή ομοιότητα που είναι μετακινημένη κατά την διάρκεια της συμπίεσης. Εάν τα κρυπτογραφημένα δεδομένα μας μπορούν να συμπιεστούν, τότε η κρυπτογράφηση μας δεν είναι πολύ καλή).

3.3 SSL και μοντέλο OSI

Είναι σημαντικό κάθε νέο πρωτόκολλο επικοινωνίας να προσαρμόζεται σε ένα τυποποιημένο πρότυπο έτσι ώστε να μπορέσει εύκολα να αντικαταστήσει ένα υπάρχον πρωτόκολλο ή να ενσωματωθεί στην υπάρχουσα δομή πρωτοκόλλων. Το SSL προσαρμόζεται στο μοντέλο 7 στρωμάτων του OSI.

Το SSL αποτελείται από δύο υπο-πρωτόκολλα, το SSL Record Protocol (SSLRP) και το SSL Handshake Protocol (SSLHP). Το SSL Record Protocol ορίζει το βασικό format των δεδομένων που ανταλλάσσονται σε κάθε session. Κάνει την συμπίεση των δεδομένων, τον έλεγχο ακεραιότητας και κρυπτογραφεί τα δεδομένα. Προκειμένου το SSL Record Protocol να κάνει την κρυπτογράφηση, να υπολογίσει την τιμή του ελέγχου ακεραιότητας, πρέπει και ο client και ο server να γνωρίζουν τα κρυπτογραφικά κλειδιά. Το πρωτόκολλο υποστηρίζει την αλλαγή των αλγορίθμων κρυπτογράφησης και των κλειδιών οποιαδήποτε στιγμή. Το SSL Handshake Protocol χρησιμοποιείται για τη διαπραγμάτευση του αλγορίθμου κρυπτογράφησης που θα χρησιμοποιηθεί, την ανταλλαγή των πιστοποιητικών και την ανταλλαγή των κλειδιών που θα χρησιμοποιηθούν στο session.

Στο σχήμα 2 μπορούμε να δούμε ότι το SSL ενεργεί επιπρόσθετα της υπάρχουσας δομής του OSI και όχι σαν πρωτόκολλο αντικατάστασης. Επίσης μπορεί να φανεί ότι η χρήση του SSL δεν αποκλείει την χρήση άλλων πρωτοκόλλων ασφάλειας που λειτουργούν σε υψηλότερο επίπεδο.



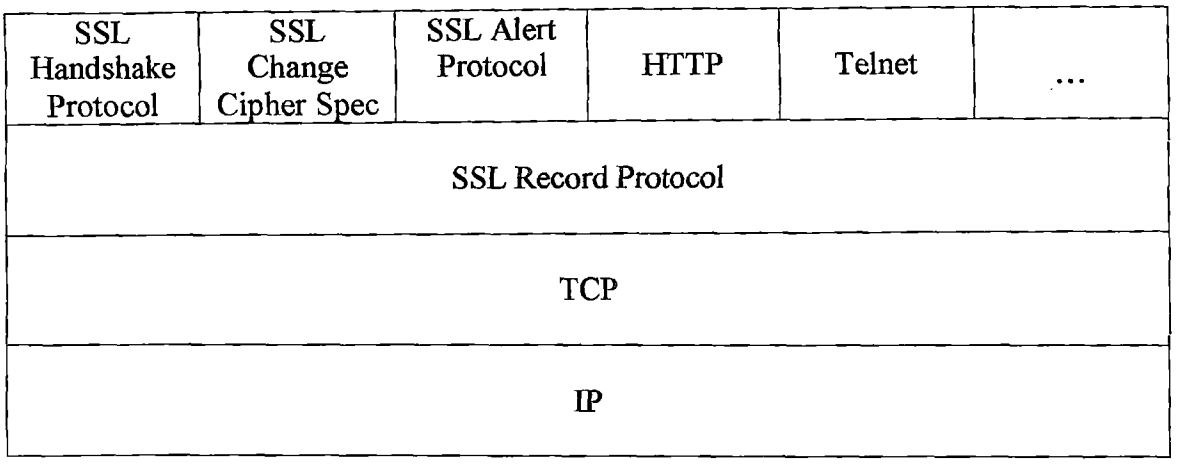
Σχήμα 3.2: Σχέση μεταξύ του SSL και του μοντέλου OSI

3.4 Αρχιτεκτονική του SSL

Το SSL Record Protocol παρέχει τις βασικές υπηρεσίες ασφάλειας στα διάφορα πρωτόκολλα υψηλότερου επιπέδου. Τρία πρωτόκολλα υψηλότερου επιπέδου ορίζονται ως τμήματα του SSL: το Handshake protocol, το Change Cipher Spec Protocol, και το Alert Protocol. Αυτά τα SSL-specific πρωτόκολλα χρησιμοποιούνται στη διαχείριση των SSL ανταλλαγών .
Δύο σημαντικές έννοιες του SSL είναι η σύνδεση (connection) και η σύνοδος (session)

- Σύνδεση (connection): Μια λογική σύνδεση client/server που παρέχει έναν κατάλληλο τύπο υπηρεσίας. Για το SSL, τέτοιες συνδέσεις είναι ένα προς ένα σχέσεις. Οι συνδέσεις είναι παροδικές. Κάθε σύνδεση σχετίζεται με μιασύνοδο.
  Σύνοδος (session): Μια συσχέτιση μεταξύ ενός client και ενός server. Οι σύνοδοι δημιουργούνται από το Handshake Protocol. Οι σύνοδοι καθορίζουν ένα σύνολο κρυπτογραφικών παραμέτρων ασφάλειας, οι

οποίες μπορούν να διαμοιραστούν σε πολλαπλές συνδέσεις. Οι σύνοδοι χρησιμοποιούνται για να αποφύγουν πολύπλοκες διαπραγματεύσεις των νέων παραμέτρων ασφάλειας για κάθε σύνδεση.



Σχήμα 3.3: Η στοίβα του SSL

Μεταξύ οποιουδήποτε ζευγαριού των συμβαλλόμενων μερών (εφαρμογές όπως το HTTP στον client και τον server), μπορούν να υπάρξουν πολλαπλές ασφαλείς συνδέσεις. Θεωρητικά, μπορούν επίσης να υπάρξουν πολλαπλές ταυτόχρονες σύνοδοι μεταξύ των συμβαλλόμενων μερών, αλλά αυτό το χαρακτηριστικό δεν χρησιμοποιείται στην πράξη.
Διάφορες καταστάσεις σχετίζονται με κάθε σύνοδο. Όταν μια σύνοδος καθιερώνεται, υπάρχει μια τρέχουσα λειτουργούσα κατάσταση και για διάβασμα και για γράψιμο (δηλαδή λήψη και αποστολή). Επιπλέον, κατά τη διάρκεια του Handshake Protocol δημιουργούνται καταστάσεις για γράψιμο και διάβασμα και θέτονται σε αναμονή. Μετά από επιτυχή τερματισμό του Handshake Protocol οι καταστάσεις σε αναμονή γίνονται τρέχουσες. Μία κατάσταση συνόδου καθορίζεται από τις ακόλουθες παραμέτρους:

- **Session Identifier:** Μια αυθαίρετη ακολουθία από bytes που επιλέγεται από τον server για να προσδιορίσει μία ενεργή ή resumable κατάσταση συνόδου.
- **Peer Certificate:** Ένα όμοιο πιστοποιητικό X509.v3. Αυτό το στοιχείο (της κατάστασης) μπορεί να είναι μηδενικό.
- **Compression method:** Ο αλγόριθμος που χρησιμοποιείται για να συμπιέσει τα στοιχεία πριν από την κρυπτογράφηση.
- **Cipher Spec:** Διευκρινίζει τον αλγόριθμο κρυπτογράφησης (όπως DES) και έναν αλγόριθμο σύνοψης (hash) (όπως MD5 ή SHA-1). Καθορίζει επίσης τις κρυπτογραφικές ιδιότητες όπως το hash μέγεθος.
- **Master Secret:** 48-byte μυστικό διαμοιραζόμενο μεταξύ του client και του server.
- **είναι resumable:** Μια μεταβλητή που δείχνει εάν η σύνοδος μπορεί να χρησιμοποιηθεί για να αρχίσει τις νέες συνδέσεις.

Μία κατάσταση σύνδεσης καθορίζεται από τις ακόλουθες παραμέτρους:

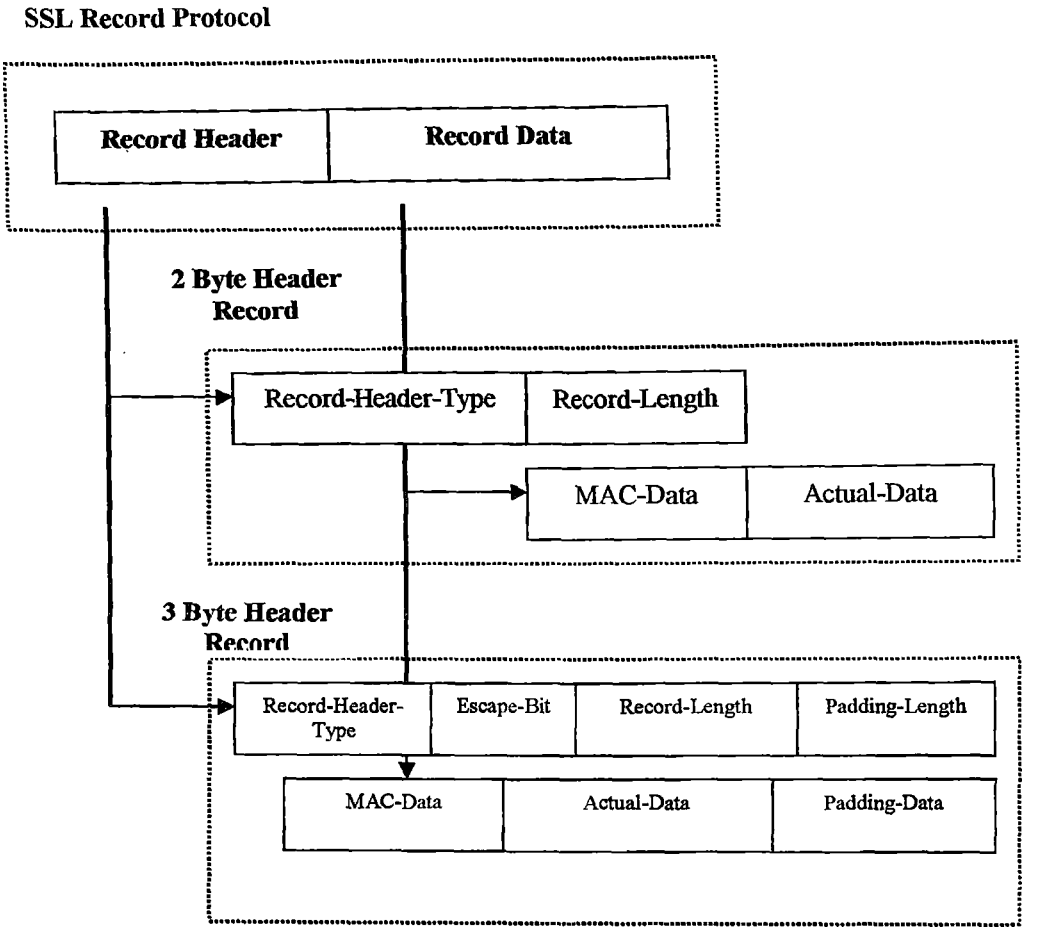
- **Server and client random:** Ακολουθίες από bytes που επιλέγονται από τον server και τον client για κάθε σύνδεση.
- **Server write MAC secret:** Το μυστικό κλειδί που χρησιμοποιείται σε MAC λειτουργίες στα δεδομένα που στέλνονται από τον server.
- **Client write MAC secret:** Το μυστικό κλειδί που χρησιμοποιείται σε MAC λειτουργίες στα δεδομένα που στέλνονται από τον client.
- **Server write key:** Το συμβατικό κλειδί κρυπτογράφησης για τα δεδομένα που κρυπτογραφούνται από τον server και που αποκρυπτογραφούνται από τον client.
- **Client write key:** Το συμβατικό κλειδί κρυπτογράφησης για τα δεδομένα που κρυπτογραφούνται από τον client και που αποκρυπτογραφούνται από τον server.
- **Initialization vectors:** Όταν χρησιμοποιείται ένας block-cipher CBC, ένα Initialization vector (IV) διατηρείται για κάθε κλειδί. Αυτό το πεδίο αρχικά Initialized από το SSL Handshake Protocol. Έκτοτε το τελικό block του κρυπτογραφήματος συντηρείται από κάθε εγγραφή για τη χρήση ως IV για την επόμενο εγγραφή.
- **Sequence numbers:** Κάθε συμβαλλόμενο μέρος διατηρεί χωριστούς τους αριθμούς ακολουθίας για τα μεταδιδόμενα και λαμβανόμενα μηνύματα για κάθε σύνδεση. Όταν ένα συμβαλλόμενο μέρος στέλνει ή λαμβάνει ένα Change Cipher Spec message, ο κατάλληλος αριθμός ακολουθίας τίθεται μηδέν.

3.5 SSL Record Protocol

Το SSL Record Protocol παρέχει δύο υπηρεσίες για SSL συνδέσεις:

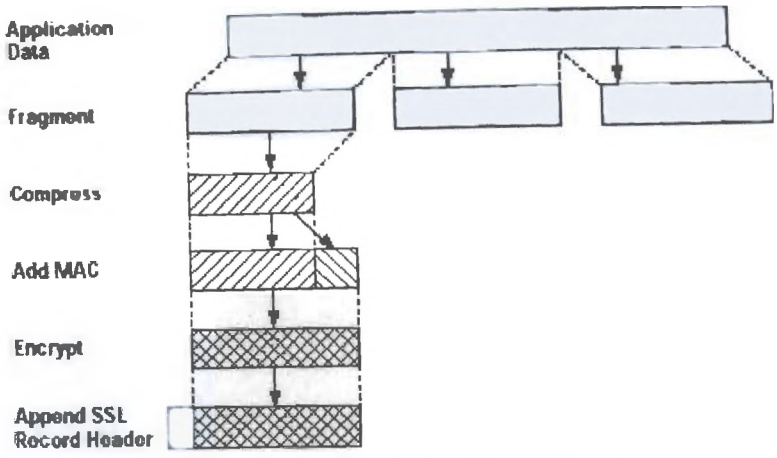
- **Εμπιστευτικότητα** με την κρυπτογράφηση των δεδομένων
- **Ακεραιότητα μηνύματος** με τη χρησιμοποίηση ενός Massage Authentication Code (MAC)

Ένα πακέτο SSL αποτελείται από δύο μέρη, την επικεφαλίδα και τα δεδομένα. Η επικεφαλίδα μπορεί να είναι είτε 3 bytes είτε 2 bytes, από τις οποίες περιπτώσεις η δεύτερη χρησιμοποιείται όταν τα δεδομένα χρειάζονται συμπλήρωμα (padding). Το πεδίο escape-bit στην περίπτωση των 3 bytes υπάρχει μόνο σε εκδόσεις μετά την δεύτερη του πρωτοκόλλου και προβλέπεται για ρύθμιση πληροφοριών out-of-band. Για την επικεφαλίδα των 2 bytes το μέγιστο μέγεθος του πακέτου είναι 32767 bytes, ενώ για την επικεφαλίδα των 3 bytes το μέγεθος είναι μέχρι 16383 bytes.
Το μέρος των δεδομένων αποτελείται από ένα Message Authentication Code (MAC), τα πραγματικά δεδομένα και δεδομένα συμπλήρωσης, εάν χρειάζονται. Αυτό το κομμάτι είναι που κρυπτογραφείται κατά την μετάδοση. Τα συμπληρωματικά δεδομένα απαιτούνται όταν οι αλγόριθμοι κρυπτογράφησης είναι εν χρήση τύπου block ciphers και ο ρόλος τους είναι να συμπληρώνουν τα πραγματικά δεδομένα ώστε το μέγεθος τους να είναι πολλαπλάσιο του μεγέθους που δέχεται σαν είσοδο ο block cipher. Εάν χρησιμοποιούνται stream ciphers τότε δεν απαιτείται συμπλήρωμα και μπορεί αν χρησιμοποιηθεί η επικεφαλίδα των 2 bytes.



Σχήμα 3.4: SSL Record Structure

Ο MAC είναι η digest ή hash value των secret-write key του αποστολέα του πακέτου, των πραγματικών δεδομένων, των συμπληρωματικών δεδομένων και ενός αριθμού ακολουθίας, στην σειρά που δίνονται. Ο αριθμός ακολουθίας είναι ένας ακέραιος αριθμός 32 bit που αυξάνεται αφότου στέλνεται κάθε μήνυμα.
Το Σχήμα 5 δείχνει τη λειτουργία του SSL Record Protocol. Το Record Protocol παίρνει το μήνυμα της εφαρμογής που θα μεταδοθεί, τμηματοποιεί τα δεδομένα σε εύχρηστα blocks, προαιρετικά συμπιέζει τα δεδομένα, εφαρμόζει ένα MAC, κρυπτογραφεί, προσθέτει μια επικεφαλίδα, και μεταδίδει το αποτέλεσμα αυτό σε ένα TCP segment. Τα δεδομένα που λαμβάνονται αποκρυπτογραφούνται, επιβεβαιώνονται, αποσυμπιέζονται, επανασυγκεντρώνονται και διανέμονται στους χρήστες των ανώτερων επιπέδων.



Σχήμα 3.5: Λειτουργία του SSL Record Protocol

Το πρώτο βήμα είναι η τμηματοποίηση. Κάθε μήνυμα υψηλότερου επιπέδου τμηματοποιείται σε blocks των 214 bytes (16384 bytes) ή λιγότερο. Η συμπίεση εφαρμόζεται προαιρετικά. Το επόμενο βήμα είναι να υπολογιστεί το message authentication code πάνω από τα συμπιεσμένα δεδομένα. Για αυτό το λόγο χρησιμοποιείται ένα διαμοιραζόμενο μυστικό κλειδί. Στη συνέχεια, το αποτέλεσμα κρυπτογραφείται χρησιμοποιώντας συμμετρική κρυπτογράφηση.

Για την κρυπτογράφηση ρεύματος, το συμπιεσμένο μήνυμα μαζί με το MAC κρυπτογραφούνται. Για block κρυπτογράφηση, μπορεί να προστεθεί padding μετά το MAC πριν τη κρυπτογράφηση. Το τελικό βήμα της επεξεργασίας του SSL Record Protocol είναι η προσθήκη μιας επικεφαλίδας με τα ακόλουθα στοιχεία:

- Τύπος περιεχομένου (8 bit)
- Κύρια έκδοση (8 bit)
- Δευτερεύουσα έκδοση (8 bit)
- Συμπιεσμένο μήκος (16 bit)

3.5.1 Change Cipher Spec Protocol

Είναι το απλούστερο από τα τρία SSL-specific πρωτόκολλα που χρησιμοποιούν το SSL Record Protocol. Αποτελείται από ένα απλό μήνυμα μήκους ενός byte με τιμή ίση με 1. Ο μόνος σκοπός αυτού του μηνύματος είναι να προκαλέσει την εκκρεμή κατάσταση να αντιγραφεί στην τρέχουσα κατάσταση που ενημερώνει το cipher suite να χρησιμοποιηθεί σε αυτή τη σύνδεση.

3.5.2 Alert Protocol

Χρησιμοποιείται για να μεταφέρει συναγερμούς στην ομότιμη οντότητα. Κάθε μήνυμα στο πρωτόκολλο αποτελείται από δύο bytes. Το πρώτο byte παίρνει την τιμή **προειδοποίηση** (1) ή **μοιραίο** (2) για να μεταφέρει τη σημασία του μηνύματος. Το δεύτερο byte περιέχει ένα κώδικα που ορίζει το συγκεκριμένο συναγερμό.

3.6 SSL Handshake Protocol

Το πρωτόκολλο SSL Handshake διαχωρίζεται σε δύο επιμέρους φάσεις: η πρώτη φάση αφορά την επιλογή των αλγόριθμων, την ανταλλαγή ενός master key και την

πιστοποίηση της ταυτότητας του server. Η δεύτερη φάση διαχειρίζεται την πιστοποίηση της ταυτότητας του client (εάν ζητηθεί) και ολοκληρώνει την διαδικασία του handshaking. Όταν το ολοκληρωθούν και οι δύο φάσεις, το στάδιο του handshake τελειώνει και η μεταφορά μεταξύ των δύο άκρων αρχίζει. Όλα τα μηνύματα κατά την διάρκεια του handshaking και μετά στέλνονται σύμφωνα με το SSL Record Protocol.
Το πακέτο των αλγορίθμων κρυπτογράφησης *(Cipher Suite)* περιλαμβάνει την μέθοδο για την ανταλλαγή των κλειδιών, τον αλγόριθμο κρυπτογράφησης και τον μηχανισμό για την παραγωγή του MAC.
Παρακάτω θα δούμε τρεις διαφορετικές περιπτώσεις επικοινωνίας.

1. Πρώτα θα εξετάσουμε την περίπτωση της αρχικής σύνδεσης, χωρίς πιστοποίηση ταυτότητας του client. Χρησιμοποιείται η σύμβαση "{data}key" για να υποδηλώσουμε κρυπτογραφημένα δεδομένα με το κλειδί "key".
Ας δούμε βήμα προς βήμα την ακολουθία μηνυμάτων.

Τύπος Μηνύματος	*Κατεύθυνση*	*Δεδομένα που μεταφέρονται*
client-hello	C → S	challenge-data, cipher-suite-specs, compressions
server-hello	C ← S	connection-id, server-certificate, cipher-kind, compression-kind
client-master-key	C → S	clear-master-key,{secret-master-key}server-public-key
client-finish	C → S	{connection-id}client-write-key
server-verify	C ← S	{challenge-data}server-write-key
server-finish	C ← S	{session-id}server-write-key

Με το μήνυμα **client-hello** στέλνει ο client στον server μια λίστα με τους αλγόριθμους που υποστηρίζει και τα challenge-data που θα χρησιμοποιηθούν αργότερα για την πιστοποίηση της ταυτότητας του.
Το μήνυμα **server-hello** επιστρέφει στον client ένα αναγνωριστικό της σύνδεσης (connection-id), την επιλογή του server όσον αναφορά πακέτο των αλγόριθμων κρυπτογράφησης και συμπίεσης (που και οι δύο υποστηρίζουν) και το πιστοποιητικό του server που θα χρησιμοποιηθεί από τον client για την απόκτηση της δημόσιας κλείδας του server. Στην τελευταία έκδοση του
Το **client-master-key** και το master-key, που ανάλογα με το που βρίσκεται κάθε υπολογιστής, μπορεί να έχει δυο διαφορετικές μορφές. Για SSL εφαρμογές έξω από τις Ηνωμένες Πολιτείες, τα 88 bits του master-key μεταδίδονται μη κρυπτογραφημένα και κρυπτογραφούνται τα υπόλοιπα 40 bits με την δημόσια κλείδα του server. Αντίθετα για SSL εφαρμογές εντός των Ηνωμένων Πολιτειών, κρυπτογραφείται όλο το master-key και το clear-master-key είναι άδειο.
Από αυτό το σημείο και μετά όλα τα μηνύματα κρυπτογραφούνται στο επίπεδο του SSL Record Protocol. Το master-key δεν χρησιμοποιείται άμεσα για κρυπτογράφηση, αλλά για την παραγωγή δύο ζευγάρια κλειδιών. Το ένα ζευγάρι ανήκει στον client και αποτελείται από το *client-write-key* που χρησιμοποιεί ο client για να κρυπτογραφήσει τα μηνύματα προς τον server και το *client-read-key* για να αποκρυπτογραφήσει ότι λαμβάνει από αυτόν. Το δεύτερο ζευγάρι ανήκει στον server και αποτελείται από το *server-write-key* για κρυπτογράφηση μηνυμάτων προς τον client και το *server-read-*

key για αποκρυπτογράφηση των παραληφθέντων. Για την ακρίβεια, το client-write-key είναι το ίδιο με το server-read-key και το client-read-key είναι το ίδιο με το server-write-key.
Το **client-finish** περιέχει το αναγνωριστικό της σύνδεσης που αρχικά είχε σταλεί από τον server κρυπτογραφημένο με το client-write-key.
Το **server-verify** περιέχει τα challenge-data που είχε στείλει ο client στον server κατά την αρχή της σύνδεσης, κρυπτογραφημένα με το server-write-key. Η παραλαβή και αποκρυπτογράφηση αυτού του μηνύματος είναι το τελικό στάδιο για την επιβεβαίωση της ταυτότητας του server καθ' ότι μόνο ο αληθινός server θα μπορούσε να αποκρυπτογραφήσει με την ιδιωτική του κλείδα το master-key.
Τέλος, το μήνυμα **server-finish** τερματίζει το handshake. Περιέχει το session-id που χρησιμοποιείται σε επόμενες διαδικασίες handshake για την αποφυγή επανάληψης της φάσης επιλογής αλγορίθμων και ανταλλαγής του master-key. Το session-id αποθηκεύεται και από τους δύο και η προτεινόμενη διάρκεια ζωής είναι 100 δευτερόλεπτα. Έπειτα, αχρηστεύεται.

2. Όταν ένα προηγούμενο session-id από τον client χρησιμοποιείται για να επαναεγκαταστήσει την σύνδεση, το handshake γίνεται ως εξής:

Τύπος Μηνύματος	*Κατεύθυνση*	*Δεδομένα που μεταφέρονται*
client-hello	C → S	challenge-data, session-id, cipher-suite-specs, compressions
server-hello	C ← S	connection-id
client-finish	C → S	{connection-id}client-write-key
server-verify	C ← S	{challenge-data}server-write-key
server-finish	C ← S	{session-id}server-write-key

Αλλάζει το **client-hello** που περιέχει επιπλέον το session-id και χρησιμοποιείται από τον server για να καθορίσει τους αλγόριθμους και το master-key. Η λίστα με τους αλγόριθμους στέλνεται ξανά για την περίπτωση όπου έχει λήξει το session-id.
Το **server-hello** στέλνεται μόνο όταν το session-id ισχύει ακόμα.

3. Όταν ζητείται πιστοποίηση της ταυτότητας του client και έχει προηγουμένως εκδοθεί session-id, η ακολουθία των μηνυμάτων του handshaking γίνεται:

Τύπος Μηνύματος	*Κατεύθυνση*	*Δεδομένα που μεταφέρονται*
client-hello	C → S	challenge-data, session-id, cipher-suite-specs
server-hello	C ← S	connection-id, server-certificate, cipher-kind
client-master-key	C → S	clear-master-key,{secret-master-key}server-public-key
client-finish	C → S	{connection-id}client-write-key
server-verify	C ← S	{challenge-data}server-write-key

request-certificate	C ← S	{auth-type, cert-chal-data}server-write-key
client-certificate	C → S	{cert-type, client-cert, resp-data}client-write-key
server-finish	C ← S	{session-id}server-write-key

Παρατηρούμε ότι τα προστίθονται δύο νέα μηνύματα στην προηγούμενη ακολουθία.
Το **request-certificate** στέλνεται από τον server και περιέχει μια δήλωση για την συνάρτηση που θα χρησιμοποιήσει ο client για την παραγωγή της digest value και τον τύπο της συμμετρική κρυπτογράφησης (auth-type). Επίσης, αποστέλλονται και δεδομένα που θα υπογράψει ο client για να αποδείξει την ταυτότητα του (cert-chal-data).
Το **client-certificate** επιστρέφει στον server το πιστοποιητικό του client, μαζί με μια δήλωση του τύπου αυτού (cert-type)και την υπογραφή των δεδομένων cert-chal-data. Ο server θα χρησιμοποιήσει την δημόσια κλείδα που περιέχεται στο πιστοποιητικό του client για να αποκρυπτογραφήσει την υπογραφή. Έπειτα, θα υπολογίσει το message digest των cert-chal-data και θα το συγκρίνει με το message digest που προήλθε από την αποκρυπτογράφηση της υπογραφής.
Κατά την διάρκεια όλων των παραπάνω ανταλλαγών μηνυμάτων, μηνύματα λάθους μπορούν να σταλούν σαν απάντηση σε μηνύματα που δεν βγάζουν νόημα. Η διαδικασία αναγνώρισης λάθους και αποστολή του κατάλληλου μηνύματος αναλαμβάνεται από το πρωτόκολλο SSL Alert Protocol και είναι μέρος του SSL Handshake Protocol. Έτσι, το μήνυμα **no-cipher-error** στέλνεται όταν ο server δεν υποστηρίζει κανένα από τους αλγόριθμους που προτείνει ο client, το μήνυμα **no-certificate-error** όταν δεν είναι διαθέσιμο το ζητηθέν πιστοποιητικό, το μήνυμα **bad-certificate** αν το πιστοποιητικό είναι άκυρο και τέλος το **unsupported-certificate-type-error**, όταν ο τύπος ενός πιστοποιητικού δεν υποστηρίζεται από κανέναν.

3.7 SSL εκδόσεις

Το Ιούλιο του 1994 γίνεται η πρώτη σχεδίαση του SSL που αποτέλεσε και την πρώτη έκδοση (version 1) και τον Οκτώβριο του ίδιου χρόνου δημοσιεύθηκε υπό μορφή RFC (Request For Comments). Η έκδοση 1.0 του πρωτοκόλλου χρησιμοποιήθηκε μέσα στο Netscape. Τον Δεκέμβριο του 1994 εκδίδεται η δεύτερη έκδοση (version 2) που αποτελεί μια αναθεώρηση του πρωτοκόλλου. Η έκδοση 2.0 του πρωτοκόλλου συμπεριλήφθηκε με τον Netscape Navigator 1 και 2. Στα τέλη του 1995 παρουσιάζεται στο κοινό η τρίτη έκδοση (version 3), ενώ από τα μέσα του 1995 αρχίζει να εφαρμόζεται στα προϊόντα της επιχείρησης (π.χ. Netscape Navigator). Στο SSL 3.0 που αποτελεί και την παρούσα έκδοση ενσωματώθηκαν και τα πλεονεκτήματα του PCT (Private Communications Technology), πρωτόκολλο επιπέδου μεταφοράς παρόμοιο με το SSL, το οποίο αναπτύχθηκε από την Microsoft.
Στο SSL 3.0 είναι βασισμένο το πρωτόκολλο TLS (Transport Layer Security), που δημιουργήθηκε από το Internet Engineering Task Force (IETF). Το TLS είναι παρόμοιο με το SSL 3.0 με κάποιες μικρές αλλαγές στην επιλογή αλγορίθμων.

3.8 SSL Ψηφιακά Πιστοποιητικά

Το SSL κάνει εκτεταμένη χρήση των πιστοποιητικών δημοσίου κλειδιού για την απόδειξη γνησιότητας τόσο του client όσο και του server στις SSL συναλλαγές. Το SSL κάνει χρήση των x.509 v3 πιστοποιητικών για τον έλεγχο των RSA ζεύγος κλειδιών, και ένα τροποποιημένο x.509 πιστοποιητικό για τον έλεγχο δημόσιων κλειδιών που χρησιμοποιούνται από το U.S. Department of Defense Forteza/DMS πρωτόκολλο ανταλλαγής κλειδιών. Τα ψηφιακά πιστοποιητικά εξηγούνται με μεγαλύτερη λεπτομέρεια στο Κεφάλαιο 4, "Ψηφιακοί Τρόποι Αναγνώρισης Ταυτότητας"
Το SSL υποστηρίζει τα παρακάτω είδη πιστοποιητικών:

- RSA πιστοποιητικά δημόσιου κλειδιού με δημόσια κλειδιά αυθαίρετου μήκους
- RSA πιστοποιητικά δημόσιου κλειδιού που περιορίζονται στα 512 bits, για χρήση
- στα κρυπτογραφικά λογισμικά που πρόκειται να εξαχθούν.
- RSA πιστοποιητικά μόνο για υπογραφή, τα οποία περιέχουν RSA δημόσια κλειδιά που χρησιμοποιούνται μόνο για την υπογραφή δεδομένων, και όχι για κρυπτογράφηση.
- DSS πιστοποιητικά
- Diffie-Hellman πιστοποιητικά

Η χρήση των πιστοποιητικών είναι προαιρετική. Το SSL απαιτεί πιστοποιητικά server εκτός αν οι SSL εφαρμογές και του client και του server χρησιμοποιούν το Diffie-Hellman πρωτόκολλο ανταλλαγής κλειδιών. Σήμερα, τα προϊόντα της Netscape δεν εφαρμόζουν τους αλγόριθμους του Diffie-Hellman.

3.9 Αντοχή του SSL σε γνωστές επιθέσεις

3.9.1 Dictionary Attack

Αυτό το είδος της επίθεσης λειτουργεί όταν ένα μέρος μη κρυπτογραφημένου κειμένου είναι στην κατοχή του ανέντιμων προσώπων. Το μέρος αυτό κρυπτογραφείται με χρήση κάθε πιθανού κλειδιού και έπειτα ερευνάται ολόκληρο το κρυπτογραφημένο μήνυμα μέχρι να βρεθεί κομμάτι του που να ταιριάζει με κάποιο από τα προϋπολογισμένα. Σε περίπτωση που η έρευνα έχει επιτυχία, τότε το κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση ολόκληρου του μηνύματος έχει βρεθεί. Το SSL δεν απειλείται από αυτήν την επίθεση αφού τα κλειδιά των αλγορίθμων του είναι πολύ μεγάλα των 128 bit. Ακόμα και οι αλγόριθμοι σε εξαγόμενα προϊόντα, υποστηρίζουν 128 bit κλειδιά και παρ' όλο που τα 88 bit αυτών μεταδίδονται ανασφάλιστα, ο υπολογισμός 2^{40} διαφορετικών ακολουθιών κάνει την επίθεση αδύνατο να επιτύχει.

3.9.2 Brute Force Attack

Η επίθεση αυτή πραγματοποιείται με την χρήση όλων των πιθανών κλειδιών για την αποκρυπτογράφηση των μηνυμάτων. Όσο πιο μεγάλα σε μήκος είναι τα χρησιμοποιούμενα κλειδιά, τόσο πιο πολλά είναι τα πιθανά κλειδιά. Τέτοια επίθεση

σε αλγορίθμους που χρησιμοποιούν κλειδιά των 128 bits είναι τελείως ανούσια. Μόνο ο DES56 bit cipher είναι ευαίσθητος σε αυτήν την επίθεση, αλλά η χρήση του δεν συνιστάται.

3.9.3 Replay Attack

Όταν ένας τρίτος καταγράφει την ανταλλαγή μηνυμάτων μεταξύ client και server και προσπαθεί να ξανά χρησιμοποιήσει τα μηνύματα του client για να αποκτήσει πρόσβαση στον server, έχουμε την επίθεση replay attack. Όμως το SSL κάνει χρήση του connection-id, το οποίο παράγεται από τον server με τυχαίο τρόπο και διαφέρει για κάθε σύνδεση. Έτσι δεν είναι δυνατόν πότε να υπάρχουν δυο ίδια connection-id και το σύνολο των είδη χρησιμοποιημένων μηνυμάτων δεν γίνονται δεκτά από τον server. Το connection-id έχει μέγεθος 128 bit για πρόσθετη ασφάλεια.

3.9.4 Man-In-The-Middle-Attack

Η επίθεση Man-In-The-Middle συμβαίνει όταν ένας τρίτος είναι σε θέση να παρεμβάλλεται στην επικοινωνία μεταξύ του server και του client. Αφού επεξεργαστεί τα μηνύματα του client και τροποποιήσει όπως αυτός επιθυμεί, τα προωθεί στον server. Ομοίως πράττει για τα μηνύματα που προέρχονται από τον server. Δηλαδή, προσποιείται στον client ότι είναι ο server και αντίστροφα.
Το SSL υποχρεώνει τον server να αποδεικνύει την ταυτότητα του με την χρήση έγκυρου πιστοποιητικού του οποίου η τροποποίηση είναι αδύνατον. Μην ξεχνάμε την δυνατότητα επικοινωνίας των κλειδιών υπογεγραμμένα.

3.10 Αδυναμίες του SSL

Μπορεί το SSL να προστατεύει τις εμπορικές, και όχι μόνο συναλλαγές, προσφέροντας έγκυρη και ασφαλή μέθοδο επικοινωνίας, αλλά δεν εξασφαλίζει τον χρήστη από διάφορους εισβολείς (π.χ. hackers, crackers) με τους οποίους μπορεί λανθασμένα να επιλέξει για συνεργασία.
Το SSL χρησιμοποιεί μια μέθοδο που είναι γνωστή σαν public key authentication για να παρέχει την εμπιστευτική σύνδεση ανάμεσα στον server και στον client. Σαν ιδέα, είναι πολύ καλή. Στην πραγματικότητα όμως, υπάρχει το πρόβλημα που σχετίζεται με το ποιοι συνδέονται μεταξύ τους, με αυτή την μέθοδο. Αν δηλαδή ο server ή ο client (πιθανότατα) έχει κάποιο πρόβλημα, τότε τα πράγματα δυσκολεύουν... Για παράδειγμα: Έστω ο Χ δέχεται μια επιταγή από κάποιον Υ, τον οποίο δεν γνωρίζει και καλεί την τράπεζά του για να δει αν όλα είναι εντάξει. Στην περίπτωση όμως του SSL server και client η «επιταγή» αυτή δεν αναγράφει από ποια τράπεζα είναι, με αποτέλεσμα να μην υπάρχει δυνατότητα για οποιανδήποτε παραπέρα έλεγχο. Στην πραγματικότητα αν ήταν κάποιος άνθρωπος στην θέση του server να μη δεχόταν την επιταγή! Αυτό σημαίνει ότι ο SSL server δεν είναι σε θέση να ελέγξει αν ο client είναι όντως ο νόμιμος ή κάποιος επιτήδειος εισβολέας που έχει υποκλέψει τα στοιχεία του νόμιμου client. Υπάρχει γενικά μια παραδοχή: Όλοι οι clients είναι αξιόπιστοι. Η παραδοχή όμως αυτήν οδηγεί πολλές φορές σε ανεξέλεγκτες καταστάσεις, οι οποίες αποδεικνύονται συνήθως δυσάρεστες. Εξάλλου ένας λόγος για τον οποίο μπορεί κανείς να ακυρώσει μια συναλλαγή η οποία διεξήχθη on-line στηρίζεται ακριβώς σε αυτό το γεγονός: Υπάρχει περίπτωση ο χρήστης που έκανε την παραγγελία να μην έχει αντίστοιχη εξουσιοδότηση.

Το πρόβλημα εντοπίζεται στο γεγονός ότι το SSL αφήνει «απ' έξω» τον χρήστη αυτοματοποιώντας τις διαδικασίες. Συνήθως ο χρήστης δέχεται τα γεγονότα στον υπολογιστή του χωρίς να προβάλει οποιαδήποτε αντίρρηση ή να ελέγξει την ορθότητα των δεδομένων. Έτσι λοιπόν ο χρήστης για να προφυλαχθεί από τις τρύπες ασφαλείας του SSL πρωτοκόλλου μπορεί να καταφύγει στις εξής λύσεις:

- Να συνδέεται σε ιστοσελίδες (sites) που γνωρίζει ότι ένα ικανοποιητικό επίπεδο ασφαλείας. Να μην εμπιστεύεται εύκολα sites τα οποία υπόσχονται πολλά, αλλά στην πραγματικότητα δεν προσφέρουν τίποτα.
- Πριν ανοίξει το πορτοφόλι του μέσω μιας πιστωτικής κάρτας, πρέπει να βεβαιωθεί για την αξιοπιστία του server που συναλλάσσεται.
- Να ελέγξει (κάνοντας κλικ στο «λουκέτο»του internet browser του) αν όντως το site που επισκέπτεται παρέχει ασφάλεια και σε ποιο επίπεδο κυμαίνεται αυτή. Όσο υψηλότερο είναι το κρυπτογραφικό κλειδί (encryption key) τόσο ασφαλέστερη θα είναι και η συναλλαγή του.

ΚΕΦΑΛΑΙΟ 4

ΨΗΦΙΑΚΕΣ ΤΕΧΝΙΚΕΣ ΑΝΑΓΝΩΡΙΣΗΣ ΤΑΥΤΟΤΗΤΑΣ

4.1 Εισαγωγή

Οι βασικότερες τεχνικές αναγνώρισης ταυτότητας του χρήστη ταξινομούνται στις παρακάτω κατηγορίες:

- Αυθεντικοποίηση από στοιχεία που έχει ο χρήστης
  - ✓ Αυθεντικοποίηση από κάτι που γνωρίζει ο χρήστης (π.χ. password, PIN)
  - ✓ Αυθεντικοποίηση από κάτι που κατέχει ο χρήστης (π.χ. μαγνητικές κάρτες, έξυπνες κάρτες)
- Αυθεντικοποίηση από τα χαρακτηριστικά του χρήστη
  - ✓ Αυθεντικοποίηση με βάση προσωπικά χαρακτηριστικά του χρήστη με χρήση βιομετρικών τεχνικών αναγνώρισης ταυτότητας (π.χ. δακτυλικά αποτυπώματα)
  - ✓ Αυθεντικοποίηση από μια πράξη του χρήστη (π.χ. τρόπος υπογραφής)

4.2 Συστήματα βασισμένα σε password:

Τα πρώτα ψηφιακά συστήματα αναγνώρισης της ταυτότητας του χρήστη ήταν βασισμένα σε συνθηματικές λέξεις (password). Κάθε χρήστης ενός συστήματος έχει το όνομα του (usemame) και την συνθηματική λέξη του. Για να αποδείξεις την ταυτότητα σου στον υπολογιστή, απλά εισάγεις το password. Εάν το password που εισάγεις ταιριάζει με αυτό που είναι αποθηκευμένο στον υπολογιστή, τότε πρέπει να είσαι αυτός που ισχυρίζεσαι ότι είσαι.
Επειδή είναι απλά στην χρήση, γνωστά, και δεν απαιτούν ειδικό hardware, τα password συνεχίζουν να είναι τα ποιο δημοφιλή συστήματα αναγνώρισης ταυτότητας που χρησιμοποιούνται σε υπολογιστές σήμερα στον κόσμο. Δυστυχώς υπάρχουν πολλά προβλήματα χρησιμοποιώντας passwords για την αναγνώριση της ταυτότητας.

4.2.1 Προβλήματα με τα password

Υπάρχουν αρκετοί τρόποι για να αποκτήσει κάποιος τον κωδικό μας. Ο πρώτος και ο πιο συνηθισμένος περιέργως είναι να τον μαντέψει! Φαίνεται παράξενο αλλά το 90% των κωδικών που έχουν "κλαπεί" έχουν πρακτικά μαντευθεί! Ο πρώτος λόγος γι' αυτό

είναι το ότι το 90% περίπου των χρηστών κωδικών διαλέγουν μια εύκολη λέξη την οποία μπορούν να θυμούνται. Αυτό είναι θετικό από μία άποψη καθώς σημαίνει ότι ο χρήστης δε θα ξεχάσει τον κωδικό του. Από την άλλη είναι ιδιαίτερα αρνητικό από άποψη ασφάλειας. Οι εύκολες αυτές λέξεις έχουν συνήθως δύο επικίνδυνα Χαρακτηριστικά: πρώτον, είναι καθημερινές λέξεις και δεύτερον λέξεις που ανήκουν σε λεξικά.

Οι καθημερινές λέξεις σημαίνουν πως με λίγη γνώση των συνηθειών και της ζωής του προσώπου που μας ενδιαφέρει, μπορούμε να βρούμε τον κωδικό. Είναι απίστευτα μεγάλο το *ποσοστό των ατόμων* που δίνουν για κωδικό το μικρό όνομά τους ή το όνομα της γυναίκας τους ή του σκύλου τους ή τη μάρκα του αυτοκινήτου τους. Είναι επίσης αστείο πώς πολλοί χρήστες χρησιμοποιούν ακριβώς τα παραπάνω προσθέτοντας τον αριθμό 1 στο τέλος τους. Έτσι αντί για κωδικό Xsara (το μοντέλο αυτοκινήτου) χρησιμοποιούντο Xsara1... Και φυσικό όσοι χρησιμοποιούν για κωδικό την ημερομηνία της γέννησής τους, τον αριθμό της αστυνομικής τους ταυτότητας, τον αριθμό του τηλεφώνου τους (σταθερού ή του κινητού δεν έχει σημασία) ή τον αριθμό του αυτοκινήτου τους, έχουν μεγάλο πρόβλημα! Το ότι το 90% των κωδικών μπορούν να βρεθούν σε λεξικά είναι επίσης ένα μεγάλο πρόβλημα. Διότι στις τεχνικές που χρησιμοποιούνται από τους επιτήδειους για να βρεθεί ένας κωδικός είναι η χρήση γενικών και ειδικών λεξικών. Τα λεξικά αυτά μπορεί να είναι για παράδειγμα όλες οι λέξεις της αγγλικής ή ελληνικής γλώσσας αλλά και ειδικότερα λεξικά όπως όλα τα μοντέλα αυτοκινήτων, γυναικεία και αντρικά ονόματα (απ' όλες τις χώρες), ποδοσφαιρικές ομάδες, ονόματα καλλιτεχνών, ηθοποιών κλπ. Το γεγονός επίσης πως οι περισσότεροι χρήστες διαλέγουν μικρούς κωδικούς (συνήθως 4-5 χαρακτήρων) διευκολύνει φοβερά τις διαδικασίες ανεύρεσης μέσω μεθόδων λεξικών και brute force, όπου δοκιμάζονται όλοι οι πιθανοί συνδυασμοί γραμμάτων και αριθμών. Για παράδειγμα ο κωδικός "Takis" (!) Χρειάζεται 26^5 συνδυασμούς brute force για να βρεθεί (πάνω από 11 εκατομμύρια δηλαδή συνδυασμούς /λέξεις) αλλά μπορεί επίσης να βρεθεί πολύ ταχύτερα με τη χρήση ενός λεξικού ονομάτων των 10.000 λέξεων. Εδώ και κάτι λιγότερο από μία δεκαετία είναι γνωστό πως οι μυστικές αλλά και φανερές κρατικές υπηρεσίες σε δύση και ανατολή, χρησιμοποιούν τεχνικές brute force για να σπάνε κωδικούς με σχετική επιτυχία, όταν οι κωδικοί είναι μικροί. Είναι γνωστό επίσης πως οι "επιτιθέμενοι" (αυτοί δηλαδή που προσπαθούν να σπάσουν έναν κωδικό) διαθέτουν πάντα πολύ ισχυρά συστήματα, έως και υπερυπολογιστές γι' αυτήν τη διαδικασία. Το ελάχιστο μέγεθος για σχετική ασφάλεια στην εποχή μας είναι οι κωδικοί 8 χαρακτήρων. Για την αποφυγή αυτού του προβλήματος οι περισσότερες υπηρεσίες/ διαδικασίες στο διαδίκτυο ζητούν από τους χρήστες τους συγκεκριμένο μέγεθος κωδικών. Το υπόλοιπο 10% των κωδικών έχει κλαπεί από τους επιτήδειους με διάφορους τρόπους. Ο πιο συνηθισμένος, όπου δε χρειάζεται κάποιος να είναι hacker, είναι αυτός με τους Trojan όλων των ειδών.

Οι σύγχρονοι trojans μπορούν να κάνουν απίστευτα πράγματα και είναι πρακτικά σαν ένα σύστημα εξ' αποστάσεως διαχείριση (remote administration) ενός υπολογιστή. Έτσι κάποιος που έχει στον υπολογιστή του έναν trojan, πρακτικά έχει και κάποιον άλλο χρήστη στο μηχάνημα του με τα ίδια δικαιώματα. Οι trojans αυτοί μπορούν είτε να καταγράψουν τους κωδικούς, είτε να τους αναζητήσουν, να τους στείλουν αυτόματα στο "αφεντικό" τους ή ο ίδιος ο χρήστης του trojan να ψάξει το σκληρό δίσκο (αλλά και τη μνήμη) του μολυσμένου υπολογιστή για να βρει τους κωδικούς.

Τέλος υπάρχουν και οι πραγματικοί hacker οι οποίοι δεν ασχολούνται σχεδόν ποτέ με απλούς χρήστες (εκτός των περιπτώσεων που υπάρχει κάποιος συγκεκριμένος λόγος), αλλά μόνο με εταιρείες. Και εταιρείες συχνά σημαίνει βάσεις δεδομένων και βάσεις δεδομένων σημαίνει και τους κωδικούς μας! Στο διαδίκτυο μπορεί ο οποιοσδήποτε να

βρει αρκετά ισχυρά προγράμματα για επιθέσεις τύπου brute force, τόσο σε κρυπτογραφημένα αρχεία διαφόρων εφαρμογών, όσο και εναντίον Web Server.

Για την ασφάλεια του συστήματος, πρέπει να είμαστε προσεκτικοί στην επιλογή των κρυφών συνθηματικών μας (password):

- Το συνθηματικό πρέπει να είναι κάτι ασυνήθιστο που ο άλλος δεν θα μπορεί να μαντέψει εύκολα και να έχει μήκος τουλάχιστον 6 χαρακτήρες. Δεν θα πρέπει να είναι π.χ. η ημερομηνία γέννησής μας, το όνομα της αγαπημένης μας ομάδας κλπ.
- Επίσης, δεν θα πρέπει να είναι μια λέξη που να υπάρχει σε λεξικό γιατί είναι επικίνδυνο να "σπάσει" από τους χάκερ με τη βοήθεια προγραμμάτων που χρησιμοποιούν λεξικά.
- Καλό είναι να επιλέγονται συνδυασμοί γραμμάτων και αριθμών. Μπορούμε για παράδειγμα να σχηματίσουμε το συνθηματικό μας παίρνοντας τα αρχικά μιας φράσης που έχει κάποια σημασία για μας και μπορούμε να τη θυμόμαστε και παρεμβάλλοντας κάποια ψηφία ή και άλλους χαρακτήρες του πληκτρολογίου όπως π.χ. "!", "@", "#", "%", "$", κλπ.
- Τέλος, καλό είναι να αλλάξουμε το συνθηματικό που μας αποδόθηκε αρχικά από το διαχειριστή συστήματος με το άνοιγμα του λογαριασμού μας και γενικότερα να αλλάζουμε κατά διαστήματα το συνθηματικό που έχουμε.

4.2.2 Συνθηματικά μιας χρήσης

Μια εναλλακτική λύση αποτελεί η χρήση 'συνθηματικών μιας χρήσης'. Για το σκοπό χρησιμοποιείται μια λίστα από συνθηματικά (ξεχωριστή για κάθε χρήστη) και κάθε φορά χρησιμοποιείται ένα από αυτά (για μια και μοναδική φορά) μέχρι να εξαντληθούν τα συνθηματικά της λίστας.
Για την υλοποίηση ενός συστήματος συνθηματικών μιας χρήσης πρέπει να προσεχθεί:

- ο τρόπος διανομής των λιστών συνθηματικών
- η προστασία αυτών των λιστών από κλοπή.

4.2.3 Αποθήκευση συνθηματικών

Η πληροφορία των συνθηματικών αποθηκεύεται στον υπολογιστή προκειμένου να ελέγχονται επιτόπου οι χρήστες που τα χρησιμοποιούν. Όμως, η αποθήκευση των συνθηματικών παρουσιάζει και αυτή σημαντικά προβλήματα ασφάλειας, καθώς όταν αποθηκεύονται σε μια μορφή χωρίς προστασία τότε τουλάχιστον οι διαχειριστές του συστήματος μπορούν να τα διαβάσουν. Αλλά κάτι τέτοιο αποτελεί σημαντική παραβίαση της ασφάλειας του συστήματος, καθώς τα συνθηματικά αποτελούν αυστηρά προσωπική πληροφορία. Η γνώση του συνθηματικού μας από άλλον χρήστη μπορεί να του επιτρέψει να χρησιμοποιήσει τις υπηρεσίες του συστήματος προσποιούμενος (1nasquerade) ότι είμαστε εμείς, οπότε για όλες τις ενέργειες που καταγράφονται από το σύστημα θεωρούμαστε εμείς υπεύθυνοι και υπόλογοι.
Η συνηθισμένη λύση σε αυτό το πρόβλημα είναι η χρήση ενός μονόδρομου αλγόριθμου *(one-way function)* κρυπτογράφησης, που να είναι εύκολο να υπολογίζεται και αδύνατο να αναστραφεί το αποτέλεσμά του. Οπότε, αντί να αποθηκεύονται

τα συνθηματικά αυτά καθαυτά, αποθηκεύεται το αποτέλεσμα της εφαρμογής του μονόδρομου αλγόριθμου σε κάθε ένα συνθηματικό ξεχωριστά.
Κατόπιν, για την επιβεβαίωση του συνθηματικού που εισάγει ο χρήστης εφαρμόζεται σε αυτό ο ίδιος μονόδρομος αλγόριθμος και η τιμή που προκύπτει συγκρίνεται με την αποθηκευμένη τιμή στο σύστημα

4.3 Συστήματα με βάση φυσικά κουπόνια (tokens)

Ένας άλλος τρόπος με τον οποίο οι άνθρωποι μπορούν να αποδείξουν την ταυτότητά τους είναι μέσω της χρήσης ενός κουπονιού - φυσικού αντικειμένου που μεταφέρεις μαζί σου, το οποίο με κάποιο τρόπο αποδεικνύει την ταυτότητα σου και σου παρέχει πρόσβαση.
Οι κάρτες πρόσβασης είναι τυπικά κουπόνια που χρησιμοποιούνται για να αποδεικνύουν την ταυτότητα στον σημερινό επιχειρηματικό κόσμο. Για να ανοίξεις μια πόρτα απλά περνάς μια κάρτα στο ειδικό αναγνώστη. Κάθε κάρτα έχει έναν μοναδικό αριθμό. Το σύστημα, από την άλλη, έχει μια λίστα των καρτών που είναι εξουσιοδοτημένες να ανοίγουν τις κατάλληλες πόρτες στην κατάλληλη χρονική στιγμή. Με σκοπό την αποτελεσματικότητα του συστήματος, οι κάρτες αυτές δεν πρέπει να δανείζονται σε άλλους.

Όπως και με τα passwords τα φυσικά κουπόνια έχουν και αυτά προβλήματα:

- Δεν αποδεικνύουν ποιος πραγματικά είσαι. Οποιοσδήποτε που έχει στην ιδιοκτησία του ένα κουπόνι μπορεί να έχει πρόσβαση σε μια περιορισμένη περιοχή.
- Εάν ένα πρόσωπο χάσει το κουπόνι, δεν μπορεί να μπει στην περιορισμένη περιοχή, αν και η ταυτότητα του δεν έχει αλλάξει
- Μερικά κουπόνια είναι εύκολο να πλαστογραφηθούν.

Έτσι, τα συστήματα που βασίζονται σε κουπόνια δεν αναγνωρίζουν την ταυτότητα ενός προσώπου αλλά ενός κουπονιού. Για το λόγο αυτό, τα συστήματα αυτά συνδυάζονται με συστήματα που βασίζονται σε passwords. Για να αποκτήσεις πρόσβαση σε ένα δωμάτιο ή έναν υπολογιστή, χρειάζεται να παρουσιάσεις και ένα κουπόνι και να εισάγεις το password. Αυτή η τεχνική χρησιμοποιείται από τις αυτόματες ταμειολογιστικές μηχανές (Automatic Teller Machines, ATMs) για να αναγνωρίζουν τους ιδιοκτήτες των τραπεζικών λογαριασμών.

4.3.1 Μαγνητικές Κάρτες

Η χρήση της *μαγνητικής κάρτας* (magnetic card) είναι πολύ διαδεδομένη σήμερα. Χρησιμοποιείται συνήθως για την αναγνώριση των χρηστών σε :

- ATM (Automatic Teller Machines): αυτόματα μηχανήματα αναλήψεων,
- POS (Point Of Sale): σημεία πωλήσεων σε καταστήματα,
- έλεγχο πρόσβασης σε ασφαλείς τοποθεσίες (zone access control).

Οι διαστάσεις και η μορφή της μαγνητικής ταινίας στο πίσω μέρος των καρτών καθορίζονται από το πρότυπο ISO 7810.
Τυπικά, στην μαγνητική ταινία αποθηκεύεται η πληροφορία αναγνώρισης χρήστη (π.χ. ο αριθμός του τραπεζικού λογαριασμού). Μια τέτοια κάρτα χρησιμοποιείται πάντοτε σε συνδυασμό με κάποιον αριθμό PIN (Personal Identification Number) για την επιβεβαίωση της ταυτότητας του νόμιμου χρήστη.
Υπάρχουν δύο κατηγορίες συστημάτων επιβεβαίωσης του PIN, off line και on line:

- Σε συστήματα off-line, το PIN αποθηκεύεται σε κρυπτογραφημένη μορφή στην κάρτα (συνήθως το αποτέλεσμα της εφαρμογής μιας μονόδρομης κρυπτογράφησης πάνω στο PIN). Πριν την κρυπτογράφηση του, το PIN πρέπει να συνδυάζεται με μια πληροφορία που εξαρτάται από τον κάτοχο της κάρτας (όπως ο αριθμός της ταυτότητάς του) ώστε να δυσκολεύονται οι επιτιθέμενοι στο να συγκρίνουν λίστες κρυπτογραφημένων PINs.
- Σε συστήματα on-line, τα PINs των χρηστών επιβεβαιώνονται κεντρικά (μέσω δικτύου) και για αυτό δεν χρειάζεται να γράφονται πάνω στην κάρτα.

4.3.2 Έξυπνες Κάρτες

Οι *έξυπνες κάρτες* (smart cards) διαθέτουν μικροεπεξεργαστές Έξυπνες Κάρτες και μνήμες RAM και ROM. Τυπικά έχουν πολύ μεγαλύτερη μνήμη (περίπου 35 KB) από τις μαγνητικές κάρτες(συνήθως γύρω στα 250 B) και έχουν το σημαντικό πλεονέκτημα της ενσωματωμένης υπολογιστικής ισχύος. Το κύριο πλεονέκτημα τους όμως είναι ότι παρέχουν φυσική προστασία των αποθηκευμένων δεδομένων.
Οι επαφές με το εσωτερικό κύκλωμα έχουν τη μορφή επιχρυσωμένων περιοχών πάνω στην επιφάνεια της κάρτας (περιλαμβανομένων των επαφών για την τροφοδοσία από εξωτερική πηγή). Η τοποθέτηση αυτών των επαφών, το μέγεθος της κάρτας και τα πρωτόκολλα που χρησιμοποιούνται στην επικοινωνία μεταξύ έξυπνης κάρτας και συσκευής ανάγνωσης καθορίζονται από το πρότυπο ISOIIEC 7816.
Μια από τις πλέον ενδιαφέρουσες ιδιότητες των έξυπνων καρτών είναι ότι είναι εξαιρετικά δύσκολο να αντιγραφούν. Στην πραγματικότητα, οι κατασκευαστές κρατούν καλά κρυμμένες τις λεπτομέρειες της εσωτερικής σχεδίασης προκειμένου να δυσκολέψουν ακόμη περισσότερο την αντιγραφή και την αναπαραγωγή τους.
Η πρώτη γενιά έξυπνων καρτών (που διατέθηκαν από τα μέσα της δεκαετίας του 1980) διέθετε απλούς επεξεργαστές των 8-bit και περιορισμένη μνήμη των 8 Kbytes. Μερικές διέθεταν περιορισμένες ενσωματωμένες λειτουργίες κρυπτογράφησης.
Στην δεύτερη γενιά έξυπνων καρτών παρέχονται πιο δυνατοί επεξεργαστές, περισσότερη μνήμη και μια ποικιλία κρυπτογραφικών λειτουργιών. Μερικά από τα τελευταίας τεχνολογίας μοντέλα μπορούν μάλιστα να εκτελούν υπολογισμούς ψηφιακών υπογραφών σε κλάσματα του δευτερολέπτου.
Η ενσωματωμένη κρυπτογραφική επεξεργασία είναι ιδιαίτερα χρήσιμη, καθώς, συνδυαζόμενη με την φυσική ασφάλεια που παρέχεται στα αποθηκευμένα δεδομένα, επιτρέπει την χρησιμοποίησ11 τους σε αλληλεπιδραστικές συσκευές αναγνώρισης. Ειδικότερα, αν το συνθηματικό του χρήστη αποθηκευθεί στην κάρτα, τότε η κάρτα μπορεί να χρησιμοποιηθεί σε ένα σχήμα αυθεντικοποίησης του χρήστη με τη μέθοδο της πρόκλησης-απόκρισης υπολογίζοντας την επιλεγμένη μονόδρομη συνάρτηση. Μια βελτιωμένη εκδοχή ενός τέτοιου σχήματος απαιτεί από τον χρήστη να εισάγει τον αριθμό PIN (μέσω του τερματικού εξοπλισμού ή της συσκευής ανάγνωσης της έξυπνης κάρτας) πριν η κάρτα εκτελέσει την λειτουργία της, για προστασία σε περίπτωση κλοπής της κάρτας.

Μαζί με την αύξηση της διαθέσιμης υπολογιστικής δύναμης και της μνήμης μεγαλώνει και ο αριθμός των εφαρμογών με έξυπνες κάρτες. Στα παραδείγματα των ολοένα αυξανόμενων εφαρμογών των έξυπνων καρτών περιλαμβάνονται τα εξής:

- Σε πολλές χώρες οι έξυπνες κάρτες αντικαθιστούν τις μαγνητικέ ς κάρτες για πιστωτικές ή χρεωστικές συναλλαγές.
- Τα κινητά τηλέφωνα (GSM) απαιτούν την εισαγωγή μιας κάρτας SIM (Subscriber Identity Module) για να λειτουργήσουν. Αυτές οι κάρτες είναι έξυπνες κάρτες στις οποίες αποθηκεύεται η πληροφορία για την ταυτότητα και το μυστικό κλειδί χρήστη (παρόλο που δεν σχετίζονται με κάποιον συγκεκριμένο χρήστη).
- Οι έξυπνες κάρτες χρησιμοποιούνται ήδη για την υποστήριξη εφαρμογών ηλεκτρονικού χρήματος.
- Υπάρχουν ακόμη έξυπνες κάρτες που παράγουν γρήγορα ψηφιακές υπογραφές.

4.4 Συστήματα με βάση βιομετρήσεις

Παρ' όλο που τα περισσότερα λεξικά ορίζουν τη βιομετρική ως τη στατιστική ανάλυση των βιολογικών χαρακτηριστικών του ανθρώπου, τα τελευταία χρόνια ο όρος τείνει να ταυτιστεί με την επιστήμη που αναλύει τα ανθρώπινα χαρακτηριστικά για σκοπούς ασφάλειας. Πράγματι, το ανθρώπινο σώμα είναι μία τεράστια πηγή μοναδικών γνωρισμάτων που θα μπορούσαν να χρησιμοποιηθούν για αναγνώριση ταυτότητας. Ένα από αυτά μάλιστα, τα δακτυλικά αποτυπώματα, ήδη χρησιμοποιείται χρόνια τώρα για τέτοιους σκοπούς, χωρίς βέβαια τη μεσολάβηση ηλεκτρονικών συσκευών και υπολογιστών. Πλέον, με τη βοήθεια που της προσφέρουν τα σύγχρονα μέσα, η βιομετρική ερευνά για μεγαλύτερη ακρίβεια και ασφάλεια σε άλλα χαρακτηριστικά του ανθρώπινου σώματος, όπως η ίριδα του ματιού, το σχήμα του προσώπου ή του χεριού και η φωνή. Και ενώ όλες οι ανωτέρω βιομετρικές μέθοδοι ασχολούνται με τα φυσικά χαρακτηριστικά ενός ατόμου, σιγά σιγά αρχίζουν να αναπτύσσονται ορισμένες οι οποίες έχουν ως βάση συμπεριφορές, όπως ο ρυθμός πληκτρολόγησης ή η υπογραφή. Όπου και να βασίζονται πάντως (φυσικό χαρακτηριστικό ή συμπεριφορά), οι βιομετρικές μέθοδοι θεωρείται αυτή τη στιγμή ότι προσφέρουν το υψηλότερο επίπεδο ασφάλειας από όλα τα υπάρχοντα συστήματα, όπως είναι τα PINs (Personal Identification Numbers - Προσωπικοί Αριθμοί Αναγνώρισης), οι κάρτες, και τα συνθηματικά. Πολλοί μεγάλοι οργανισμοί, όπως τράπεζες ή κρατικές υπηρεσίες, αρχίζουν δειλά δειλά να υιοθετούν τη νέα τεχνολογία με σκοπό την αύξηση της ασφάλειας των συστημάτων τους αλλά και την καλύτερη εξυπηρέτηση των πελατών τους.

4.4.1 Διαδικασία

Για να καταστεί δυνατή η βιομετρική αναγνώριση κάποιου ατόμου, προηγείται όπως είναι φυσικό μία διαδικασία λήψης του βιομετρικού δείγματος. Στην πραγματικότητα, λαμβάνεται από το άτομο ένας αριθμός δειγμάτων (συνήθως τρία), τα οποία συνδυάζονται βελτιώνοντας και συμπληρώνοντας το ένα το άλλο, ώστε το αποτέλεσμα που θα προκύψει να είναι όσο το δυνατόν τελειότερο. Με αυτόν τον τρόπο κατασκευάζεται ένα βιομετρικό πρότυπο, με το οποίο θα συγκρίνεται κάθε

φορά το δείγμα που θα λαμβάνεται όταν ο χρήστης απαιτεί την είσοδό του στο προστατευμένο σύστημα. Το βήμα αυτό είναι από τα σημαντικότερα, αφού η ποιότητα του προτύπου θα κρίνει κατά το μεγαλύτερο ποσοστό την αξιοπιστία του όλου συστήματος. Τη δημιουργία του βιομετρικού προτύπου ακολουθεί το στάδιο της αποθήκευσής του. Εδώ οι επιλογές είναι συνήθως τρεις: (1) αποθήκευση του προτύπου στη βιομετρική συσκευή αναγνώρισης (2) αποθήκευση σε μία κεντρική βάση δεδομένων (3) αποθήκευση σε φορητό μέσο (συνήθως κάποια κάρτα και πάλι), το οποίο μεταφέρει ο ίδιος ο χρήστης. Τέλος, έχουμε τη διαδικασία αίτησης εισόδου του χρήστη στο σύστημα, κατά την οποία λαμβάνεται ένα νέο βιομετρικό δείγμα προκειμένου να συγκριθεί με το βιομετρικό πρότυπο. Αν το δείγμα ταιριάζει έστω και με μικρές αποκλίσεις (εξαρτάται πόσο "αυστηρό" έχει ρυθμιστεί να είναι το σύστημα), η είσοδος επιτρέπεται.

4.4.2 Δακτυλικά αποτυπώματα

Χωρίς να προσφέρουν τη μέγιστη ακρίβεια, τα βιομετρικά συστήματα δακτυλικών αποτυπωμάτων αποτελούν μία πολύ αξιόπιστη μέθοδο εξακρίβωσης ταυτότητας.
Ενώ οι υπόλοιπες βιομετρικές μέθοδοι είναι σχετικά μικρής ηλικίας και έχουν ακόμα πολλά προβλήματα να λύσουν, τα δακτυλικά αποτυπώματα κλείνουν σχεδόν έναν αιώνα πρακτικής εφαρμογής. Ο συνδυασμός της νέας τεχνολογίας, λοιπόν, με τη μελέτη που έχει κάνει ο άνθρωπος όλα αυτά τα χρόνια πάνω στο θέμα δεν μπορεί παρά να προσφέρει τα καλύτερα δυνατά αποτελέσματα. Ακριβώς αυτή η σε βάθος τεχνογνωσία αλλά και το γεγονός ότι το είδος των συγκεκριμένων βιομετρήσεων δεν απαιτεί υπερβολικά ακριβό εξοπλισμό έκαναν έναν μεγάλο αριθμό εταιριών να στρέψουν εκεί την προσοχή τους. Ιδιαίτερο ενδιαφέρον για τους χρήστες ηλεκτρονικών υπολογιστών έχει το γεγονός ότι πάρα πολλά από αυτά τα προϊόντα συνδέονται σε υπολογιστή και μέσω ειδικού λογισμικού (software) αναλαμβάνουν την προστασία του (για περισσότερες λεπτομέρειες δείτε την ενότητα "Προϊόντα για το PC σας"). Τέλος, δεν πρέπει να παραλείψουμε να αναφέρουμε ότι, σε σχέση με άλλες βιομετρικές μεθόδους, τα δακτυλικά αποτυπώματα απαιτούν ελάχιστη προσπάθεια από το χρήστη, όση δηλαδή χρειάζεται για την τοποθέτηση του αντίχειρά του στην ειδική υποδοχή.
Ασφαλώς, υπάρχουν και μειονεκτήματα. Από τα σοβαρότερα είναι το γεγονός ότι η σωστή "ανάγνωση" των δακτυλικών αποτυπωμάτων δυσκολεύει πολύ κάτω από ειδικές (αλλά όχι και τόσο σπάνιες) συνθήκες, όπως βρώμικα δάχτυλα, τραυματισμοί στα χέρια, πολύ ξηρό ή πολύ λιπαρό δέρμα. Ακόμα, ο τρόπος με τον οποίο ο χρήστης αλληλεπιδρά με το σύστημα μπορεί να προκαλέσει προβλήματα. Για παράδειγμα, υπερβολική πίεση του δαχτύλου μπορεί να έχει ως αποτέλεσμα λανθασμένη λήψη του αποτυπώματος. Οι διάφοροι κατασκευαστές προσπαθούν να ξεπεράσουν τα προβλήματα εξελίσσοντας τις υπάρχουσες μεθόδους ανάγνωσης και δημιουργώντας άλλες εντελώς καινούριες, όπως η μέθοδος των ακουστικών κυμάτων.
Τα συστήματα αναγνώρισης δακτυλικών αποτυπωμάτων χωρίζονται, καταρχήν, σε δύο κατηγορίες: Στην πρώτη κατηγορία τοποθετούνται αυτά που κάνουν εξακρίβωση ταυτότητας (ονομάζονται και AFIS - Automatic Fingerprint Identification Systems), ενώ στη δεύτερη εκείνα που κάνουν απλή επιβεβαίωση. Αν και αυτή η διάκριση ισχύει για όλα τα βιομετρικά συστήματα, στα δακτυλικά αποτυπώματα είναι πολύ πιο έντονη λόγω των διαφορών που υπάρχουν στη διαδικασία, τις μεθόδους που χρησιμοποιούνται αλλά και στον απαραίτητο εξοπλισμό. Επίσης, λόγω του γεγονότος ότι μέχρι τώρα τα δακτυλικά αποτυπώματα χρησιμοποιούνταν μόνο για ποινικούς σκοπούς, συνήθως τα σημερινά συστήματα υπόκεινται σε μία περαιτέρω διάκριση, αυτήν της ποινικής ή πολιτικής χρήσης. Όσον αφορά στις μεθόδους ανάγνωσης,

σήμερα έχουν ήδη αναπτυχθεί αρκετές, φιλοδοξώντας να λύσουν πολλά από τα προβλήματα που προαναφέρθηκαν. Στη συνέχεια θα δούμε αναλυτικότερα τις σημαντικότερες.
Οπτική ανάγνωση: Η παλαιότερη και πλέον δοκιμασμένη μέθοδος, μοιάζει αρκετά με τη διαδικασία των κοινών scanners. Ο χρήστης αρχικά τοποθετεί το δάχτυλό του σε μία γυάλινη πλάκα. Στη συνέχεια, και αφού η άκρη του δαχτύλου φωτιστεί κατάλληλα, λαμβάνεται η εικόνα του δακτυλικού αποτυπώματος. Οι οπτικοί αναγνώστες δακτυλικών αποτυπωμάτων είναι σήμερα οι πιο συνηθισμένοι. Τα τελευταία χρόνια, εκμεταλλευόμενοι την ανάπτυξη της τεχνολογίας, γίνονται ολοένα μικρότεροι σε μέγεθος αλλά και πιο φθηνοί. Δυστυχώς, είναι και οι πιο επιρρεπείς σε προβλήματα, όταν οι συνθήκες λήψης του αποτυπώματος δεν είναι οι καλύτερες.
Ανάγνωση με υπέρηχους: Η μέθοδος αυτή χρησιμοποιεί ακουστικά κύματα μη αντιληπτά από το ανθρώπινο αυτί. Τα κύματα αυτά "βομβαρδίζουν" το δάκτυλο του χρήστη μετρώντας την πυκνότητα των δακτυλικών του αποτυπωμάτων. Το εμφανές πλεονέκτημα της μεθόδου σε σχέση με τις υπόλοιπες είναι ότι δεν απαιτεί άμεση επαφή του δακτύλου με τον scanner. Κάτι τέτοιο απλώς σημαίνει ότι δεν επηρεάζεται από πολύ βρώμικα δάχτυλα ή ακόμα και από λεπτά γάντια!
Θερμική ανάγνωση και ανάγνωση αφής: Χρησιμοποιώντας εξελιγμένα chips, αυτές οι μέθοδοι θεωρούνται εξαιρετικά ακριβείς. Ο χρήστης τοποθετεί το δάκτυλό του σε κάποιον αισθητήρα, ο οποίος συλλαμβάνει τη θερμότητα ή την πίεση από το δάχτυλο και τη μετατρέπει σε δεδομένα

4.4.3 Εξέταση ίριδας και αμφιβληστροειδούς

Κάποιοι ισχυρίζονται ότι τα μοναδικά χαρακτηριστικά της ίριδας και του αμφιβληστροειδούς, καθιστούν την τεχνητή αναπαραγωγή τους αδύνατη. Δεν αποτελεί, λοιπόν, έκπληξη το γεγονός ότι τα βιομετρικά συστήματα που βασίζονται στα δύο αυτά μέρη του ματιού είναι τα ακριβέστερα και προσφέρουν τη μεγαλύτερη ασφάλεια.
Εκτός από τη μοναδικότητά τους, η ίριδα και ο αμφιβληστροειδής χιτώνας συγκεντρώνουν και ορισμένες άλλες ιδιότητες που τα καθιστούν θαυμάσια εκλογή για την αναγνώριση της ταυτότητας ενός ατόμου: επηρεάζονται ελάχιστα από το πέρασμα του χρόνου, ενώ δεν είναι ιδιαίτερα δεκτικά σε τραυματισμούς ή άλλους παράγοντες, όπως η κούραση. Πολύ στενά συνδεδεμένα με τον ανθρώπινο εγκέφαλο είναι από τα πρώτα μέρη του ανθρώπινου σώματος που αποσυντίθενται μετά το θάνατο. Έτσι, ακόμα και αυτή η ακραία περίπτωση χρήσης ίριδας ή αμφιβληστροειδούς μετά το θάνατο με σκοπό τη διάπραξη απάτης θα πρέπει να αποκλειστεί. Η εξέταση αμφιβληστροειδούς, μάλιστα, θεωρείται η ασφαλέστερη βιομετρική μέθοδος με πρακτικά μηδενικές πιθανότητες παραβίασης.
Όπως ήδη ίσως υποπτεύεστε, η κορυφαία ασφάλεια είναι λογικό να κοστίζει και ανάλογα. Πράγματι, η εξέταση ίριδας και αμφιβληστροειδούς είναι τα ακριβότερα βιομετρικά συστήματα, με κόστος που κάποιες φορές φτάνει αρκετές χιλιάδες ευρώ. Έτσι, μπορούμε να συμπεράνουμε ότι το κοινό στο οποίο απευθύνονται είναι κυρίως μεγάλες εταιρίες και οργανισμοί που ενδιαφέρονται να εξασφαλίσουν το καλύτερο που μπορεί να τους προσφέρει η σύγχρονη τεχνολογία στον τομέα της ασφάλειας.
Η διαδικασία εξέτασης της ίριδας είναι σχετικά απλή: Μία κάμερα συλλαμβάνει την εικόνα της ίριδας και τη μετατρέπει σε ένα είδος μοναδικού μαθηματικού κώδικα, τον οποίο συγκρίνει στη συνέχεια με το βιομετρικό πρότυπο. Απαραίτητη προϋπόθεση για τη σωστή λειτουργία του συστήματος είναι το περιβάλλον στο οποίο θα είναι εγκαταστημένο να έχει πολύ καλό φωτισμό, ώστε η "φωτογραφία" της ίριδας να είναι

όσο το δυνατόν καλύτερη. Υπάρχουν δύο είδη μεθόδων αναγνώρισης της ίριδας, η ενεργητική και η παθητική. Κατά την ενεργητική μέθοδο απαιτείται η συμμετοχή του χρήστη, ο οποίος πρέπει να βοηθήσει την κάμερα του συστήματος να εστιάσει στην ίριδα μετακινώντας το κεφάλι του μερικά εκατοστά εμπρός και πίσω. Το γεγονός αυτό σίγουρα υπονομεύει τη λειτουργικότητα και την ευελιξία της μεθόδου, αφού είναι φανερό ότι για να διασφαλιστούν σωστά αποτελέσματα ο χρήστης χρειάζεται καθοδήγηση από κάποιον που θα επιβλέπει την όλη διαδικασία. Αντίθετα, κατά την παθητική εξέταση ίριδας αντί για μία κάμερα υπάρχουν πολλές, οι οποίες εντοπίζουν αυτόματα πρώτα το πρόσωπο, μετά το μάτι, και τέλος την ίριδα του χρήστη, χωρίς να είναι αναγκαία καμία απολύτως συμμετοχή από τον ίδιο. Δεν χρειάζεται να σημειώσουμε ότι το συγκεκριμένο σύστημα έχει τον υψηλότερο δείκτη ευχρηστίας από όλα τα υπόλοιπα (επίσης δεν χρειάζεται να αναφέρουμε ότι είναι και το ακριβότερο).
Θα περίμενε κάποιος ότι τουλάχιστον η παθητική εξέταση ίριδας θα έβρισκε σχετικά υψηλή αποδοχή από το κοινό. Το γεγονός όμως ότι σε όλες τις παραλλαγές τις μεθόδου ο χρήστης βρίσκεται αντιμέτωπος με κάμερες φαίνεται ότι λειτουργεί ιδιαίτερα αρνητικά στην ψυχολογία του. Άλλωστε, σε κανέναν δεν αρέσει να νοιώθει ότι παρακολουθείται ή, ακόμα περισσότερο, ότι βιντεοσκοπείται ή φωτογραφίζεται.

4.4.4 Αναγνώριση φωνής

Έχοντας το πλεονέκτημα ότι δεν απαιτεί τίποτα περισσότερο από μια κάρτα ήχου και ένα μικρόφωνο, η αναγνώριση φωνής είναι η τέλεια λύση για όσους χρήστες θέλουν να προστατεύσουν τον υπολογιστή τους με μια ελάχιστη οικονομική επιβάρυνση, και παράλληλα είναι διατεθειμένοι να κάνουν κάποιες παραχωρήσεις σε θέματα ακριβείας.
Παρ' όλο που η αναγνώριση φωνής είναι μια βιομετρική μέθοδος που υστερεί σε αρκετά σημεία σε σύγκριση με τους κοντινότερους "ανταγωνιστές" της, φαίνεται πως σιγά-σιγά η προσοχή κατασκευαστών και κοινού στρέφεται επάνω της. Αυτό συμβαίνει για δύο κυρίως λόγους: Ο πρώτος είναι ότι σ' έναν κόσμο που τρέχει όλο και με γρηγορότερους ρυθμούς, η ανάγκη επαλήθευσης της ταυτότητας ατόμων μέσω των τηλεφωνικών γραμμών αυξάνεται συνέχεια. Όπως καταλαβαίνετε, η αναγνώριση φωνής είναι η μόνη βιομετρική μέθοδος που θα μπορούσε να εφαρμοστεί σε μια τέτοια κατάσταση. Ο δεύτερος λόγος είναι ότι το απαιτούμενο hardware (κάρτα ήχου και μικρόφωνο) συμπεριλαμβάνεται πια στον βασικό εξοπλισμό κάθε προσωπικού υπολογιστή, γεγονός που κάνει τη λύση της αναγνώρισης φωνής πολύ ελκυστική σε όποιον χρήστη ενδιαφέρεται να αυξήσει την ασφάλεια του υπολογιστικού του συστήματος. Πολλές εταιρείες λοιπόν, βλέποντας την τεράστια αγορά των προσωπικών υπολογιστών να ανοίγεται μπροστά τους στρέφονται στην αναγνώριση φωνής, βελτιώνοντας την υπάρχουσα τεχνολογία και προσπαθώντας να εξαλείψουν τα εγγενή μειονεκτήματα της μεθόδου.
Το βασικότερο πρόβλημα, πηγή ίσως και όλων των υπολοίπων, είναι το γεγονός ότι το σύστημα δεν μπορεί να λειτουργήσει ικανοποιητικά σε περιβάλλοντα με σχετικά μεγάλο υψηλό εξωτερικό θόρυβο. Αν και κανείς δεν σκοπεύει να χρησιμοποιήσει αναγνώριση φωνής σε ATM (ο θόρυβος του δρόμου καθιστά απαγορευτικές τέτοιες σκέψεις), κανείς δεν μπορεί να εξασφαλίσει ότι και σε οποιαδήποτε άλλη χρήση του συστήματος ο χρήστης θα βρίσκεται στο κατάλληλο περιβάλλον. Ένα ανοιχτό παράθυρο σε πολυσύχναστο δρόμο, συνάδελφοι ή πελάτες που συζητούν, μηχανές που λειτουργούν, είναι σίγουρο ότι θα δημιουργούσαν πολλά προβλήματα στο ειδικό λογισμικό που θα προσπαθούσε να εξακριβώσει αν όντως ο χρήστης είναι αυτός που

ισχυρίζεται.
Ακόμα κι αν ο θόρυβος είναι ανεκτός όμως, δεν πρέπει να ξεχνάμε ότι οι φωνητικές χορδές είναι από τα πιο ευαίσθητα μέρη του ανθρώπινου σώματος. Αν λοιπόν ο χρήστης είναι κρυωμένος (ή απλώς το προηγούμενο βράδυ έσπευσε να υποστηρίξει την αγαπημένη του ομάδα στον υπέρ πάντων αγώνα) ίσως αντιμετωπίσει δυσκολίες να επιβεβαιώσει την ταυτότητά του σε ένα σύστημα αναγνώρισης φωνής. Και όσο για βαριές περιπτώσεις όπως λαρυγγίτιδα, ας μην το συζητάμε. Η απώλεια φωνής σε ένα βιομετρικό σύστημα αναγνώρισης φωνής, ισοδυναμεί με την απώλεια δαχτύλου σε ένα σύστημα δακτυλικών αποτυπωμάτων. Τέλος, κάτι άλλο που αφήνει έντονα σημάδια στην ανθρώπινη φωνή είναι φυσικά το πέρασμα του χρόνου.
Όλα αυτά έχουν σαν αποτέλεσμα να δυσχεραίνεται η λειτουργία του συστήματος, το οποίο αρχίζει να απαιτεί μεγάλη συμμετοχή από το χρήστη, ζητώντας του κουραστικές επαναλήψεις ή βάζοντάς τον να απαγγείλει υπερβολικά μεγάλες φράσεις. Με αυτόν τον τρόπο αυξάνεται ο όγκος των δεδομένων προς σύγκριση, και διευκολύνεται έτσι η σωστότερη απόφαση. Η αντίδραση των κατασκευαστών βιομετρικών συστημάτων αναγνώρισης φωνής ήταν η ανάπτυξη ειδικής τεχνολογίας αφαίρεσης του εξωτερικού θορύβου από το βιομετρικά δείγματα, στην οποία ήδη έχουν γίνει σημαντικά βήματα. Μάλιστα, αν ρίξετε μια ματιά στις σελίδες των εταιρειών αναγνώρισης φωνής στο Internet, θα δείτε ότι οι περισσότερες διαφημίζουν την ακρίβεια των προϊόντων τους ως παρόμοια με αυτήν των δακτυλικών αποτυπωμάτων. Παρ' όλα αυτά, η αλήθεια είναι ότι σε αυτόν τον τομέα η αναγνώριση φωνής είναι ακόμα αρκετά πίσω σε σύγκριση με τα δακτυλικά αποτυπώματα., κάτι που φαίνεται κι από το συγκριτικό διάγραμμα που φιλοξενείται στον επίλογο του αφιερώματος.

4.4.4.1 Βασικές αρχές

Η αναγνώριση φωνής είναι ένα υβριδικό βιομετρικό σύστημα που συνδυάζει φυσικά χαρακτηριστικά με συμπεριφορές, αυξάνοντας με αυτόν τον τρόπο την ποιότητα του βιομετρικού προτύπου. Ξεκινώντας από τα φυσικά χαρακτηριστικά, να πούμε ότι η ανθρώπινη φωνή εξαρτάται από πάρα πολλούς παράγοντες. Το μήκος των φωνητικών χορδών για παράδειγμα, είναι ένας από αυτούς. Το σχήμα του στόματος, των ρινικών κοιλοτήτων, και του λάρυγγα έχει επίσης ιδιαίτερη σημασία. Όλα αυτά αλληλεπιδρούν μεταξύ τους και διαμορφώνουν ένα σύνολο ιδιοτήτων (χροιά, ύψος κ.λπ.) το οποίο χαρακτηρίζει με μοναδικό τρόπο κάθε ανθρώπινη φωνή. Στο σύνολο των φυσικών ιδιοτήτων έρχονται να προστεθούν και μερικές ιδιότητες με βάση συμπεριφορές, όπως ο ρυθμός ομιλίας ή ο τονισμός, οι οποίες διασφαλίζουν ακόμα περισσότερο τη μοναδικότητα του τελικού δείγματος.

4.4.5 Γεωμετρία και θερμογραφία προσώπου

Ανέκαθεν οι άνθρωποι χρησιμοποιούσαν τα χαρακτηριστικά του προσώπου για να θυμούνται και να αναγνωρίζουν ο ένας τον άλλο. Προσπαθώντας να προσομοιώσει τον τρόπο που συμβαίνει αυτό, η μέθοδος της αναγνώρισης προσώπου φιλοδοξεί να αποκτήσει μεγαλύτερη ακρίβεια και ικανότητα προσαρμογής στις αλλαγές.
Η αναγνώριση της ταυτότητας κάποιου ατόμου από την ανάλυση των χαρακτηριστικών του προσώπου του, είναι μια διαδικασία που κάθε άλλο παρά απλή θα μπορούσε να χαρακτηριστεί. Κατ' αρχήν μια κάμερα συλλαμβάνει την εικόνα του προσώπου του χρήστη, και στη συνέχεια το σύστημα προσπαθεί να εντοπίσει διάφορα βασικά σημεία πάνω σ' αυτήν, όπως τις θέσεις των ματιών, του στόματος, της μύτης κ.λπ. Αφού γίνει αυτό, οι αποστάσεις μεταξύ των βασικών σημείων

μετριούνται και τα αποτελέσματα αποθηκεύονται για να αποτελέσουν το βιομετρικό πρότυπο του χρήστη. Πιο εξελιγμένα συστήματα δημιουργούν τρισδιάστατα μοντέλα του προσώπου, προσφέροντας έτσι άλλη μια διάσταση για περισσότερο ακριβείς μετρήσεις.
Παρόμοια τεχνική είναι και η θερμογραφία προσώπου, η οποία χρησιμοποιεί υπέρυθρη κάμερα για να "χαρτογραφήσει" τη ροή του αίματος κάτω από την επιφάνεια του δέρματος. Οι σχηματισμοί θερμότητας των αιμοφόρων αγγείων που βρίσκονται κάτω από το δέρμα του προσώπου, είναι αρκετοί για να επιβεβαιώσουν την ταυτότητα κάποιου, αφού είναι μοναδικοί για κάθε άνθρωπο. Η μέθοδος της θερμογραφίας πλεονεκτεί σε σχέση με αυτήν της γεωμετρίας στο γεγονός ότι μπορεί να λειτουργήσει ικανοποιητικά σε περιβάλλοντα όχι καλά φωτισμένα. Από την άλλη πλευρά, ο εξοπλισμός που απαιτεί είναι πολύ πιο ακριβός.
Το βασικότερο πρόβλημα της αναγνώρισης προσώπου αποτελεί το γεγονός ότι πολλά από τα χαρακτηριστικά στα οποία βασίζεται η αναγνώριση μπορούν να αλλάξουν πολύ εύκολα με την πάροδο του χρόνου. Για παράδειγμα, το μήκος των μαλλιών. Γυαλιά που μπορεί να φοράει ο χρήστης κατά την αναγνώριση, μούσι ή μουστάκι θα δημιουργούσαν το ίδιο πρόβλημα. Κάποια παραπάνω κιλά ή ακόμα και μια μικρή κλίση του κεφαλιού θα μπορούσαν επίσης να μπερδέψουν το σύστημα. Για να αντεπεξέλθουν στις δυσκολίες αυτές, τα περισσότερα συστήματα αναγνώρισης προσώπου χρησιμοποιούν εξελιγμένες μεθόδους τεχνητής νοημοσύνης και αυτό-εκμάθησης. Με τον τρόπο αυτό προσαρμόζονται στις πιθανές αλλαγές, ώστε να μπορούν να συγκρίνουν με ακρίβεια τα νέα δείγματα με το βιομετρικό πρότυπο του χρήστη που είχε δημιουργηθεί κάποια στιγμή στο παρελθόν.
Στα συν της μεθόδου θα πρέπει να καταλογιστεί το υψηλό επίπεδο ακριβείας που επιτυγχάνεται, καθώς επίσης και η σχετικά καλή αποδοχή που έχει από το κοινό (παρόμοια με αυτήν των απλών φωτογραφιών). Τέλος, σημαντικό πλεονέκτημα είναι ότι η μέθοδος δεν κουράζει το χρήστη, ο οποίος το μόνο που έχει να κάνει είναι να σταθεί ακίνητος για μερικά δευτερόλεπτα.

4.4.6 Άλλες βιομετρικές μέθοδοι

4.4.6.1 Ρυθμός πληκτρολόγησης

Ο ρυθμός πληκτρολόγησης θεωρείται βιομετρική μέθοδος με βάση συμπεριφορά, και ήδη η ανάπτυξή του βρίσκεται σε καλό σημείο. Η μέθοδος εστιάζει στον τρόπο που πληκτρολογεί κάποιο άτομο, ελέγχοντας παραμέτρους όπως η καθυστέρηση ανάμεσα σε συγκεκριμένα πλήκτρα, ο μέσος όρος ταχύτητας κ.λπ. Το βασικό πρόβλημα της μεθόδου (όπως και όλων των μεθόδων βάσει συμπεριφοράς) είναι ότι η συμπεριφορά του χρήστη αλλάζει σχετικά εύκολα. Για παράδειγμα, καθώς η μέρα περνάει ο ρυθμός πληκτρολόγησης κάποιου πέφτει, αφού η κούραση αρχίζει να ενεργεί. Όσον αφορά τη χρήση της μεθόδου σε μεγάλες μάζες, την καθιστά απαγορευτική το γεγονός ότι πληκτρολόγηση δεν ξέρουν όλοι οι άνθρωποι, και όπως καταλαβαίνετε κάτω από κάποιες ταχύτητες παύει να υφίσταται οποιαδήποτε έννοια μέτρησης. Η εταιρεία NetNanny (http://www.netnanny.com) μας δίνει την ευκαιρία να πάρουμε μια ιδέα για τη Βιομετρική του αύριο, με το προϊόν BioPassword, ένα βιομετρικό σύστημα αναγνώρισης ρυθμού πληκτρολόγησης για προσωπικούς υπολογιστές. Στη σελίδα http://www.biopassword.com θα βρείτε περισσότερες πληροφορίες.

4.4.6.2 Αναγνώριση φλεβικής δομής

Η συγκεκριμένη μέθοδος προσπαθεί να "διαβάσει" τη φλεβική δομή που γίνεται αρκετά έντονη στο επάνω μέρος της ανθρώπινης παλάμης. Για να καταστεί αυτό δυνατό, χρησιμοποιείται υπέρυθρη ακτινοβολία. Συνήθως, για να τονιστεί ακόμα περισσότερο το "δέντρο" των φλεβών, ο χρήστης υποχρεούται να σφίξει το χέρι του σε γροθιά. Η ανάπτυξη της μεθόδου έχει ξεκινήσει αρκετά χρόνια τώρα, και μάλιστα κάποια προϊόντα υπάρχουν ήδη στην αγορά. Το γεγονός ότι τοποθετείται στα "μελλοντικά" συστήματα οφείλεται κυρίως στο ότι η πρακτική εφαρμογή της είναι ακόμα αρκετά περιορισμένη. Κάποια βιομετρικά προϊόντα ανάγνωσης της φλεβικής δομής μπορείτε να βρείτε στη σελίδα της Advanced Biometrics (http://www.adv-bio.net). Ενδιαφέρουσες πληροφορίες υπάρχουν και στη διεύθυνση http://innotts.co.uk/~joerice.

4.4.6.3 Αναγνώριση γεωμετρίας αυτιού

Αυτή η παράξενη βιομετρική μέθοδος, που από όλα τα μέρη του σώματος διάλεξε το αυτί ως το μέσο αναγνώρισης, θεωρείται αρκετά ακριβής και εφαρμόζεται ήδη σήμερα από αρκετές αστυνομίες ανά τον κόσμο. Οι βασικές της αρχές είναι παρόμοιες με τα υπόλοιπα συστήματα αναγνώρισης γεωμετρίας, αυτά του προσώπου και του χεριού. Μένει μόνο να δούμε αν κάποια στιγμή θα χρησιμοποιηθεί και για πιο γενικούς σκοπούς.

4.4.6.4 Έλεγχος DNA

Αν και ο έλεγχος DNA είναι σήμερα εφικτός μέσα σε διάστημα 10 λεπτών, δεν μπορεί να χαρακτηριστεί βιομετρική μέθοδος αφού η αναγνώριση δεν γίνεται αυτόματα. Αν αυτό γίνει κάποια στιγμή δυνατό, η νέα βιομετρική μέθοδος θα υποσκελίσει όλες τις άλλες στο θέμα της ακριβείας. Παρόλα αυτά, θα πρέπει να βελτιωθεί ο τρόπος λήψης του βιομετρικού δείγματος, αφού όλοι οι σημερινοί τρόποι (λήψη αίματος, σάλιου, ή άλλου σωματικού υγρού) είναι εξαιρετικά προβληματικοί και ανεφάρμοστοι σε ευρύτερη κλίμακα.

4.4.6.5 Αναγνώριση σωματικής οσμής

Αν έχετε ταξιδέψει με τον ηλεκτρικό καλοκαίρι και μεσημβρινές ώρες, σίγουρα θα έχετε διαπιστώσει ότι η σωματική μυρωδιά μπορεί να χαρακτηρίσει κάποιον με πολύ μοναδικό τρόπο... Ακριβώς αυτό το γεγονός προσπαθεί λοιπόν να εκμεταλλευτεί μια νέα βιομετρική μέθοδος, η οποία βρίσκεται ακόμα σε πολύ πρώιμο στάδιο. Το σύστημα βασίζεται στην ανάλυση της χημικής σύστασης της οσμής που εκπέμπει το ανθρώπινο σώμα, ενώ το δείγμα συνήθως λαμβάνεται από το πίσω μέρος της παλάμης.

4.4.6.6 Αποτυπώματα παλάμης

Το σύστημα αυτό λειτουργεί παρόμοια με τα συστήματα των δακτυλικών αποτυπωμάτων, διαβάζοντας αντί για την άκρη του δαχτύλου τις γραμμώσεις της παλάμης του χρήστη. Μέχρι τώρα έχει χρησιμοποιηθεί μόνο σε ποινικές εφαρμογές, αλλά οι εταιρείες που ασχολούνται με τη μέθοδο ελπίζουν κάποια στιγμή να τη φέρουν και στην πολιτική χρήση. Η μέθοδος θεωρείται αρκετά ακριβής.

4.5 Ψηφιακές υπογραφές

Οι ψηφιακές υπογραφές χρησιμοποιούν την κρυπτογραφία δημοσίου κλειδιού. Ο χρήστης διαθέτει δύο κλειδιά (το δημόσιο και το ιδιωτικό) τα οποία συνδέονται με κάποιο μαθηματικό συσχετισμό. Η σχέση των κλειδιών είναι τέτοια όπου αν κάποιος γνωρίζει το ένα κλειδί να είναι πρακτικά αδύνατον να υπολογίσει το άλλο. Το ένα κλειδί χρησιμοποιείται για τη δημιουργία της υπογραφής και το άλλο για την επαλήθευσή της. Η διαφοροποίηση από την κρυπτογράφηση, έγκειται στο ότι για τη δημιουργία της ηλεκτρονικής υπογραφής ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί και για την επαλήθευσή της ο παραλήπτης χρησιμοποιεί το δημόσιο κλειδί του αποστολέα.
Στη διαδικασία της δημιουργίας και επαλήθευσης της υπογραφής εμπλέκεται και η έννοια της συνάρτησης κατακερματισμού (ή κατατεμαχισμού one way hash). Με την εφαρμογή της συνάρτησης κατακερματισμού, από ένα μήνυμα ανεξαρτήτου μεγέθους, παράγεται η «σύνοψή του», η οποία είναι μία σειρά από bits συγκεκριμένου μεγέθους (π.χ. 128 ή 160 bits). Η σύνοψη του μηνύματος (fingerprint ή message digest) είναι μία ψηφιακή αναπαράσταση του μηνύματος, η οποία είναι μοναδική για το μήνυμα και το αντιπροσωπεύει.
Η συνάρτηση κατακερματισμού είναι μονόδρομη διότι από την σύνοψη που δημιουργεί, είναι υπολογιστικά αδύνατον κάποιος να εξάγει το αρχικό μήνυμα. Η πιθανότητα δύο μηνύματα να έχουν την ίδια σύνοψη είναι εξαιρετικά μικρή. Αυτό σημαίνει ότι αν το μήνυμα του αποστολέα έχει κάποια συγκεκριμένη σύνοψη και το μήνυμα που λάβει ο παραλήπτης (χρησιμοποιώντας την ίδια συνάρτηση κατακερματισμού) παράγει διαφορετική σύνοψη, τότε το μήνυμα κατά την μετάδοσή του έχει αλλοιωθεί (μη ακεραιότητα). Οποιαδήποτε αλλαγή σε ένα μήνυμα συνεπάγεται και τη δημιουργία διαφορετικής σύνοψης.
Η ηλεκτρονική υπογραφή, στην ουσία είναι η κρυπτογραφημένη με το ιδιωτικό κλειδί του αποστολέα σύνοψη. Δηλαδή, η ψηφιακή υπογραφή (σε αντίθεση με την ιδιόχειρη υπογραφή) είναι διαφορετική για κάθε μήνυμα!
Θεωρώντας ότι ο αποστολέας έχει ένα συγκεκριμένο ζευγάρι κλειδιών και το ιδιωτικό του κλειδί είναι στην πλήρη κατοχή του, τότε το γεγονός ότι ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί για να κρυπτογραφήσει το μήνυμα, πιστοποιεί στον παραλήπτη που το αποκρυπτογραφεί με το αντίστοιχο δημόσιο κλειδί (του αποστολέα) την ταυτότητα του αποστολέα (αυθεντικότητα). Η ψηφιακή υπογραφή είναι ένας τρόπος αυθεντικοποίησης του αποστολέα του μηνύματος.
Μία ψηφιακή υπογραφή μπορεί να 'πλαστογραφηθεί' εάν ο δικαιούχος του ιδιωτικού κλειδιού δεν το έχει υπό τον πλήρη έλεγχό του (π.χ. χάσει το μέσο στο οποίο έχει αποθηκευτεί το ιδιωτικό κλειδί).

Για να υποκαταστήσουν οι ψηφιακές υπογραφές τις χειρόγραφες είναι απαραίτητο να πληρούν τις εξής απαιτήσεις:

- **Ο παραλήπτης να μπορεί να επιβεβαιώνει την ταυτότητα που δηλώνει ο αποστολέας.**
  Η πρώτη απαίτηση είναι απαραίτητη, για παράδειγμα στα οικονομικά συστήματα. Όταν ο υπολογιστής ενός πελάτη δώσει εντολή στον υπολογιστή μιας τράπεζες για την αγορά μιας ποσότητας χρυσού, ο υπολογιστής της τράπεζας απαιτείται είναι ικανός να διασφαλίσει ότι ο υπολογιστής που δίνει

την εντολή ανήκει πράγματι στη συγκεκριμένη εταιρία, της οποίας ο λογαριασμός πρέπει να χρεωθεί.

- **Ο αποστολέας να μη μπορεί αργότερα να αρνηθεί το περιεχόμενο του μηνύματος**
  Η δεύτερη απαίτηση είναι αναγκαία για την προστασία της τράπεζας από απάτη Υποθέτουμε ότι η τράπεζα αγοράζει την ποσότητα χρυσού (για λογαριασμό το πελάτη) και αμέσως μετά η τιμή του χρυσού πέφτει απότομα. Ένας μη έντιμος πελάτης θα μπορούσε να κάνει αγωγή στην τράπεζα, ισχυριζόμενος ότι ποτέ δεν έδωσε εντολή για αγορά χρυσού. Όταν η τράπεζα παρουσιάσει το μήνυμα στο δικαστήριο, ο πελάτης δεν παραδέχεται ότι το έστειλε.

- **Ο παραλήπτης να μη μπορεί να κατασκευάσει το μήνυμα από μόνος του.**
  Η τρίτη απαίτηση χρειάζεται για να προστατέψει τον πελάτη από το γεγονός ότι τιμή του χρυσού εκτινάχτηκε στα ύψη και η τράπεζα προσπαθεί να κατασκευάσει ένα υπογεγραμμένο μήνυμα στο οποίο ο πελάτης θα φαίνεται να ζητά, για παράδειγμα, μια ράβδο χρυσού αντί για έναν τόνο!

4.5.1 Δημιουργία και επαλήθευση ψηφιακής υπογραφής

Η χρήση της ηλεκτρονικής υπογραφής περιλαμβάνει δύο διαδικασίες: τη δημιουργία της υπογραφής και την επαλήθευσή της. Παρακάτω, θα αναφέρουμε βήμα προς βήμα τις ενέργειες του αποστολέα και του παραλήπτη ώστε να γίνει κατανοητός ο μηχανισμός της δημιουργίας και επαλήθευσης της ψηφιακής υπογραφής.

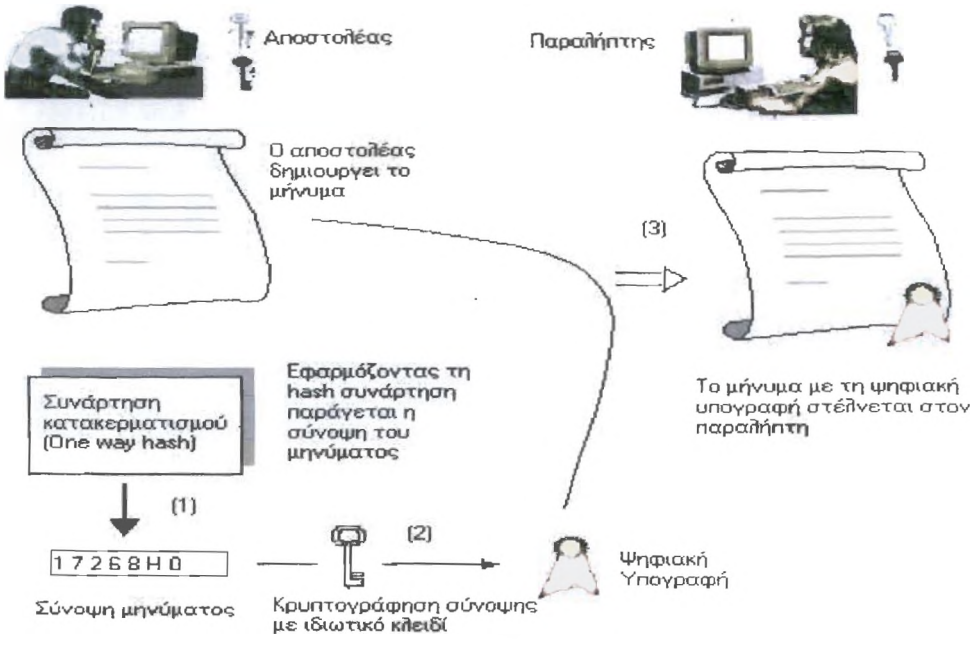
Αποστολέας

1. Ο αποστολέας χρησιμοποιώντας κάποιον αλγόριθμο κατακερματισμού (one way hash) δημιουργεί τη σύνοψη του μηνύματος (message digest) που θέλει να στείλει. Ανεξάρτητα από το μέγεθος του μηνύματος, αυτό που θα παραχθεί θα είναι μία συγκεκριμένου μήκους σειρά ψηφίων.
2. Με το ιδιωτικό του κλειδί, ο αποστολέας κρυπτογραφεί τη σύνοψη. Αυτό που παράγεται είναι η ψηφιακή υπογραφή. Η υπογραφή είναι ουσιαστικά μία σειρά ψηφίων συγκεκριμένου πλήθους.
3. Η κρυπτογραφημένη σύνοψη (ψηφιακή υπογραφή) προσαρτάται στο κείμενο και το μήνυμα με τη ψηφιακή υπογραφή μεταδίδονται μέσω του δικτύου (σημειώνεται ότι ο αποστολέας αν επιθυμεί μπορεί να κρυπτογραφήσει το μήνυμά του με το δημόσιο κλειδί του παραλήπτη).

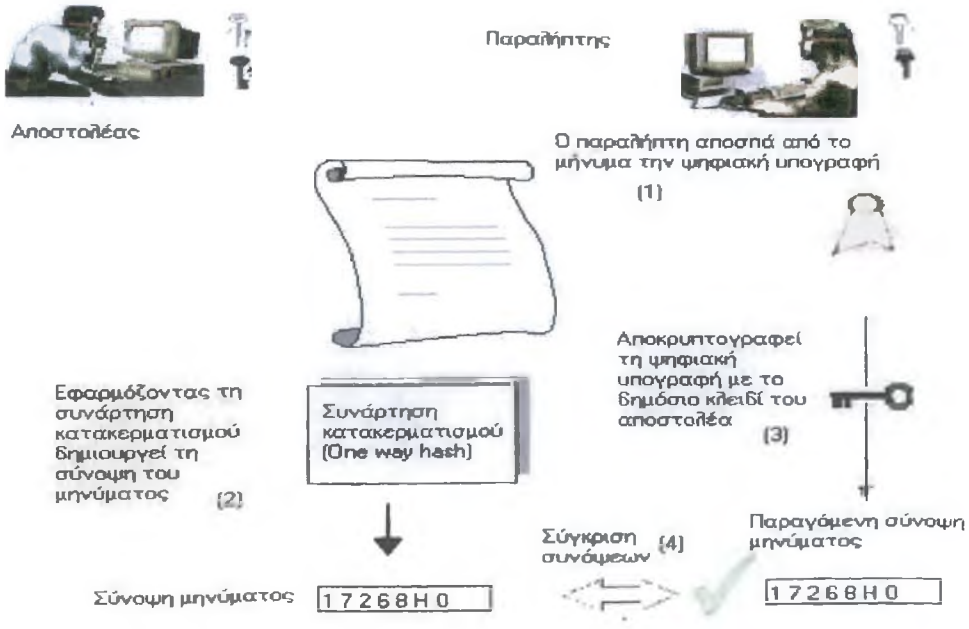
Παραλήπτης

1. Ο παραλήπτης αποσπά από το μήνυμα την ψηφιακή υπογραφή (κρυπτογραφημένη, με το ιδιωτικό κλειδί του αποστολέα, σύνοψη).
2. Εφαρμόζοντας στο μήνυμα που έλαβε τον ίδιο αλγόριθμο κατακερματισμού, ο παραλήπτης δημιουργεί τη σύνοψη του μηνύματος.
3. Στη συνέχεια, αποκρυπτογραφεί με το δημόσιο κλειδί του αποστολέα, την κρυπτογραφημένη σύνοψη του μηνύματος (ψηφιακή υπογραφή).

4. Συγκρίνονται οι δύο συνόψεις και αν βρεθούν ίδιες, αυτό σημαίνει ότι το μήνυμα που έλαβε ο παραλήπτης είναι ακέραιο. Αν το μήνυμα έχει μεταβληθεί, η σύνοψη που θα παράγει ο παραλήπτης θα είναι διαφορετική από την σύνοψη που έχει κρυπτογραφηθεί.



Σχήμα 4.1: Δημιουργία και επαλήθευση ψηφιακής υπογραφής



Σχήμα 4.2: Επαλήθευση ψηφιακής υπογραφής

4.5.2 Διαχείριση κλειδιών

Ορισμένα κρυπτοσυστήματα, της RSA έχουν την ιδιότητα ότι τόσο το δημόσιο κλειδί όσο και το ιδιωτικό κλειδί μπορούν να χρησιμοποιηθούν και για την κρυπτογράφηση και για την αποκρυπτογράφηση. Κατά συνέπεια το ίδιο ζεύγος κλειδιών μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση της πληροφορίας και για την ψηφιακή υπογραφή του μηνύματος. Όταν το ζεύγος των κλειδιών χρησιμοποιείται για ψηφιακές υπογραφές, δεν θα πρέπει να δημιουργούνται αντίγραφα ασφαλείας του ιδιωτικού κλειδιού, ενώ θα πρέπει να καταστρέφεται στο τέλος της ενεργούς του ζωής, καθώς αν ποτέ το ιδιωτικό κλειδί αποκαλυφθεί μπορεί να χρησιμοποιηθεί για την πλαστογράφηση υπογραφών. Αντίθετα, αν το ζεύγος κλειδιών χρησιμοποιείται για την κρυπτογράφηση πληροφορίας το ιδιωτικό κλειδί είναι αναγκαίο να φυλάσσεται για όσο το δυνατόν περισσότερο καθώς η απώλεια του θα έχει ως αποτέλεσμα να μην είναι δυνατή η ανάγνωση των δεδομένων που έχουν κρυπτογραφηθεί με το δημόσιο ανάλογο του. Η αντίθεση αυτή της απαιτήσεις για κάθε περίπτωση έχει οδηγήσει στο να είναι γενικά προτιμητέα η χρησιμοποίηση δύο ζευγών κλειδιών, ένα για την κρυπτογραφία και ένα για της ψηφιακές υπογραφές.

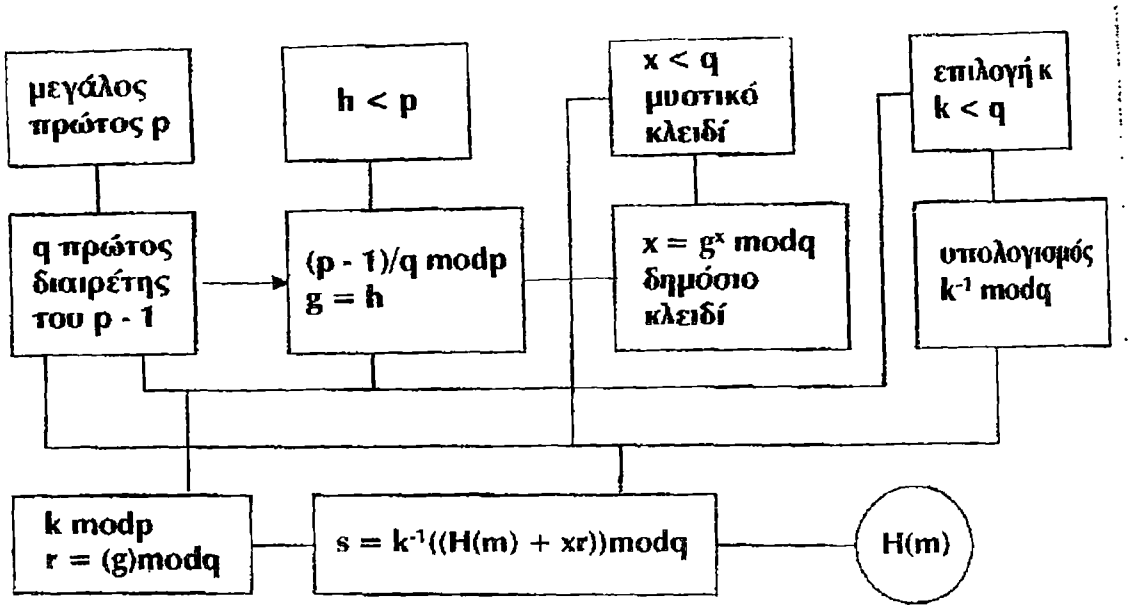
4.5.3 Digital Signature Algorithm (DSA)

Ο αλγόριθμο ς δημόσιου κλειδιού DSA αναπτύχθηκε από το γραφείο Εθνικής Ασφάλειας των Η.Π.Α (NSA) για την παραγωγή ψηφιακών υπογραφών. Το Εθνικό Ινστιτούτο Προτυποποίησης και Τεχνολογίας (NIST) δημοσίευσε τον αλγόριθμο στο Πρότυπο Ψηφιακής Υπογραφής (Digital Signature Standard, DSS) ώστε να αποτελέσει το πρότυπο της ψηφιακής πιστοποίησης της αμερικανικής κυβέρνησης. Η προτυποποίηση του αλγορίθμου έγινε τον Μάιο του 1994. Ο αλγόριθμος DSA μοιάζει με τον αλγόριθμο El Gamal.

Ο DSA όπως και ο El Gamal βασίζεται στη δυσκολία υπολογισμού των διακριτών λογαρίθμων. Σε σχέση με τον RSA που μπορεί να χρησιμοποιηθεί τόσο για κρυπτογράφηση όσο και για ψηφιακές υπογραφές, ο DSA μπορεί να εφαρμοστεί μόνο στο χώρο των ψηφιακών υπογραφών.

Τα βήματα του αλγορίθμου DSA είναι:

1. Επιλέγεται ένας μεγάλος πρώτος αριθμός p μεταξύ 512 και 1024 bits.
2. Βρίσκεται ένας πρώτος παράγοντας q του p-1.
3. Υπολογίζεται $g=h^{(p-1)/q} \bmod p$, όπου h ένας αριθμός μικρότερος από p-1.
4. Διαλέγουμε έναν άλλο αριθμό $x<q$ ως το private key του αποστολέα.
5. Υπολογίζεται $y=g^x \bmod p$ και χρησιμοποιείται ως το public key του αποστολέα.
6. Ο αποστολέας υπογράφει το μήνυμα με το ζευγάρι (r,s) όπου $r=(g^k \bmod p) \bmod q$ και $s=(k^{-1} (SHA1(m)+xr)) \bmod q$, όπου m το μήνυμα, k ένας τυχαίος αριθμός και SHA1 η συνάρτηση για message digest.
7. Επιλέγεται ένας μεγάλος πρώτος αριθμός p μεταξύ 512 και 1024 bits.



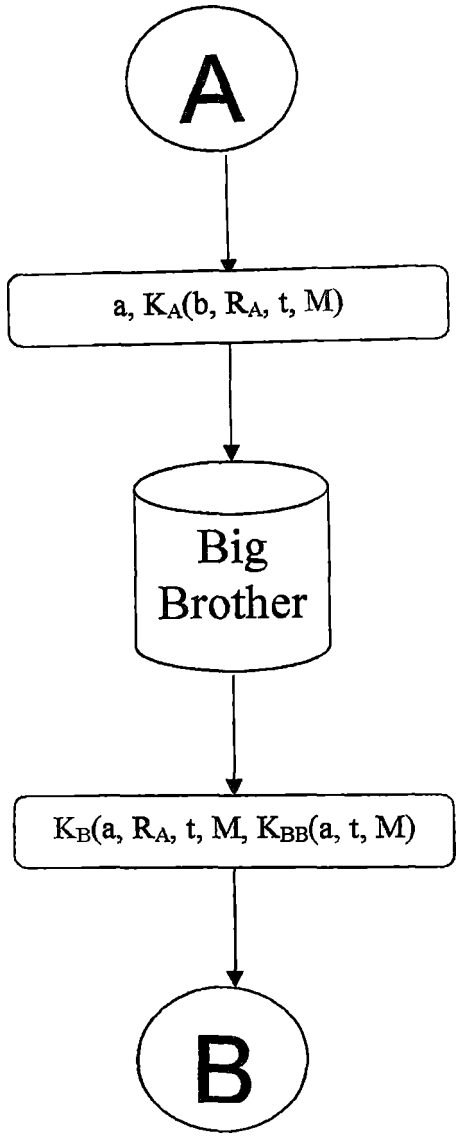
Σχήμα 4.3: διαδικασία λειτουργίας του DSA

4.5.4 Ψηφιακές υπογραφές με χρήση συμμετρικής κρυπτογραφίας

Για την κατασκευή ψηφιακής υπογραφής με κρυπτογραφία μυστικού κλειδιού θεωρούμε ότι υπάρχει μια κεντρική εξουσία (την ονομάζουμε Big Brother) η οποία έχει γνώση όλων των πραγμάτων και την οποία εμπιστεύονται όλοι.
Σύμφωνα με αυτή την τεχνική κάθε χρήστης επιλέγει ένα μυστικό κλειδί το οποίο μεταφέρει με ένα ασφαλές μέσο στον Big Brother. Έτσι κάθε χρήστης θα έχει ένα μυστικό κλειδί που θα γνωρίζουν μόνο αυτός και ο Big Brother και θα το χρησιμοποιούν για τις μεταξύ τους επικοινωνίες.
Έστω ότι ο χρήστης Α θέλει να στείλει ένα υπογεγραμμένο μήνυμα καθαρού κειμένου, *M*, στον Β

1. Ο Α δημιουργεί το K_A(b, R_A, t, M) όπου *b* είναι η ταυτότητα του χρήστη Β, R_A η πρόκληση από το χρήστη Α και *t* μια χρονοσφραγίδα και το στέλνει στον Big Brother
2. Στη συνέχεια ο Big Brother βλέπει το μήνυμα του Α, το αποκρυπτογραφεί και στέλνει ένα μήνυμα στον Β που περιέχει το μήνυμα καθαρού κειμένου του Α και το υπογεγραμμένο μήνυμα K_{BB} *(a,t, M)*
3. Τέλος ο Β ανταποκρίνεται στην απαίτηση του Α.

Ο Α δεν μπορεί να αρνηθεί ότι έστειλε το μήνυμα στον Β, γιατί ο Β έχει το υπογεγραμμένο μήνυμα K_{BB} *(a,t, M)*. Αυτό το υπογεγραμμένο μήνυμα προέρχεται από τον Big Brother που αν το αποκρυπτογραφήσει αποδεικνύει ότι ο Α έστειλε το *M* στον Β, αφού ο Big Brother δε μπορεί να δεχθεί ένα μήνυμα από τον Α παρά μόνο αν αυτό είναι κρυπτογραφημένο με το K_A
Η διαδικασία αυτή απεικονίζεται στο παρακάτω σχήμα:



Σχήμα 4.4: Ψηφιακές υπογραφές με την τεχνική του Big Brother.

Η κατασκευή ψηφιακής υπογραφής με κρυπτογραφία μυστικού κλειδιού έχει πολλά προβλήματα:
Ένα πρόβλημα είναι η δυνατότητα επανάληψης των μηνυμάτων από έναν εισβολέα. Η εξάλειψη του προβλήματος επιτυγχάνεται με τη χρήση χρονοσφραγίδων. Επιπλέον, ο χρήστης Β μπορεί να ελέγχει όλα τα πρόσφατα μηνύματα ώστε να βλέπει αν το R_A, χρησιμοποιήθηκε σε κάποιο από αυτά. Αν συμβαίνει κάτι τέτοιο, το μήνυμα απορρίπτεται ως επανάληψη κάποιου άλλου. Σημειώνουμε επίσης ότι ο Β μπορεί να απορρίψει αρκετά παλιά μηνύματα βασιζόμενος και στις χρονοσφραγίδες. Για προστασία ενάντια στις επιθέσεις "στιγμιαίας επανάληψης", ο Β μπορεί να ελέγχει το R_A του κάθε εισερχόμενου μηνύματος και να βλέπει αν έχει λάβει ένα τέτοιο μήνυμα από τον Α στη προηγούμενη ώρα. Αν όχι, ο Β μπορεί με ασφάλεια να θεωρήσει ότι πρόκειται για μια καινούργια απαίτηση.

Το μεγαλύτερο όμως πρόβλημα που εμφανίζεται με τη χρήση κρυπτογραφίας μυστικού κλειδιού για τις ψηφιακές υπογραφές είναι ότι οι πάντες πρέπει να συμφωνήσουν ώστε να εμπιστεύονται τον Big Brother. Επιπλέον, ο Big Brother είναι σε θέση να διαβάζει όλα τα υπογεγραμμένα μηνύματα. Οι περισσότερο λογικοί υποψήφιοι για τη διαχείριση του Big Brother server είναι οι κυβερνήσεις, οι τράπεζες, ή οι δικαστικές αρχές. Οι οργανισμοί όμως αυτοί δεν τυγχάνουν καθολικής εμπιστοσύνης σε όλες τις χώρες. Θα ήταν επομένως καλύτερα αν τα υπογεγραμμένα έγγραφα δεν απαιτούσαν μια έμπιστη αρχή. Η λύση στο πρόβλημα αυτό είναι η χρήση της κρυπτογραφίας δημοσίου κλειδιού.
Αξίζει να σημειωθεί ότι η κατασκευή ψηφιακής υπογραφής με κρυπτογραφία μυστικού κλειδιού χρησιμοποιείται ελάχιστα έως καθόλου.

4.5.5 Βασικές διαφορές ψηφιακών και χειρόγραφων υπογραφών

Όταν χρησιμοποιείται χειρόγραφη υπογραφή σε έγγραφο, η τελευταία αποτελεί αναπόσπαστο μέρος του υπογεγραμμένου φυσικού εγγράφου. Από την άλλη πλευρά, μια ψηφιακή υπογραφή «συνενώνεται» στο τέλος του ηλεκτρονικού εγγράφου (μηνύματος) ή εμπεριέχεται στην κωδικοποιημένη του μορφή.
Μια συμβατική υπογραφή επικυρώνεται όταν συγκρίνεται με άλλες αυθεντικές υπογραφές. Για παράδειγμα, όταν κάποιος υπογράφει μια επιταγή, υποθέτουμε ότι ο πωλητής συγκρίνει την υπογραφή που βάζει ο πελάτης στην επιταγή με εκείνη που υπάρχει στο πίσω μέρος της πιστωτικής του κάρτας. Τότε επαληθεύει την υπογραφή. Φυσικά, αυτή η μέθοδος δεν είναι πολύ ασφαλής, αφού η πλαστογράφηση μιας υπογραφής δεν είναι και πολύ δύσκολη. Οι ψηφιακές υπογραφές, από την άλλη, μπορεί να επαληθευτούν με τη χρήση ενός γνωστού σε όλους αλγόριθμου επαλήθευσης. Έτσι, ο οποιοσδήποτε μπορεί να επαληθεύσει μια ψηφιακή υπογραφή. Η χρήση ενός ασφαλούς σχήματος ηλεκτρονικών υπογραφών αποτρέπει ενδεχόμενες πλαστογραφίες.
Μια άλλη αξιοσημείωτη διαφορά ανάμεσα στις χειρόγραφες και τις ηλεκτρονικές υπογραφές είναι και ότι το αντίγραφο της ηλεκτρονικής υπογραφής ενός μηνύματος είναι πανομοιότυπο με το πρωτότυπο, σε αντίθεση με το αντίγραφο χειρόγραφης υπογραφής, το οποίο μπορεί να διακριθεί από το πρωτότυπο. Για το λόγο αυτό θα πρέπει να αποτρέπεται η εκ νέου χρησιμοποίηση αντιγράφων υπογεγραμμένων μηνυμάτων. Για παράδειγμα, αυτά θα μπορούσε να είναι εντολές πληρωμής, με συνέπεια την πρόκληση οικονομικής ζημιάς του υπογράφοντος. Αν ο χρήστης Α αποστείλει ένα ηλεκτρονικά υπογεγραμμένο μήνυμα - εντολή πληρωμής το οποίο θα επιτρέπει στο χρήστη Β να πάρει από τον τραπεζικό του λογαριασμό 1000 ευρώ, τότε θα πρέπει ο Α να είναι βέβαιος ότι ο Β θα μπορεί να κάνει χρήση της εντολής πληρωμής μια μόνο φορά. Αυτός ο κίνδυνος αντιμετωπίζεται με την ενσωμάτωση στο μήνυμα και άλλων πληροφοριών, όπως αύξοντος αριθμού, ημερομηνίας και χρόνου έκδοσης. Η ηλεκτρονική υπογραφή εξαρτάται, ασφαλώς, και από αυτές τις πρόσθετες πληροφορίες, εμποδίζοντας έτσι την επαναχρησιμοποίηση του ηλεκτρονικά υπογεγραμμένου μηνύματος.

4.6 Πρωτόκολλα Πιστοποίησης Αυθεντικότητας

Το γενικό μοντέλο που χρησιμοποιούν τα πρωτόκολλα για την πιστοποίηση αυθεντικότητας όταν ένας χρήστης (στην ουσία μια διεργασία) επιθυμεί να εγκαταστήσει μια ασφαλή σύνδεση με έναν δεύτερο χρήστη είναι το ακόλουθο:

1. Ο πρώτος χρήστης ξεκινάει στέλνοντας ένα μήνυμα στον άλλον ή σε ένα *κέντρο διανομής κλειδιών* (Key Distribution Center, KDC) το οποίο είναι αξιόπιστο. Καθώς τα μηνύματα αυτά στέλνονται, ένας εισβολέας μπορεί να υποκλέψει, να τροποποιήσει και να ξαναστείλει τα μηνύματα με σκοπό να παραπλανήσει τους χρήστες. Παρόλα αυτά, όταν το πρωτόκολλο έχει ολοκληρωθεί οι δύο χρήστες είναι σίγουροι ότι μιλάνε ο ένας με τον άλλον.

2. Επιπλέον, στα περισσότερα πρωτόκολλα, εγκαθίσταται μεταξύ των δύο χρηστών ένα μυστικό *κλειδί συνόδου* (session key) για χρήση στην επερχόμενη συνομιλία. Στην πράξη, για λόγους απόδοσης, όλη η κίνηση δεδομένων κρυπτογραφείται χρησιμοποιώντας κρυπτογραφία μυστικού κλειδιού, ενώ η κρυπτογραφία δημόσιου κλειδιού χρησιμοποιείται στα πρωτόκολλα πιστοποίησης αυθεντικότητας καθώς και για την κρυπτογράφηση των κλειδιών συνόδου. Ο λόγος για τον οποίο χρησιμοποιείται ένα νέο και τυχαία επιλεγμένο κλειδί συνόδου για κάθε νέα σύνδεση είναι η ελαχιστοποίηση της ποσότητας πληροφορίας που διακινείται χρησιμοποιώντας τα δημόσια ή μυστικά κλειδιά των χρηστών. Με τον τρόπο αυτόν επιτυγχάνουμε μείωση της ποσότητας του κρυπτογραφημένου κειμένου που μπορεί να υποκλέψει και να επεξεργαστεί ένας εισβολέας.

Τα σύμβολα που θα χρησιμοποιήσουμε για την ανάλυση των πρωτοκόλλων πιστοποίησης αυθεντικότητας είναι τα ακόλουθα:

α: η ταυτότητα του χρήστη Α
β: η ταυτότητα του χρήστη Β
R_i: οι προκλήσεις, όπου ο δείκτης συμβολίζει το χρήστη που προκαλεί
K_i: τα κλειδιά, όπου ο δείκτης συμβολίζει τον ιδιοκτήτη του κλειδιού
K_s: το κλειδί συνόδου

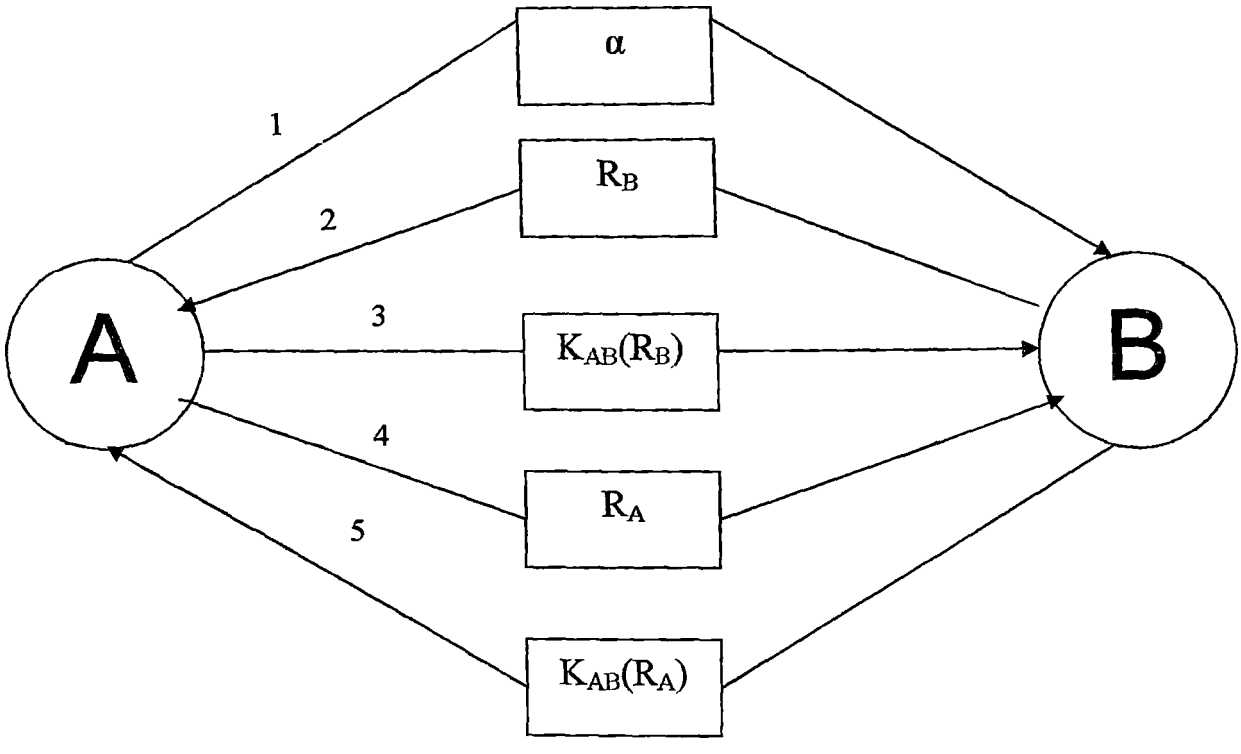
4.6.1 Πιστοποίηση Αυθεντικότητας βάση μοιραζόμενου μυστικού κλειδιού

Έστω οι χρήστες Α και Β μοιράζονται ένα μυστικό κλειδί K_A. Αυτό συμφωνείται μέσα από ένα ασφαλές κανάλι επικοινωνίας (π.χ. προσωπική συνάντηση, τηλέφωνο). Το πρωτόκολλο αυτό ονομάζεται challenge-response (πρόκλησης-απόκρισης). Ο ένας χρήστης στέλνει στον άλλο έναν τυχαίο αριθμό και μετασχηματίζοντάς τον με ειδικό τρόπο επιστρέφει το αποτέλεσμα. Στο σχήμα βλέπουμε μια αμφίδρομη πιστοποίηση αυθεντικότητας που απαιτεί ένα πρωτόκολλο challenge-response.

1. Στο πρώτο μήνυμα ο χρήστης Α στέλνει την ταυτότητά του, *α*, στο χρήστη Β με τέτοιο τρόπο ώστε να γίνεται κατανοητός από αυτόν.

2. Ο χρήστης Β, που δεν έχει τρόπο να γνωρίζει αν το μήνυμα αυτό προέρχεται από το χρήστη Α ή από έναν εισβολέα, επιλέγει μια πρόκληση, δηλαδή ένα μεγάλο τυχαίο αριθμό, R_B, και τον στέλνει πίσω στον Α ως μήνυμα 2 σε καθαρό κείμενο.

3. Στη συνέχεια, ο Α κρυπτογραφεί το μήνυμα με το κλειδί που μοιράζεται με τον Β και στέλνει το κρυπτογραφημένο κείμενο, $K_{AB}(R_B)$, πίσω ως μήνυμα 3.



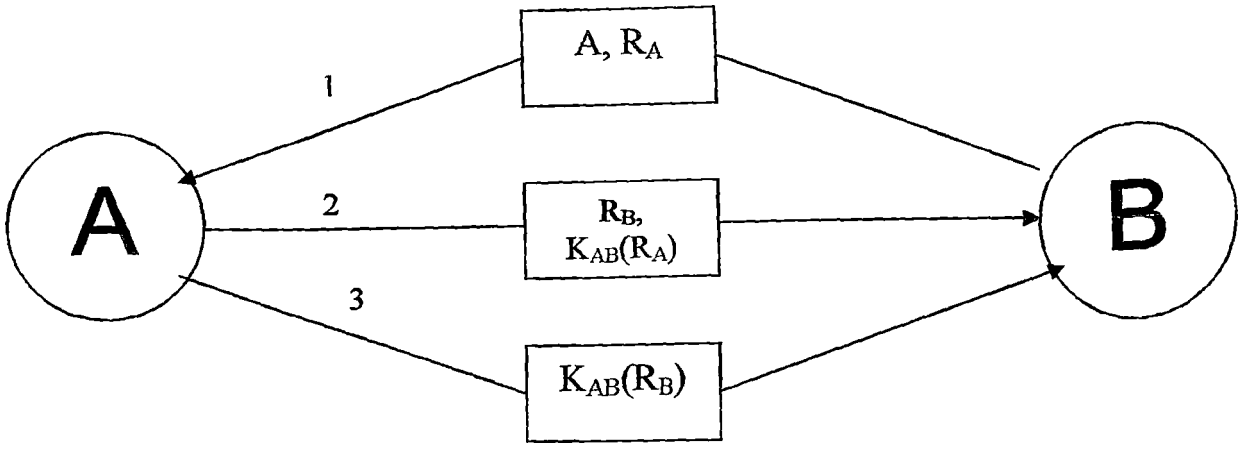
Σχήμα 4.5: Αμφίδρομο πρωτόκολλο πιστοποίησης αυθεντικότητας

4. Όταν ο Β δει το μήνυμα αυτό, γνωρίζει άμεσα ότι προέρχεται από τον Α αφού ένας εισβολέας δε θα γνώριζε το K_{AB} και επομένως δε θα μπορούσε να παράγει το μήνυμα αυτό. Επιπλέον, εφόσον το R_B είναι τυχαία επιλεγμένο είναι απίθανο ο εισβολέας να έχει υποκλέψει το R_B καθώς και την απόκρισή του σε προηγούμενη σύνοδο.

5. Στο σημείο αυτό, ο Β είναι σίγουρος ότι επικοινωνεί με τον Α, αλλά ο Α δεν είναι σίγουρος για τίποτα. Ο εισβολέας μπορεί να έχει υποκλέψει το μήνυμα 1 και να έχει στείλει αυτός το R_B. Για να μάθει ο Α με ποιον μιλάει, επιλέγει ένα τυχαίο αριθμό, R_A, και τον στέλνει στον Β ως μήνυμα 4 σε μορφή καθαρού κειμένου.

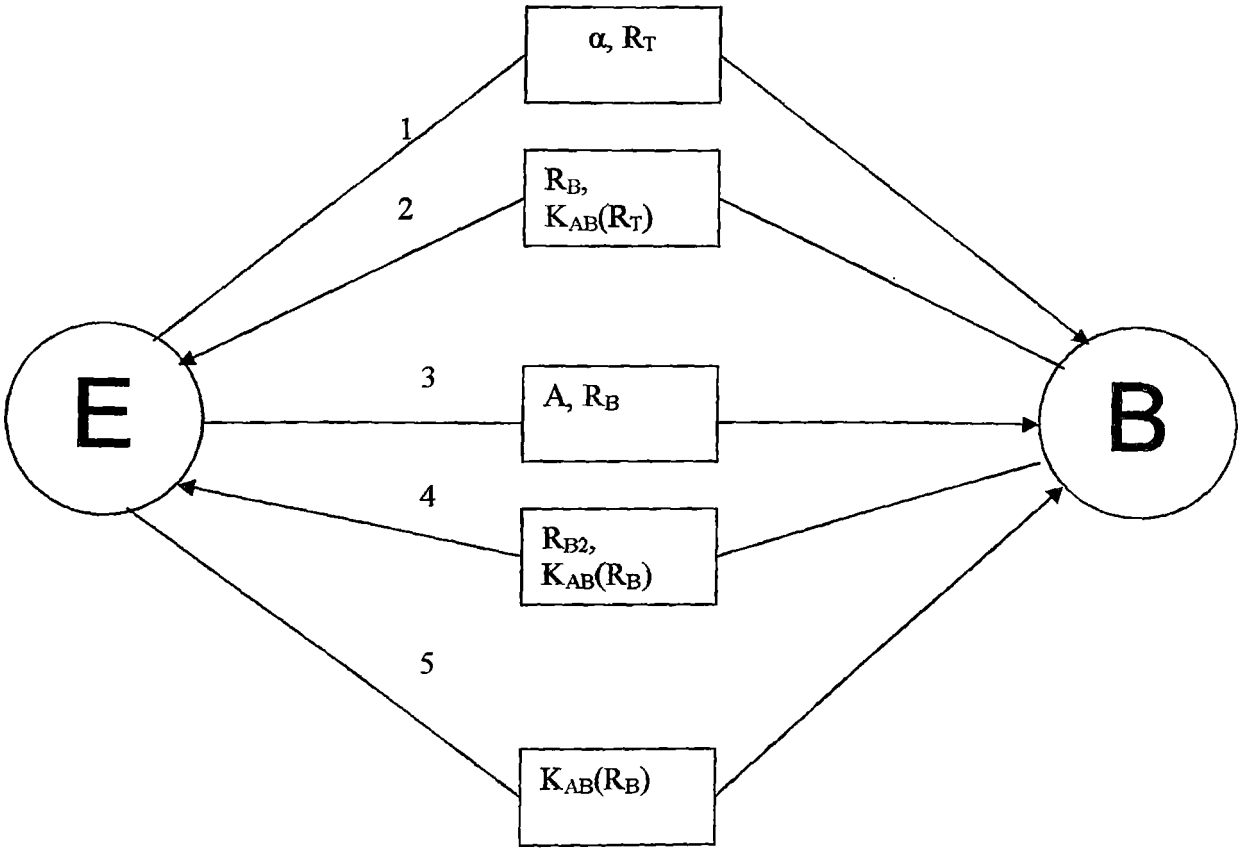
6. Όταν ο Β απαντήσει με το $K_{AB}(R_A)$, ο Α γνωρίζει ότι μιλάει με τον Β. Αν και οι δύο επιθυμούν να εγκαταστήσουν αυτή τη στιγμή ένα κλειδί συνόδου, ο Α μπορεί να επιλέξει ένα τέτοιο K_s και να το στείλει στον Β κρυπτογραφημένο με το K_{AB}.

Παρατηρώντας το πρωτόκολλο του σχήματος θα μπορούσε κάποιος εύκολα να θεωρήσει ότι το πρωτόκολλο έχει πλεονάζοντα μηνύματα και να το απλοποιήσει κάνοντας λιγότερα βήματα, όπως δείχνει το σχήμα 4.6.



Σχήμα 4.6: Απλοποιημένο αμφίδρομο πρωτόκολλο πιστοποίησης αυθεντικότητας

Στο σχήμα 4.7 βλέπουμε ότι το πρωτόκολλο αποτελείται από τρία μηνύματα αντί για πέντε. Ο χρήστης Α ξεκινά από μόνος του τη διαδικασία challenge-response αντί να περιμένει να γίνει αυτό πρώτα από τον Β. Το πρωτόκολλο είναι συντομότερο, όμως δυστυχώς είναι και λανθασμένο. Ο εισβολέας χρησιμοποιώντας την επίθεση της αντανάκλασης (reflection attack) υπό συγκεκριμένες συνθήκες μπορεί να παρέμβει στην επικοινωνία. Στο σχήμα 4.7 βλέπουμε πως λειτουργεί η επίθεση αντανάκλασης.



Σχήμα 4.7: Η επίθεση της αντανάκλασης

1. Αυτή ξεκινάει με τον εισβολέα ο οποίος διεκδικεί τη θέση του χρήστη Α και στέλνει το R_T.
2. Ο χρήστης Β αποκρίνεται, κατά τα γνωστά, στέλνοντας τη δική του πρόκληση *RB*.
3. Τώρα ο εισβολέας είναι μπερδεμένος, εφόσον δεν γνωρίζει το $K_{AB}(R_B)$. Αυτό που μπορεί να κάνει είναι να ανοίξει μία δεύτερη σύνοδο με το μήνυμα 3, έχοντας στη διάθεσή του ως πρόκληση το R_B που πήρε από το μήνυμα 2.
4. Ο Β κρυπτογραφεί το τρίτο μήνυμα και στέλνει πίσω το $K_{AB}(R_B)$ ως μήνυμα 4. Ο εισβολέας τώρα έχει τη χαμένη πληροφορία, έτσι μπορεί να συμπληρώσει την αρχική σύνοδο και να αγνοήσει τη δεύτερη. Ο Β τώρα είναι πεπεισμένος ότι ο εισβολέας είναι ο χρήστης Α.

Με βάση τα προηγούμενα καταλήγουμε στο συμπέρασμα ότι:
Η σχεδίαση ενός σωστού πρωτοκόλλου πιστοποίηση αυθεντικότητας πρέπει να ακολουθεί τρεις γενικούς κανόνες.

1. Αυτός που ξεκινάει τη διαδικασία θα πρέπει να αποδεικνύει την ταυτότητά του πριν χρειαστεί να το κάνει ο αποδέκτης.

2. Και οι δύο πλευρές θα πρέπει να χρησιμοποιούν διαφορετικά κλειδιά για απόδειξη, ακόμη και αν αυτό σημαίνει ότι θα υπάρχουν δύο μοιραζόμενα κλειδιά, $K_{AB'}$ και $K_{B'}$

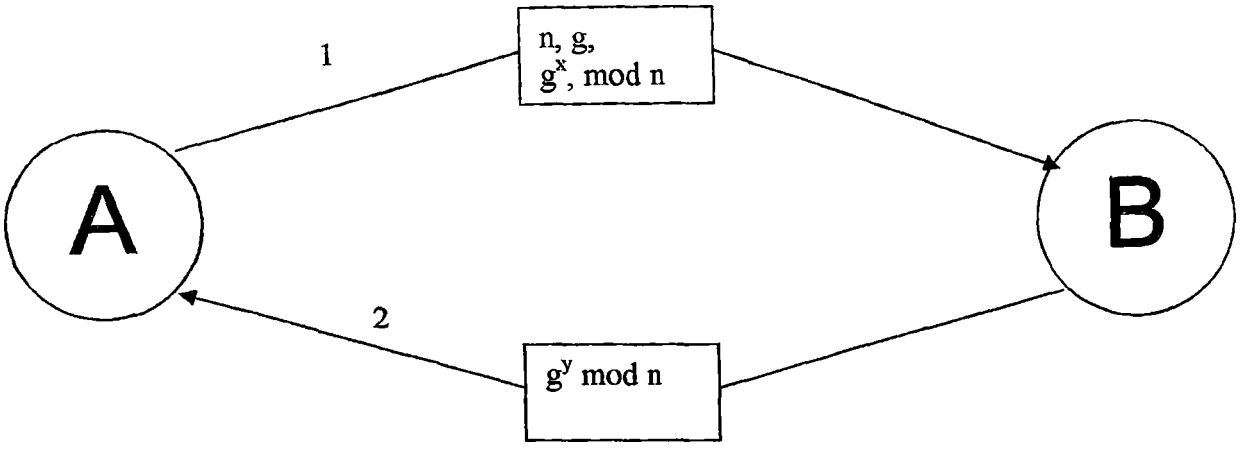
3. Τέλος, θα πρέπει και οι δύο πλευρές να επιλέγουν τις προκλήσεις τους από διαφορετικά σύνολα. Για παράδειγμα, ο ένας χρήστης μπορεί να χρησιμοποιεί άρτιους αριθμούς ενώ ο άλλος περιττούς.

4.6.2 Εγκατάσταση μοιραζόμενου κλειδιού

Έστω ότι οι χρήστες Α και Β δεν έχουν κάποιο μυστικό κλειδί και δεν γνωρίζονται μεταξύ τους. Μια πρώτη σκέψη είναι να τηλεφωνήσει ο Α στον Β και να συμφωνήσουν το κλειδί που θα χρησιμοποιήσουν για την επικοινωνία τους. Ο Β όμως δεν είναι σίγουρος αν στο τηλέφωνο ήταν ο Α ή κάποιος εισβολέας. Μια άλλη σκέψη είναι να κανονίσουν μια συνάντηση, αλλά αυτό είναι δύσκολο και μη πρακτικό. Η λύση είναι να εγκαταστήσουν ένα μυστικό κλειδί με την μέθοδο Diffie-Hellman. Ο αλγόριθμος Diffie-Hellman επιτρέπει σε δύο άτομα να επικοινωνήσουν με ασφάλεια, έστω και αν παρακολουθούνται τα μηνύματα τους από κάποιον εισβολέα. Στο σχήμα 4 βλέπουμε το πρωτόκολλο ανταλλαγής κλειδιού Diffie-Hellman.

1. Οι χρήστες Α και Β έχουν συμφωνήσει σε δύο μεγάλους πρώτους αριθμούς n και g, όπου $(n-1)/2$ είναι επίσης ένας πρώτος αριθμός. Οι αριθμοί αυτοί μπορεί να είναι δημόσιοι, έτσι είτε ο ένας είτε ο άλλος μπορούν απλά να επιλέξουν τα n και g και να τα κοινοποιήσουν στον άλλο ανοιχτά.

2. Στη συνέχεια, ο Α επιλέγει έναν μεγάλο αριθμό, *x*, και τον κρατάει μυστικό. Όμοια, ο Β επιλέγει και αυτός έναν μεγάλο αριθμό, *y*.



Σχήμα 4.8: Πρωτόκολλο ανταλλαγής κλειδιού Diffie-Hellman

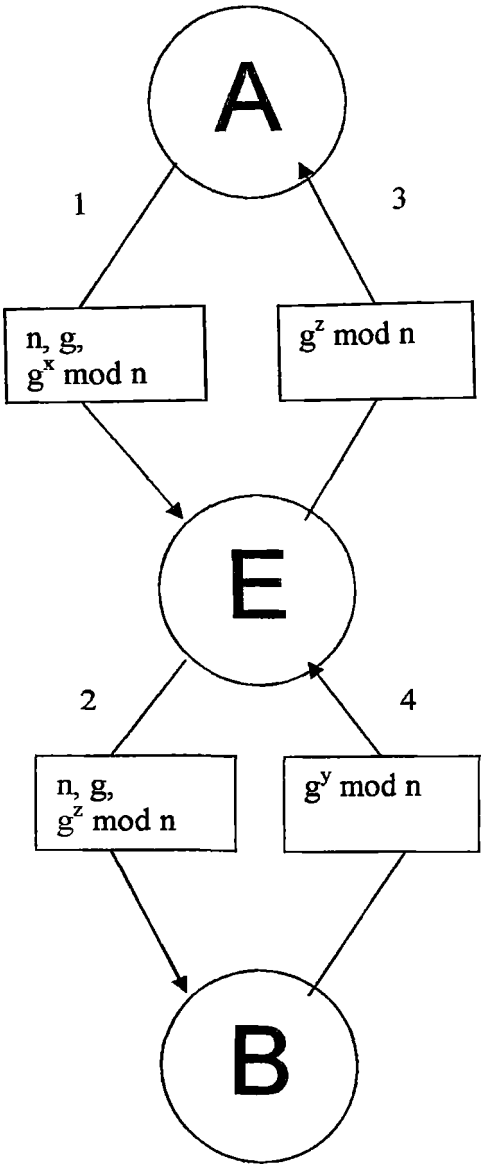
3. Ο χρήστης Α ξεκινάει στέλνοντας στον Β ένα μήνυμα που περιέχει τους εξής αριθμούς *(n, g, g^x modn)*, όπως δείχνει το σχήμα 4.8

4. Ο Β αποκρίνεται στέλνοντας στον Α ένα μήνυμα που περιέχει τον αριθμό g^y mod *n*.

5. Ο χρήστης Α υψώνει τον αριθμό που πήρε από τον Β στην x-οστή δύναμη και παίρνει τον όρο $(g^y \text{ modn})^x$

6. Ο χρήστης Β εκτελεί μία παρόμοια λειτουργία και παίρνει το *$(g^y$ modn)^x* Σύμφωνα με τους κανόνες που ισχύουν για την άθροιση mod και οι δύο υπολογισμοί δίνουν το ίδιο αποτέλεσμα. Με αυτόν τον τρόπο ο Α και Β μοιράζονται το μυστικό κλειδί.

Έστω ότι ο εισβολέας έχει δει τα δύο μηνύματα. Τότε γνωρίζει τους αριθμούς g και *n* από το πρώτο μήνυμα, αν μπορέσει να υπολογίσει *τα x* και y, τότε θα γνωρίζει και το μυστικό κλειδί. Το πρόβλημα είναι ότι, δεδομένου μόνο του αριθμού *g^y* mod *n*, δε μπορεί να βρει το *x*. Δεν υπάρχουν πρακτικοί αλγόριθμοι για τον υπολογισμό διακριτών λογαρίθμων mod.
Το πρόβλημα που δημιουργείται είναι ότι: όταν ο χρήστης Β λαμβάνει μια τριάδα (n, g, g^x mod n), δεν είναι σίγουρος αν προέρχεται από τον Α ή από κάποιον εισβολέα ο εισβολέας μπορεί να χρησιμοποιήσει την επίθεση bucket brigate) και να εξαπατήσει τους Α και Β. Η επίθεση bucket brigate φαίνεται στο σχήμα 4.9.



Σχήμα 4.9: Η επίθεση bucket brigade

Ενώ οι Α και Β επιλέγουν το *x* και *y* αντίστοιχα, ο εισβολέας επιλέγει έναν δικό του τυχαίο αριθμό z. Ο Α στέλνει το μήνυμα 1 που προορίζεται για τον Β. Ο εισβολέας υποκλέπτει το μήνυμα 1 και στέλνει αντί αυτού στον Β το μήνυμα 2, χρησιμοποιώντας τα σωστά g και *n* (τα οποία είναι δημόσια) αλλά με το δικό του μυστικό αριθμό *z* αντί για τον *x*. Επιπλέον, στέλνει και ένα μήνυμα 3 πίσω στον Α. Αργότερα, ο Β στέλνει το μήνυμα 4 προς τον Α, το οποίο ο εισβολέας επίσης υποκλέπτει και το κρατάει.

Με αυτόν τον τρόπο, ο κάθε μεσάζωντας μπορεί να πραγματοποιήσει τους υπολογισμούς modulo n. Ο χρήστης Α υπολογίζει το μυστικό κλειδί ως g^{xz} *mod n*, το ίδιο κάνει και ο εισβολέας. Ο Β υπολογίζει το g^{xz} *mod n* και το ίδιο κάνει και ο

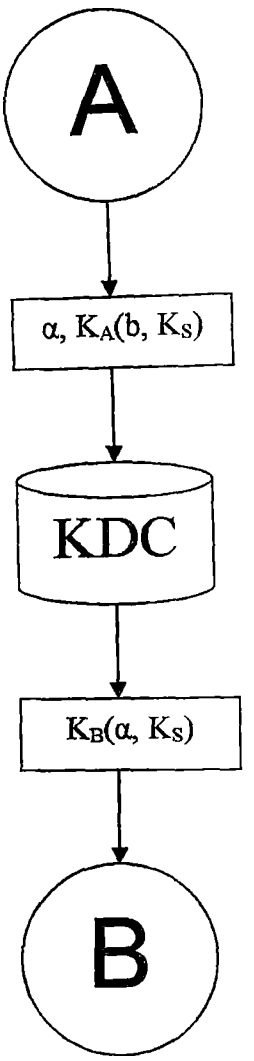
εισβολέας. Ο Α νομίζει ότι μιλάει με τον Β και έτσι εγκαθίσταται ένα κλειδί συνόδου (με τον εισβολέα). Κάθε μήνυμα που στέλνεται από το χρήστη Α συλλαμβάνεται από τον εισβολέα, αποθηκεύεται, τροποποιείται αν αυτός το επιθυμεί και στη συνέχεια (προαιρετικά) αποστέλλεται στον Β. Παρόμοια διαδικασία γίνεται και προς την άλλη διεύθυνση. Ο εισβολέας βλέπει τα πάντα και μπορεί να τροποποιεί όλα τα μηνύματα, ενώ οι χρήστες Α και Β έχουν την εντύπωση ότι έχουν ένα ασφαλές κανάλι επικοινωνίας. Η επίθεση αυτή ονομάζεται bucket brigade.

4.6.3 Πιστοποίηση Αυθεντικότητας με τη χρήση Κέντρου Διανομής κλειδιών.

Έστω ότι με την μέθοδο εγκατάστασης μοιραζόμενου κλειδιού θέλουμε να επικοινωνήσουμε με Χ άτομα. Χρειάζεται επομένως να έχουμε Χ κλειδιά. Η διαχείριση των κλειδιών αυτών είναι μεγάλο πρόβλημα. Για τον λόγο αυτό εισάγουμε ένα έμπιστο κέντρο διανομής κλειδιών (KDC). Εδώ κάθε χρήστης έχει ένα μυστικό κλειδί το οποίο μοιράζεται με το KDC. Η πιστοποίηση αυθεντικότητας και η διαχείριση κλειδισύ συνόδου γίνεται με την μεσολάβηση του KDC. Στο σχήμα 4.10 βλέπουμε την επικοινωνία δύο χρηστών με το πρωτόκολλο πιστοποίηση αυθεντικότητας με τη χρήση KDC.

Με τον παραπάνω τρόπο η πιστοποίηση αυθεντικότητας, πραγματοποιείται αξιόπιστα. Το KDC γνωρίζει ότι το μήνυμα 1 προέρχεται από το χρήστη Α, εφόσον κανένας άλλος δεν είναι ικανός να το κρυπτογραφήσει με το μυστικό κλειδί του Α. Όμοια, ο Β γνωρίζει ότι το μήνυμα 2 προέρχεται από το KDC, το οποίο εμπιστεύεται, εφόσον κανείς άλλος δε γνωρίζει το μυστικό του κλειδί. Το πρόβλημα που προκύπτει σ' αυτό το πρωτόκολλο είναι ότι ένας εισβολέας μπορεί να αντιγράψει τα μηνύματα που αποστέλλονται μεταξύ των δύο χρηστών και να τα αναμεταδώσει.

Υπάρχουν αρκετές λύσεις για την επίθεση επανάληψης. Μια από αυτές συμπεριλαμβάνει τη χρήση μιας "χρονοσφραγίδας" (timestamp) για κάθε μήνυμα. Με αυτόν τον τρόπο, όταν κάποιος λάβει ένα παλιό μήνυμα, μπορεί να το απορρίψει. Το πρόβλημα σε αυτή τη προσέγγιση είναι ότι τα ρολόγια του δικτύου δεν είναι ποτέ ακριβώς συγχρονισμένα, έτσι υπάρχει σχεδόν πάντα κάποιο χρονικό διάστημα στο οποίο μία χρονοσφραγίδα θα παραμένει έγκυρη, ενώ δεν είναι. Ο εισβολέας μπορεί να επαναλάβει το μήνυμα κατά τη διάρκεια αυτού του διαστήματος. Μία δεύτερη λύση είναι η τοποθέτηση κάθε φορά ενός μοναδικού αριθμού σε κάθε μήνυμα, ο αριθμός αυτός συνήθως ονομάζεται *nonce*. Ο χρήστης με αυτόν τον τρόπο μπορεί να απορρίπτει κάθε μήνυμα που περιέχει έναν παλαιότερα χρησιμοποιημένο nonce. Πρέπει να επισημάνουμε ότι σε αυτήν την προσέγγιση χρειάζεται να θυμόμαστε τα nonce για πάντα, γιατί κάποιος εισβολέας μπορεί να επιχειρήσει να επαναλάβει ένα μήνυμα που είχε σταλεί πριν από κάποιο μεγάλο χρονικό διάστημα. Αν κάποια μηχανή χάσει την λίστα της με τα nonce, τότε είναι πάλι ευπαθής στην επίθεση επανάληψης. Μπορούμε βέβαια να συνδυάσουμε τις χρονοσφραγίδες με τα nonce, έτσι ώστε να έχουμε ένα όριο στο πλήθος nonce που θα πρέπει να θυμόμαστε, αλλά με αυτόν τον τρόπο το πρωτόκολλο θα γίνει περισσότερο σύνθετο.

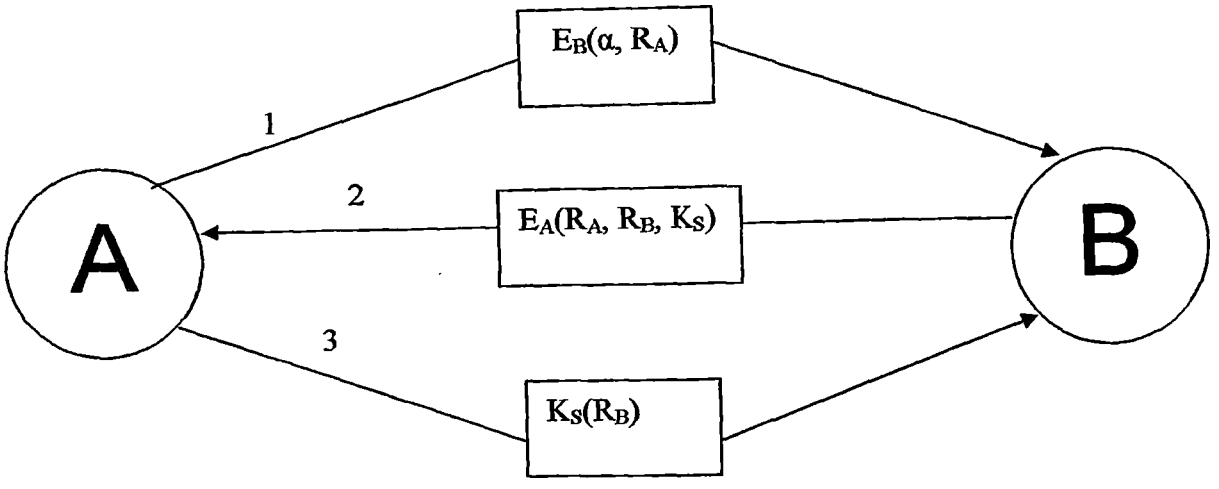


Σχήμα 4.10: Πρωτόκολλο πιστοποίησης αυθεντικότητας με τη χρήση KDC

4.6.4 Πιστοποίηση αυθεντικότητας με τη χρήση κρυπτογραφίας δημοσίου κλειδιού

Η πιστοποίηση της αμοιβαίας αυθεντικότητας μπορεί να επιτευχθεί και με τη χρήση της κρυπτογραφίας δημοσίου κλειδιού. Έστω ότι οι χρήστες Α και Β γνωρίζουν ο ένας το δημόσιο κλειδί του άλλου. Οι δύο πλευρές θέλουν να εγκαταστήσουν μία σύνοδο και στη συνέχεια να χρησιμοποιήσουν για λόγους ταχύτητας κρυπτογραφία μυστικού κλειδιού (είναι από 100 έως 1000 φορές γρηγορότερη σε σχέση με την κρυπτογραφία δημοσίου κλειδιού). Στόχος της αρχικής συναλλαγής είναι η πιστοποίηση αυθεντικότητας και των δύο πλευρών και η συμφωνία χρήσης ενός μοιραζόμενου μυστικού κλειδιού συνόδου.

Η εγκατάσταση αυτή μπορεί να γίνει με διάφορους τρόπους. Ένας από τους τρόπους αυτούς φαίνεται στο σχήμα 4.11



Σχήμα 4.11: Πιστοποίηση αυθεντικότητας με τη χρήση κρυπτογραφίας δημοσίου κλειδιού

1. Ο χρήστης Α ξεκινάει κρυπτογραφώντας την ταυτότητα του και έναν τυχαίο αριθμό, R_A, χρησιμοποιώντας το δημόσιο κλειδί, E_B, του χρήστη Β.

2. Λαμβάνοντας ο Β το μήνυμα και μη γνωρίζοντας αν προέρχεται από τον Α ή από κάποιον εισβολέα στέλνει ένα μήνυμα στον Α που περιέχει τον R_A, έναν δικό του τυχαίο αριθμό, R_B, και ένα προτεινόμενο κλειδί συνόδου, K_S'

3. Όταν ο Α πάρει το μήνυμα 2, το αποκρυπτογραφεί χρησιμοποιώντας το ιδιωτικό του κλειδί. Τότε, βλέπει ότι μέσα σε αυτό υπάρχει το R_A. Το μήνυμα προέρχεται από τον Β, εφόσον ο εισβολέας δεν έχει τρόπο για να καθορίσει το R_A. Επιπλέον, το μήνυμα πρέπει να είναι καινούργιο και όχι μία επανάληψη, εφόσον ο Α μόλις έστειλε στον Β το R_A.

4. Ο Α συμφωνεί για τη σύνοδο στέλνοντας πίσω το μήνυμα 3.

5. Όταν ο Β δει το R_B που είναι κρυπτογραφημένο με το κλειδί συνόδου καταλαβαίνει ότι ο Α πήρε το μήνυμα 2 και επαλήθευσε το R_A.

Έτσι ένας εισβολέας δε μπορεί να υπονομεύσει το πρωτόκολλο, γιατί αν προσπαθήσει να πλαστογραφήσει το μήνυμα 1 και εξαπατήσει τον Β παίρνοντας τη θέση του Α, ο Α θα διαπιστώσει στη συνέχεια ότι το R_A που πήρε δεν είναι αυτό που έστειλε και δεν θα συνεχίσει περαιτέρω. Ο εισβολέας δεν μπορεί επίσης να παραποιήσει πειστικά το μήνυμα 3 εφόσον δε γνωρίζει το R_B ή Ks και δεν μπορεί να καθορίσει κανένα απ' αυτά χωρίς το ιδιωτικό κλειδί του Α.

ΚΕΦΑΛΑΙΟ 5
ΑΡΧΕΣ ΠΙΣΤΟΠΟΙΗΣΗΣ ΚΑΙ ΠΙΣΤΟΠΟΙΗΤΙΚΑ SERVER

5.1 Αρχές Πιστοποίησης

Μια Αρχή Πιστοποίησης είναι ένας οργανισμός που λειτουργεί με ασφάλεια κάτω από αυστηρές προδιαγραφές με σκοπό τη δημιουργία και διανομή ψηφιακών πιστοποιητικών. Οι Αρχές Πιστοποίησης (Certification Authorities - CAs) επιβεβαιώνουν τις ταυτότητες των οντοτήτων και εκδίδουν τα αντίστοιχα ψηφιακά πιστοποιητικά.
Μια CA μπορεί:

- **είτε να είναι ένας Έμπιστος Τρίτος Φορέας (Trusted Third Party - TTP)**

  Μια εταιρία ή μια κυβέρνηση μπορεί να λειτουργεί μια CA η οποία να συνδέει τα δημόσια κλειδιά με τα νόμιμα ονόματα ανθρώπων ή επιχειρήσεων. Μια τέτοια CA μπορεί να χρησιμοποιηθεί για να επιτρέπει σε άτομα χωρίς καμία προηγούμενη σχέση να αποδεικνύουν ο ένας στον άλλον την ταυτότητα του και να μετέχουν σε νόμιμες συναλλαγές

- **είτε να λειτουργεί στα πλαίσια ενός οργανισμού ως:**

  Εσωτερική αρχή (Internal CA)
  Ένας οργανισμός μπορεί να λειτουργεί μια CA για να πιστοποιεί στους εργαζομένους του, τις θέσεις τους, και το επίπεδο της εξουσίας τους. Μια τέτοια ιεραρχία πιστοποίησης μπορεί να χρησιμοποιηθεί για τον έλεγχο πρόσβασης στις εσωτερικές πηγές πληροφοριών του οργανισμού. Για παράδειγμα, κάθε εργαζόμενος σε έναν οργανισμό μπορεί να δημιουργήσει ένα κλειδί και να αποκτήσει ένα πιστοποιητικό, για αυτό το κλειδί, που να αναφέρεται μόνο στα υπολογιστικά συστήματα στα οποία θα έχει πρόσβαση ο εργαζόμενος. Οι υπολογιστές του οργανισμού μπορούν τότε να αποφασίζουν εάν θα παρέχουν ή όχι} σε έναν εργαζόμενο πρόσβαση, βασιζόμενοι στην πιστοποίηση του κλειδιού τους. Με αυτόν τον τρόπο, οι επιχειρήσεις αποφεύγουν την αναγκαιότητα τις διανομής μιας λίστας ελέγχου πρόσβασης και τις ύπαρξης αρχείου password σε όλους τους κατανεμημένους υπολογιστές

  Αρχή εξωτερικής προέλευσης υπαλλήλου (Outsourced employee CA)
  Μια εταιρία ίσως συμφωνήσει με μια εξωτερική φίρμα να παρέχει υπηρεσίες πιστοποίησης για τους δικούς της εργαζόμενους, όπως μια εταιρία ίσως συμφωνήσει με ένα εργαστήριο φωτογραφίας για να κατασκευάσει ταυτότητες.

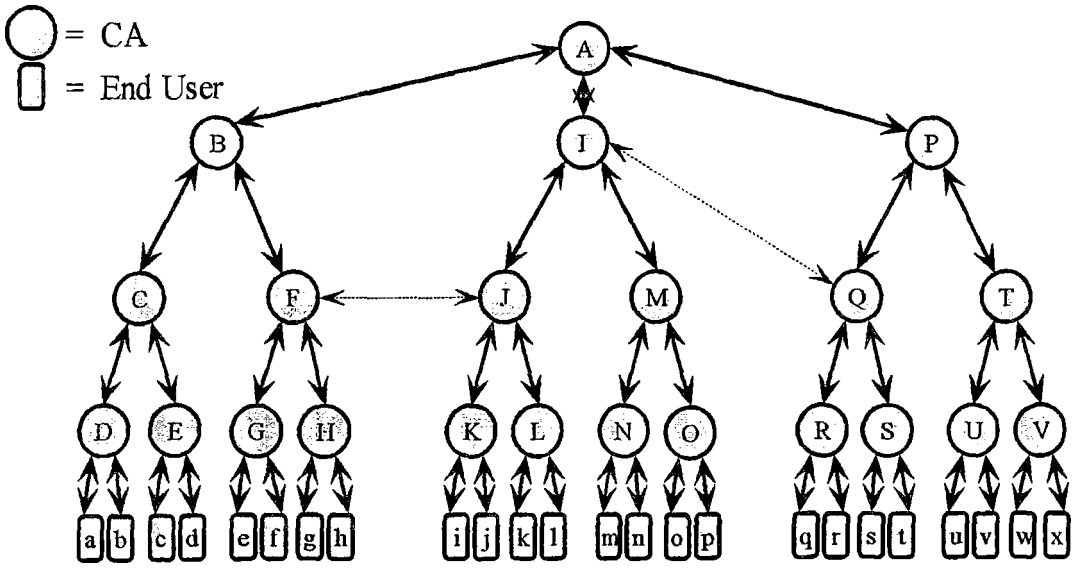
  Αρχή εξωτερικής προέλευσης πελάτη (Outsourced customer CA)
  Μια εταιρία ίσως συμφωνήσει με μια εξωτερική φίρμα να διευθύνει μια αρχή πιστοποίησης η οποία να λειτουργήσει για τους τρέχων ή για τους πιθανούς

πελάτες της εταιρίας. Βασιζόμενη στις μεθόδους πιστοποίησης της εξωτερικής φίρμας, η εταιρία θα γλιτώσει την δαπάνη της δημιουργίας δικών τις διαδικασιών πιστοποίησης.

Στα σχετικά προγράμματα των χρηστών (Web browsers) διατηρούνται συλλογές από έμπιστα πιστοποιητικά CA. Με βάση αυτά τα πιστοποιητικά CA καθορίζεται ο τρόπος αποδοχής των άλλων πιστοποιητικών (εξυπηρετητών, πελατών, κ.ά.). Στην απλούστερη περίπτωση, επικυρώνονται αυτόματα μόνο με βάση το πιστοποιητικό μιας CA, αλλά συνήθως ένα έμπιστο πιστοποιητικό CA συμμετέχει σε μια αλυσίδα πιστοποιητικών CA που αντιστοιχούν σε μια ιεραρχία CA.

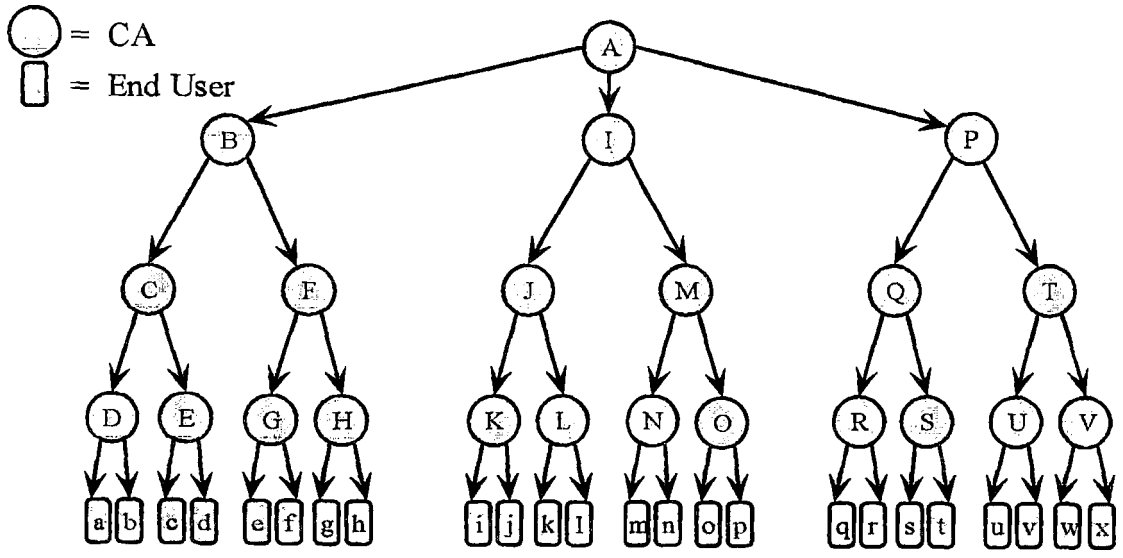
5.2 Ιεραρχίες Πιστοποίησης

Κάθε CA πρέπει θεωρητικά να συμμετέχει σε μια ευρύτερη PKI, συνήθως ιεραρχικής δομής, όπου οι ανώτερες CA πιστοποιούν τις κατώτερες. Σε κάθε χώρα μπορεί να υπάρχουν μια ή περισσότερες CA, συνήθως κατά περιοχή εφαρμογής (τράπεζες, υγεία, παιδεία, κ.λ.π.).
Η ύπαρξη αυθαίρετου αριθμού από CAs είναι δυνατή σε μία διαδρομή από ένα χρήστη σε κάποιον άλλο. Έτσι, ο αποστολέας που επιθυμεί να στείλει ένα ασφαλές μήνυμα σε κάποιον που πιστοποιείται από μία άλλη CA θα πρέπει να επαληθεύσει την ταυτότητα όλων των CA που μεσολαβούν μέχρι να αποκτήσει το πιστοποιητικό του παραλήπτη. Η διαδικασία αυτή καλείται *επαλήθευση διαδρομής πιστοποίησης* (certification path validation). Το μήκος της διαδρομής πιστοποίησης είναι ο αριθμός των CA που μεσολαβούν από τον αποστολέα στον παραλήπτη, ή ο αριθμός των πιστοποιητικών που πρέπει να επαληθεύσει ο αποστολέας μέχρι να αποκτήσει το δημόσιο κλειδί του παραλήπτη.
Όπως φαίνεται στο Σχήμα 5.1 μερικές CA χρησιμοποιούν μία γενική ιεραρχία: κάθε CA πιστοποιεί τον γονέα και τα παιδιά της. Με διακεκομμένες γραμμές φαίνονται τα *cross certificates*, που δεν ακολουθούν την βασική ιεραρχία.



Σχήμα 5.1: Γενική ιεραρχία πιστοποίησης

Άλλες PKIs χρησιμοποιούν την κατερχόμενη ιεραρχία (top - down hierarchy) που είναι μία παραλλαγή της γενικής ιεραρχίας. Εδώ οι CAs πιστοποιούν μόνο τα παιδιά τους και η CA του ανώτατου επιπέδου είναι η αφετηρία όλων των διαδρομών πιστοποίησης. Η CA που αποτελεί την αφετηρία της διαδρομής πιστοποίησης καλείται *root CA*.



Σχήμα 5.2: Κατερχόμενη ιεραρχία πιστοποίησης

Άλλες PKIs δεν παρουσιάζουν καμία δομή (στην πράξη κάθε CA είναι root CA του εαυτού της και έχει πλήρη έλεγχο στην απόδοση της εμπιστοσύνης. Οι αδόμητες αυτές CA μπορούν να λειτουργούν με διάφορους τρόπους. Για παράδειγμα, το Pretty Good Privacy χρησιμοποιεί μία αδόμητη PKI στην οποία κάθε CA βασίζει την εμπιστοσύνη της στα πιστοποιητικά των άλλων CA. Αν αρκετές από τις υπόλοιπες CA έχουν εκδώσει πιστοποιητικά που δένουν μία οντότητα με ένα συγκεκριμένο κλειδί, τότε η CA μπορεί να την αποδεχτεί με κάποιο επίπεδο εμπιστοσύνης. Η διευθέτηση αυτή καλείται *ιστός εμπιστοσύνης* (web of trust).

Οι σχέσεις των CA μίας PKI καθορίζουν την δυνατότητα αλλαγής κλίμακας (scalability) της PKI. Μία διευθέτηση ενός απλού ιστού εμπιστοσύνης δεν κλιμακώνεται καλά καθώς η ανακάλυψη της διαδρομής πιστοποίησης σε έναν ελεύθερης μορφής ιστό είναι πολύ δύσκολη. Επίσης, η διευθέτηση αυτή εισάγει μία υποκειμενικότητα στην απόδοση της εμπιστοσύνης.

Το ιεραρχικό μοντέλο ανταποκρίνεται καλύτερα στην αλλαγή κλίμακας αλλά παρουσιάζει άλλα μειονεκτήματα. Σε μία κατερχόμενη ιεραρχία, όλοι οι χρήστες πρέπει να χρησιμοποιούν την CA του ανώτατου επιπέδου σαν την ρίζας (root CA). Το γεγονός αυτό σημαίνει ότι όλοι οι χρήστες χρειάζονται το δημόσιο κλειδί της CA του ανώτατου επιπέδου πριν να αρχίσουν να χρησιμοποιούν την PKI. Επίσης η CA του ανώτατου επιπέδου γίνεται ιδιαίτερα ελκυστικός στόχος, καθώς η υποκλοπή του ιδιωτικού της κλειδιού μπορεί να χρησιμοποιηθεί για την πλαστογράφηση των μηνυμάτων.

Μία γενική ιεραρχία επιτρέπει σε οποιαδήποτε CA να είναι η root CA. Παρόλα αυτά, η δομή αυτή βασίζεται επίσης αρκετά στις CA των ανώτερων επιπέδων και ιδιαίτερα της CA του ανώτατου επιπέδου καθώς ένας μεγάλος αριθμός των διαδρομών

πιστοποίησης διέρχεται από αυτή. Οι διαδρομές πιστοποίησης σε μία γενική ιεραρχία μπορούν επίσης να γίνουν πολύ μεγάλες. Η διαδικασία του cross-certification βοηθά στην μείωση των μηκών διαδρομών, περιπλέκοντας όμως την ανακάλυψη των διαδρομών.

Γενικά, η πιστοποίηση στα πλαίσια μιας PKI βασίζεται σε μια *ιεραρχική δομή* στην οποία συμμετέχουν οι ακόλουθες οντότητες.

Αρχή Έγκρισης Πολιτικής (Policy Approval Authority - PPA)

- θέτει τις αρχές που θα ακολουθούν τα PCAs, που βρίσκονται πιο κάτω στην ιεραρχία, εγκρίνει τις πολιτικές των PCAs και εκδίδει πιστοποιητικά για αυτά.
- εκδίδει πιστοποιητικά ρίζας (root certficates) που τα υπογράφει ψηφιακά με το ιδιωτικό κλειδί της. Η περίοδος ισχύος των πιστοποιητικών αυτών είναι μεγαλύτερη αυτών που εκδίδονται από τις PCAs και από τις CAs. Η έκδοση των πιστοποιητικών αυτών γίνεται off-line.

Αρχή Πιστοποίησης Πολιτικής (Policy Certification Authority - PCA)

- θέτει τη πολιτική που θα ακολουθούν οι CAs που βρίσκονται χαμηλότερα στην ιεραρχία και ελέγχει αν λειτουργούν σύμφωνα με αυτή.
- εκδίδει πιστοποιητικά για CAs, αλλά όχι για τους τελικούς χρήστες. Η έκδοση αυτών γίνεται επίσης off-line.
- επειδή η περίοδος ισχύος των PCA πιστοποιητικών είναι μεγαλύτερη από αυτή των CAs, η ανανέωση της ισχύος των CA πιστοποιητικών δεν δημιουργεί προβλήματα στους τελικούς χρήστες που έχουν αυτά τα πιστοποιητικά.
- Αρχή Έκδοσης Πιστοποιητικών (Certification Authority - CA)
- ακολουθεί τη πολιτική που έχει ορίσει η PCA και εκδίδει πιστοποιητικά για άλλες CAs, τελικούς χρήστες και RAs.
- μερικές φορές θέτει και δικές τις πολιτικές, που είναι όμως σύμφωνες με αυτές τις PCA.

Αρχή Καταχώρησης (Registration Authority - RA)

- μια RA είναι υπεύθυνη για τη διαδικασία εγγραφής (registration) των τελικών χρηστών που θα αποκτήσουν πιστοποιητικό της CA. Δεν εκδίδει η ίδια πιστοποιητικά.
- ελέγχει τις πληροφορίες ταυτότητας που δηλώνουν οι τελικοί χρήστες, σύμφωνα με τις διαδικασίες που έχει ορίσει η CA.

Τελικός χρήστης (End entity)

Ο τελικός χρήστης είναι ένας ιδιώτης, μια επιχείρηση, ένας υπολογιστής ή οποιαδήποτε οντότητα που χρησιμοποιεί το πιστοποιητικό.

5.3 Υποδομή Δημόσιου Κλειδιού (PKI)

Μια Υποδομή Δημόσιου Κλειδιού (PKI) είναι ένας συνδυασμός από λογισμικό, τεχνολογίες κρυπτογράφησης και υπηρεσίες, ώστε να διασφαλιστούν οι επικοινωνίες και οι συναλλαγές στο Internet και να επιτευχθούν οι τέσσερις βασικές αρχές ασφάλειας κατά τη μετάδοση πληροφοριών:
{Εμπιστευτικότητα, Ακεραιότητα, Ταυτοποίηση, Μη-απάρνηση}

Για να επιτύχει όλα τα παραπάνω, μια PKI πρέπει να ενσωματώνει τουλάχιστον μια Αρχή Έκδοσης Πιστοποιητικών (Certification Authority-CA), καθώς και εργαλεία για τη διαχείριση, την ανανέωση και την ανάκληση πιστοποιητικών.

5.3.1 Συστατικά Μέρη της Υποδομής Δημόσιου Κλειδιού

Μια PKI παρέχει τις βασικές υπηρεσίες ασφάλειας που είναι απαραίτητες για να ολοκληρωθεί μια ηλεκτρονική συναλλαγή μεταξύ χρηστών που δεν γνωρίζονται ή βρίσκονται σε διάφορα μέρη του κόσμου και θέλουν να επικοινωνήσουν με ασφάλεια. Βασίζεται στη χρήση των ψηφιακών πιστοποιητικών (digital certificates ή digital IDs), τα οποία είναι υπεύθυνα για τη σύνδεση της ψηφιακής υπογραφής .ενός χρήστη με το δημόσιο κλειδί του.

Μια PKI πρέπει οπωσδήποτε να περιλαμβάνει, τουλάχιστον:

1. **Μια πολιτική ασφάλειας (Security Policy).**

   Η πολιτική ασφάλειας ορίζει τις αρχές που πρέπει να ακολουθούνται για την ασφάλεια των πληροφοριών, καθώς και τους κανόνες για τη χρήση της κρυπτογραφίας. Συνήθως, περιλαμβάνει οδηγίες για το χειρισμό των κλειδιών και των σημαντικών πληροφοριών, ενώ ακόμη ορίζει διάφορα επίπεδα ελέγχου ανάλογα με το επίπεδο ευαισθησίας κάθε πληροφορίας.
   Όλα τα παραπάνω δηλώνονται με μια *δήλωση πρακτικής πιστοποίησης* (Certificate Practice Statement - CPS). Το CPS είναι ένα λεπτομερές έγγραφο που περιέχει όλες τις λειτουργικές διαδικασίες που πρέπει να ακολουθηθούν ώστε να εφαρμοστεί η πολιτική ασφάλειας στην πράξη. Περιλαμβάνει ορισμούς για το:

   - πώς είναι κατασκευασμένα και πως λειτουργούν τα CAs,
   - πως δημιουργούνται και ανακαλούνται τα πιστοποιητικά, καθώς και πληροφορίες για:
     - τη δημιουργία, κατοχύρωση και πιστοποίηση των κλειδιών,
     - το πώς αποθηκεύονται και πως γίνονται διαθέσιμα στους χρήστες, κ.ά.

2. **Μια Αρχή Πιστοποίησης (Certification Authority).**

   Η *Αρχή Πιστοποίησης* (CA) αποτελεί το βασικό μέρος μιας PKI και διαχειρίζεται τα πιστοποιητικά δημόσιων κλειδιών για ολόκληρο το κύκλο ζωής τους. Οι βασικές λειτουργίες του είναι:

- Δημιουργία πιστοποιητικών που συνδέουν τη ταυτότητα ενός χρήστη ή συστήματος με ένα δημόσιο κλειδί με τη βοήθεια ψηφιακών υπογραφών.
- Προγραμματισμός των ημερομηνιών λήξης των πιστοποιητικών.
- Διασφάλιση για την ανάκληση των πιστοποιητικών όταν είναι απαραίτητο, με τη δημοσίευση των *λιστών ανάκλησης πιστοποιητικών* (Certification Revocation Lists- CRLs).

Κάθε οργανισμός που ορίζει μια δική του υποδομή δημόσιου κλειδιού, μπορεί να ορίσει ένα δικό του CA ή να χρησιμοποιήσει τις υπηρεσίες ενός υπάρχοντος εμπορικού CA ή μιας έμπιστης τρίτης πλευράς (TTP).

Λίστες Ανάκλησης Πιστοποιητικών (Certificate Revocation Lists)
Μία λίστα ανάκλησης πιστοποιητικών περιέχει πιστοποιητικά που έχουν ακυρωθεί πριν από την προγραμματισμένη ημερομηνία λήξης. Υπάρχουν αρκετοί λόγοι γιατί ένα πιστοποιητικό μπορεί να ανακληθεί. Για παράδειγμα η κλείδα που ορίζεται στο πιστοποιητικό μπορεί να μην ασφαλή ή το άτομο για το οποίο εκδόθηκε το πιστοποιητικό να μην έχει πια την δικαιοδοσία να το χρησιμοποιεί. Ας φανταστούμε την περίπτωση όπου ένας υπάλληλος μια εταιρείας έχει πιστοποιητικό που έχει εκδώσει για λογαριασμό του η εταιρεία. Εάν ο υπάλληλος απολυθεί, η εταιρεία θα ακυρώσει το πιστοποιητικό, ώστε να μην έχει την δυνατότητα να υπογράφει έγγραφα με αυτήν την κλείδα.
Κατά την επαλήθευση μιας υπογραφής, πρέπει κάθε χρήστης να συμβουλεύεται μία CRL για να διαπιστώσει εάν το εν λόγω πιστοποιητικό δεν έχει αποσυρθεί. Το αν αξίζει τον κόπο να πραγματοποιήσει τέτοιον έλεγχο, εξαρτάται από την σημασία του εγγράφου. Οι λίστες διατηρούνται και ανανεώνονται από τις CA, και κάθε CA διαχειρίζεται τις λίστες που παρέχουν πληροφορίες για τα ανακληθέντα πιστοποιητικά που είχαν εκδοθεί από την ίδια. Επίσης, οι λίστες περιέχουν τα πιστοποιητικά των οποίων δεν έχει περάσει η ημερομηνία λήξης. Αυτά τα πιστοποιητικά δεν γίνονται δεκτά σε καμία περίπτωση.

3. **Μια Αρχή Καταχώρησης (Registration Authority).**

Μια *Αρχή Καταχώρησης* - RA (Registration Authority) παρέχει τη διεπαφή (interface) μεταξύ του χρήστη και του CA. Είναι υπεύθυνη για τη πιστοποίηση της ταυτότητας του χρήστη και μεταφέρει στο CA έτοιμες όλες τις αιτήσεις για τη δημιουργία των αντίστοιχων πιστοποιητικών. Η ποιότητα της διαδικασίας ταυτοποίησης καθορίζει και το επίπεδο εμπιστοσύνης που παρέχεται από το πιστοποιητικό.

4. **Ένα σύστημα διανομής ψηφιακών πιστοποιητικών.**

Η διανομή των πιστοποιητικών μπορεί να γίνει με διάφορους τρόπους και εξαρτάται από τη δομή της PKI. Υπεύθυνοι για αυτή θα μπορούσαν να είναι οι ίδιοι οι χρήστες ή να γίνεται μέσω μια *υπηρεσίας καταλόγου* (directory service). Αντί οι χρήστες να αποθηκεύουν τα πιστοποιητικά τους τοπικά, αυτά μπορούν να αποθηκεύονται σε έναν εξυπηρετητή καταλόγου. Οι περισσότερες PKI διαθέτουν τέτοιους εξυπηρετητές για την αποθήκευση πιστοποιητικών

που ακολουθούν το πρότυπο X.500. Όταν μια Αρχή Πιστοποίησης εκδώσει ένα πιστοποιητικό, το αποθηκεύει σε μια *Αποθήκη Πιστοποιητικών* (Certificate Repository). Όταν κάποιος αναζητά ένα πιστοποιητικό που υπάρχει σε αυτή την αποθήκη, μπορεί να το πάρει χωρίς να χρειάζεται να το ζητήσει από τον κάτοχό του.

5. **Εφαρμογές που να αξιοποιούν τις υπηρεσίες μιας PKI (PKI-enabled applications).**

   Μια PKI παρέχει το πλαίσιο μέσα στο οποίο διάφορες εφαρμογές μπορούν να αναπτυχθούν και να λειτουργήσουν με ασφάλεια. Ως παραδείγματα τέτοιων εφαρμογών μπορούμε να αναφέρουμε :

   - την επικοινωνία μεταξύ Web servers και browsers.
   - το ηλεκτρονικό ταχυδρομείο (e-mail).
   - τις ηλεκτρονικές ανταλλαγές δεδομένων (π.χ. σύμφωνα με το πρότυπο Electronic Data Interchange - EDI).
   - τις συναλλαγές με πιστωτικές κάρτες στο Internet.
   - τα Εικονικά Ιδιωτικά Δίκτυα (Virtual Private Networks - VPNs), κ.α..

5.3.2 Υπηρεσίες Υποδομής Δημόσιου Κλειδιού

Μια υποδομή δημόσιου κλειδιού πρέπει να παρέχει ένα αριθμό από υπηρεσίες. Οι υπηρεσίες αυτές μπορούν να χωριστούν σε τρεις κατηγορίες:

1. **Υπηρεσίες κρυπτογράφησης.**
   Μια PKI πρέπει να είναι σε θέση να παρέχει, όποτε της ζητηθεί, υπηρεσίες κρυπτογράφησης. Τέτοιες υπηρεσίες είναι:

   - η δημιουργία ζευγών των κλειδιών (private/public) κρυπτογράφησης.
   - η δημιουργία ψηφιακών υπογραφών.
   - η επιβεβαίωση της εγκυρότητας ψηφιακών υπογραφών.

2. **Υπηρεσίες διαχείρισης πιστοποιητικών**
   Οι υπηρεσίες διαχείρισης πιστοποιητικών αποτελούν το πυρήνα μιας PKI Τέτοιες υπηρεσίες είναι:

   - η έκδοση πιστοποιητικού (Certificate Issuance)
   - η ανάκληση πιστοποιητικού (Certificate Revocation)
   - η δημοσίευση πιστοποιητικού (Certificate Publishing)
   - η αρχειοθέτηση πιστοποιητικού (Certificate Archiving)

3. **Βοηθητικές υπηρεσίες**
   Εκτός από τις παραπάνω, υπάρχουν και άλλες υπηρεσίες που θεωρούνται βασικά μέρη μιας τέτοιας υποδομής, όπως:

   - **Καταχώρηση (Registration)**

Οι υπηρεσίες αυτές είναι υπεύθυνες για την αναγνώριση και τη διαχείριση των προσωπικών δεδομένων οποιουδήποτε ζητά ένα πιστοποιητικό. Ελέγχουν όλες τις πληροφορίες που είναι απαραίτητες για την έκδοση ή την ανάκληση των πιστοποιητικών. Μετά από αυτό τον έλεγχο μπορεί να γίνεται η έκδοση του ψηφιακού πιστοποιητικού.

- **Αρχειοθέτηση δεδομένων (Data Archiving)**
  Οι υπηρεσίες αυτές αναλαμβάνουν την αρχειοθέτηση και τη διαχείριση των ψηφιακών εγγράφων και των υπόλοιπων δεδομένων για μεγάλες χρονικές περιόδους. Φροντίζουν για την ασφαλή αποθήκευσή τους σε διάφορα μέσα, ώστε να μην μεταβληθούν και να μην έχουν πρόσβαση σε αυτά μη εξουσιοδοτημένοι χρήστες.
- **Συμβολαιογραφική αυθεντικοποίηση (Notarial Authentication)**
  Αφορά την ταυτοποίηση του αποστολέα και την ακεραιότητα των ψηφιακών εγγράφων.
- **Ανάκτηση κλειδιού (Key Recovery)**
  Η υπηρεσία αυτή ασχολείται με τη δημιουργία κρυφών αντιγράφων των κλειδιών για τις περιπτώσεις που κάποιος χρήστης χάσει το κλειδί του ή ξεχάσει το συνθηματικό (password) που απαιτείται για να έχει πρόσβαση σε αυτό.
- **Αρχείο προσωπικών δεδομένων (Repository)**
  Ασχολούνται με τη διαχείριση εκείνων των δεδομένων που αφορούν τον κάθε χρήστη. Τα δεδομένα αυτά περιλαμβάνουν, εκτός από το ίδιο το πιστοποιητικό, και άλλα, όπως το τηλέφωνό του, τη διεύθυνση κ.ά.
- **Άλλες υπηρεσίες**
  Ακόμη, μπορεί να απαιτούνται διάφορες άλλες υπηρεσίες. Αν, για παράδειγμα, το κλειδί αποθηκεύεται σε μια έξυπνη κάρτα (smart card), τότε χρειάζονται πρόσθετες υπηρεσίες για τη δημιουργία των κλειδιών και την εγγραφή τους στη κάρτα.

5.4 Ψηφιακά πιστοποιητικά

Τα πιστοποιητικά είναι ψηφιακά έγγραφα που αποδεικνύουν την σχέση μεταξύ ενός δημόσιου κλειδιού και μίας οντότητας. Επιτρέπουν, δηλαδή, την επαλήθευση του ισχυρισμού ότι ένα συγκεκριμένο δημόσιο κλειδί ανήκει σε μια συγκεκριμένη οντότητα. Τα πιστοποιητικά αποτρέπουν κάποιον να υποδυθεί κάποιον άλλο με την χρήση ψεύτικου κλειδιού.

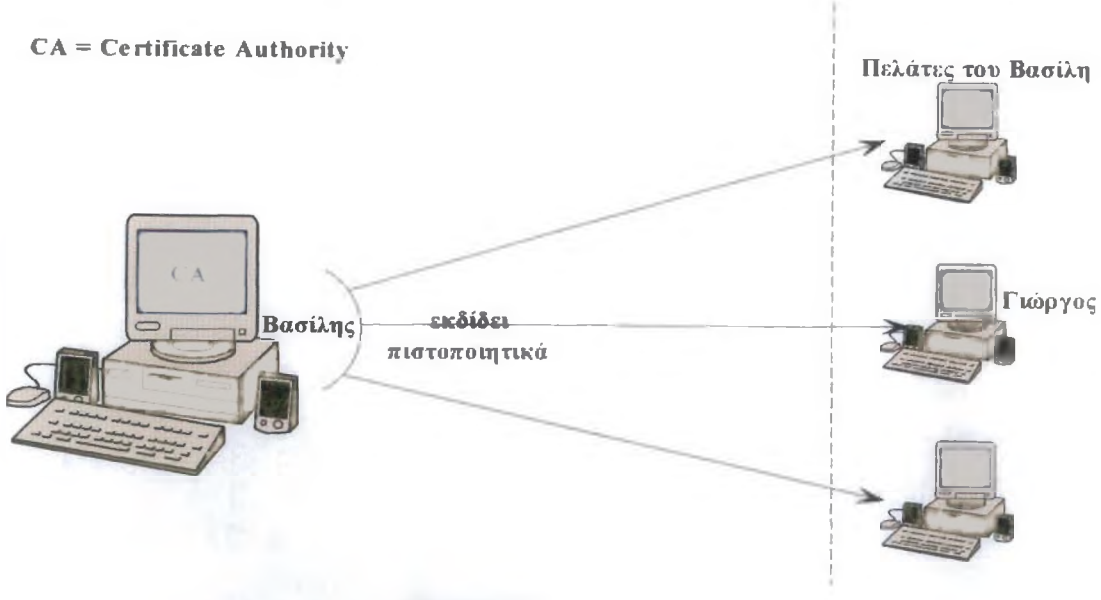
Ένα πιστοποιητικό περιέχει τις ακόλουθες πληροφορίες:

- το όνομα του κατόχου,
- το όνομα της του εκδοτικού οργανισμού – CA,
- την δημόσια κλείδα του ονόματος που αναγράφεται στο πιστοποιητικό,
- την ημερομηνία λήξης του πιστοποιητικού,
- ένα σειριακό αριθμό (serial number),
- την ψηφιακή υπογραφή του εκδοτικού οργανισμού.

Η τυποποιημένη μορφή ενός πιστοποιητικού ακολουθεί το πρωτόκολλο X.509. Το ψηφιακό πιστοποιητικό, είναι στον ηλεκτρονικό κόσμο ότι είναι το διαβατήριο στο φυσικό κόσμο. Το πιστοποιητικό μεταφέρεται, συνήθως, μαζί με την ψηφιακή υπογραφή. Για την επαλήθευση της ψηφιακής υπογραφής ο παραλήπτης πρέπει να έχει την σωστή δημόσια κλείδα του αποστολέα. Επίσης, το πιστοποιητικό στέλνεται κατά την εγκαθίδρυση μιας σύνδεσης μεταξύ δύο άκρων, για την γνωστοποίηση της δημόσιας κλείδας κάθε πλευράς στην άλλη πλευρά και για την χρήση της στην κρυπτογράφηση της επικοινωνίας. Το πιστοποιητικό δεν χρειάζεται να αποστέλλεται κάθε φορά που ξεκινά μία συναλλαγή. Αρκεί να σταλεί μία φορά κατά την έναρξη της σύνδεσης.

5.4.1 Παράδειγμα μιας εμπορικής συναλλαγής με χρήση ψηφιακών πιστοποιητικών

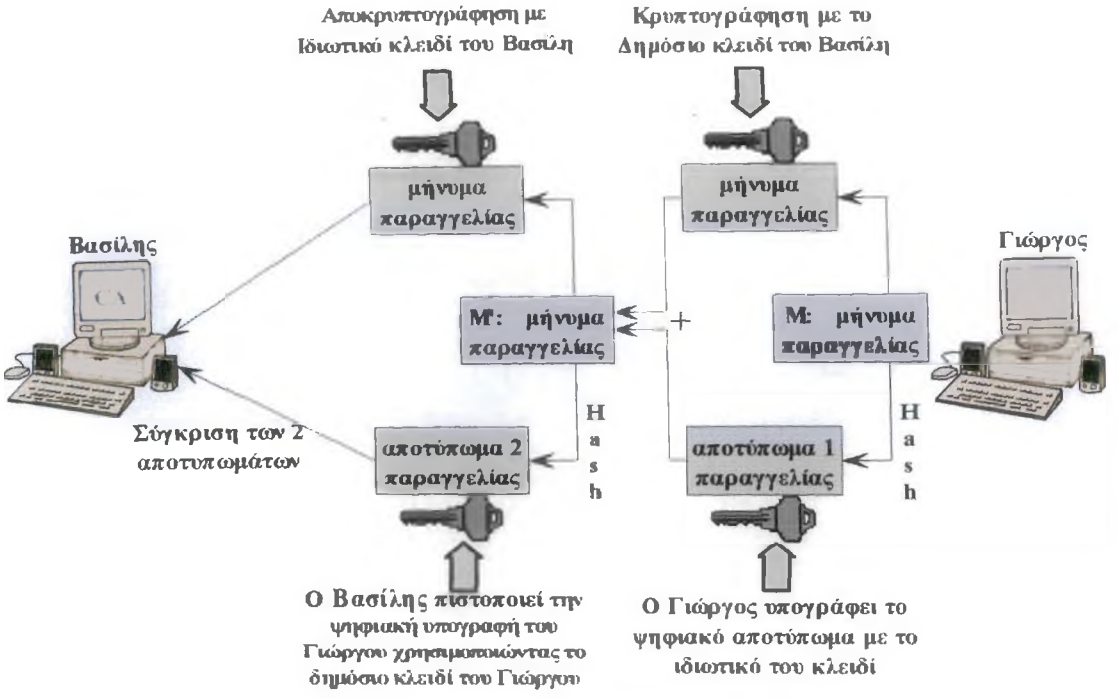
Έστω μια υποθετική συναλλαγή ηλεκτρονικού εμπορίου ανάμεσα σε εμπορικούς συνεργάτες. Ο Γιώργος αγοράζει ατσάλι από τον Βασίλη. Για να ενθαρρυνθούν τέτοιες ηλεκτρονικές – δικτυακές συναλλαγές, ο Βασίλης εξέδωσε ψηφιακά πιστοποιητικά σε όλους τους πελάτες του, συμπεριλαμβανομένου και του Γιώργου. Ο Βασίλης δρα λοιπόν σαν CA , εκδίδοντας ψηφιακά πιστοποιητικά από μόνος του. Το πιστοποιητικό του Γιώργου περιλαμβάνει το όνομά του και το δημόσιο κλειδί του. Ο Βασίλης έχει και αυτός ένα ψηφιακό πιστοποιητικό που περιλαμβάνει το δημόσιο κλειδί του και την ψηφιακή υπογραφή του digital certificate vendor.



Σχήμα 5.3

Κατά τη διάρκεια της παραγγελίας ο browser του Γιώργου πρώτα εξετάζει το ψηφιακό πιστοποιητικό του Βασίλη για να επαληθεύσει ότι είναι αυθεντικό. Ο server του Βασίλη κάνει έναν ακόμα έλεγχο πριν προχωρήσει: κοιτάζει μια λίστα με πιστοποιητικά που ανακλήθηκαν (certificate revocation list CRL) για να αποφασίσει αν το πιστοποιητικό του Γιώργου έχει ανακληθεί για οποιονδήποτε λόγο. Αφότου εξακριβωθούν οι ταυτότητες των μελών και ότι το πιστοποιητικό του Γιώργου δεν έχει εκπνεύσει, τα μηνύματα μεταξύ τους κρυπτογραφούνται χρησιμοποιώντας τα δημόσια κλειδιά. Η παραγγελία του Γιώργου θα κρυπτογραφηθεί με το δημόσιο

κλειδί του Βασίλη και έτσι μόνο ο Βασίλης μπορεί να τη διαβάσει χρησιμοποιώντας το ιδιωτικό κλειδί του. Αργότερα στη διαδικασία, η επιβεβαίωση της παραγγελίας θα κρυπτογραφηθεί με το δημόσιο κλειδί του Γιώργου για να εξασφαλίσει ότι μόνο ο Γιώργος μπορεί να την αποκρυπτογραφήσει και να την διαβάσει. Πώς μπορεί ο Βασίλης να είναι σίγουρος ότι αυτό που λαμβάνει είναι η παραγγελία του Γιώργου και ότι δεν είχε αναχαιτιστεί και αλλαχθεί πριν κρυπτογραφηθεί; Η ψηφιακή υπογραφή του Γιώργου αποδεικνύει ότι αυτός έστειλε την παραγγελία.
Η ψηφιακή υπογραφή επίσης αποδεικνύει ότι έστειλε αυτή ακριβώς την παραγγελία – μια εξασφάλιση που οι φυσικές υπογραφές δεν μπορούν να προσφέρουν. Με τα ψηφιακά πιστοποιητικά ένας αλγόριθμος που λέγεται one way-hash γεννά ένα αποτύπωμα για την παραγγελία. Αν η παραγγελία αλλαζόταν κατά οποιονδήποτε τρόπο τότε ο hash αλγόριθμος θα γεννούσε ένα τελείως διαφορετικό αποτέλεσμα. Ακόμα και μικρές αλλαγές στη χρήση κεφαλαίων και μικρών γραμμάτων, τη στίξη ή τα διάκενα μεταξύ των λέξεων θα οδηγήσει σε διαφορετικά αποτελέσματα. Επιπλέον, είναι αδύνατο να πάρει κανείς το αποτύπωμα και από αυτό να παραγάγει την αρχική παραγγελία, γι αυτό και ο αλγόριθμος λέγεται one-way hash. Ο browser του Γιώργου δημιουργεί ένα hash της παραγγελίας και το προσθέτει στην παραγγελία. Στη συνέχεια κρυπτογραφεί το hash με το ιδιωτικό του κλειδί. Αυτή είναι η ψηφιακή υπογραφή. Αντίθετα με τις φυσικές υπογραφές, οι ψηφιακές υπογραφές είναι μοναδικές για κάθε μήνυμα γιατί το αποτύπωμα για το μήνυμα είναι ενσωματωμένο σε αυτές.
Ο server του Βασίλη παίρνει την παραγγελία για το ατσάλινο πλέγμα και χρησιμοποιεί τον ίδιο one-way hash αλγόριθμο για να γεννήσει ένα ψηφιακό αποτύπωμα για την παραγγελία. Στη συνέχεια χρησιμοποιεί το δημόσιο κλειδί του Γιώργου για να αποκρυπτογραφήσει την ψηφιακή υπογραφή του. Αν ο Γιώργος έστειλε την παραγγελία, μόνο το δικό του δημόσιο κλειδί μπορεί να αποκρυπτογραφήσει την υπογραφή. Ο server του Βασίλη στη συνέχεια συγκρίνει το ψηφιακό αποτύπωμα που γέννησε με αυτό που έστειλε ο Γιώργος. Αν τα δύο αποτυπώματα είναι ίδια τότε ο Βασίλης μπορεί να είναι σίγουρος ότι η παραγγελία που έστειλε ο Γιώργος δεν έχει αλλαχθεί με κανένα τρόπο.
Αν και μπορεί να φαίνεται πολύπλοκη, η περιγραφή της παραγγελίας ατσαλιού του Γιώργου είναι ελαφρώς απλοποιημένη. Στην πραγματικότητα η κρυπτογράφηση με τη χρήση δημόσιου κλειδιού είναι πολύ αργή για να κρυπτογραφηθούν ολόκληρα μηνύματα. Αντίθετα τα πλεονεκτήματα της κρυπτογράφησης δημοσίου κλειδιού συνδυάζονται με την αυξημένη ταχύτητα της κρυπτογράφησης μονού κλειδιού. Με την κρυπτογράφηση μονού κλειδιού και ο αποστολέας και ο παραλήπτης μοιράζονται το ίδιο κλειδί. Το πρόβλημα με αυτή τη μέθοδο κρυπτογράφησης είναι ότι το κλειδί πρέπει να περαστεί με ασφάλεια. Η κρυπτογράφηση δημοσίου κλειδιού παρέχει μια λύση σε αυτό το πρόβλημα, επιτρέποντας στα δυο συστήματα να χρησιμοποιούνται σε συνδυασμό. Αντί να χρησιμοποιείται η πιο αργή κρυπτογράφηση δημοσίου κλειδιού για την κρυπτογράφηση της παραγγελίας, οι browsers και οι servers χρησιμοποιούν κρυπτογράφηση μονού κλειδιού και στη συνέχεια κρυπτογραφούν το κλειδί με κρυπτογράφηση δημοσίου κλειδιού και το επικολλούν στην παραγγελία.



Σχήμα 5.4

Αυτή η πολύπλοκη διαδικασία είναι σχεδόν διαφανής στον χρήστη. Οι browsers μπορούν να ελέγχουν ψηφιακές υπογραφές αυτόματα και να παρακολουθούν πολλά πιστοποιητικά για διάφορους σκοπούς. Όταν ο server του Βασίλη ζητά το ψηφιακό πιστοποιητικό του Γιώργου, ο browser του στέλνει ένα μήνυμα και ζητά από το Γιώργο τον κωδικό που θα επιτρέψει στο πρόγραμμα να έχει πρόσβαση στο ιδιωτικό του κλειδί και να δημιουργήσει την ψηφιακή του υπογραφή. Αφού δώσει τον κωδικό, ο Γιώργος καταλαβαίνει μόνο τη διαδικασία της παραγγελίας. Οι διαδικασίες κρυπτογράφησης, αποκρυπτογράφησης, και επιβεβαίωσης των ψηφιακών υπογραφών συμβαίνουν διάφανα. Αν και η τεχνολογία που χρησιμοποιείται είναι πολύπλοκη, τα ψηφιακά πιστοποιητικά είναι πολύ εύκολα στη χρήση τους από πελάτες και εμπορικούς συνεργάτες. Φυσικά κάθε δυσκολία στη διαδικασία (ο Γιώργος να δώσει λάθος κωδικό ή απόπειρα χρήσης ενός ληγμένου πιστοποιητικού για παράδειγμα) θα ενεργοποιούσε ένα μήνυμα λάθους και θα οδηγούσε τη συνδιαλλαγή σε αποτυχία. Οι επιτυχημένες συνδιαλλαγές είναι διαφανείς προς τον χρήστη.

5.5 Είδη Πιστοποιητικών

Υπάρχουν τέσσερις διαφορετικοί τύποι ψηφιακών πιστοποιητικών σε χρήση στο Internet:

Πιστοποιητικά Αρχών Πιστοποίησης (Certification authority certificates)

Ένα πιστοποιητικό μιας αρχής πιστοποίησης είναι ένα πιστοποιητικό που περιλαμβάνει το όνομα και το δημόσιο κλειδί της αρχής πιστοποίησης. Αυτά τα πιστοποιητικά μπορούν να υπογραφούν από μόνα τους (self-signed). Αυτό σημαίνει ότι η αρχή πιστοποίησης μας λέει ότι το κλειδί της είναι καλό, και εμείς πρέπει να το εμπιστευτούμε. Αλλιώς, αυτά μπορούν να υπογραφτούν από μια άλλη αρχή. Επίσης

οι αρχές μπορούν να διασταυρώνουν η μια με την άλλη την πιστότητα των κλειδιών τους ή ακόμα και να υπογράφει η μια της άλλης τα κλειδιά..
Τα πιστοποιητικά αυτά διανέμονται με την προοπτική να τα εμπιστευτούμε όπως είναι, αυτό φαίνεται από το γεγονός ότι ενσωματώνονται απευθείας στους web browsers.

Πιστοποιητικά Server (Server certificates)
Κάθε SSL server πρέπει να έχει ένα SSL πιστοποιητικό server. Όταν ένας browser συνδέεται σε ένα web server χρησιμοποιώντας το SSL πρωτόκολλο, ο server στέλνει στον browser το δημόσιο κλειδί του σε ένα χ.509 v3 πιστοποιητικό. Το πιστοποιητικό χρησιμοποιείται για να αποδείξει την ταυτότητα του server και για να διανέμει το δημόσιο κλειδί του server, το οποίο χρησιμοποιείται για να κρυπτογραφήσει την αρχική πληροφορία που στέλνεται στον server από τον client.

Προσωπικά πιστοποιητικά (personal certificates)
Αυτά τα πιστοποιητικά περιλαμβάνουν το όνομα ενός ατόμου και το δημόσιο κλειδί αυτού του προσώπου. Επίσης μπορούν να έχουν και άλλες πληροφορίες, όπως την ηλεκτρονική διεύθυνση του ατόμου, την ταχυδρομική διεύθυνση του, ή οτιδήποτε άλλο.

Πιστοποιητικά εκδοτών λογισμικού (Software publisher certificates)
Αυτά τα πιστοποιητικά χρησιμοποιούνται για να υπογράφουν προγράμματα που πρόκειται να διανεμηθούν.

5.5.1 Απόκτηση Πιστοποιητικού για έναν Server

Για να αποκτήσουμε ένα πιστοποιητικό για, τον server μας, χρειαζόμαστε να ακολουθήσουμε τα παρακάτω βήματα:

1. Δημιουργία ενός RSA δημόσιου / προσωπικού ζεύγους κλειδιών χρησιμοποιώντας ένα πρόγραμμα που θα το προμηθευτούμε από τον πωλητή του server.
2. Αποστολή του δημόσιου κλειδιού, το διακεκριμένο και το κοινό όνομα στην αρχήπιστοποίησης που επιθυμούμε να χρησιμοποιήσουμε. Η αποστολή συνήθως γίνεται με την χρήση email.
3. Θα πρέπει να ακολουθήσουμε την διαδικασία πιστοποίησης της CA . Συμπλήρωση διαφόρων στοιχείων στο web site της CA, αποστολή εγγράφων με email-fax ή και με ταχυδρομείο. Επίσης μπορεί να χρειαστεί να πληρώσουμε και την CA.
4. Αναμονή για την επεξεργασία της αίτησης από την CA.
5. Όταν η CA πειστεί ότι η αίτηση πληροί τις προϋποθέσεις, θα εκδώσει ένα πιστοποιητικό αποτελούμενο από το δημόσιο κλειδί μας, το διακεκριμένο όνομα μας, άλλες πληροφορίες, και την ψηφιακή υπογραφή του. Η αποστολή συνήθως γίνεται με την χρήση email.
6. Εγκατάσταση του κλειδιού χρησιμοποιώντας ένα πρόγραμμα που θα το προμηθευτούμε από τον πωλητή του server

Βέβαια όπως όλα τα έγγραφα απόδειξης ταυτότητας, έτσι και τα x.509 v3 πιστοποιητικά λήγουν και χρειάζονται τότε την κατάλληλη ανανέωση πιστοποιητικού που εκτελείται από τις CAs. Η ημερομηνία λήξης κυμαίνεται στους 3-12 μήνες για λόγους ασφάλειας.
Μπορούμε να δούμε τα πιστοποιητικά των διαφόρων sites επιλέγοντας την επιλογή "Document info" του Netscape Navigator. Στην παρακάτω εικόνα φαίνονται οι πληροφορίες για την σελίδα της Hellas on Line που υποστηρίζει το πρωτόκολλο SSL για τις ασφαλείς μεταφορές δεδομένων.

ΚΕΦΑΛΑΙΟ 6
ΨΗΦΙΑΚΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ ΑΠΟ ΤΗ ΜΕΡΙΑ ΤΟΥ ΧΡΗΣΤΗ

6.1 Πιστοποιητικά πελάτη (client)

Ένα client πιστοποιητικό είναι ένα ψηφιακό πιστοποιητικό το οποίο είναι σχεδιασμένο για να πιστοποιεί την ταυτότητα ενός ατόμου. Όπως και με τα πιστοποιητικά των Web sites, τα client πιστοποιητικά συνδέουν ένα συγκεκριμένο όνομα με ένα συγκεκριμένο μυστικό κλειδί. Αυτά εκδίδονται από τις αρχές πιστοποίησης (CAs).

Τα client πιστοποιητικά έχουν πολλές χρήσεις και οφέλη:

- Τα ψηφιακά πιστοποιητικά μπορούν να απομακρύνουν την ανάγκη της απομνημόνευσης των usemames και των passwords. Απλά υπογράφουμε με την ψηφιακή υπογραφή μας οποτεδήποτε εισβάλουμε σε περιορισμένο χώρο.
- Αντί να αναπτύσσουν μια μεγάλη διασκορπισμένη βάση δεδομένων, οι οργανισμοί μπορούν απλά να χρησιμοποιήσουν ένα ψηφιακό πιστοποιητικό εκδομένο από μια ειδική CA σαν απόδειξη ιδιότητας μέλους στον οργανισμό αυτό.
- Είναι δυσκολότερο για μια ομάδα ατόμων να μοιραστούν ένα μονό ψηφιακό ID από ότι είναι να μοιραστούν ένα ζεύγος usemame-password. Αυτό συμβαίνει επειδή η υπογραφή του ονόματος μας με ένα ψηφιακό πιστοποιητικό απαιτεί πρόσβαση σε ένα μυστικό κλειδί.. Έτσι υπάρχουν τεχνικά εμπόδια στο να μπορούν να μοιράζονται κοινά μυστικά κλειδιά οι χρήστες μεταξύ τους, κυρίως επειδή οι χρήστες είναι απρόθυμοι στο να μοιράζονται ένα μυστικό κλειδί που είναι χρήσιμο για περισσότερες από μια εφαρμογές.
- Επειδή τα ψηφιακά πιστοποιητικά περιέχουν ένα δημόσιο κλειδί (που ανήκει στον ιδιοκτήτη του πιστοποιητικού), εμείς μπορούμε να χρησιμοποιήσουμε το ψηφιακό πιστοποιητικό κάποιου για να του στείλουμε κρυπτογραφημένο email.
- Τα πιστοποιητικά που δείχνουν την ηλικία ενός προσώπου μπορούν να χρησιμοποιηθούν για περιορισμούς σε πονηρού περιεχομένου δεδομένα ή και chat groups.
- Τα πιστοποιητικά που δείχνουν το φύλο ενός προσώπου μπορούν να χρησιμοποιηθούν για την ελεύθερη πρόσβαση σε χώρους μόνο για άνδρες ή μόνο για γυναίκες.

Δημιουργώντας ισχυρά συστήματα αναγνώρισης της ταυτότητας των χρηστών, τα πιστοποιητικά βοηθούν για την αντιμετόπιση της ανωνυμίας. Επίσης είναι περισσότερο αποτελεσματικά και από τα «cookies». Ένα cookie απλώς αφήνει ένα ίχνος, που έχει να κάνει με τα σημεία από τα οποία εμείς περάσαμε στην επίσκεψη

μας σε ένα web site. Ένα ψηφιακό πιστοποιητικό από την άλλη μεριά, αφήνει πίσω το όνομα μας, την ηλεκτρονική μας διεύθυνση, ή και άλλες πληροφορίες αναγνώρισης ταυτότητας οι οποίες έχουν την δυνατότητα να ξαναγυρίσουν σε εμάς και να μα δώσουν πληροφορίες για την ταυτότητα του site που επισκεφτήκαμε. Επειδή τα πιστοποιητικά ελαχιστοποιούν την ανωνυμία, μερικό χρήστες του Internet είναι αντίθετοι στη χρήση τους, βασιζόμενοι στο ότι αυτά εκθέτουν την μυστικότητα του χρήστη. Αυτό κάνουν, αυτός είναι και ο σκοπός που δημιουργήθηκαν τους άλλωστε. Όπως σήμερα κατασκευάζονται, ωστόσο, τα πιστοποιητικά δεν στέλνονται ποτέ από έναν web browser χωρίς την γνώση και την άδεια του χρήστη. Επίσης, τα πιστοποιητικά δεν περιέχουν πληροφορίες που είναι άγνωστες στον χρήστη. Φυσικά, και οι δύο αυτές περιπτώσεις μπορούν να αλλάξουν στο μέλλον.

6.2 Υποστήριξη για τα Client-side ψηφιακά πιστοποιητικά

Τα client-side ψηφιακά πιστοποιητικά υποστηρίζονται από τον Internet Explorer, και τον Netscape Navigator, και άλλες εφαρμογές βασισμένες στο SSL. Η υποστήριξη αποτελείται από τέσσερα συστατικά κλειδιού:

Δημιουργία κλειδιού

Η εφαρμογή (browser) περιέχει κώδικα για την δημιουργία δημόσιου/προσωπικού ζεύγους κλειδιών, στέλνοντας το μυστικό κλειδί σε μία CA μέσα στην φόρμα μιας HTTP συναλλαγής.

Απόκτηση πιστοποιητικού

Η εφαρμογή (browser) μπορεί να δεχτεί ένα πιστοποιητικό από μια CA μέσω HTTP.

Κλήση / Ανταπόκριση

Η εφαρμογή μπορεί να κάνει χρήση ενός αποθηκευμένου μυστικού κλειδιού για την υπογραφεί τυχαίων κλήσεων ενός SSL server.

Ασφαλής αποθήκευση

Ο browser παρέχει ένα μέρος για την ασφαλή αποθήκευση του μυστικού κλειδιού. Οι εκδόσεις του Interi1et Explorer, και του Netscape Navigator επιτρέπουν στο κλειδί να αποθηκεύεται κρυπτογραφημένο. Σε μελλοντικές εκδώσεις οι εφαρμογές θα επιτρέπουν στα κλειδιά να αποθηκεύονται σε floppy disks ή σε smart cards.

6.3 Απόκτηση Ψηφιακού Πιστοποιητικού / Υπογραφής

Για την απόκτηση ενός δοκιμαστικού ψηφιακού πιστοποιητικού / υπογραφής ακολουθούμε με προσοχή τα παρακάτω βήματα:

1. Επισκεπτόμαστε έναν από τους γνωστούς τόπους (sites) παροχής πιστοποιητικών διαφόρων χρήσεων, όπως για παράδειγμα:

   http:// www.verisign.com/client/enrollment/index.html

http:// www.globalsign.com/digital_certificate/personalsign/index.cfm

2. Ακολουθώντας την (λίγο διαφορετική κατά περίπτωση) διαδικασία, συμπληρώνουμε την (on-line) φόρμα εγγραφής και υποβάλλουμε ηλεκτρονικά το αιτημά μας για την παροχή ενός πιστοποιητικού πελάτη (personal certificate / digital ID).

3. Με βάση την ηλεκτρονική διεύθυνση που καταχωρήσαμε, λαμβάνουμε ένα μήνυμα στο οποίο περιλαμβάνεται έναν σύνδεσμος (1ink) για το αυτόματο "κατέβασμα" (download) του πιστοποιητικού από τον εξυπηρετητή στον προσωπικό υπολογιστή μας. Συνήθως, ακολουθεί αυτόματη εγκατάσταση του πιστοποιητικού στη βάση δεδομένων του προγράμματος ηλεκτρονικού ταχυδρομείου που χρησιμοποιούμε (π.χ. Microsoft Outlook ή Netscape Messenger).

4. Εξάγουμε (export) την ψηφιακή υπογραφή μας σε μια δισκέτα και αποθηκεύουμε την δισκέτα σε ένα σίγουρο και ασφαλές μέρος (backup) για περίπτωση ανάκτησής του (recovery) μετά από μια καταστροφή στο σκληρό δίσκο.

5. Χρησιμοποιούμε την δισκέτα για να εισάγουμε (import) την ψηφιακή υπογραφή μας σε άλλους υπολογιστές (π.χ. στο σπίτι ή σε φορητό *HN).*

6.4 Πρότυπα Αρχείων Πιστοποιητικών

Τα πιστοποιητικά εξάγονται σε αρχεία που η μορφή τους συμφωνεί με ένα από τα παρακάτω πρότυπα:

PKCS#12
Το πρότυπο PKCS #12 επιτρέπει τη μεταφορά του πιστοποιητικού και του προσωπικού κλειδιού από τον ένα υπολογιστή στον άλλο με τη βοήθεια μιας δισκέτας. Ένα αρχείο τέτοιας μορφής έχει κατάληξη (extension) PFX.

PKCS#7
Το πρότυπο PKCS #7 επιτρέπει τη μεταφορά του πιστοποιητικού και όλων των πιστοποιητικών της αλυσίδας πιστοποίησης (ιεραρχίας αρχών πιστοποίησης) από τον ένα υπολογιστή στον άλλο με τη βοήθεια μιας δισκέτας. Ένα αρχείο τέτοιας μορφής έχει κατάληξη P7B.

DER
Το πρότυπο DER χρησιμοποιείται από αρχές πιστοποίησης. Ένα αρχείο τέτοιας μορφής έχει κατάληξη CER.

Base64
Το πρότυπο Base64 χρησιμοποιείται και αυτό από αρχές πιστοποίησης. Ένα αρχείο τέτοιας μορφής έχει επίσης κατάληξη CER

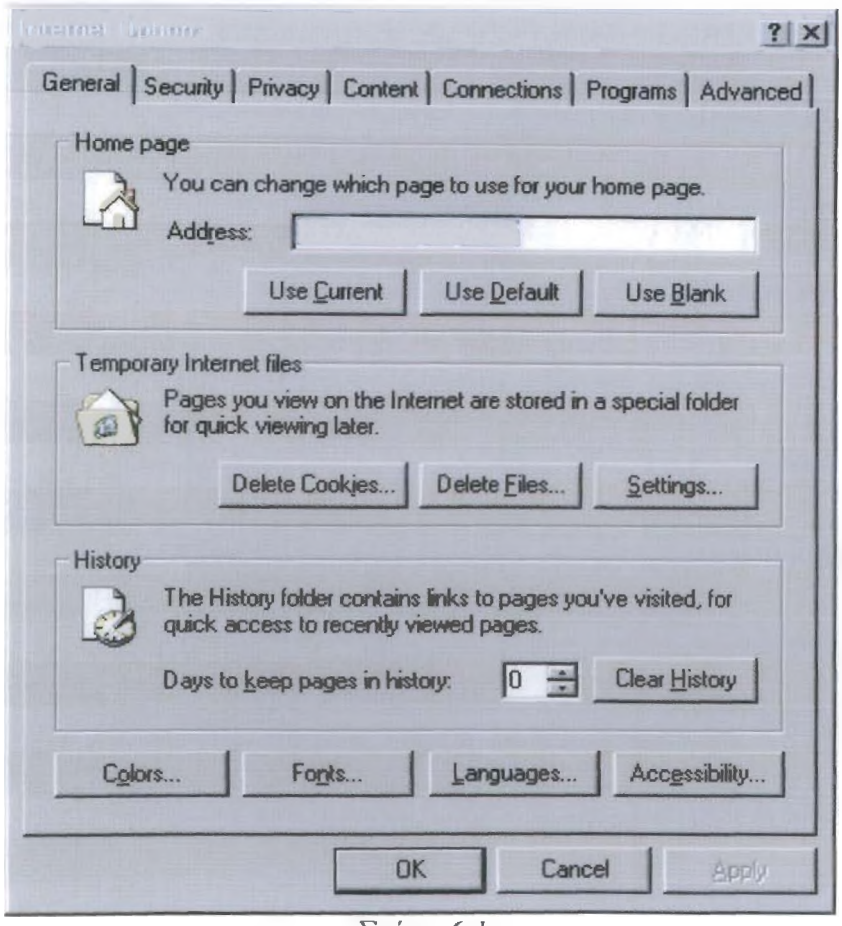
6.5 Εισαγωγή και εξαγωγή ψηφιακού πιστοποιητικού

Οι βασικοί λόγοι που κάνουμε εισαγωγή και εξαγωγή ψηφιακών πιστοποιητικών είναι οι εξής:

- Να έχετε ένα αντίγραφο του πιστοποιητικού σας σε μια δισκέτα για ασφαλή κράτηση
- Να αντιγράφετε το πιστοποιητικό από τον υπολογιστή εργασίας σας στον προσωπικό υπολογιστή σας. Μπορείτε να έχετε το πιστοποιητικό σας και στους δύο υπολογιστές ή σε διάφορους υπολογιστές.
- Σας επιτρέπει να κινήσετε το πιστοποιητικό σας από τον Netscape Navigator στον Microsoft Internet Explorer και αντίστροφα.

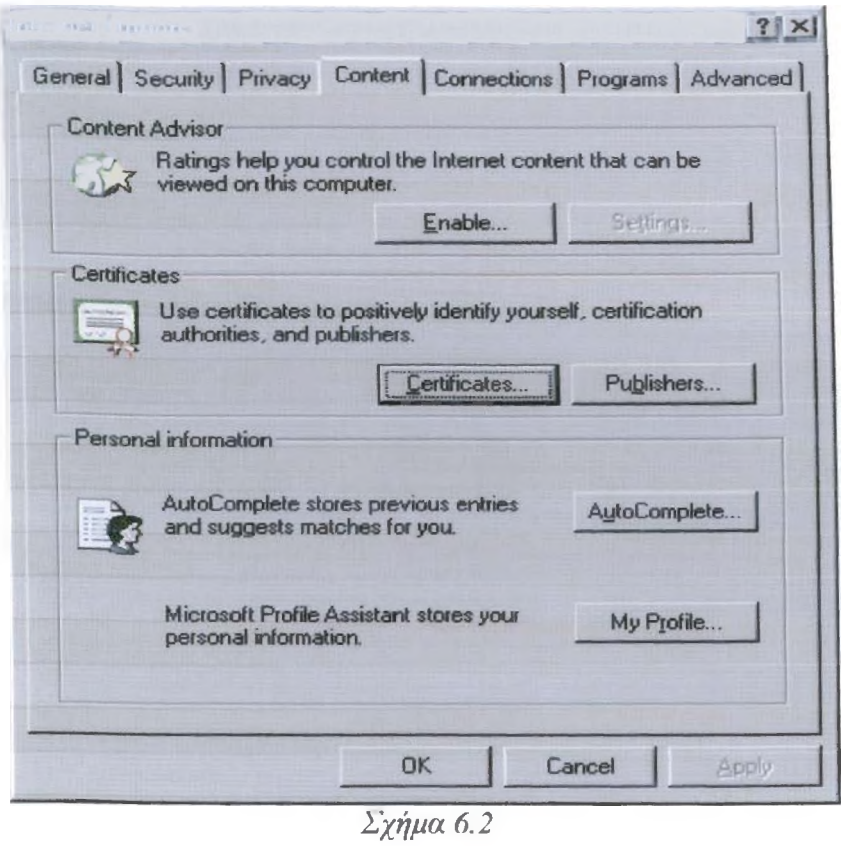
6.5.1 Εξαγωγή ψηφιακού πιστοποιητικού στον Internet Explorer

Επιλέγουμε "tools" και μετά "internet options". Στο παράθυρο που εμφανίζεται παρακάτω επιλέγουμε την καρτέλα "content".



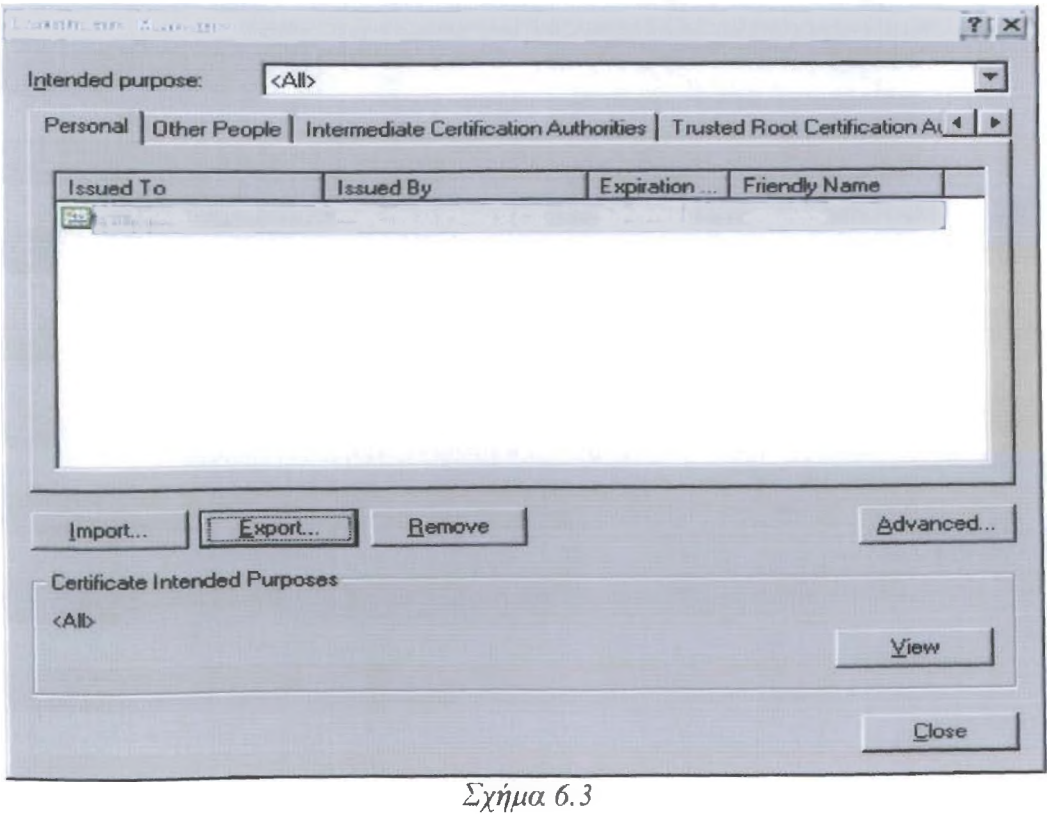
Σχήμα 6.1

Στην καρτέλα "contents" επιλέγουμε το κουμπί "certificates"



Σχήμα 6.2

Εμφανίζεται το παράθυρο "certificate manager" με προεπιλεγμένη την καρτέλα "personal". Επιλέγουμε το πιστοποιητικό που θέλουμε να εξάγουμε και πατάμε το κουμπί "export", όπως φαίνεται παρακάτω.

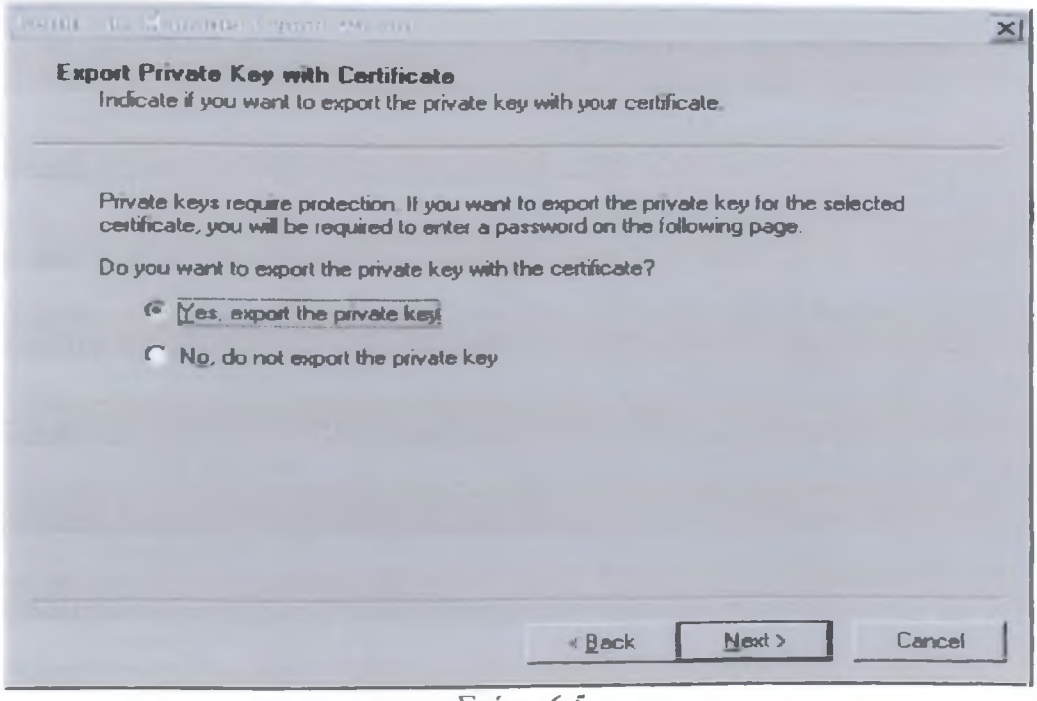


Σχήμα 6.3

Εμφανίζεται το πρώτο από τα παράθυρα του "certificate manager export wizard"και επιλέγουμε "next >"

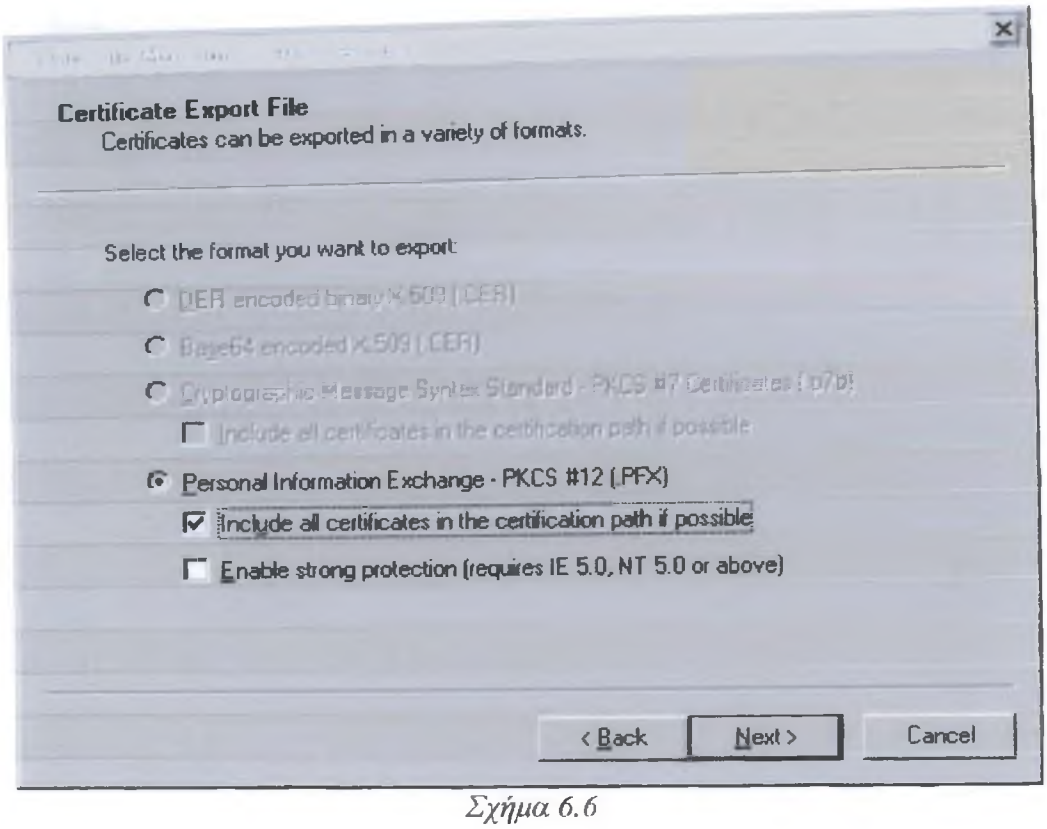
Σχήμα 6.4

Στο δεύτερο παράθυρο του "certificate manager export wizard" επιλέγουμε "Yes, export the private key" για να εξαχθεί το ιδιωτικό κλειδί μας για φύλαξη και για να μπορέσουμε να το εισάγουμε κατόπιν σε άλλους υπολογιστές.



Σχήμα 6.5

Στο τρίτο παράθυρο σημειώνουμε τις όλες τις επιλογές, όπως παρακάτω

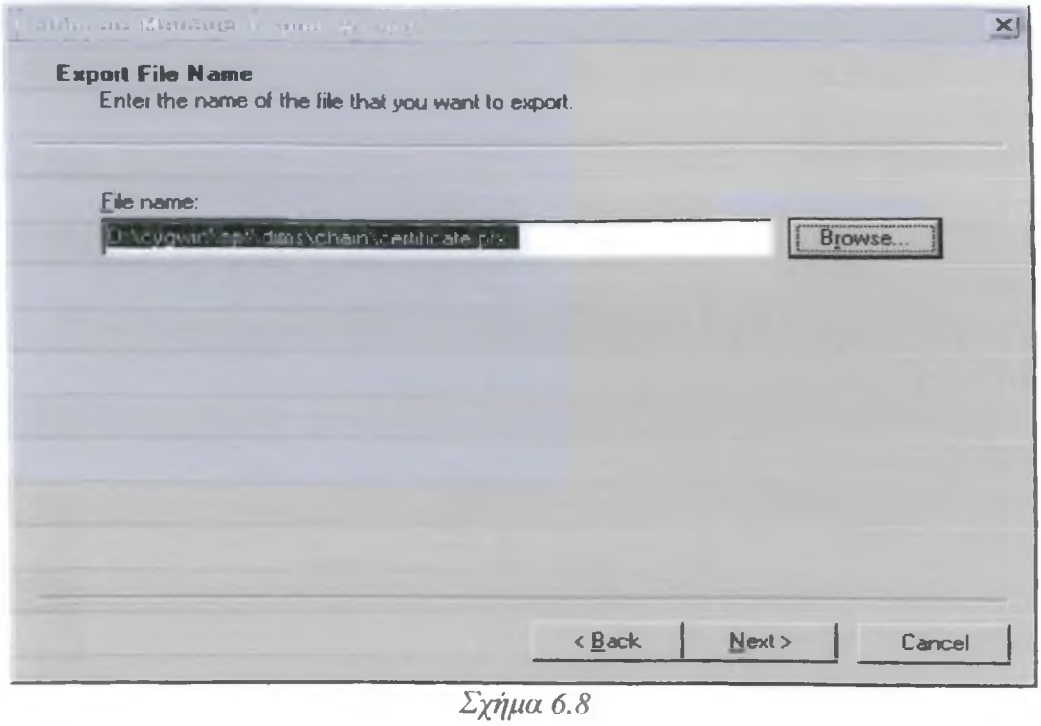


Σχήμα 6.6

Στο τέταρτο παράθυρο εισάγουμε ένα συνθηματικό που θα προστατεύει το κλειδί μας στη δισκέτα όπου θα το αποθηκεύσουμε.

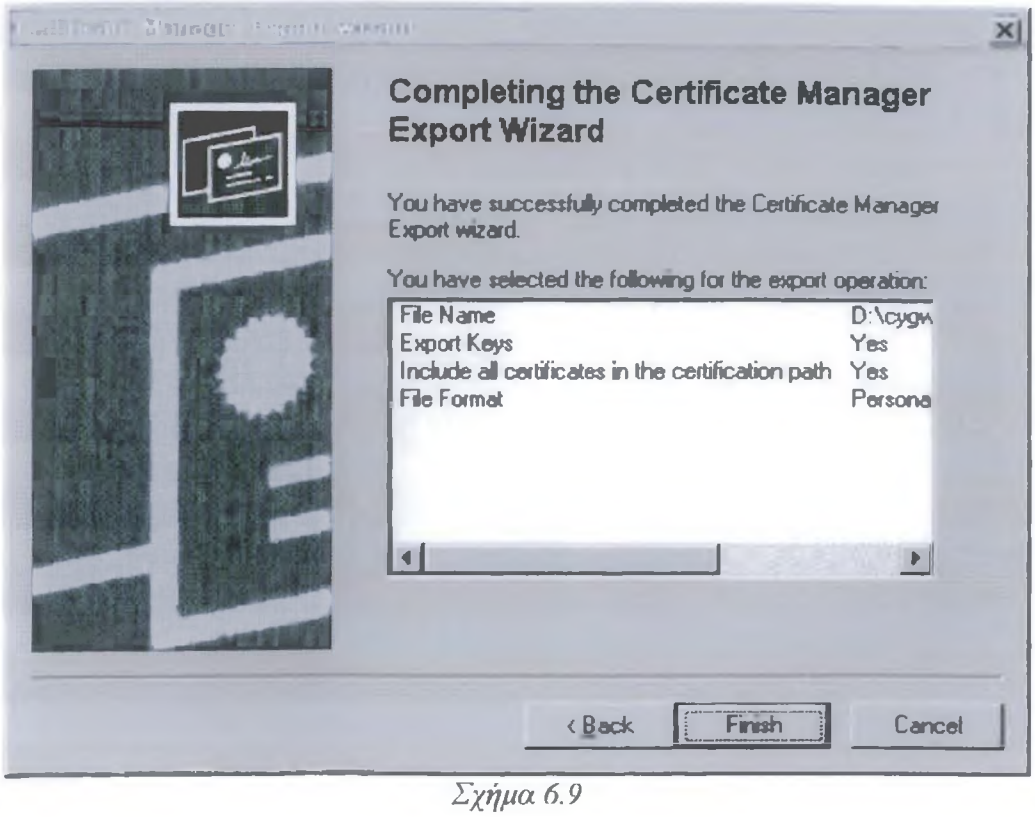
Σχήμα 6.7

Στο πέμπτο παράθυρο εισάγουμε ένα όνομα για το αρχείο όπου θα σωθεί η ψηφιακή μας υπογραφή.



Σχήμα 6.8

Το έκτο παράθυρο μας ενημερώνει ότι έχουμε ολοκληρώσει την διαδικασία του οδηγού. Παρ' όλα αυτά υπάρχουν πρόσθετα παράθυρα που εμφανίζονται αφού πατήσουμε το κουμπί "finish".

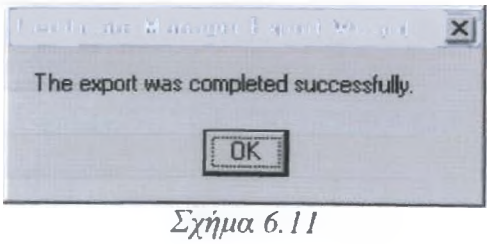


Σχήμα 6.9

Μετά το πάτημα του κουμπιού "finish" ζητείται το πιστοποιητικό για το Personal Security Environment (PSE).

Σχήμα 6.10

Το σύστημα μας ειδοποιεί μόλις ολοκληρωθεί η εξαγωγή



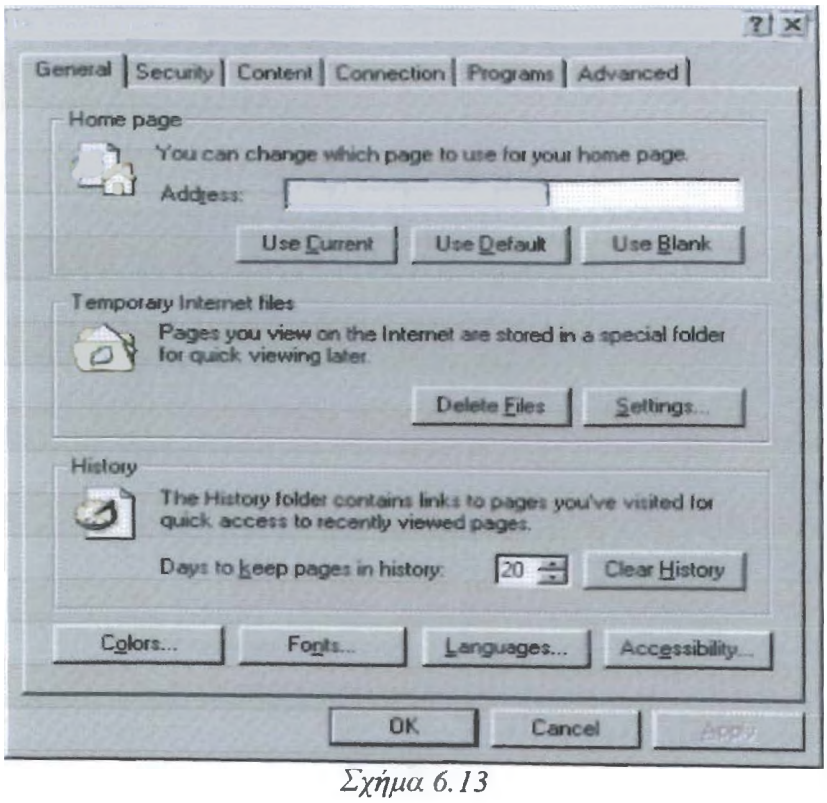
Σχήμα 6.11

6.5.2 Εισαγωγή ψηφιακού πιστοποιητικού στον Internet Explorer

Για την εισαγωγή ψηφιακού πιστοποιητικού στον Microsoft Internet Explorer αρχικά επιλέγουμε "tools" και κατόπιν "internet options"

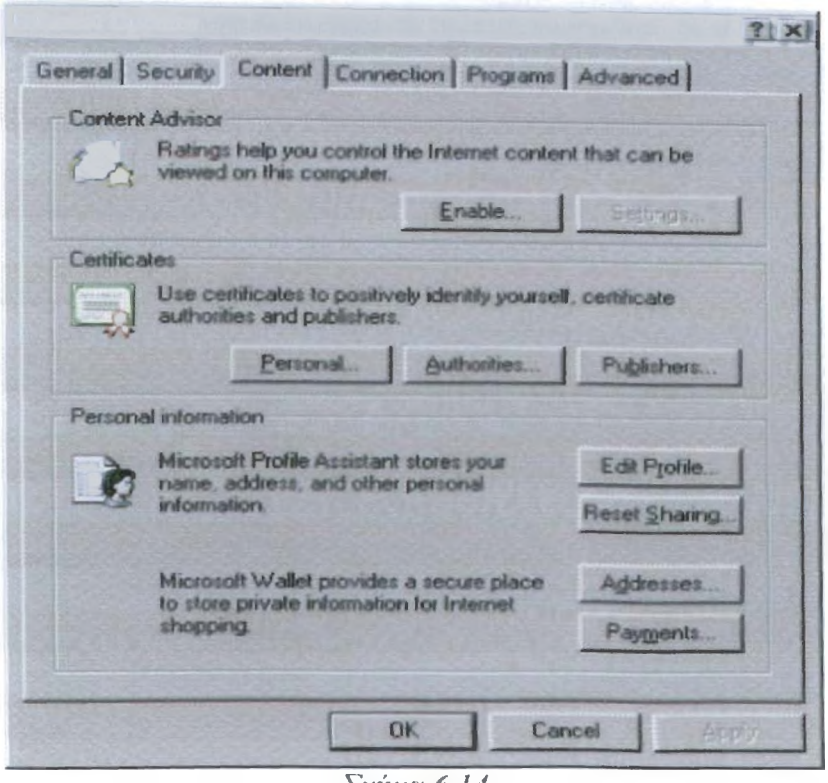
Σχήμα 6.12

Στο παρακάτω παράθυρο επιλέγουμε την καρτέλα "content"



Σχήμα 6.13

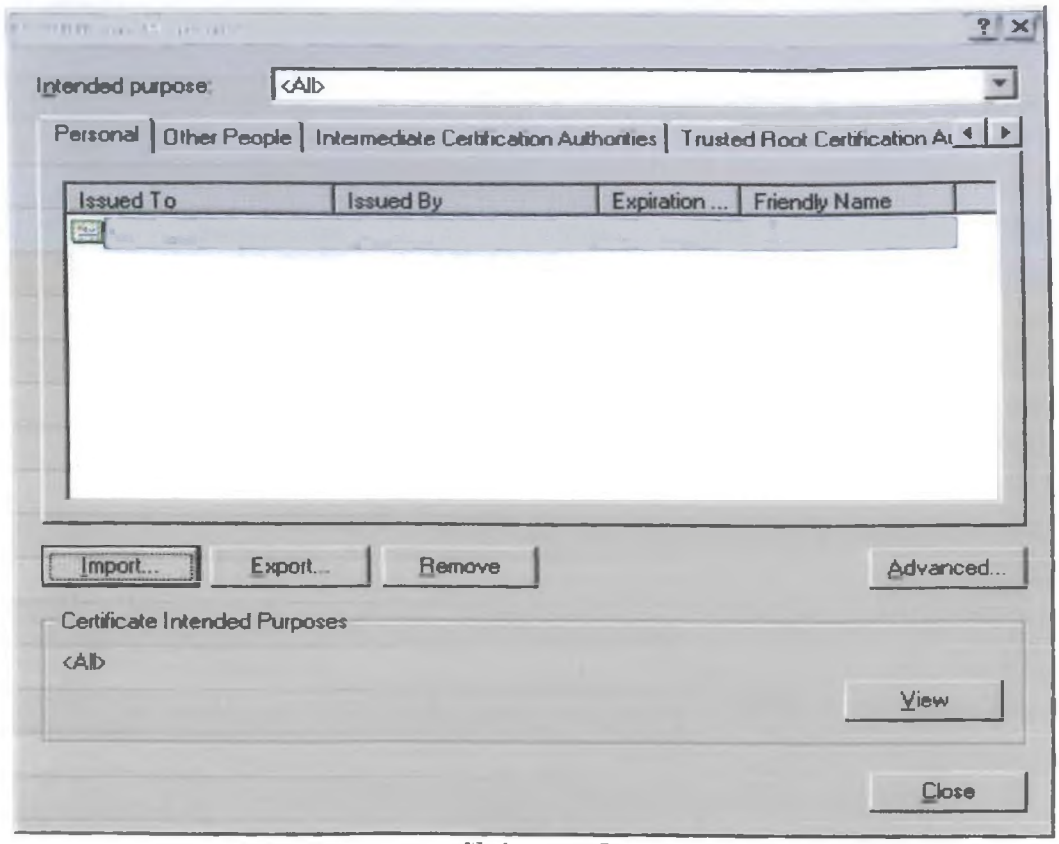
Ύστερα επιλέγουμε το κουμπί "personal" από το "certificates"



Σχήμα 6.14

Το παράθυρο "Certificate Manager" εμφανίζεται με προεπιλεγμένο το tab "Personal".

Επιλέγουμε το κουμπί "import"

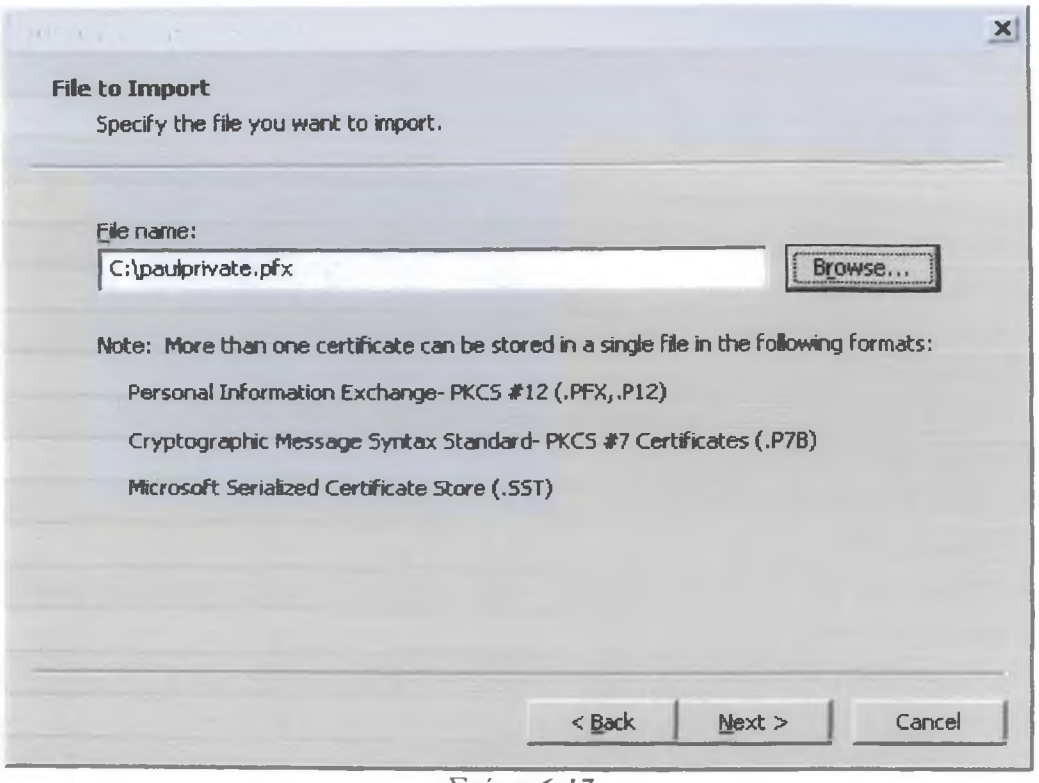


Σχήμα 6.15

Εμφανίζεται το πρώτο από τα παράθυρα του "certificate import wizard"και επιλέγουμε "next >"

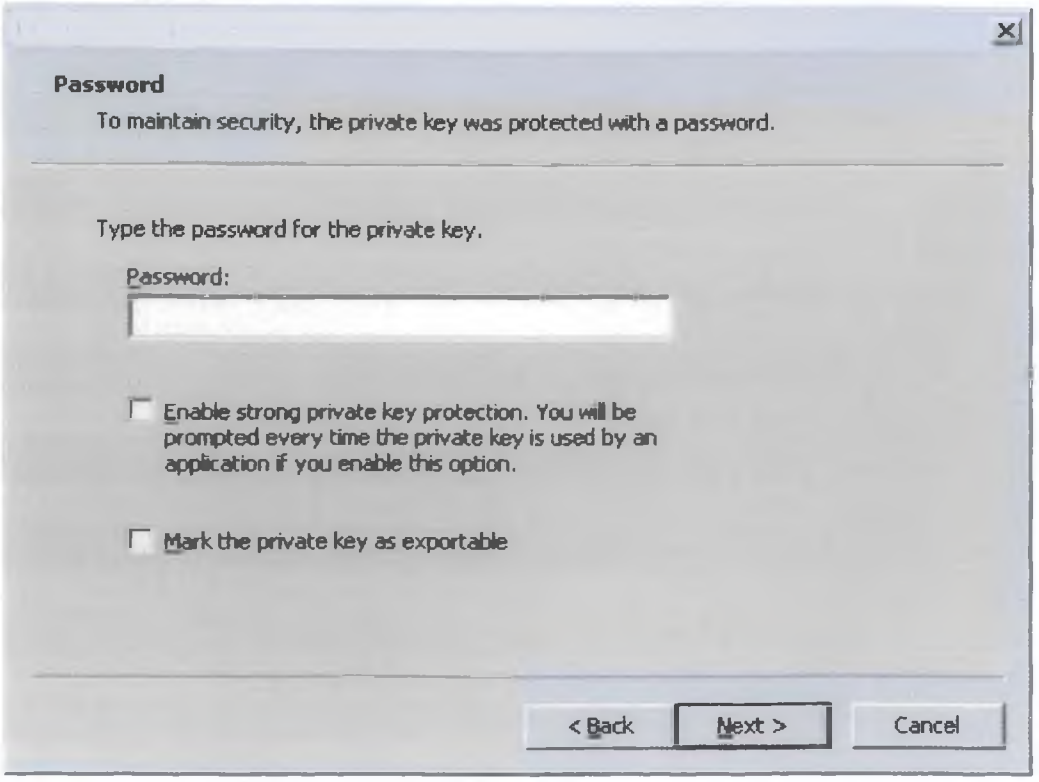
Σχήμα 6.16

Στο δεύτερο παράθυρο του "certificate import wizard" εισάγουμε το πιστοποιητικό από το αρχείο όπου το αποθηκεύσαμε



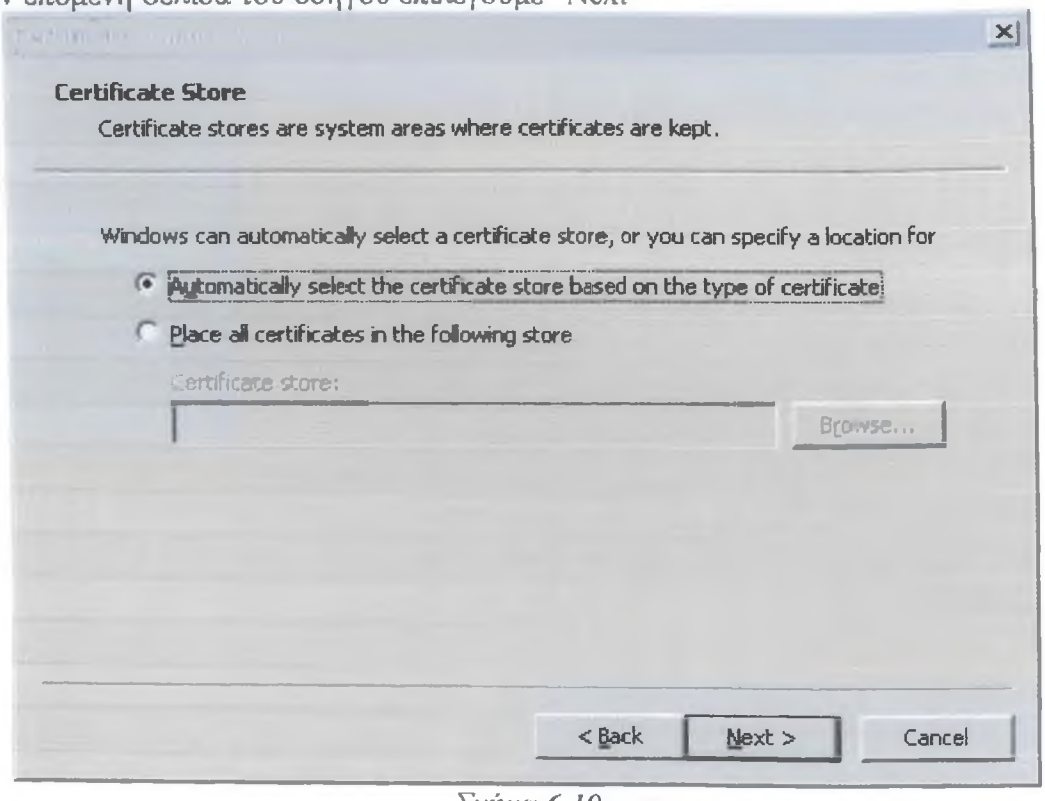
Σχήμα 6.17

Πληκτρολογούμε το password και σημειώνουμε τις επιλογές που θέλουμε να κάνουμε



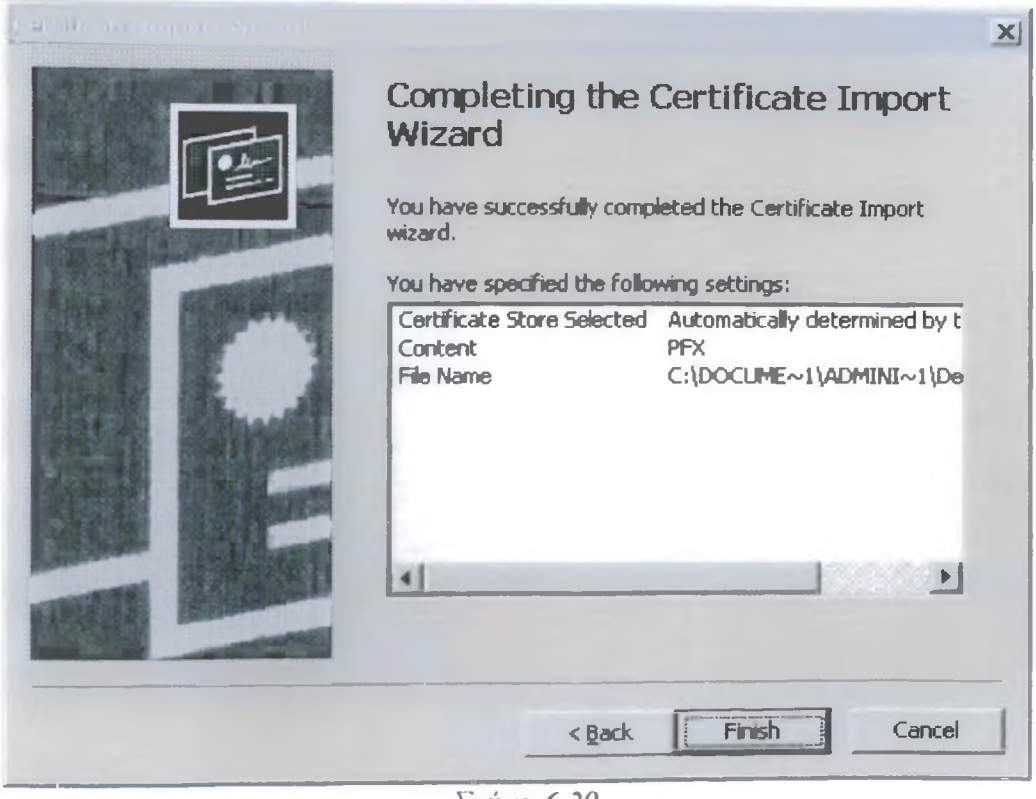
Σχήμα 6.18

Στην επόμενη σελίδα του οδηγού επιλέγουμε "Next>"



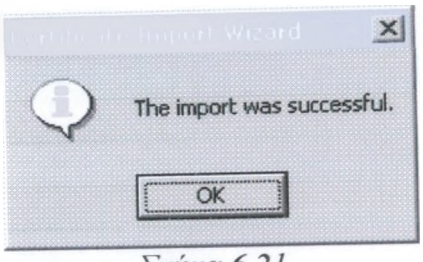
Σχήμα 6.19

Στο τελευταίο παράθυρο του οδηγού πατάμε το κουμπί "finish"



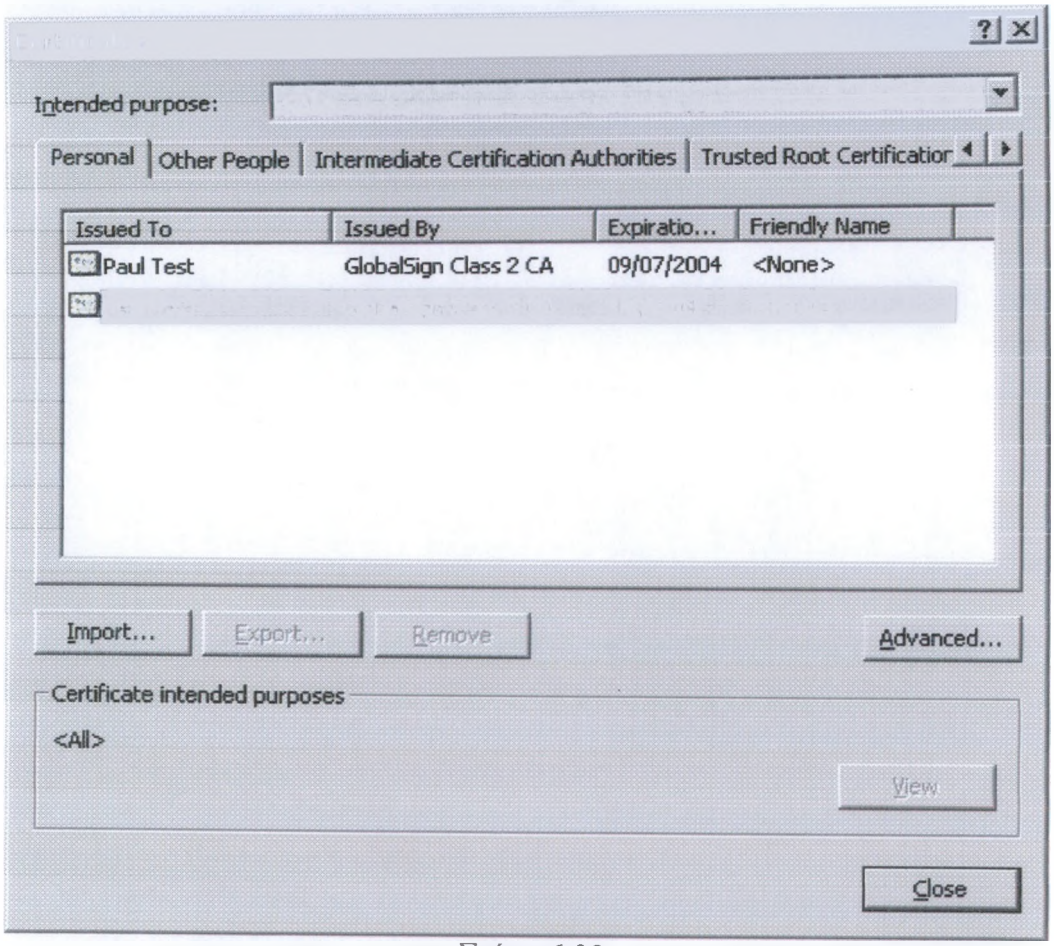
Σχήμα 6.20

Το πιστοποιητικό έχει εισαχθεί με επιτυχία και μπορούμε να το χρησιμοποιήσουμε με ασφάλεια.



Σχήμα 6.21

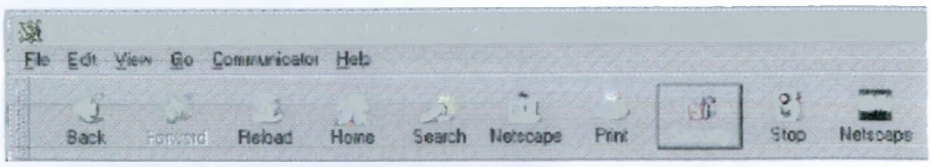
Τέλος το πιστοποιητικό εμφανίζεται στον κατάλογο των πιστοποιητικών μας.



Σχήμα 6.22

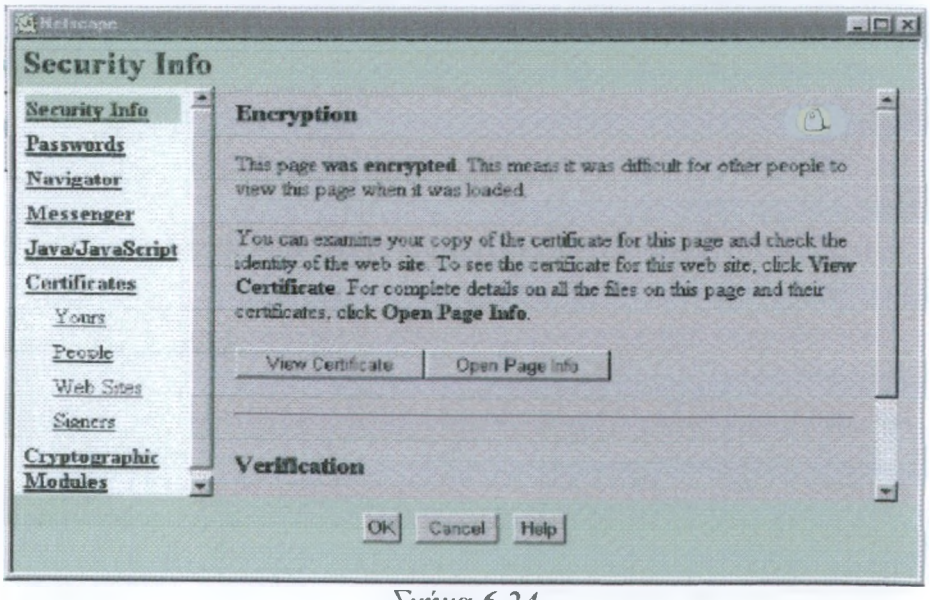
6.5.3Εξαγωγή ψηφιακού πιστοποιητικού από τον Netscape Navigator

Για την εξαγωγή ψηφιακού πιστοποιητικού από τον Netscape Navigator αρχικά επιλέγουμε από την μπάρα εργαλείων "Navigator Toolbar"το "security icon"



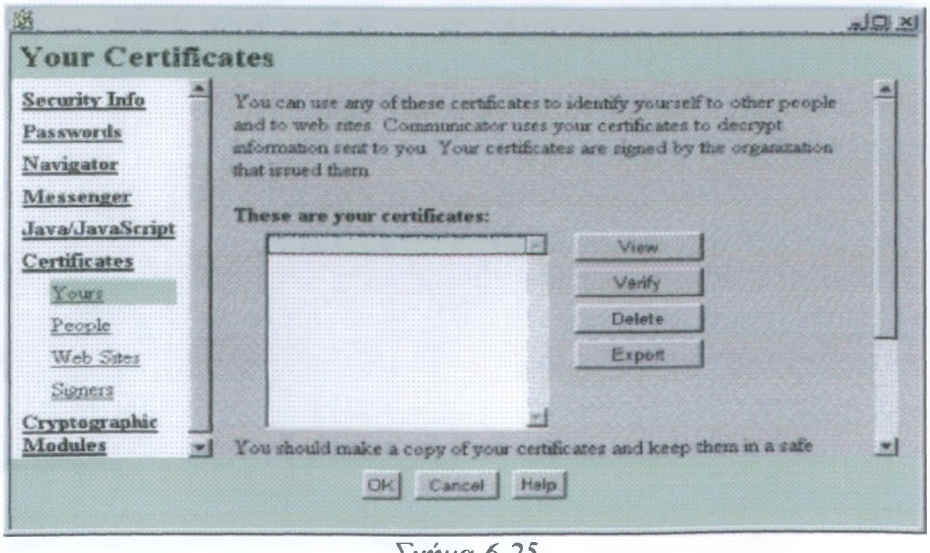
Σχήμα 6.23

Εμφανίζεται το παράθυρο "Security Info" και επιλέγουμε "Yours"



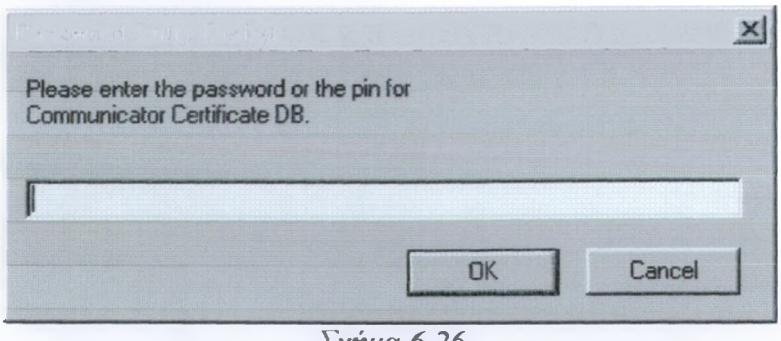
Σχήμα 6.24

Επιλέγουμε το πιστοποιητικό που θέλουμε να εξάγουμε και πατάμε το κουμπί "Export"



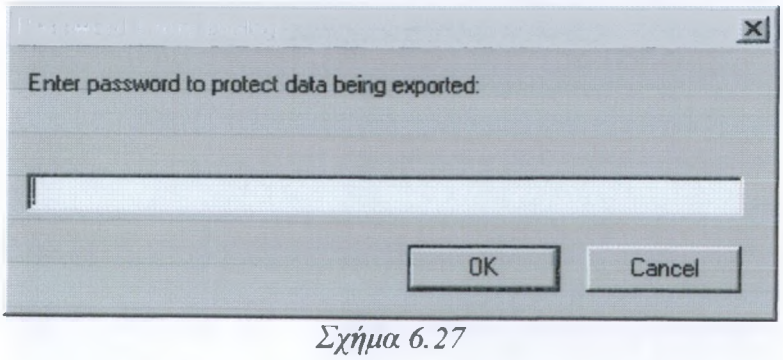
Σχήμα 6.25

Θα εμφανιστεί το παράθυρο "Password Entry Dialog" όπου εισάγουμε το συνθηματικό για το Personal Security Environment (PSE) ώστε να μπορέσουμε να εξάγουμε το ψηφιακό μας πιστοποιητικό.



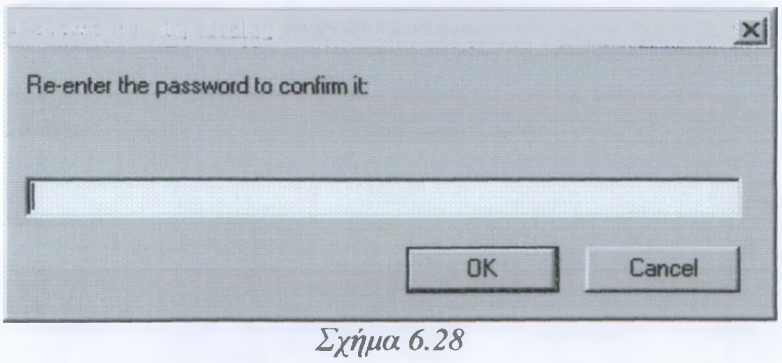
Σχήμα 6.26

Έπειτα εμφανίζεται ένα άλλο παράθυρο "Password Entry Dialog" όπου εισάγουμε ακόμη ένα συνθηματικό για να προστατέψουμε το ψηφιακό μας πιστοποιητικό στη δισκέτα



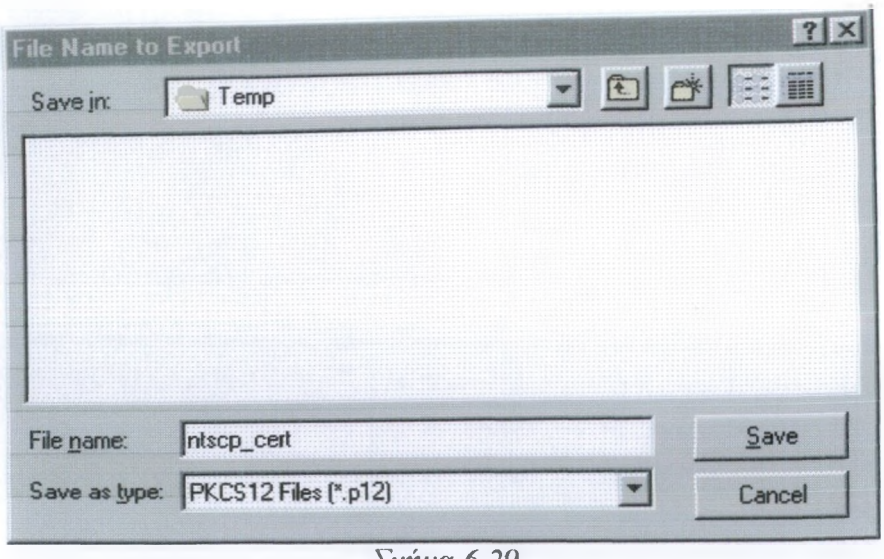
Σχήμα 6.27

Ξαναπληκτρολογούμε τον κωδικό και πατάμε OK



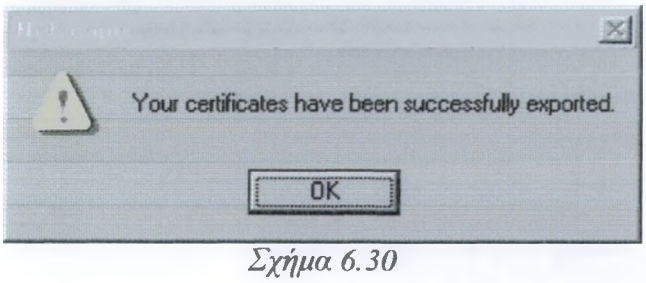
Σχήμα 6.28

Στη συνέχεια εμφανίζεται το παράθυρο επιλογής αρχείου και επιλέγουμε που θέλουμε να αποθηκευθεί το ψηφιακό μας πιστοποιητικό.



Σχήμα 6.29

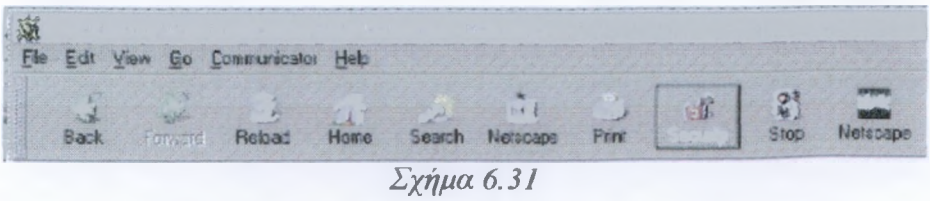
Το σύστημα μας ειδοποιεί μόλις ολοκληρωθεί η εξαγωγή



Σχήμα 6.30

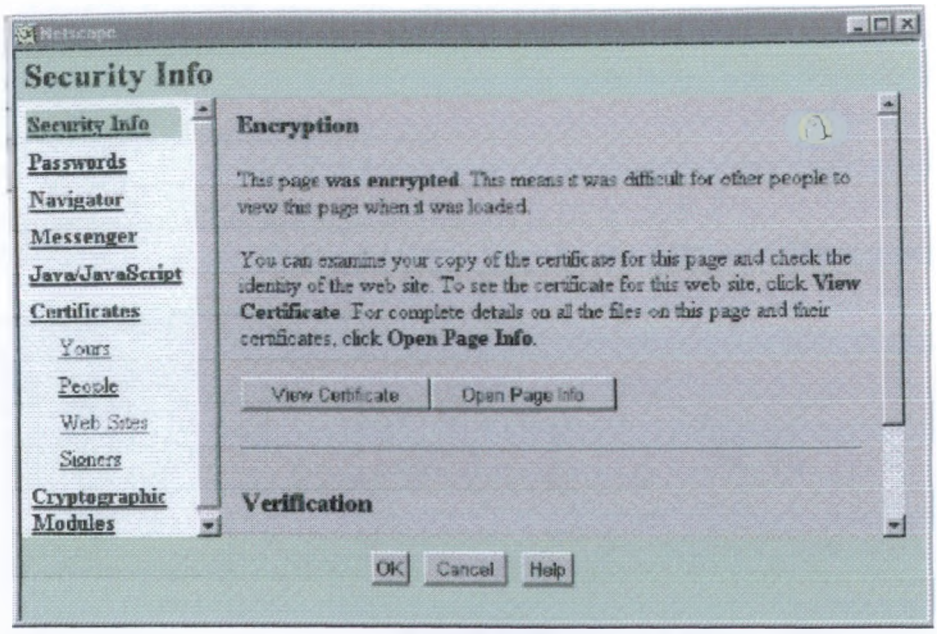
6.5.4 Εισαγωγή ψηφιακού πιστοποιητικού στον Netscape Navigator

Για την εισαγωγή ψηφιακού πιστοποιητικού στον Netscape Navigator αρχικά επιλέγουμε από την μπάρα εργαλείων "Navigator Toolbar"το "security icon"



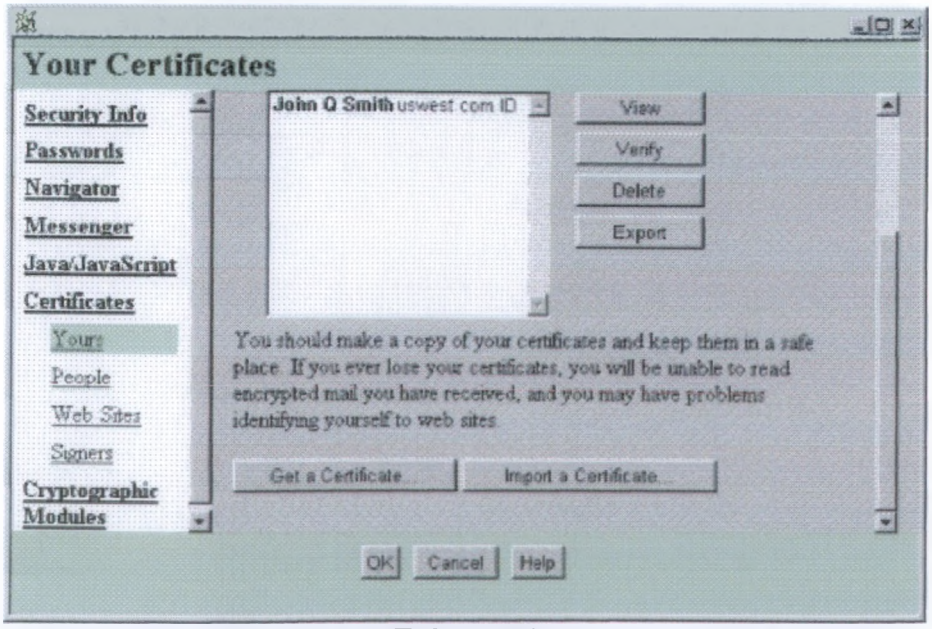
Σχήμα 6.31

Εμφανίζεται το παράθυρο "Security Info" και επιλέγουμε "yours"



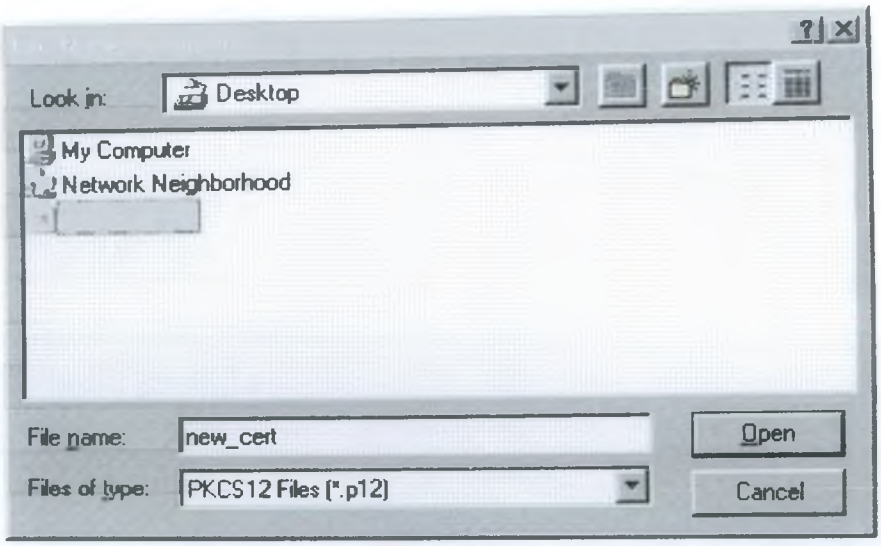
Σχήμα 6.32

Για να εισάγουμε ένα ψηφιακό πιστοποιητικό επιλέγουμε το κουμπί "import a certificate"



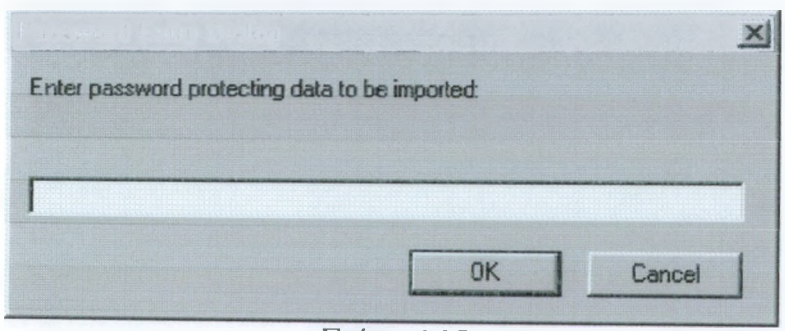
Σχήμα 6.33

Ανοίγει το παράθυρο επιλογής αρχείου και επιλέγουμε το αρχείο που περιέχει το ψηφιακό μας πιστοποιητικό



Σχήμα 6.34

Πληκτρολογούμε τον προσωπικό κωδικό του πιστοποιητικού που εισάγουμε και πατάμε OK



Σχήμα 6.35

Το πιστοποιητικό μας έχει εισαχθεί.

ΚΕΦΑΛΑΙΟ 7
PGP (Pretty Good Privacy)

7.1 Εισαγωγή

Το PGP (Pretty Good Privacy) είναι ένα σύστημα κρυπτογράφησης δημόσιου κλειδιού, το οποίο αναπτύχθηκε το 1991 στις ΗΠΑ από τον τότε μηχανικό λογισμικού, Phil Zimmermann. Μέχρι το 1999, η εξαγωγή κρυπτογραφικού υλικού σε ηλεκτρονική μορφή εκτός της χώρας απαγορευόταν, αφού οι τεχνολογίες του είδους είχαν χαρακτηριστεί «πυρομαχικά». Ωστόσο, χάρη στην εθελοντική πρωτοβουλία PGP International (εν συντομία PGPi,), το πρόγραμμα διαδόθηκε ευρέως σε ολόκληρο τον κόσμο, ήδη από το 1997. Κάθε φορά που κυκλοφορούσε στις ΗΠΑ μια νέα έκδοση του PGP, οι άνθρωποι που συμμετείχαν στην πρωτοβουλία αγόραζαν από την Αμερική βιβλία με τον πηγαίο κώδικα του προγράμματος και τα έστελναν στην Ευρώπη. Στη συνέχεια, τα βιβλία σαρώνονταν σελίδα προς σελίδα, περνούσαν από πρόγραμμα OCR, και όταν ο πηγαίος κώδικας είχε μεταφερθεί ολόκληρος στον υπολογιστή, μεταγλωττίζονταν. Σήμερα στις ΗΠΑ έχουν χαλαρώσει οι περιορισμοί εξαγωγών κρυπτογραφικού υλικού, γεγονός που μεταξύ άλλων σημαίνει ότι το PGP μπορεί πλέον να εξάγεται και σε ηλεκτρονική μορφή. Ωστόσο, το πρότζεκτ PGPi συνεχίζει να έχει τον έλεγχο της διανομής των εκδόσεων του προγράμματος στον υπόλοιπο κόσμο, μαζί με τον πηγαίο κώδικα.
Το PGP διατίθεται δωρεάν για προσωπική χρήση, όμως απαιτείται άδεια για τη χρησιμοποίησή του σε εμπορικές εφαρμογές. Το Ινστιτούτο Τεχνολογίας της Μασσαχουσέτης (MIT) λειτουργεί ως κέντρο προώθησης του λογισμικού που προορίζεται για προσωπική χρήση σε συνεργασία με τον Zimmermann ο οποίος ίδρυσε και μια ομώνυμη με το λογισμικό, εταιρία (Pretty Good Privacy, Inc.) για να προωθήσει την εμπορική έκδοση του λογισμικού.
Σκοπός του PGP ήταν η χρήση του σε συνδυασμό με το σύστημα ηλεκτρονικού ταχυδρομείου που προϋπήρχε και είναι συμβατό με σχεδόν κάθε πλατφόρμα. Η βασική ιδέα του PGP ήταν ότι είναι ανώφελο να επιχειρήσει κάποιος να εμποδίσει την εξέταση πληροφοριών που διακινούνται σε δίκτυα μέσω του ηλεκτρονικού ταχυδρομείου ή κάποιου άλλου μέσου επικοινωνίας. Έτσι, η μοναδική μορφή προστασίας είναι η εξασφάλιση ότι τα δεδομένα που παρακολουθούνται είναι ακατανόητα σε όλους τους άλλους εκτός από τους νόμιμους παραλήπτες τους. Αυτό επιτυγχάνεται με ισχυρή κρυπτογράφηση.

7.2 Συστατικά στοιχεία του PGP

Το PGP αποτελείται από τέσσερα στοιχεία κρυπτογράφησης και έναν αριθμό συστατικών μερών λογισμικού, συμβατών μεταξύ τους. Ο πυρήνας των μηχανισμών ασφάλειας είναι:

- Ο αλγόριθμος κρυπτογράφησης δεδομένων IDEA (International Data Encryption Algorithm).
- Το σύστημα κρυπτογράφησης δημοσίου κλειδιού RSA για τη διαχείριση

κλειδιών.

- Η συνάρτηση κατακερματισμού MD5.
- Μια γεννήτρια τυχαίων αριθμών.

Τα άλλα συστατικά του PGP υλοποιούν τυπικές λειτουργίες όπως, για παράδειγμα, την αλληλεπίδραση με το χρήστη, τη διαχείριση αρχείων και τη συμπίεση των δεδομένων.

7.3 Η Γεννήτρια Τυχαίων Αριθμών

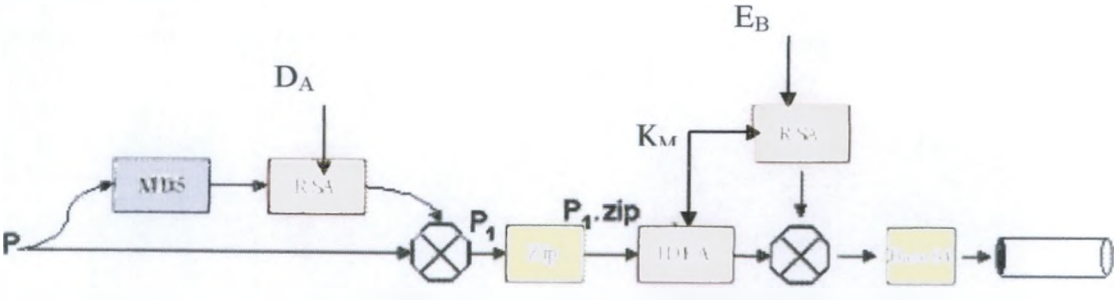
Ένα άλλο συστατικό στοιχείο του PGP είναι η γεννήτρια τυχαίων αριθμών. Χρησιμοποιείται για τη δημιουργία ενός τυχαία επιλεγμένου κλειδιού συνόδου που χρησιμοποιείται για την κρυπτογράφηση των μηνυμάτων με τον αλγόριθμο IDEA. Ακόμα και αν κάποιος εισβολέας κατορθώσει να αποκτήσει ένα τέτοιο κλειδί που χρησιμοποιήθηκε σε κάποιο μήνυμα, το κλειδί αυτό θα του φανεί χρήσιμο μόνο στην ανάγνωση του συγκεκριμένου μηνύματος, καθώς σε επόμενη επικοινωνία θα χρησιμοποιηθεί νέο κλειδί. Επιπλέον, και το δημόσιο κλειδί δημιουργείται τυχαία, ή έστω δημιουργούνται τυχαία οι πρώτοι αριθμοί από τους οποίους παράγεται.
Εξαιτίας της απαίτησης για παραγωγή κλειδιών που δε μπορούν να προβλεφθούν, η Γεννήτρια Τυχαίων Αριθμών του PGP (Random Number Generator - RNG) παρουσιάζει διαφορές συγκριτικά με τις κλασσικές «γεννήτριες». Απαιτεί περισσότερο χρόνο για την παραγωγή τυχαίου αριθμού, ο οποίος όμως είναι πολύ λιγότερο προβλέψιμος. Οι κλασικές «γεννήτριες» παράγουν συνήθως γνωστές ακολουθίες τυχαίων αριθμών και είναι εύκολο να συμπεράνει κανείς την εσωτερική κατάστασή τους εξετάζοντας μια σχετικά μικρή ακολουθία αριθμών στην έξοδο. Για να εμποδίσει επιθέσεις αυτής της μορφής, το PGP συγκεντρώνει τους χρόνους άφιξης των χαρακτήρων που πληκτρολογούνται σ' αυτό. Η απόσταση μεταξύ των χρόνων άφιξης δύο διαδοχικών χαρακτήρων έχει ένα τυχαίο παράγοντα ο οποίος δεν είναι εύκολα προβλέψιμος. Το απρόβλεπτο κομμάτι φιλτράρεται και χρησιμοποιείται για την επανατροφοδότηση της «γεννήτριας». Αυτοί οι τυχαίοι αριθμοί χρησιμοποιούνται στη συνέχεια ως κλειδιά συνόδου ή σε παρόμοιες χρήσεις.

7.4 Η Λειτουργία του PGP (Pretty Good Privacy)

Στο σχήμα 7.1 φαίνεται πώς λειτουργεί το σύστημα PGP. Θεωρούμε ότι ο χρήστης Α θέλει να στείλει ένα μήνυμα ηλεκτρονικού ταχυδρομείου, *P*, στον Β. Οι δύο χρήστες έχουν τα δικά τους ιδιωτικά (D_X) και δημόσια (E_X) κλειδιά RSA και θεωρούμε ότι ο ένας γνωρίζει το δημόσιο κλειδί του άλλου.

1. Αρχικά, το πρόγραμμα PGP στον υπολογιστή του Α περνάει το μήνυμα, *P*, από τη συνάρτηση κατακερματισμού (hash) MD5.
2. Στη συνέχεια, το hash κρυπτογραφείται με το ιδιωτικό RSA κλειδί του Α, D_A. Όταν ο Β τελικά λάβει το μήνυμα, τότε θα μπορέσει να αποκρυπτογραφήσει το hash με το δημόσιο κλειδί, E_A, και να επιβεβαιώσει ότι είναι σωστό.

3. Κατόπιν, το κρυπτογραφημένο hash και το αρχικό μήνυμα διατάσσονται σε ένα νέο μήνυμα P1 και συμπιέζονται ώστε να παραχθεί το *P1.ZIP*.
4. Στη συνέχεια, παράγεται τυχαία ένα κλειδί για τον αλγόριθμο IDEA, K_M, το οποίο ισχύει μόνο για τη συγκεκριμένη αποστολή ηλεκτρονικού ταχυδρομείου. Το κλειδί αυτό χρησιμοποιείται για τη κρυπτογράφηση του *P1.ZIP* με το IDEA.
5. Επιπλέον, το κλειδί κρυπτογραφείται με το δημόσιο κλειδί του Β.
6. Τα δύο αυτά τμήματα διατάσσονται και αποστέλλονται στο δίκτυο.
7. Όταν ο Β λάβει το μήνυμα, αποκρυπτογραφεί το κλειδί K_M χρησιμοποιώντας το ιδιωτικό του κλειδί RSA (D_B).
8. Χρησιμοποιώντας το K_M αποκρυπτογραφεί το μήνυμα που είναι κρυπτογραφημένο με τον αλγόριθμο IDEA και λαμβάνει το *P1.ZIP*.
9. Μετά την αποσυμπίεση ο Β ξεχωρίζει το hash από το καθαρό μήνυμα και το αποκρυπτογραφεί χρησιμοποιώντας το δημόσιο κλειδί του Α.
10. Αν το hash συμφωνεί με τον υπολογισμό MD5 που εκτελεί ο ίδιος, τότε γνωρίζει ότι το μήνυμα είναι αυτό που έστειλε ο Α.



Σχήμα 7.1: Λειτουργία του PGP

7.5 Χαρακτηριστικά του PGP

7.5.1 Εξακρίβωση γνησιότητας

Για την εξακρίβωση γνησιότητας (authentication) πρώτα ο αποστολέας στέλνει το μήνυμα. Στη συνέχεια ο MD5 χρησιμοποιείται για να παράγει ένα 128-bit hash code του μηνύματος. Ο κωδικός αυτός κρυπτογραφείται χρησιμοποιώντας RSA και το private key του αποστολέα και το αποτέλεσμα προσκολλάται στο μήνυμα. Ο παραλήπτης του μηνύματος χρησιμοποιεί με τη σειρά τον RSA με το public key του αποστολέα για να αποκρυπτογραφήσει και να βρει τον hash code. Τέλος, ο παραλήπτης παράγει ένα νέο hash code για το μήνυμα και το συγκρίνει με το αποκρυπτογραφημένο hash code που έχει βρει. Αν ταιριάζουν, τότε δέχεται το μήνυμα ως αυθεντικό.

Όπως βλέπουμε, ο συνδυασμός του MD5 και του RSA παρέχουν έναν αποτελεσματικό σχήμα ηλεκτρονικής υπογραφής (digital signature). Ακόμα, μπορούν να υποστηριχθούν υπογραφές που παράγονται και μεταδίδονται ξεχωριστά από το μήνυμα.

7.5.2 Εμπιστευτικότητα

Αυτή παρέχεται με την κρυπτογράφηση των μηνυμάτων προτού αποσταλούν ή αποθηκευτούν σαν αρχεία. Και στις δύο περιπτώσεις χρησιμοποιείται ο αλγόριθμος IDEA, και συγκεκριμένα η 64-bit cipher feedback (CFB) mode του IDEA με πίνακα αρχικοποίησης (initialization vector) όλο μηδενικά.
Στο PGP κάθε συμβατικό (conventional) κλειδί χρησιμοποιείται μόνο μία φορά, οπότε για κάθε μήνυμα παράγεται με τυχαίο τρόπο ένα κλειδί 128-bits. Για την προστασία του, το κλειδί αυτό, προτού μεταδοθεί, κρυπτογραφείται με βάση το public key του παραλήπτη. Η σειρά των γεγονότων έχει ως εξής: Ο αποστολέας παράγει ένα μήνυμα και ένα τυχαίο 128-bit αριθμό για να χρησιμοποιηθεί σαν session key για το μήνυμα αυτό μόνο. Στη συνέχεια το μήνυμα κρυπτογραφείται χρησιμοποιώντας το IDEA μαζί με το session key. Το session key κωδικοποιείται με RSA, χρησιμοποιώντας το public key του παραλήπτη και προσδένεται στο μήνυμα. Τέλος, ο παραλήπτης χρησιμοποιεί RSA με το δικό του private key, για να βρει το session key, το οποίο χρησιμοποιεί για να αποκρυπτογραφήσει το μήνυμα.
Για το μέγεθος του κλειδιού που θα χρησιμοποιήσει ο RSA, υπάρχουν οι δυνατότητες του Συνήθους (Casual - 384 bits), του Εμπορικού (commercial - 512 bits) και του στρατιωτικού (Military – 1024 bits) κλειδιού.

7.5.3 Εμπιστευτικότητα και Εξακρίβωση γνησιότητας

Όταν και οι δύο υπηρεσίες χρησιμοποιούνται, αρχικά, ο αποστολέας παράγει μία ηλεκτρονική υπογραφή το, με βάση το private key του, και την τοποθετεί στο τέλος του μηνύματος. Στη συνέχεια, το μήνυμα μαζί με την υπογραφή κρυπτογραφείται χρησιμοποιώντας τον IDEA και ένα session key Το session key κρυπτογραφείται χρησιμοποιώντας τον RSA και το public key του παραλήπτη.

7.5.4 Συμπίεση

Το PGP συμπιέζει από μόνο του το μήνυμα αφού τοποθετηθεί η υπογραφή και πριν κρυπτογραφηθεί. Έτσι κερδίζουμε χώρο και κατά την μετάδοση και κατά την αποθήκευση του μηνύματος. Ο αλγόριθμος που χρησιμοποιείται είναι ο ZIP.

7.5.5 Συμβατότητα ηλεκτρονικού ταχυδρομείου

Όταν χρησιμοποιείται PGP, ολόκληρο ή τουλάχιστον ένα μέρος του block που αποστέλλεται είναι κρυπτογραφημένο και αποτελείται από μία σειρά από τυχαία 8-bit octets. Λόγω του περιορισμού που υπάρχει σε ορισμένα συστήματα ηλεκτρονικού ταχυδρομείου για μόνο ASCII text μηνύματα, το PGP παρέχει μία υπηρεσία που μετατρέπει τη σειρά αυτή σε εκτυπώσιμους ASCII χαρακτήρες. Για το σκοπό αυτό χρησιμοποιείται η **radix-64 μετατροπή**, που παίρνει κάθε ομάδα τριών octets και τα μετατρέπει σε 4 χαρακτήρες ASCII, καθώς επίσης προσθέτει στο τέλος ένα CRC, για την ανίχνευση τυχόν λαθών.
Το PGP ακόμα, μπορεί να μετατρέπει σε radix-64 μορφή μόνο το μέρος όπου υπάρχει η υπογραφή, ώστε ο αποστολέας να μπορεί να διαβάζει τα μηνύματα, χωρίς να χρησιμοποιεί PGP, και μόνο αν θέλει να πιστοποιήσει την υπογραφή να χρειάζεται το PGP.

7.5.6 Τμηματοποίηση και συναρμολόγηση

Το PGP μπορεί να υποδιαιρεί ένα μήνυμα που είναι πολύ μεγάλο σε μικρότερα τμήματα, ώστε να γίνεται κατάλληλο για αποστολή και σε ορισμένες περιπτώσεις που το μέγεθος των μηνυμάτων που μπορούν να αποσταλούν είναι περιορισμένο. Η τμηματοποίηση γίνεται μετά από όλες τις άλλες επεξεργασίες.

7.6 Αλυσίδες Κλειδιών (Key Rings)

Τα δημόσια κλειδιά φυλάσσονται σε ξεχωριστά πιστοποιητικά κλειδιών (key certificates) τα οποία περιλαμβάνουν την ταυτότητα του ιδιοκτήτη τους (το όνομα του ιδιοκτήτη), μια σφραγίδα χρόνου που δείχνει πότε το ζεύγος των κλειδιών δημιουργήθηκε και τέλος το ίδιο το υλικό του κλειδιού. Τα πιστοποιητικά δημοσίων κλειδιών περιλαμβάνουν το υλικό των δημοσίων κλειδιών ενώ τα πιστοποιητικά των μυστικών κλειδιών περιλαμβάνουν το υλικό των μυστικών κλειδιών. Κάθε μυστικό κλειδί κρυπτογραφείται επιπλέον με τον κωδικό του σε περίπτωση που κλαπεί. Ένα αρχείο κλειδιών ή ένα μπρελόκ κλειδιών (key ring) περιέχει ένα ή περισσότερα από αυτά τα πιστοποιητικά κλειδιών. Τα δημόσια μπρελόκ περιέχουν τα δημόσια πιστοποιητικά κλειδιών ενώ τα ιδιωτικά μπρελόκ περιέχουν τα ιδιωτικά πιστοποιητικά κλειδιά.

Τα κλειδιά χαρακτηρίζονται από ένα "key id" (ταυτότητα κλειδιού) η οποία είναι μια συντομογραφία του δημόσιου κλειδιού (τα 64 λιγότερο σημαντικά bits του δημοσίου κλειδιού). Καθώς πολλά κλειδιά μπορεί να μοιράζονται το ίδιο user id (ταυτότητα χρήστη), για πρακτικούς λόγους κανένα κλειδί δεν μοιράζεται το ίδιο key id με κανένα άλλο.

Το PGP χρησιμοποιεί τις περιλήψεις μηνυμάτων (message digests) για να δημιουργήσει υπογραφές. Μια περίληψη μηνύματος είναι μια κρυπτογραφικά πολύ δυνατή μονόδρομη (hash) συνάρτηση 128 bit του μηνύματος. Αντίθετα βέβαια με το CRC είναι υπολογιστικά αδύνατο για κάποιον επιτιθέμενο να φτιάξει ένα υποκατάστατο μήνυμα το οποίο θα μπορούσε να παράγει την ίδια περίληψη μηνύματος. Η περίληψη μηνύματος κρυπτογραφείται με το μυστικό κλειδί και έτσι σχηματίζει την ψηφιακή υπογραφή.

Τα κείμενα υπογράφονται με την εισαγωγή στην αρχή τους ψηφιακών πιστοποιητικών υπογραφών οι οποίες περιέχουν το key id του κλειδιού που χρησιμοποιήθηκε για την υπογραφή τους, μια υπογεγραμμένη με το μυστικό κλειδί περίληψη του κειμένου και μια χρονική σφραγίδα της δημιουργίας της υπογραφής. Το key id χρησιμοποιείται από τον παραλήπτη για την ανεύρεση του δημόσιου κλειδιού του αποστολέα έτσι ώστε να ελέγξει την ψηφιακή υπογραφή. Το λογισμικό του παραλήπτη αναζητεί αυτόματα το δημόσιο κλειδί του αποστολέα και το user id του στο μπρελόκ δημοσίων κλειδιών που έχει στην κατοχή του ο παραλήπτης.

Τα κρυπτογραφημένα αρχεία περιέχουν στην αρχή τους το key id του δημοσίου κλειδιού που χρησιμοποιήθηκε στην κρυπτογράφησή τους. Ο παραλήπτης χρησιμοποιεί αυτό το key id για την ανεύρεση του μυστικού κλειδιού που απαιτείται για την αποκρυπτογράφηση του μηνύματος. Το λογισμικό του παραλήπτη αναζητεί αυτόματα το απαραίτητο μυστικό κλειδί αποκρυπτογράφησης στο μπρελόκ μυστικών κλειδιών του παραλήπτη.

Αυτοί οι δυο τύποι μπρελόκ κλειδιών είναι η κύρια μέθοδος της αποθήκευσης και διαχείρισης των δημόσιων και ιδιωτικών κλειδιών. Αντί να κρατάμε ξεχωριστά κλειδιά σε ξεχωριστά αρχεία κλειδιών τα μαζεύουμε σε μπρελόκ κλειδιών έτσι ώστε να διευκολύνουμε την αυτόματη ανεύρεσή τους είτε με τη χρήση του key id είτε με τη χρήση του user id. Κάθε χρήστης διατηρεί το δικό του ζεύγος μπρελόκ. Ένα ξεχωριστό δημόσιο κλειδί αποθηκεύεται προσωρινά σε ένα ξεχωριστό αρχείο μόνο για το χρόνο που χρειάζεται για την αποστολή του σε κάποιο φίλο ο οποίος κατόπιν θα το προσθέσει στο δικό του μπρελόκ κλειδιών.

7.7 Προστασία Δημοσίων Κλειδιών

Σε ένα κρυπτοσύστημα δημοσίων κλειδιών δεν υπάρχει ανάγκη προστασίας των δημοσίων κλειδιών, διότι το επιδιωκόμενο είναι η όσο το δυνατόν ευρύτερη διάδοσή τους. Το σημαντικό και αυτό που θα πρέπει να διασφαλίζεται είναι το να είμαστε σίγουροι ότι κάποιο δημόσιο κλειδί που φαίνεται ότι ανήκει σε κάποιον, όντως να ανήκει σε αυτόν. Αυτό μπορεί να είναι και το πιο σημαντικό μειονέκτημα του κρυπτοσυστήματος δημόσιων κλειδιών. Ας εξετάσουμε το λόγο:
Ας υποθέσουμε ότι ο Bob θέλει να στείλει ένα προσωπικό μήνυμα στην Alice. Για να το κάνει αυτό κατεβάζει το πιστοποιητικό δημοσίων κλειδιών από κάποιο σύστημα ηλεκτρονικού πίνακα ανακοινώσεων (BBS). Κατόπιν, κρυπτογραφεί το γράμμα προς την Alice με αυτό δημόσιο κλειδί και το στέλνει σε αυτήν μέσω της λειτουργίας e-mail του BBS.
Ατυχώς, τόσο για τον αποστολέα (Bob) όσο και για την Alice κάποιος τρίτος χρήστης – ας υποθέσουμε ο Charlie - έχει δημιουργήσει ένα δημόσιο κλειδί με το user id της Alice και το έχει βάλει στη θέση του πραγματικού κλειδιού της Alice. Ο Bob χρησιμοποίησε αυτό το πλαστογραφημένο κλειδί για να κρυπτογραφήσει το μήνυμα προς την Alice αντί του αληθινού κλειδιού της Alice. Όπως φαίνεται όλα δείχνουν φυσιολογικά διότι το πλαστογραφημένο κλειδί έχει το user id της Alice. Έτσι ο Charlie μπορεί να αποκρυπτογραφήσει το μήνυμα που προοριζόταν για την Alice μια και έχει το κλειδί που αντιστοιχεί στο πλαστογραφημένο δημόσιο κλειδί της Alice. Όμως το πρόβλημα δεν τελειώνει εδώ. Ο Charlie μπορεί επιπλέον να επανακρυπτογραφήσει το μήνυμα και να το προωθήσει στην Alice οπότε κανείς δεν πρόκειται να υποπτευθεί τίποτα. Εάν θέλει, μπορεί να προχωρήσει στη δημιουργία ψηφιακών υπογραφών της Alice με το πλαστογραφημένο κλειδί μια και όλοι θα το χρησιμοποιούν για να ελέγχουν τις υπογραφές της.
Όπως τελικά φαίνεται ο κίνδυνος είναι πολύ μεγάλος. Ο μόνος τρόπος να αποτραπούν τέτοιες καταστάσεις είναι η αποφυγή της υποκλοπής και του μπερδέματος των δημοσίων κλειδιών. Εάν κάποιος έχει πάρει το δημόσιο κλειδί της Alice κατευθείαν από την ίδια τότε δεν υπάρχει πρόβλημα. Αυτό βέβαια μπορεί να είναι πολύ δύσκολο εάν η Alice είναι χιλιάδες χιλιόμετρα μακριά ή απλά προσωρινά απρόσιτη.
Μία διέξοδος σε αυτό το πρόβλημα είναι η χρήση κάποιου τρίτου κοινά αποδεκτού "φίλου" ο οποίος έχει στη κατοχή του ένα καλό αντίγραφο του δημόσιου κλειδιού της Alice. Για παράδειγμα ας θεωρήσουμε ότι αυτός είναι ο David ο οποίος μπορεί να υπογράψει το δημόσιο κλειδί της Alice με τη δικό του μυστικό κλειδί και να εγγυηθεί με αυτό το τρόπο την αυθεντικότητα του κλειδιού της Alice.
Αυτή η διαδικασία θα παρήγαγε ένα υπογεγραμμένο πιστοποιητικό δημόσιου κλειδιού που θα αποδείκνυε την ακεραιότητα του κλειδιού της Alice. Αυτή η διαδικασία, βέβαια, προϋποθέτει την δυνατότητα ελέγχου του κλειδιού του David άρα την κατοχή ενός γνήσιου αντίγραφου του δημόσιου κλειδιού του. Ο David θα μπορούσε επιπλέον να στείλει στην Alice ένα υπογεγραμμένο αντίγραφο του δημόσιου κλειδιού του Bob. Με αυτό το τρόπο λειτουργεί σαν μεσάζοντας (introducer) μεταξύ του Bob και της Alice.
Το υπογεγραμμένο κλειδί για την Alice μπορεί να σταλεί από τον David ή την Alice στο BBS και από εκεί να το πάρει αργότερα όποιος το χρειαστεί. Αυτός το μόνο που θα χρειαστεί να κάνει, για να σιγουρευτεί για την ακεραιότητα του δημόσιου κλειδιού

της Alice, είναι να την ελέγξει μέσω του δημόσιου κλειδιού του David. Κανένας δεν μπορεί να ξεγελάσει πλέον όποιον έχει το υπογεγραμμένο από τον David δημόσιο κλειδί της Alice διότι κανείς δεν μπορεί να πλαστογραφήσει την υπογραφή του David.

Κάποιο άτομο που τυγχάνει ευρείας εμπιστοσύνης θα μπορούσε να εξειδικευτεί στην παροχή αυτής της υπηρεσίας, δηλαδή της παροχής υπογραφών σε πιστοποιητικά δημοσίων κλειδιών άλλων χρηστών. Αυτό το κοινά αποδεκτό άτομο θα μπορούσε να είναι κάποιος "key server" ή κάποια υπηρεσία πιστοποίησης. Κάθε πιστοποιητικό δημόσιου κλειδιού που φέρει την υπογραφή αυτού του key server θα μπορεί να θεωρείται γνήσιο και έτσι άξιο της εμπιστοσύνης κάποιου. Το μόνο που χρειάζεται να κάνουν όσοι χρήστες θα ήθελαν να συμμετέχουν σε αυτή τη διαδικασία είναι να αποκτήσουν ένα καλό αντίγραφο του δημοσίου κλειδιού του key server έτσι ώστε να είναι σε θέση να επιβεβαιώσουν την υπογραφή αυτού.

Κάποιος κεντρικός key server ή μια υπηρεσία πιστοποίησης, θα ήταν κατάλληλη για κάποια μεγάλη και απρόσωπη επιχείρηση ή κυβερνητική υπηρεσία.

Η αποκεντρωμένη έκδοση του σχήματος αυτού είναι εκείνη που επιτρέπει σε όλους τους χρήστες να δρουν σαν μεσάζοντες, ο ένας για τον άλλο, κάτι που έχει καλύτερα αποτελέσματα από έναν και μοναδικό key server. Το PGP τείνει προς αυτή τη κατεύθυνση διότι αντανακλά καλύτερα το φυσικό τρόπο με τον οποίο αλληλεπιδρούν μεταξύ τους οι άνθρωποι στις σχέσεις τους και ταυτόχρονα επιτρέπει σε αυτούς να διαλέξουν ποιόν εμπιστεύονται για τη διαχείριση των κλειδιών τους.

Αυτή η διαδικασία προστασίας των δημοσίων κλειδιών είναι το μοναδικό δύσκολο πρόβλημα στις πρακτικές εφαρμογές της κρυπτογράφησης δημοσίων κλειδιών. Θα μπορούσαμε να πούμε ότι είναι η Αχίλλειος φτέρνα της κρυπτογράφησης δημοσίων κλειδιών και έχει καταβληθεί μεγάλη προσπάθεια για την αντιμετώπισή της.

Η χρήση ενός δημόσιου κλειδιού δεν θα πρέπει να ξεκινάει εάν δεν είμαστε σίγουροι ότι πρόκειται για ένα καλό δημόσιο κλειδί το οποίο ανήκει σε αυτόν που ισχυρίζεται ότι ανήκει. Μπορούμε να είμαστε σίγουροι για την προέλευση του κλειδιού εάν έχουμε κάποιο πιστοποιητικό από τον ιδιοκτήτη του ή κάποιον άλλο που εμπιστευόμαστε, από τον οποίο όμως έχουμε ήδη ένα εγγυημένο δημόσιο κλειδί. Επιπλέον το user id θα πρέπει να έχει ολόκληρο το όνομα του ιδιοκτήτη και όχι απλά το μικρό του ή κάποιο ψευδώνυμο.

Δεν έχει σημασία πόσο σίγουροι μπορεί να αισθανόμαστε για κάποιο δημόσιο κλειδί που κατεβάσαμε από κάποιον ηλεκτρονικό πίνακα ανακοινωθέντων—ΠΟΤΕ δεν θα πρέπει να εμπιστευόμαστε οτιδήποτε δεν έχει την υπογραφή κάποιου που εμπιστευόμαστε. Ένα δημόσιο κλειδί που απλά κατεβάσαμε δίχως να το ελέγξουμε είναι πιθανόν να έχει αλλοιωθεί από κάποιον τρίτο, ακόμα και από το διαχειριστή του ηλεκτρονικού πίνακα. Εάν ποτέ μας ζητηθεί να υπογράψουμε το δημόσιο κλειδί κάποιου άλλου θα πρέπει να σιγουρευτούμε ότι αυτό πραγματικά του ανήκει. Αυτό πρέπει να γίνει διότι η υπογραφή μας στο δημόσιο κλειδί εγγυάται την αυθεντικότητά του. Εάν έχουμε κάνει λάθος, τότε όσοι μας εμπιστεύονται θα εμπιστευτούν και το κλειδί με αβέβαια αποτελέσματα. Ο κανόνας λέει ότι υπογράφουμε δημόσια κλειδιά για τα οποία έχουμε ιδία γνώση της αυθεντικότητάς τους. Για να αποκτήσουμε αυτή τη γνώση μπορούμε για παράδειγμα να μιλήσουμε στον ιδιοκτήτη του κλειδιού στο τηλέφωνο και να επιβεβαιώσουμε τα στοιχεία που έχουμε στα χέρια μας. Με το να βάλουμε την υπογραφή μας σε ένα δημόσιο κλειδί για το οποίο ήμαστε σίγουροι δεν χάνουμε την αξιοπιστία μας ακόμα και αν αυτό ανήκει σε κάποιον ψυχοπαθή. Αυτό συμβαίνει διότι με την υπογραφή μας δεν λέμε τίποτα παραπάνω από το ότι αυτό το κλειδί ανήκει σε αυτόν που ισχυρίζεται ότι ανήκει—το ότι κάποιος μπορεί να

εμπιστευθεί το κλειδί δεν έχει καμία σχέση με το αν μπορεί να εμπιστευθεί ή όχι τον ιδιοκτήτη του.
Η εμπιστοσύνη δεν είναι αναγκαστικά κάτι μεταβιβάσιμο. Για παράδειγμα μπορεί έχουμε κάποιον φίλο που εμπιστευόμαστε και ξέρουμε ότι δεν λέει ψέματα. Αυτός μπορεί να εμπιστεύεται τον πρόεδρο της κυβέρνησης. Όπως είναι αυτονόητο αυτό δεν σημαίνει ότι και εμείς εμπιστευόμαστε τον πρόεδρο της κυβέρνησης – κοινή λογική. Ανάλογα εάν εμπιστευόμαστε την υπογραφή της Alice σε ένα δημόσιο κλειδί και η Alice με τη σειρά της εμπιστεύεται την υπογραφή του Charlie σε κάποιο άλλο κλειδί, αυτό δεν σημαίνει ότι και εμείς εμπιστευόμαστε την υπογραφή του Charlie σε εκείνο το κλειδί.
Θα ήταν καλή ιδέα, οι χρήστες να κρατούσαν το δημόσιο κλειδί τους μαζί με ένα σύνολο από πιστοποιητικά για αυτό από διαφόρους μεσάζοντες με την ελπίδα ότι οι περισσότεροι χρήστες εμπιστεύονται κάποιον από αυτούς. Μπορεί λοιπόν, κάποιος χρήστης να ανακοινώσει το δημόσιο κλειδί του μαζί με τη συλλογή των πιστοποιητικών που διαθέτει για αυτό. Όταν υπογράφουμε το δημόσιο κλειδί κάποιου πρέπει να του το επιστρέφουμε μαζί με την υπογραφή μας ώστε να την προσθέσουνε στη συλλογή πιστοποιητικών για το δημόσιο κλειδί τους.
Το PGP κρατάει στοιχεία για το ποια από τα δημόσια κλειδιά που έχουμε στην κατοχή μας είναι πιστοποιημένα με υπογραφές που εμπιστευόμαστε. Το μόνο που εμείς πρέπει να κάνουμε είναι να πούμε στο PGP ποιους εμπιστευόμαστε σαν μεσάζοντες και να πιστοποιήσουμε τα κλειδιά τους με το δικό μας. Το PGP αναλαμβάνει από εκεί και πέρα να κρίνει αυτόματα κάποιο δημόσιο κλειδί ως έγκυρο ή όχι.
Πρέπει να διασφαλίσουμε ότι κανένας δεν πρόκειται να αλλοιώσει το μπρελόκ με τα κλειδιά μας. Ο έλεγχος ενός νέου υπογεγραμμένου δημοσίου κλειδιού πρέπει να εξαρτάται ολοκληρωτικά από την ακεραιότητα των κλειδιών τα οποία ήδη έχουμε στο μπρελόκ μας και τα οποία φυσικά εμπιστευόμαστε. Πρέπει να διατηρούμε συνεχή φυσικό έλεγχο των μπρελόκ δημοσίων κλειδιών μας σε κάποιο PC εκτός δικτύου όπως ακριβώς θα κάναμε και με το μυστικό κλειδί μας. Επιπλέον πρέπει να κρατάμε ένα αντίγραφο του δημόσιου και μυστικού κλειδιού μας σε κάποιο προστατευμένο μέσο όπου αποκλείεται ποτέ να τα σβήσουμε κατά λάθος. Από τη στιγμή κατά την οποία το δημόσιο κλειδί μας χρησιμοποιείται ως ο τελικός κριτής για τη πιστοποίηση ή μη όλων των άλλων κλειδιών του μπρελόκ είναι σημαντική για την ασφάλεια όλου του συστήματος η διασφάλισή του. Το PGP μπορεί αυτόματα να συγκρίνει το δημόσιο κλειδί μας με ένα αντίγραφό του σε κάποιο προστατευμένο φυσικό μέσο.
Το PGP γενικά θεωρεί ότι διατηρούμε το σύστημά μας, τα μπρελόκ και το PGP ασφαλές σε φυσικό επίπεδο. Εάν κάποιος έχει πρόσβαση στο σκληρό δίσκο του συστήματός μας τότε θεωρητικά μπορεί να αλλοιώσει το ίδιο το PGP έτσι ώστε αυτό να αδυνατεί να ανιχνεύσει οποιαδήποτε αλλοίωση σε άλλα κλειδιά.
Ένας ακόμα τρόπος να προστατεύσουμε ολόκληρο το μπρελόκ με τα κλειδιά μας είναι να το υπογράψουμε ολόκληρο με το μυστικό μας κλειδί. Βέβαια θα έπρεπε πάλι να έχουμε κάπου αλλού προστατευμένο ένα αντίγραφο του δημοσίου κλειδιού μας για να είμαστε σε θέση να ελέγξουμε την υπογραφή μας. Όπως είναι φυσικό δεν μπορούμε να βασιστούμε στο δημόσιο κλειδί μας, που βρίσκεται στο μπρελόκ, για τον έλεγχο της υπογραφής μας διότι αυτό είναι μέρος αυτού που πάμε να προστατέψουμε.

7.8 Διαδικασία Αναγνώρισης Έγκυρων Κλειδιών

Το PGP παρακολουθεί ποια από τα κλειδιά που υπάρχουν στο μπρελόκ δημοσίων κλειδιών είναι πιστοποιημένα και ποια όχι με υπογραφές χρηστών που εμπιστευόμαστε. Το μόνο που πρέπει να κάνουμε είναι να "πούμε" στο PGP ποιους χρήστες εμπιστευόμαστε σαν μεσάζοντες και να πιστοποιήσουμε τα κλειδιά τους με το δικό μας κλειδί. Το PGP αναλαμβάνει να κινήσει αυτόματα διαδικασίες ελέγχου της εγκυρότητας κλειδιών που είναι υπογεγραμμένα από τους μεσάζοντες που εμείς ορίσαμε. Υπάρχει βέβαια πάντα η δυνατότητα να υπογράψουμε κλειδιά και εμείς οι ίδιοι.
Υπάρχουν δύο διαφορετικά κριτήρια βάση των οποίων το PGP κρίνει τη χρησιμότητα των κλειδιών και τα οποία δεν πρέπει να συγχέουμε:
Το κλειδί ανήκει σε αυτόν που ισχυρίζεται ότι ανήκει; (έχει πιστοποιηθεί από κάποιον του οποίου την υπογραφή εμπιστευόμαστε;)
Ανήκει σε κάποιον που μπορούμε να εμπιστευθούμε για την πιστοποίηση άλλων κλειδιών;
Το PGP μπορεί να υπολογίσει την απάντηση στην πρώτη ερώτηση. Η απάντηση στη δεύτερη πρέπει να δοθεί αποκλειστικά από το χρήστη. Όταν ο χρήστης δώσει την απάντηση στην δεύτερη ερώτηση τότε το PGP μπορεί να υπολογίσει την απάντηση στην πρώτη ερώτηση για άλλα κλειδιά τα οποία υπογράφονται από αυτόν που έχουμε ορίσει σαν έμπιστο. Κλειδιά τα οποία έχουν πιστοποιηθεί από κάποιον που έχουμε ορίσει ως έμπιστο θεωρούνται έγκυρα από το PGP. Τα κλειδιά που ανήκουν σε έμπιστους μεσάζοντες πρέπει να πιστοποιηθούν είτε από εμάς τους ίδιους είτε από κάποιον άλλο που έχουμε ορίσει ως έμπιστο.
Το PGP δίνει επιπλέον τη δυνατότητα ορισμού διαφορετικών επιπέδων εμπιστοσύνης για διαφορετικούς μεσάζοντες. Το ότι εμπιστευόμαστε κάποιον να δράσει ως μεσάζοντας δεν σημαίνει μόνο ότι τον εμπιστευόμαστε αλλά επιπλέον ότι τον θεωρούμε αρκετά ικανό να διαχειριστεί κλειδιά επιλέγοντας ποια από αυτά πρέπει και ποια όχι να υπογράψει. Μπορεί να ορίσουμε έναν χρήστη - μεσάζοντα στο PGP σαν άγνωστο, μη έμπιστο, μερικώς έμπιστο και εντελώς έμπιστο για να πιστοποιεί δημόσια κλειδιά. Αυτή η πληροφορία, που αφορά το βαθμό εμπιστοσύνης κάποιου μεσάζοντα, περιέχεται στο μπρελόκ των κλειδιών μαζί με το αντίστοιχο κλειδί (του μεσάζοντα) και δεν αντιγράφεται σε καμία περίπτωση κατά την αντιγραφή κάποιου κλειδιού του μπρελόκ. Αυτό συμβαίνει διότι θεωρείται εμπιστευτική πληροφορία μια και αντικατοπτρίζει την άποψη του κατόχου του για τους μεσάζοντες - απόλυτα προσωπικό στοιχείο.
Όταν το PGP ελέγχει την εγκυρότητα ενός κλειδιού αυτό που κάνει είναι να ελέγχει τον βαθμό εμπιστοσύνης όλων των συνημμένων υπογραφών πιστοποίησής του. Κατόπιν υπολογίζει ένα μέσο επίπεδο εμπιστοσύνης - για παράδειγμα δύο μερικώς έμπιστες υπογραφές ισοδυναμούν με μία πλήρως έμπιστη. Το σκεπτικό λειτουργίας του PGP προσαρμόζεται στις απαιτήσεις του χρήστη και ρυθμίζεται αναλόγως (για παράδειγμα μπορούμε να ρυθμίσουμε το PGP να θεωρεί ένα κλειδί έγκυρο μόνο εάν αυτό φέρει δύο πλήρως έμπιστες υπογραφές ή τρεις μερικώς έμπιστες).
Το δικό μας κλειδί θεωρείται έγκυρο από το PGP αξιωματικά και για αυτό το λόγο δεν χρειάζεται την πιστοποίηση από κανέναν. Το PGP γνωρίζει ποια δημόσια κλειδιά είναι δικά μας κοιτάζοντας να βρει τα αντίστοιχα μυστικά κλειδιά στο μπρελόκ τους.
Το PGP θεωρεί επιπλέον ότι εμπιστευόμαστε τους εαυτούς μας για να πιστοποιούν άλλα κλειδιά.

Όσο θα περνάει ο καιρός θα λαμβάνουμε όλο και περισσότερα κλειδιά από χρήστες που ίσως να θέλουμε να ορίσουμε ως μεσάζοντες. Κάθε ένας από αυτούς θα έχει τους δικούς του μεσάζοντες των οποίων τα πιστοποιητικά - υπογραφές θα μοιράζει μαζί με το κλειδί του με την ελπίδα ότι όποιος τα λάβει να εμπιστεύεται κάποιο από όλα. Έτσι δημιουργείται ένα αποκεντρωμένο δίκτυο εμπιστοσύνης για όλα τα δημόσια κλειδιά.
Αυτή η μοναδική προσέγγιση έρχεται σε αντίθεση με τα κατεστημένα κυβερνητικά σχήματα διαχείρισης κλειδιών, όπως το PEM (Internet Privacy Enhanced Mail), τα οποία βασίζονται σε συστήματα κεντρικού ελέγχου και υποχρεωτικής εμπιστοσύνης σε αυτά. Τα σχήματα αυτά απαρτίζονται από ιεραρχικές οντότητες που υπαγορεύουν ποιόν πρέπει να εμπιστευόμαστε. Αυτό είναι φανερό ότι έρχεται σε πλήρη αντίθεση με τη σχεδιαστική αρχή του PGP η οποία επιτρέπει στον καθένα και ανεξάρτητα από οποιονδήποτε και οτιδήποτε άλλο να καθορίσει ο ίδιος την πολιτική που θέλει να ακολουθήσει στη διαχείριση των κλειδιών του. Έτσι το PGP βάζει το χρήστη και όχι το σύστημα στην κορυφή της προσωπικής του πυραμίδας πιστοποίησης.

7.9 Προστασία του Μυστικού Κλειδιού

Η προστασία του μυστικού κλειδιού και της φράσης-κλειδί του, είναι κάτι το αυτονόητο στο οποίο πρέπει να δοθεί μεγάλη προσοχή. Εάν ποτέ το μυστικό κλειδί πέσει σε λάθος χέρια – τα οποία είναι οποιαδήποτε άλλα εκτός των δικών μας—τότε θα πρέπει άμεσα, τόσο για τη δική μας ασφάλεια όσο και των άλλων, να ειδοποιήσουμε τους πάντες για το γεγονός προτού κάποιος αρχίσει να υπογράφει με το "όνομά" μας. Θα μπορούσε, για παράδειγμα, να υπογράψει ένα σύνολο από δημόσια κλειδιά δημιουργώντας έτσι πρόβλημα σε πολλούς χρήστες ειδικά εάν η υπογραφή μας τυγχάνει ευρείας εμπιστοσύνης και αποδοχής. Φυσικά, κίνδυνο διατρέχουμε και από το γεγονός της έκθεσης όλων των μηνυμάτων μας στα μάτια αυτού που έχει το προσωπικό μας κλειδί.
Η προστασία του μυστικού κλειδιού πρέπει να αρχίζει με τη φυσική του διασφάλιση. Μπορούμε να το κρατάμε σε κάποιο PC στο σπίτι ή κάποιο φορητό υπολογιστή μια και αυτά τα έχουμε υπό την επίβλεψή μας συνεχώς. Εάν ποτέ υπάρξει ανάγκη χρησιμοποίησης υπολογιστή στο γραφείο ή οπουδήποτε αλλού τότε θα πρέπει να μεταφέρουμε το μυστικό κλειδί μας σε αυτόν μέσο κάποιας δισκέτας ενδεχομένως και για όσο χρειάζεται ενώ όταν τελειώσουμε τη δουλεία μας δεν πρέπει να αφήσουμε πίσω οτιδήποτε μπορεί να οδηγήσει στην αποκάλυψη του. Δεν είναι επίσης σωστό να αφήνουμε το μυστικό κλειδί μας σε κάποιο απομακρυσμένο μηχάνημα (ένας Unix dial-in server) διότι μπορεί κάποιος που παρακολουθεί τις επικοινωνίες μέσω modem να υποκλέψει τη μυστική φράση (pass phrase) και να αποκτήσει το μυστικό από το απομακρυσμένο σύστημα. Συμπερασματικά λέμε ότι θα πρέπει να γίνεται χρήση του μυστικού κλειδιού μόνο σε συστήματα στα οποία έχουμε φυσικό έλεγχο.
Επιπρόσθετα, πρέπει να προσέξουμε πού αποθηκεύουμε τη μυστική φράση-κλειδί. Δεν πρέπει ποτέ αυτή να βρίσκεται στον ίδιο υπολογιστή με αυτόν που έχει το αρχείο του μυστικού κλειδιού μας. Η αποθήκευση τόσο του μυστικού κλειδιού όσο και της μυστικής φράσης στον ίδιο υπολογιστή είναι το ίδιο επικίνδυνη με την φύλαξη του PIN ενός τραπεζικού ATM λογαριασμού στο ίδιο πορτοφόλι με την κάρτα ATM. Ένα πράγμα είναι σίγουρο - δεν θέλουμε σε καμία περίπτωση αυτός που θα έχει στα χέρια του τον σκληρό δίσκο με το μυστικό μας κλειδί να έχει στη διάθεσή του και τη

μυστική φράση. Το ιδανικό θα ήταν να απομνημονεύαμε τη μυστική φράση και να μην την φυλάγαμε σε κανένα άλλο μηχάνημα εκτός του εγκεφάλου μας. Εάν, ωστόσο, νιώθουμε ότι πρέπει να τη γράψουμε κάπου θα πρέπει να την ασφαλίσουμε καλύτερα ίσως και από το ίδιο το μυστικό μας κλειδί.
Κάτι άλλο επίσης σημαντικό, που πρέπει να κάνουμε, είναι να παίρνουμε backup του μυστικού μπρελόκ μας διότι μόνο εμείς έχουμε το μοναδικό αντίγραφο αυτού και πιθανή απώλειά του θα ισοδυναμούσε με αχρήστευση όλων των δημοσίων κλειδιών που διανείμαμε στον κόσμο.
Το αποκεντρωτικό σχήμα φιλοσοφίας αλλά και λειτουργίας που έχει επιλέξει να χρησιμοποιήσει το PGP εκτός από τα πλεονεκτήματα στη διαχείριση των κλειδιών έχει και τα μειονεκτήματα του. Δεν υπάρχει μία κεντρική λίστα που να περιέχει τα μη έγκυρα κλειδιά κάνοντας πιο δύσκολη την γνώση τους. Έτσι αν κάτι πάει στραβά η διαδικασία γνωστοποίησής του είναι επίπονη. Εάν τελικά το μυστικό κλειδί και η μυστική φράση πέσουν στα χέρια άλλων θα πρέπει να φτιάξουμε και να διανείμουμε ένα "πιστοποιητικό απολεσθέντος κλειδιού" (key compromise certificate). Αυτός ο τύπος πιστοποιητικού χρησιμοποιείται για να προειδοποιεί άλλους χρήστες να σταματήσουν να χρησιμοποιούν το αντίστοιχο δημόσιο κλειδί μας. Μπορούμε να χρησιμοποιήσουμε το PGP στη δημιουργία αυτού του πιστοποιητικού και κατόπιν να το στείλουμε σε όλους τους φίλους και συνεργάτες μας σε όλο τον κόσμο. Η έκδοση του PGP που τρέχει σε αυτούς θα αναλάβει να εγκαταστήσει το πιστοποιητικό του απολεσθέντος κλειδιού στα δημόσια μπρελόκ τους και από εκείνη τη στιγμή θα αποτρέπεται αυτόματα η επαναχρησιμοποίησή τους. Μπορούμε κατόπιν να δημιουργήσουμε ένα νέο ζεύγος μυστικού/δημοσίου κλειδιού και να αρχίσουμε πλέον να δουλεύουμε με αυτά.

7.10 Δουλεύοντας με το PGP

Μετά την απλούστατη διαδικασία εγκατάστασης του προγράμματος (αρχείο «PGP v6.58-Win32.Zip»), μπορούμε αμέσως να αρχίσουμε να το χρησιμοποιούμε. Ακολουθώντας τη διαδρομή <Start * Programs *PGP *PGPtools>, θα δούμε μια μικρή μπάρα εργαλείων, η οποία μας δίνει πρόσβαση σε διάφορες επιμέρους λειτουργίες της εφαρμογής. Το πρώτο που πρέπει να κάνουμε είναι να δημιουργήσουμε ένα ζεύγος ιδιωτικού - δημόσιου κλειδιού, εκτός και αν ήδη διαθέτουμε ένα. Στην πρώτη περίπτωση δεν έχουμε παρά να κάνουμε ένα κλικ στο κουμπάκι «PGPkeys» της μπάρας και να ακολουθήσουμε τις προτροπές του οδηγού «Key Generation Wizard». Στις περισσότερες των περιπτώσεων, οι εξ' ορισμού επιλογές μπορούν να μείνουν ως έχουν. Ιδιαίτερη προσοχή χρειάζεται στο σημείο όπου δίνουμε τη συνθηματική φράση (Pass-phrase), η οποία θα μας δίνει πρόσβαση στο ιδιωτικό κλειδί. Συνιστάται να είναι «καλή», υπό την έννοια ότι θα πρέπει να περιέχει χαρακτήρες, ψηφία και σύμβολα, να μη βασίζεται σε κανονικές λέξεις κ.λπ. Στο δικτυακό τόπο [illegible] υπάρχει μια μηχανή αυτόματης παραγωγής συνθηματικών φράσεων, βάσει ορισμένων παραμέτρων που καθορίζουμε εμείς οι ίδιοι. Στη συνέχεια έχουμε να επιλέξουμε αν θα στείλουμε το δημόσιο κλειδί μας σε κάποιο διακομιστή κλειδιών, ώστε άλλοι χρήστες να μπορούν εύκολα να το παίρνουν και να μας στέλνουν κρυπτογραφημένα δεδομένα. Εναλλακτικά, για να διανέμουμε το κλειδί στα άτομα που μας ενδιαφέρουν άμεσα, μπορούμε, απλά, να το επισυνάπτουμε στα e-mail που τους στέλνουμε. Πάντως, ακόμα και αν δεν στείλουμε

άμεσα το δημόσιο κλειδί μας σε κάποιο διακομιστή, μπορούμε να το κάνουμε αργότερα.
Αφού δημιουργήσουμε το ζεύγος κλειδιών, μια καλή ιδέα είναι να εξαγάγουμε (export) το δημόσιο κλειδί μας σε ένα αρχείο κειμένου, ώστε να μπορούμε να το διανέμουμε εύκολα. Αρκεί να επιλέξουμε το χρήστη που μας ενδιαφέρει εν προκειμένω τον εαυτό μας, να κάνουμε δεξί κλικ πάνω του και να πάμε στο [Export...]. Την πρώτη φορά που θα κλείσουμε το παράθυρο «PGPkeys», το πρόγραμμα θα μας προτρέψει να αποθηκεύσουμε το ζεύγος κλειδιών που μόλις δημιουργήσαμε σε ένα ασφαλές μέρος: αν έπειτα από «χτύπημα» του δίσκου χάσουμε το ζεύγος κλειδιών, τότε τα δεδομένα που έχουμε σε κρυπτογραφημένη μορφή θα μας είναι παντελώς άχρηστα. Κατά τη διαδικασία εξαγωγής, θα παρατηρήσουμε να γίνεται λόγος για δύο δακτυλίους κλειδιών (key ring): τον ιδιωτικό και το δημόσιο. Στον ιδιωτικό κρατούνται όλα τα ιδιωτικά κλειδιά που έχουμε στην κατοχή μας, ενώ στο δημόσιο όλα τα δημόσια (ανήκουν σε άλλους χρήστες). Σε πολλές περιπτώσεις έχει νόημα να διαθέτουμε περισσότερα από ένα ζεύγη κλειδιών. Το ένα θα το χρησιμοποιούμε, π.χ., για την προσωπική μας αλληλογραφία και το άλλο για την επαγγελματική, όπου κατά πάσα πιθανότητα τα χρησιμοποιούμενα κλειδιά θα έχουν μεγαλύτερο μήκος (σε bit), επομένως είναι και δυσκολότερο να παραβιαστούν. Εξάλλου, για να εισαγάγουμε ένα δημόσιο κλειδί κάποιου άλλου χρήστη στο δημόσιο δακτύλιο, ανοίγουμε το παράθυρο «PGPkeys» και επιλέγουμε <Keys *Import...> ή πατάμε [CTRL+M].
Η κρυπτογράφηση ενός αρχείου είναι θέμα ενός μόνο κλικ, στο αντίστοιχο εικονίδιο της μπάρας εργαλείων. Αφού επιλέξουμε το αρχείο που μας ενδιαφέρει από το παράθυρο που θα εμφανιστεί, προσθέτουμε στη λίστα «Recipients» τους χρήστες στους οποίους απευθύνεται: είναι εκείνοι που θα μπορέσουν να το αποκρυπτογραφήσουν. Βεβαίως, εννοείται ότι διαθέτουμε ήδη τα δημόσια κλειδιά τους (ειδάλλως δεν θα περιλαμβάνονταν στην πάνω λίστα του υπό συζήτηση παραθύρου). Εάν θέλουμε να είμαστε σε θέση να το αποκρυπτογραφήσουμε και εμείς, τότε στη λίστα αυτή θα πρέπει να προσθέσουμε και τον εαυτό μας. Το κρυπτογραφημένο αρχείο θα έχει την κατάληξη «.pgp». Εάν αργότερα θελήσουμε να το αποκρυπτογραφήσουμε με την προϋπόθεση ότι κρυπτογραφήθηκε και ως προς το δικό μας δημόσιο κλειδί, κάνουμε διπλό κλικ επάνω του, διαλέγουμε το χρήστη που αντιστοιχεί στον εαυτό μας και δίνουμε τη συνθηματική φράση.
Τα υπόλοιπα εικονίδια της μπάρας PGPtools μάς επιτρέπουν να υπογράφουμε ή και να κρυπτογραφούμε, να αποκρυπτογραφούμε, καθώς και να διαγράφουμε ένα αρχείο από το δίσκο. Η τελευταία λειτουργία γίνεται πολύ περισσότερο «επιμελώς» μέσω PGP, σε σύγκριση με το λειτουργικό σύστημα. Παρόμοια είναι και η λειτουργία της «τακτοποίησης» του ελεύθερου χώρου του δίσκου (Freespace Wipe: μετά το πέρας της λειτουργίας, όλα τα «ίχνη» των αρχείων έχουν εξαφανιστεί δια παντός).
Ολοκληρώνοντας την εισαγωγή μας στο PGP, να πούμε ότι το πρόγραμμα έρχεται με κατάλληλο plug-in για να συνεργάζεται με το Outlook. Έτσι, αφού συντάξουμε ένα e-mail και επισυνάψουμε τυχόν αρχεία, έχουμε την επιλογή να κρυπτογραφήσουμε ή και να υπογράψουμε το μήνυμά μας. Βεβαίως, θα πρέπει να διαθέτουμε το δημόσιο κλειδί του παραλήπτη. Όμοια και για τα κρυπτογραφημένα e-mail που λαμβάνουμε: μπορούμε να τα «ανοίγουμε» κατευθείαν μέσα από το Outlook.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Δικτυακοί τόποι

www.cisco.com
www.netscape.com
www.first.org
www.cert.org
www.ciac.org/ciac/
www.ietf.org
www.w3.org/security
www.rsasecurity.com
www.redbooks.ibm.com
www.visa.com
www.verisign.com
www.globalsign.com
www.openssl.org
www.ssl.com
www.homeport.org/~adam/ssl.html
www.homeport.org/~adam/shttp.html
www.hsc.fr
www.ssh.fi
http://web.mit.edu:80/kerberos/www/
www.pgpi.org
www.cam.ac.uk.pgp.net/pgpnet

Βιβλία

1. Andrew S. Tanenbaum , Computer Networks, Prentice Hall,1996
2. William Stallings, Cryptography and Network Security, Prentice Hall,1999
3. William Stallings, Data and Computer Communications, Prentice Hall,1997
4. Douglas E. Comer, Δίκτυα και διαδίκτυα υπολογιστών, Εκδόσεις Κλειδάριθμος
5. Σ. Κάτσικας, Ασφάλεια Δικτύων, Ελληνικό Ανοικτό Πανεπιστήμιο, 2000
6. Σ. Κάτσικας, Προστασία Δεδομένων, Ελληνικό Ανοικτό Πανεπιστήμιο, 2000
7. Β. Ζορκάδης, Κρυπτογραφία, Ελληνικό Ανοικτό Πανεπιστήμιο, 2002
8. Σ. Γκρίζαλης, Σ. Κάτσικας, Δ. Γκριζαλης, Ασφάλεια Δικτύων Υπολογιστών, Εκδόσεις Παπασωτηρίου, Αθήνα 2003
9. Γ. Πάγκαλος, Ι. Μαυρίδης, Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων, Εκδόσεις Ανίκουλα
10. Ν. Αλεξανδρής, Ε. Κιουντούζης, Β. Τραπεζάνογλου, Ασάλεια Πληροφοριών, Εκδόσεις Νέων Τεχνολογιών, Αθήνα 1995
11. Γ. Δουκίδης, Μ. Θεμιστοκλέους, Β. Δράκος, Ν. Παπαζαφειροπούλου, Ηλεκτρονικό Εμπόριο, Οικονομικό Πανεπιστήμιο Αθηνών