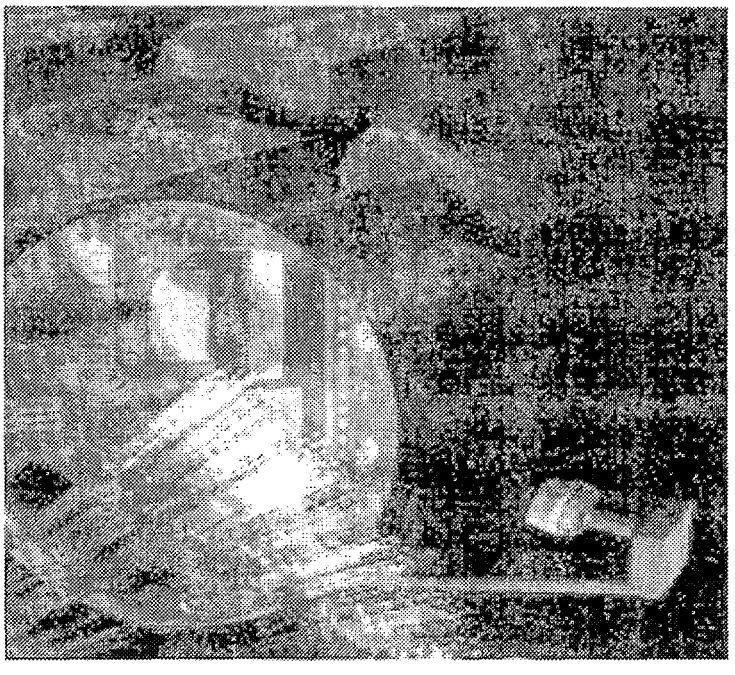
ΕΦΑΡΜΟΓΗ ΣΥΓΧΡΟΝΩΝ ΤΕΧΝΙΚΩΝ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ ΣΕ ΣΗΜΑΤΑ ΜΙΑΣ Η ΠΕΡΙΣΣΟΤΕΡΩΝ ΔΙΑΣΤΑΣΕΩΝ: ΠΑΡΟΥΣΙΑΣΗ ΤΕΧΝΙΚΩΝ ΚΑΙ ΥΛΟΠΟΙΗΣΕΩΝ.

Επιμέλεια:
Ασκητόπουλος Σ. Κωνσταντίνος

Εισηγητής:
Δρ. Καραγιάννης Γεώργιος

ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ
ΜΕΣΟΛΟΓΓΙΟΥ

ΕΦΑΡΜΟΓΗ ΣΥΓΧΡΟΝΩΝ ΤΕΧΝΙΚΩΝ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ ΣΕ ΣΗΜΑΤΑ ΜΙΑΣ Η ΠΕΡΙΣΣΟΤΕΡΩΝ ΔΙΑΣΤΑΣΕΩΝ: ΠΑΡΟΥΣΙΑΣΗ ΤΕΧΝΙΚΩΝ ΚΑΙ ΥΛΟΠΟΙΗΣΕΩΝ.



Επιμέλεια:
Ασκητόπουλος Σ. Κωνσταντίνος

Εισηγητής:
Δρ. Καραγιάννης Γεώργιος

Περιεχόμενα

Πρόλογος

Κάθε λίγα χρόνια, στο άμεσο μέλλον, η ασφάλεια των υπολογιστών θα πρέπει να αναδιαμορφώνεται και να οριοθετεί τις νέες απαιτήσεις. Οι εξελισσόμενες τεχνολογίες και εφαρμογές φέρνουν νέες απειλές, αναγκάζοντας τους αναλυτές να ανακαλύπτουν νέους μηχανισμούς προστασίας. Οι επιδημίες ιών άρχισαν να εμφανίζονται όταν ένας μεγάλος αριθμός χρηστών επιδόθηκε στην ανταλλαγή προγραμμάτων. Όταν πια το Διαδίκτυο «απογειώθηκε», η τεχνολογία των Πυλών Προστασίας (firewalls) ήταν μια αρχική προσέγγιση για την επιθυμητή ασφάλεια των ψηφιακών πόρων και δεδομένων. Η κρυπτογράφηση έγινε σημαντική όταν οι επιχειρήσεις άρχισαν να χτίζουν, να οικοδομούν δίκτυα υπολογιστικών συστημάτων.

Η κρυπτογράφηση βρίσκει σήμερα εφαρμογή σε πολλές δραστηριότητες. Η αναπτυσσόμενη τεχνολογία της είναι βασικό συστατικό για την βιωσιμότητα πολλών επιχειρήσεων, ενώ ο ρόλος που θα διαμορφώσει στο μέλλον είναι κάτι παραπάνω από σίγουρο πως θα επαναπροσδιορίσει απόψεις και πρότυπα.

Η ιδιαιτερότητα μου για ενασχόληση με νέους, εξελίξιμους τομείς, με ευρύτερα όρια εφαρμογής, με ώθησε στην αναζήτηση και την επιλογή καταγραφής των σύγχρονων μεθόδων της τεχνολογίας της κρυπτογράφησης. Με την ολοκλήρωση αυτής της διπλωματικής εργασίας, αφενός υιοθέτησα γνώσεις για το αντικείμενο της και αφετέρου διαμόρφωσα νέους στόχους και πεποιθήσεις.

Κωνσταντίνος Ασκητόπουλος Σεπτέμβριος 2004

"Τα «προϊόντα» της Κρυπτογράφησης μπορεί να χαρακτηριστούν από κάποιους παράνομα, αλλά οι πληροφορίες ποτέ".

Bruce Shneier.

«Αφιερωμένο στον πατέρα μου ως ελάχιστη ανταμοιβή,
για όλα αυτά που μου πρόσφερε».

1. Το σύστημα της Κρυπτογραφίας

1.1 Ορισμοί και εισαγωγικά στοιχεία

Η τεχνολογία και τα επιτεύγματα της δεν αποτελούν πλέον ένα συμπλήρωμα ή απλά μια πλευρά του σύγχρονου κόσμου. Έχουν προσαρτηθεί στην ταυτότητα του σύγχρονου ανθρώπου και επηρεάζουν, ταυτόχρονα, μέσα από την γνώση αλλά και την λογική που ενσωματώνουν, την συμπεριφορά και τις αποφάσεις μας. Η ανάγκη για την διασφάλιση των πληροφοριών, που προσφέρουν αυτή την γνώση, είναι πλέον διάχυτη. Ως αποτέλεσμα, έχει αναπτυχθεί ένας αξιοθαύμαστος μηχανισμός με τεχνικές ασφάλειας των πληροφοριών, αλλά και των συστημάτων τους. Ως τεχνική ασφάλειας μπορεί να χαρακτηριστεί ένα **Σύστημα Κρυπτογράφησης**. Το περιεχόμενο και ο στόχος αυτού του συγγράμματος είναι να δώσει μια αναλυτικότερη και σαφέστερη εικόνα των σύγχρονων τεχνικών κρυπτογράφησης και να κάνει πιο κατανοητό τον τρόπο εφαρμογής τους.

Προσπαθώντας να δώσουμε την έννοια της **Κρυπτογράφησης** (encryption), μπορούμε να την ορίσουμε ως την διεργασία αυτή του μετασχηματισμού ενός μηνύματος σε μια ακατανόητη μορφή, με την χρήση ενός κρυπτογραφικού αλγόριθμου, έτσι ώστε αυτό να μην είναι αναγνώσιμο από τρίτα μη εξουσιοδοτημένα μέρη, εκτός του παραλήπτη .

Κατά αυτό τον τρόπο, **Αποκρυπτογράφηση** (decryption) είναι η διεργασία ανάκτησης του αρχικού μηνύματος σε αναγνώσιμη μορφή, από μία έκδοση που έχει παραχθεί από μια διαδικασία κρυπτογράφησης. Η αποκρυπτογράφηση εκτελείται από κάποια εξουσιοδοτημένη οντότητα, αντίθετα με την κρυπτανάλυση. Η προσπάθεια να «σπάσει» μια κρυπτογραφική τεχνική ονομάζεται **Κρυπτανάλυση**, με κύριο χαρακτηριστικό την αναίρεση της ασφαλής μετάδοσης πληροφοριών.

Αρχικό κείμενο (plaintext) είναι το μήνυμα που αποτελεί την είσοδο σε μια διεργασία κρυπτογράφησης. Με αλλά λόγια είναι όλα τα δεδομένα αυτά που κρυπτογραφούνται . Ως plaintext μπορεί να θεωρηθεί κάποια επιστολή, κείμενο ή γράμμα που διακινείται μέσω του ηλεκτρονικού ταχυδρομείου, αλλά και οποιοδήποτε αρχείο δεδομένων μιας επιχείρησης σε ψηφιακή μορφή που τρέφει ασφάλειας. Όσον αφορά έναν υπολογιστή, το plaintext μπορεί να είναι απλά μια σειρά από δυαδικά στοιχεία.

Κρυπτογραφημένο κείμενο (chipertext) είναι το αποτέλεσμα της εφαρμογής μιας κρυπτογραφικής τεχνικής ή ενός αλγόριθμου πάνω στο αρχικό κείμενο. Το chipertext μπορεί να έχει το ίδιο μέγεθος ή να είναι μεγαλύτερο από το plaintext.

Θεωρείται ως το προσδοκούμενο αποτέλεσμα της κρυπτογράφησης και είναι αυτό που θα λάβει ο παραλήπτης, πριν βεβαίως χρησιμοποιήσει πάνω σε αυτό την διαδικασία αποκρυπτογράφησης. Η κρυπτανάλυση εκτελείται στο chipertext από κάποιο μη εξουσιοδοτημένο μέρος και χωρίς φυσικά την γνώση του κλειδιού αποκρυπτογράφησης .

Γενικότερα, το σύστημα κρυπτογράφησης είναι βασισμένο σε μαθηματικούς κανόνες και αναλύεται σύμφωνα με την επιστήμη των μαθηματικών. Ο κλάδος των μαθηματικών που καλύπτει την κρυπτογραφία αλλά και την κρυπτολογική ανάλυση ονομάζεται **Κρυπτολογία**. Για αυτό το λόγο οι παρακάτω μαθηματικής φύσεως σχέσεις ίσως δώσουν μια πιο ολοκληρωμένη εικόνα των κρυπτογραφικών εννοιών :

Έστω ότι η διαδικασία κρυπτογράφησης είναι E πάνω σε ένα κείμενο M. Εάν το κρυπτογραφημένο κείμενο ορίζεται ως C τότε σε μαθηματική θρολογία θα ισχύει :
$E(M) = C$

Αν η διαδικασία αποκρυπτογράφησης είναι D, για να παραχθεί το αρχικό κείμενο M η ισότητα που θα ισχύει θα έχει τη μορφή :
$D(C) = M$

Κατά αυτό τον τρόπο, η γενική τεχνική της κρυπτογράφησης μέχρι να ανακτηθεί το plaintext θα πρέπει να διέπεται από την μαθηματική σχέση :
$D(E(M)) = M$

Κάθε κρυπτογραφική εφαρμογή εξαρτάται κυρίως από δυο συστατικά: Τον αλγόριθμο και το κρυπτογραφικό κλειδί που αυτός χρησιμοποιεί. Στα σύγχρονα κρυπτογραφικά συστήματα σύνθετοι μαθηματικοί τύποι αποτελούν τους αλγόριθμους ενώ τα κλειδιά είναι μεγάλες ακολουθίες από δυαδικά ψηφία. Για να υλοποιηθεί μεταξύ δυο μερών κρυπτογραφημένη επικοινωνία είναι απαραίτητο αυτά να χρησιμοποιούν τον ίδιο αλγόριθμο κρυπτογράφησης και το ίδιο ή συμβατά κλειδιά όπως θα δούμε παρακάτω. Η ανθεκτικότητα της επικοινωνίας και κατ' επέκταση της κρυπτογράφησης εξαρτάται περισσότερο από το μέγεθος των κλειδιών παρά από το πόσο ανθεκτικός είναι ο αλγόριθμος που χρησιμοποιεί αυτά τα κλειδιά.

Στο παρακάτω σχήμα φαίνεται η όλη διαδικασία, κατά την οποία ένα κείμενο κρυπτογραφείται για λόγους μυστικότητας και αποκρυπτογραφείται έτσι ώστε να φτάσει σε αναγνώσιμη μορφή.

1.2 Ασφάλεια πληροφοριών και Κρυπτογραφία

Η ασφάλεια ενός πληροφοριακού συστήματος και των δεδομένων του συνάγεται στο επίπεδο προστασίας της ακεραιότητας και της ανθεκτικότητας τους. Διάφορες διαδικασίες και τεχνικές αποτελούν τα μέτρα προστασίας των πληροφοριών του συστήματος. Οι τεχνικές αυτές μειώνουν την πιθανότητα να προκληθεί ζημιά ή οποιαδήποτε ανεπιθύμητη ενέργεια από μια ευπάθεια ή ένα ευάλωτο σημείο του συστήματος. Μια τέτοια τεχνική είναι και η Κρυπτογράφηση. Η κρυπτογράφηση είναι παραδοσιακά συνδεδεμένη με την μυστικότητα και την ασφάλεια των πληροφοριών. Ο στόχος της ασφάλειας των πληροφοριών δεν μπορεί να επιτευχθεί, φυσικά, μόνο με την παρουσία των κρυπτογραφικών αλγορίθμων και πρωτοκόλλων, αλλά σίγουρα αποτελούν τις τεχνικές αυτές για να μπορέσουμε να πετύχουμε το επιθυμητό επίπεδο ασφάλειας.

Ένα από τα θεμελιώδη εργαλεία που χρησιμοποιούνται στην ασφάλεια πληροφοριών είναι η ψηφιακή υπογραφή. Η ψηφιακή υπογραφή έχει εξελιχθεί για να είναι ένα αναπόσπαστο τμήμα της ταυτότητας ενός προσώπου. Προορίζεται να είναι μοναδική για το κάθε άτομο και χρησιμεύει ως ένα μέσο για να προσδιορισθεί η έγκριση του μηνύματος και η πιστοποίηση του αποστολέα. Τα σύγχρονα συστήματα κρυπτογράφησης παρέχουν πολλές υπηρεσίες στον τομέα της ασφάλειας των δεδομένων, όπως ηλεκτρονικές υπογραφές αλλά και πιστοποίηση πως τα δεδομένα δεν έχουν μεταβληθεί.

Τα κρυπτογραφικά συστήματα χρησιμοποιούνται για να παρέχουν αλλά και μπορούν να εξασφαλίσουν: εμπιστευτικότητα (confidentiality), ακεραιότητα των δεδομένων (data integrity), πιστοποίηση των χρηστών (authentication) και αδυναμία απάρνησης (non-repudiation).

- Η *εμπιστευτικότητα* (confidentiality) αναφέρεται κυρίως στο τρόπο προστασίας του περιεχόμενου των πληροφοριών αλλά και των πόρων του συστήματος. Οι πληροφορίες αυτές προστατεύονται από οντότητες που δεν έχουν δικαίωμα πρόσβασης. Ταυτόχρονα το σύστημα πρέπει να είναι ευέλικτο έτσι ώστε να προσφέρει πρόσβαση σε εξουσιοδοτημένες οντότητες. Υπάρχουν πολυάριθμες προσεγγίσεις στην παροχή της

εμπιστευτικότητας που κυμαίνονται από κάποιου είδους φυσική προστασία έως και μαθηματικούς αλγορίθμους που καθιστούν τα στοιχεία ακατανόητα. Τα κρυπτογραφικά συστήματα θεμελιώνουν την εμπιστευτικότητα των πόρων του συστήματος, μην επιτρέποντας σε μια οντότητα να δημοσιοποιήσει εμπιστευτικές πληροφορίες σε μια άλλη μη εξουσιοδοτημένη και απαγορεύοντας την πρόσβαση των μη εξουσιοδοτημένων οντοτήτων σε αυτές.

- Η *ακεραιότητα των δεδομένων* (data integrity) είναι η ιδιότητα που εξασφαλίζει την διατήρηση των δεδομένων του συστήματος στην μορφή που πρέπει να έχουν, απαγορεύοντας σε μη εξουσιοδοτημένες οντότητες να έχουν το δικαίωμα του χειρισμού πληροφοριών. Ο χειρισμός των πληροφοριών περιγράφει διαδικασίες όπως την εισαγωγή, διαγραφή, αλλά και μεταβολή δεδομένων του συστήματος από χρήστες. Οι κρυπτογραφικές τεχνικές πιστοποιούν τις οντότητες που έχουν το δικαίωμα πρόσβασης, εξασφαλίζοντας την ακεραιότητα των δεδομένων του συστήματος.

- Η *πιστοποίηση των χρηστών* (authentication) σχετίζεται με το τρόπο που προσδιορίζονται δυο οντότητες οι οποίες επικοινωνούν μεταξύ τους. Δύο μέρη που υλοποιούν μια διαδικασία επικοινωνίας προσδιορίζουν την ταυτότητα τους και την πιστοποιούν. Οι μέθοδοι κρυπτογράφησης υποστηρίζουν τόσο την ταυτοποίηση οντοτήτων όσο και την πιστοποίηση τους, κυρίως με την τεχνική των ηλεκτρονικών υπογραφών. Σε μια τέτοια περίπτωση χρησιμοποιείται ένας αλγόριθμος δημοσίου κλειδιού, όπως θα δούμε. Αυτή η σημαντική πτυχή του συστήματος κρυπτογραφίας υποδιαιρείται συνήθως σε δύο σημαντικές κατηγορίες: την πιστοποίηση των οντοτήτων και την επικύρωση της προέλευσης των στοιχείων.

- Η *αδυναμία απάρνησης* (non-repudiation) ή όπως λέγεται μη-αποκήρυξη είναι η ιδιότητα που αποτρέπει μια οντότητα να αρνηθεί μια ενέργεια του, που έλαβε χώρα σε πόρους του συστήματος. Για παράδειγμα, πρέπει να υπάρχει βεβαιότητα πως κάποια οντότητα έχει παραλάβει ένα μήνυμα που στάλθηκε έτσι ώστε να μην μπορεί να αρνηθεί την παραλαβή του. Οι κρυπτογραφικές τεχνικές ορίζουν μια διαδικασία επίλύσης της οποιασδήποτε απάρνησης, η οποία υλοποιείται από μια έμπιστη τρίτη οντότητα.

Οι μέθοδοι κρυπτογράφησης, είτε αυτές είναι συμμετρικές είτε μη-συμμετρικές όπως θα δούμε, αξιολογούνται με βάση κάποια κριτήρια. Αυτά ορίζονται με την ανάλυση των ίδιων των μεθόδων αλλά και με βάση τα χαρακτηριστικά των πόρων του πληροφοριακού συστήματος που τρέφει ασφάλειας. Το πιο σημαντικό κριτήριο είναι το ζητούμενο επίπεδο ασφάλειας. Συχνά εδώ υφίσταται μια αντίφαση, καθώς ένα μεγάλο επίπεδο ασφάλειας μπορεί να αποτρέψει την ευλυγισία του συστήματος και να μην επιτρέπει ακόμα και απλής φύσεως

εργασίες. Γενικότερα, το επίπεδο ασφάλειας δεν υπολογίζεται και ορίζεται από την σημαντικότητα των δεδομένων του συστήματος.

Οι προκαθορισμένοι στόχοι της ασφάλειας ενός υπολογιστικού συστήματος συχνά «επιβάλουν» και την μέθοδο ή τον συνδυασμό των κατάλληλων μεθόδων κρυπτογράφησης, ανάλογα με την διαφορετική λειτουργία ή χρήση που οι τεχνικές αυτές επιτελούν. Κριτήριο αξιολόγησης μιας μεθόδου κρυπτογράφησης είναι και η αποδοτικότητα του. Παραδείγματος χάριν, ένας αλγόριθμος κρυπτογράφησης μπορεί να εκτιμηθεί από τον αριθμό των χαρακτήρων που μπορεί να κρυπτογραφήσει ανά δευτερόλεπτο. Σήμερα όλο και περισσότερες κρυπτογραφικές εφαρμογές σε περιβάλλον λογισμικού ή και υλικού χαρακτηρίζονται από πολυπλοκότητα. Αυτό το χαρακτηριστικό τους, σε συνδυασμό με τους ενδεχόμενους ελεύθερους πόρους ενός συστήματος αποτελεί μέτρο αξιολόγησης ενός αλγορίθμου κρυπτογράφησης.

Θεωρητικά, η επιλογή της μεθόδου κρυπτογράφησης και η διαδικασία υλοποίησης της σε ένα πληροφοριακό σύστημα εξαρτάται από την αξιολόγηση του αλλά και από το ζητούμενο επίπεδο ασφάλειας. Σήμερα οι τεχνικές που έχουν τυποποιηθεί θεωρούνται ευρέως αποδεκτές, έχουν αξιολογηθεί και εγκριθεί από ομάδες ειδικών στους πόρους του συστήματος που καλύπτουν, ενώ εγγυώνται υψηλό επίπεδο διαλειτουργικότητας μεταξύ εξοπλισμού διαφορετικών ενδεχομένως κατασκευαστών.

1.3 Ιστορική αναδρομή

Το σύστημα της κρυπτογραφίας έχει μια μακροχρόνια και συναρπαστική ιστορία. Οι κρυπτογραφικές τεχνικές μέσα στην πάροδο του χρόνου καταγράφονται ως ιστορικά ντοκουμέντα. Η κρυπτογραφία και η περιορισμένη χρήση της από τους Αιγυπτίους περίπου 4000 έτη πριν, έως και τον εικοστό αιώνα όπου διαδραμάτισε έναν σημαντικό ρόλο στην έκβαση και των δύο παγκόσμιων πολέμων, εξελίχθηκε και αναπτύχθηκε ως μέθοδος ασφάλειας κρίσιμων πληροφοριών.

Το σύστημα της κρυπτογραφίας, ως κλάδος της μαθηματικής σκέψης, χρησιμοποιήθηκε αρχικά σαν ένα εργαλείο για να προστατεύσει εθνικά μυστικά, διπλωματικές διαδικασίες και υψηλού συμφέροντος στρατηγικές. Η ανάπτυξη της τεχνολογίας των υπολογιστικών συστημάτων και των συστημάτων επικοινωνιών, λίγο μετά τα μέσα του προηγούμενου αιώνα, καταγράφηκε ως μια απαίτηση από τον ιδιωτικό τομέα αλλά και όχι μόνο, για προστασία των πληροφοριών σε ψηφιακή μορφή και παροχή υπηρεσιών ασφάλειας των δεδομένων.

Στην αρχαιότητα, ο Καίσαρας χρησιμοποίησε την πρώτη κρυπτογραφική τεχνική που καταγράφηκε στην ιστορία. Τις επιστολές που έγραφε για άλλους άρχοντες της ρωμαϊκής αυτοκρατορίας, τις μετέτρεπε σε κρυπτογραφημένο κείμενο με μια εξαιρετική, για την εποχή, μέθοδο που γνώριζε αυτός και ο παραλήπτης, για τον φόβο μήπως αυτές διαβαστούν από κάποιους που απειλούσαν τα στρατηγικά του συμφέροντα. Το κρυπτογραφικό κλειδί που χρησιμοποιούσε ήταν ένας αριθμός που υπαγόρευε ποιο γράμμα του λατινικού αλφάβητου θα αντικαταστήσει κάθε χαρακτήρα του αρχικού κειμένου. Έτσι, εάν ο αριθμός αυτός ήταν το 2 τότε κάθε χαρακτήρας αντικαθιστούταν με τον δεύτερο κατά σειρά στο αλφάβητο. Το γράμμα 'a' θα γινόταν 'c' και με τον ίδιο τρόπο το 'b' θα ήταν 'd' και το 'c' , 'e'. Ο παραλήπτης, που ήξερε, το κλειδί αποκρυπτογραφούσε το κείμενο για να μπορέσει να το διαβάσει. Η κρυπτογραφική τεχνική που υλοποίησε ο Καίσαρας αναλύεται παρακάτω με ένα παράδειγμα όπου το «κλειδί» είναι το 2.

Αρχικό κείμενο **«my name is kostas».**

Κρυπτογραφημένο κείμενο **«oa pcog ku mquvcu»** .

Σήμερα, η μέθοδος αυτή εκφράζεται από την σχέση: c = m + k mod 26, όπου κάθε χαρακτήρας του αρχικού κειμένου που έχει την m-ιοστή θέση αντικαθίσταται από τον χαρακτήρα στην c-ιοστή θέση. Βλέπουμε πόσο σημαντικό ρόλο σε αυτή την διαδικασία έχει το κλειδί (k), πράγμα που συμβαίνει με όλες τις κρυπτογραφικές τεχνικές. Στο παραπάνω παράδειγμα το k θα είναι 2 (2 mod 26=2), ενώ παρατηρούμε πως το αποτέλεσμα θα είναι το ίδιο και για k=28 (28 mod 26=2).

Στην σύγχρονη ιστορία, οι σύμμαχοι στον δεύτερο παγκόσμιο πόλεμο χρησιμοποίησαν κρυπτογραφικές τεχνικές για την προστασία υψηλής σημασίας εθνικών μυστικών και στρατηγικών αποφάσεων. Αργότερα, την δεκαετία του '70 υιοθετήθηκαν πρότυπα επεξεργασίας ομοσπονδιακών πληροφοριών της αμερικανικής κυβέρνησης. Αυτά τα πρότυπα κρυπτογράφησης στοιχείων, είναι ο πιο γνωστός κρυπτογραφικός μηχανισμός στην ιστορία. Παραμένουν μέχρι και σήμερα τυποποιημένα μέσα κρυπτογράφησης στο ηλεκτρονικό εμπόριο και χρησιμοποιούνται από πολλούς χρηματοδοτικούς και μη οργανισμούς σε όλο τον κόσμο.

Η πιο εντυπωσιακή ανάπτυξη στην ιστορία του συστήματος κρυπτογραφίας ήρθε το 1976 όταν οι Diffie και Hellman δημοσίευσαν το βιβλίο τους «Νέες κατευθύνσεις στην Κρυπτογραφία». Αυτό το βιβλίο εισήγαγε την επαναστατική έννοια του συστήματος κρυπτογράφησης δημοσίου-κλειδιού, όπου παρείχε μια νέα μέθοδο ασφάλειας δεδομένων και κατέληξε σήμερα να θεωρείται ως η πιο σημαντική ανακάλυψη. Οι συντάκτες του όμως, δεν αναφέρθηκαν σε καμία πρακτική υλοποίησης της τεχνικής δημοσίου κλειδιού. Παρόλαυτα, μπορούμε να πούμε πως εκφράστηκε μεγάλο ενδιαφέρον στην κρυπτογραφική κοινότητα για αυτή την ιδέα και αποτελεί έως και τώρα την βάση για την παραγωγή νέων

μεθόδων κρυπτογράφησης. Αυτοί οι μέθοδοι ανήκουν στην κατηγορία αλγορίθμων δημοσίου κλειδιού.

Το 1978 οι Rivest, Shamir, και Adleman δημιούργησαν τον πρώτο αλγόριθμο κρυπτογράφησης δημόσιου κλειδιού (RSA) που υλοποιείται τόσο στην κρυπτογραφημένη επικοινωνία όσο και στις ψηφιακές υπογραφές. Η σχεδίαση του RSA είναι βασισμένη σε ένα μαθηματικό πρόβλημα εντοπισμού μεγάλων ακέραιων πρώτων αριθμών. Η εφαρμογή του αναζωογόνησε τις προσπάθειες παραγωγής και σχεδίασης αποδοτικότερων μεθόδων. Έτσι την δεκαετία του '80 καταγράφονται σημαντικές πρόοδοι στην ανάπτυξη αλγορίθμων δημοσίου κλειδιού.

Μια άλλη κατηγορία ασφαλών και πρακτικών μεθόδων δημόσιου κλειδιού δημοσιοποιήθηκε από τον ElGamal το 1985. Το 1991 υιοθετήθηκαν τα πρώτα διεθνή πρότυπα για τις ψηφιακές υπογραφές (ISO/IEC) βασισμένα στον RSA. Το 1994 η Αμερικανική κυβέρνηση άρχισε να χρησιμοποιεί τα πρώτα ψηφιακά πρότυπα υπογραφών, ένας μηχανισμός βασισμένος στη μέθοδο κρυπτογράφησης δημοσίου-κλειδιού του ElGamal. Η αναζήτηση νέων σχεδίων-αλγορίθμων δημοσίου κλειδιού απασχολεί μέχρι και σήμερα τα πρότυπα των θεμάτων ασφάλειας των υπολογιστικών συστημάτων. Οι μηχανισμοί κρυπτογράφησης συνεχίζουν να αναπτύσσονται με γρήγορο ρυθμό για να καλύψουν τις ανάγκες ασφάλειας μιας αναπτυσσόμενης κοινωνίας πληροφοριών, οι ανάγκες της οποίας αυξάνουν καθημερινά .

1.4 Ο χαρακτήρας της κρυπτογράφησης σήμερα

Η κρυπτογράφηση βρίσκει σήμερα εφαρμογή σε πολλές δραστηριότητες. Τα ψηφιακά κινητά τηλέφωνα, με την τεχνολογία τους βασισμένη στην κρυπτογράφηση, παρέχουν μεγαλύτερη ασφάλεια στην επικοινωνία. Οι τράπεζες χρησιμοποιούν ισχυρή κρυπτογράφηση για την οικονομικής φύσεως επικοινωνία τους. Όλη η τεχνολογία της συνδρομητικής τηλεόρασης καθώς και η νέα τεχνολογία αποθήκευσης ψηφιακού ήχου και εικόνας βασίζονται κατά κύριο λόγο στον ρυθμό ανάπτυξης των κρυπτογραφικών συστημάτων. Στο Internet, οι χρήστες χρησιμοποιούν σήμερα την κρυπτογράφηση για την προστασία των δεδομένων τους. Η υλοποίηση μεθόδων κρυπτογράφησης έχει προσφέρει ασφάλεια σε υπηρεσίες όπως το tele-shopping και το e-banking αλλά και στη διασφάλιση του ιατρικού απόρρητου. Η ενσωμάτωση πλήρων μηχανισμών κωδικοποίησης στις έξυπνες κάρτες (smart cards) είναι ήδη πραγματικότητα.

Η ταχεία εξέλιξη του διαδικτύου θα σηματοδοτήσει μια αξιοσημείωτη αλλαγή στη χρήση της κρυπτογράφησης μέσα στα επόμενα χρόνια. Θα γίνουμε δέκτες της πλήρης ενσωμάτωσης της σε κάθε δραστηριότητα των υπολογιστικών

συστημάτων, τόσο σε προσωπικό όσο και σε επιχειρηματικό επίπεδο. Ήδη οι χρήστες έχουν εύκολη πρόσβαση σε πακέτα κρυπτογραφίας τα οποία μπορούν να προμηθευτούν. Όσον αφορά το ακαδημαϊκό επίπεδο, πολλά πανεπιστήμια σε όλο τον κόσμο διδάσκουν τις έννοιες της κρυπτογραφίας και της κρυπτολογίας. Η συνεχιζόμενη πρόοδος της ψηφιακής τεχνολογίας ώθησε εκατοντάδες εταιρίες πληροφορικής και τηλεπικοινωνιών να κατασκευάζουν και να πουλάνε προϊόντα και συστήματα που αφορούν στην κρυπτογράφηση.

Φυσικά, πάντα υπάρχει και η άλλη όψη του νομίσματος, ειδικότερα σε καινοτομίες. Ο Walter Wriston, αφιέρωσε ένα κεφάλαιο του βιβλίου του «Το Λυκόφως της Κυριαρχίας» (The Twilight of Sovereignty) στην εξέλιξη της κρυπτογραφίας. Ο Wriston προέβλεψε ότι η δύναμη της τεχνολογίας θα οδηγήσει αναπόφευκτα στην αποδυνάμωση των εθνικών κυβερνήσεων και αναγνώρισε τον ρόλο που πρόκειται να διαδραματίσει η κρυπτογραφία σ' αυτήν την εξέλιξη. Καταγράφει συνειδητοποιημένα, πως η αναπτυσσόμενη τεχνολογία της κρυπτογραφίας είναι το βασικό συστατικό για τη μεταφορά της κοινωνικής και κυρίως της οικονομικής εξουσίας από τις κυβερνήσεις των εθνικών κρατών, στον πληθυσμό αυτό που θα χρησιμοποιεί τις δυνατότητες του ηλεκτρονικού υπολογιστή. Με την εξάπλωση του διαδικτύου και τη δυνατότητα αγοράς εφαρμογών ισχυρής κρυπτογραφίας, υποστηρίζει ότι η ραγδαία της εξάπλωση είναι αναπόφευκτη. «Οι κυβερνήσεις δεν μπορούν να κάνουν τίποτε γι' αυτό», γράφει χαρακτηριστικά ο Wriston. «Πρόκειται για ένα ακόμη φαινόμενο μπροστά στο οποίο φαίνεται να είναι εντελώς ανίσχυρες». Ίσως τέτοιες απόψεις να χαρακτηρίζονται ακόμα ως υπερβολικές, αλλά αυτό που είναι σίγουρο είναι ότι βρισκόμαστε μπροστά σε μια ακόμη πρόκληση της τεχνολογίας. Το σύστημα της κρυπτογραφίας και ο ρόλος που θα διαμορφώσει στο άμεσο μέλλον είναι κάτι παραπάνω από βέβαιο πως θα επαναπροσδιορίσει απόψεις και θα αιφνιδιάσει.

2. Αλγόριθμοι Κρυπτογράφησης και κλειδιά

2.1 Τι είναι οι Αλγόριθμοι κρυπτογράφησης

Όπως αναφέρθηκε και πιο πάνω, οι κρυπτογραφικές τεχνικές και εφαρμογές που χρησιμοποιούνται στα σύγχρονα πληροφοριακά συστήματα έχουν ως γνώμονα μια συγκεκριμένη μέθοδο κρυπτογράφησης και το κρυπτογραφικό κλειδί. Αυτή η μέθοδος κρυπτογράφησης συχνά καλείται **αλγόριθμος κρυπτογράφησης** (algorithm encryption). Ο αλγόριθμος κρυπτογράφησης πρακτικά συμπεριλαμβάνει μαθηματικούς τύπους που χρησιμοποιούνται τόσο για την κρυπτογράφηση, όσο και την αποκρυπτογράφηση. Γενικά, υπάρχουν δύο, σχετικές μεταξύ τους, λειτουργίες του μία για την κρυπτογράφηση και η άλλη για την αποκρυπτογράφηση .

Ο αλγόριθμος κρυπτογράφησης ως μια τεχνική μπορεί να θεωρηθεί ως το πιο σημαντικό χαρακτηριστικό της διαδικασίας της κρυπτογράφησης εφόσον είναι η βάση πάνω στην οποία θα υλοποιηθεί η κρυπτογραφημένη επικοινωνία. Κύρια χαρακτηριστικά των αλγορίθμων και άξια αναφοράς είναι το επίπεδο ασφάλειας που μπορεί να προσφέρει στην κρυπτογραφημένη επικοινωνία είτε σε ένα πληροφοριακό σύστημα καθώς και ο βαθμός αξιολόγησης του κατά την διαδικασία επιλογής.

Η επιλογή της μεθόδου κρυπτογράφησης και ιδιαίτερα του αλγορίθμου που θα χρησιμοποιηθεί γίνεται από ειδικευμένους σε θέματα ασφάλειας και κάθε άλλο παρά ασήμαντη μπορεί να καταστεί. Ένας δημοσιευμένος αλγόριθμος, με την πεποίθηση ότι έχει διερευνηθεί από πολλούς αλλά δεν έχει κρυπταναλυθεί ακόμα θεωρείται ασφαλής. Συνηθισμένο φαινόμενο είναι και η εμπιστοσύνη στην επιλογή ενός γνωστού κατασκευαστή, ο οποίος διαφυλάσσοντας την φήμη του δεν θα διακινδυνέψει την πώληση εξοπλισμού ή εφαρμογών με κατώτερους αλγόριθμους.

Διαφορετικοί αλγόριθμοι προφανώς προσφέρουν και διαφορετικούς βαθμούς ασφάλειας που εξαρτώνται από τον τρόπο και με τον οποίο πρόκειται αυτοί να «σπάσουν» αλλά και την πιθανότητα να συμβεί αυτό. Εάν το κόστος που απαιτείται για να «σπάσει» ένας αλγόριθμος, είναι μεγαλύτερο από την αξία των κρυπτογραφημένων δεδομένων του συστήματος, τότε ο αλγόριθμος μπορεί να θεωρηθεί ασφαλής. Εάν ο χρόνος που χρειάζεται μια μη εξουσιοδοτημένη οντότητα (εισβολέας) να «σπάσει» έναν αλγόριθμο είναι μεγαλύτερος από το χρόνο που η κρυπτογραφημένη επικοινωνία ή τα δεδομένα πρέπει να παραμείνουν μυστικά, τότε η ασφάλεια του αλγορίθμου κυμαίνεται στα ζητούμενα επίπεδα.

Εάν η ασφάλεια του αλγορίθμου είναι βασισμένη μόνο στην διαδικασία κατά την οποία αυτός θα κρατηθεί κρυφός τότε έχουμε ένα παράδειγμα περιορισμένου αλγόριθμου όπως αυτός αναφέρεται. Μπορεί οι *περιορισμένοι αλγόριθμοι* να έχουν μεγάλο ιστορικό ενδιαφέρον αλλά καταγράφονται ως ανεπαρκείς σύμφωνα με τα σύγχρονα πρότυπα. Κάθε ενδεχόμενη ομάδα χρηστών θα πρέπει συνέχεια να καταργεί κάποιον αλγόριθμο και να σχεδιάζει κάποιον άλλον κάθε φορά που κάποιος χρήστης αποχωρεί από την ομάδα, για το ενδεχόμενο που αποκαλυφθεί ο μαθηματικός τύπος του αλγόριθμου. Οι περιορισμένοι αλγόριθμοι επίσης δεν υποστηρίζουν τον ποιοτικό έλεγχο αλλά και την διαδικασία πιστοποίησης που είναι σημαντική πρακτική βασισμένη πάνω στην τεχνική κρυπτογράφησης. Έτσι, για να θεωρηθεί ασφαλές το όλο σύστημα κάθε ομάδα χρηστών θα πρέπει να έχει το δικό της και μοναδικό αλγόριθμό κρυπτογράφησης που είναι προφανώς πρακτικά αδύνατο και μη συμβατό με τις απαιτήσεις της τεχνολογίας.

2.2 Κρυπτογραφικά κλειδιά, δημόσια και ιδιωτικά

Με γνώμονα τα παραπάνω σημαντικά μειονεκτήματα των περιορισμένων αλγόριθμων τα σύγχρονα κρυπτογραφικά συστήματα λύνουν το πρόβλημα με την ύπαρξη ενός κρυπτογραφικού κλειδιού. Ένα **κρυπτογραφικό κλειδί** (encryption key) μπορεί να είναι μια τιμή από μια πολύ μεγάλη λίστα τιμών που χρησιμοποιείται από τις διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης. Η ασφάλεια του αλγορίθμου σε αυτή την περίπτωση είναι βασισμένη στο αλγοριθμικό κλειδί και το κατά πόσο κρυφό θα κρατηθεί αλλά και πόσο δύσκολο είναι να υπολογιστεί. Οι λειτουργίες κρυπτογράφησης και αποκρυπτογράφησης εάν ορίσουμε το κλειδί ως K, αναπτύσσονται σύμφωνα και με τα παραπάνω, στους αντιστοίχους μαθηματικούς τύπους:

$E_K(M)=C$
$D_K(C)=M$

Η διαδικασία κρυπτογράφησης συμβολίζεται με E και αντίστοιχα η αποκρυπτογράφηση με D. Το M είναι το αρχικό κείμενο και C το κρυπτογραφημένο αποτέλεσμα. Παρατηρούμε πως κατά την κρυπτογράφηση είσοδοι αποτελούν το κείμενο καθώς και το κλειδί (K). Το κλειδί χρησιμοποιείται και στην διεργασία ανάκτησης του αρχικού κειμένου, απόδειξη της σημαντικότητας τόσο της ύπαρξης, αλλά και της διαχείρισης του (key management) .

Μερικοί αλγόριθμοι χρησιμοποιούν ένα διαφορετικό κλειδί κρυπτογράφησης και ένα άλλο κλειδί αποκρυπτογράφησης, για περισσότερη βαρύτητα στο ζήτημα της ασφάλειας όπως θα δούμε και παρακάτω. Αυτό σημαίνει ότι ο αλγόριθμος

μπορεί να είναι δημοσιευμένος και αναλυμένος χωρίς να υπάρχει επίπτωση στην ασφάλεια της κρυπτογραφημένης επικοινωνίας. Κάποιο τρίτο μέρος (μη εξουσιοδοτημένο) ενδέχεται να γνωρίζει τον αλγόριθμο και το πως αυτός λειτουργεί, μην έχοντας όμως το ιδιαίτερο κλειδί δεν μπορεί να διαβάσει τα κρυπτογραφημένα μηνύματα. Χρησιμοποιείται λοιπόν το κλειδί κρυπτογράφησης (K1) στην διαδικασία μετασχηματισμού του αρχικού κειμένου και το κλειδί αποκρυπτογράφησης (K2) κατά την εργασία ανάκτησης του κειμένου σε μορφή αναγνώσιμη. Οι παραπάνω μαθηματικές εξισώσεις σε μια τέτοια περίπτωση έχουν την μορφή :

$E_{K1}(M)=C$
$D_{K2}(C)=M$

Συγκεκριμένη αναφορά πρέπει να γίνει στην κατηγορία αυτή που διαχωρίζει τα κρυπτογραφικά κλειδιά σε δημόσια και ιδιωτικά με βάση με την δημοσίευση τους ή όχι. **Δημόσιο κλειδί** (public key) είναι το κλειδί ενός αλγόριθμου κρυπτογράφησης που μπορεί να γίνει δημόσια γνωστό, χωρίς να κλονιστεί η ασφάλεια του συστήματος κρυπτογράφησης. **Ιδιωτικό κλειδί** (private key) είναι το κλειδί ενός αλγόριθμου κρυπτογράφησης το οποίο κρατείτε μυστικό και προστατεύεται από υποκλοπή ή τροποποίηση του.

Είναι προφανές πως αυτά τα κλειδιά χρησιμοποιούνται ως ένα ζεύγος και παράγονται κατά αυτό τον τρόπο. Ένας αλγόριθμος που χρησιμοποιεί αυτό το ζεύγος κλειδιών τα παράγει με μια συγκεκριμένη διεργασία, όπως θα δούμε και παρακάτω, πράγμα που τα χαρακτηρίζει αλληλοεξαρτώμενα. Κείμενο και δεδομένα που κρυπτογραφούνται με την βοήθεια ενός κλειδιού αποκρυπτογραφούνται μόνο με την γνώση και χρησιμοποίηση του άλλου, είτε αυτό είναι ιδιωτικό είτε δημόσιο.

Η κρυπτογράφηση ενός μηνύματος με το ιδιωτικό κλειδί του αποστολέα εξασφαλίζει στον παραλήπτη την *πιστοποίηση* του αποστολέα. Κανένας άλλος δεν μπορεί να χρησιμοποιήσει το ιδιωτικό κλειδί εφόσον αυτό παραμείνει κρυφό. Η αποκρυπτογράφηση του μηνύματος σε αυτή την περίπτωση γίνεται με το δημόσιο κλειδί του αποστολέα. Για την παραγωγή ενός εμπιστευτικού μηνύματος ο αποστολέας κάνει χρήση του δημόσιου κλειδιού του παραλήπτη για να κρυπτογραφήσει το μήνυμα , έτσι ώστε να μείνει απόρρητο έως ότου αποκρυπτογραφηθεί από το ιδιωτικό κλειδί του παραλήπτη. Προφανώς κανείς άλλος εκτός του παραλήπτη δεν μπορεί να το αποκρυπτογραφήσει γιατί κανείς άλλος δεν έχει το απαιτούμενο ιδιωτικό κλειδί (ούτε καν ο αποστολέας). Σε μια τέτοια περίπτωση εξασφαλίζεται η *εμπιστευτικότητα* του περιεχομένου του μηνύματος.

Η παραγωγή, η μεταφορά, η χρησιμοποίηση, η αποθήκευση και τελικά η καταστροφή ενός κλειδιού οριοθετούν την έννοια της **διαχείρισης** του **κρυπτογραφικού κλειδιού** (key management). Στην σύγχρονη τεχνολογία, το key management και οι διαδικασίες που αυτό συνεπάγεται είναι το δυσκολότερο

μέρος του συστήματος της κρυπτογραφίας. Ο σχεδιασμός των ασφαλών κρυπτογραφικών αλγορίθμων και πρωτοκόλλων δεν είναι εύκολος, αλλά σίγουρα ο κορμός της εξεύρεσης και παραγωγής τους στηρίζεται στην ακαδημαϊκή έρευνα. Η παραγωγή, μετάδοση, και αποθήκευση των κλειδιών κρυπτογράφησης είναι το σημαντικότερο κομμάτι της όλης διαδικασίας. Φυσικά στόχος της όλης προσπάθειας είναι να κρατηθεί το κλειδί μυστικό κατά την διαχείριση του.

Σε μια συνηθισμένη κρυπτογραφημένη επικοινωνία ο αποστολέας αρχικά θα δημιουργήσει το κρυπτογραφημένο κείμενο με την χρήση ενός αλγορίθμου και του κρυπτογραφικού του κλειδιού. Έπειτα θα στείλει το κείμενο στον παραλήπτη ενώ θα πρέπει να τον ενημερώσει για το κλειδί που θα χρησιμοποιήσει αυτός για την κρυπτογράφηση ή να του το παραδώσει. Η μεταφορά του μηνύματος ενδεχομένως να γίνει μέσω ενός μη ασφαλούς καναλιού επικοινωνίας. Η μεταφορά όμως του κλειδιού θα πρέπει να γίνεται σε ένα απόλυτα ασφαλές κανάλι επικοινωνίας. Το πώς ακριβώς θα γίνει αυτή η μετάδοση και η ασφάλεια που μπορεί να παρέχει έχει απασχολήσει πολύ την ερευνητική κοινότητα. Συχνά, πριν ακόμα από την υλοποίηση της επικοινωνίας παραλήπτης και αποστολέας έχουν συμφωνήσει για τη τιμή του κρυπτογραφικού κλειδιού οπότε τους είναι ήδη γνωστό. Σε μια φυσικά αντίθετη περίπτωση οι ενέργειες που γίνονται εξαρτώνται από αλλά μέσα επικοινωνίας όπως το τηλέφωνο ή άλλες ασφαλής διαδικασίες.

Τα κλειδιά που χρησιμοποιούνται σε μια κρυπτογραφημένη επικοινωνία έχουν συχνά διάρκεια ζωής πραγματικού χρόνου, όσο διαρκεί μια χρήση τους. Είναι ασφαλέστερο η παραγωγή νέου κλειδιού σε ενδεχόμενη νέα επικοινωνία. Τα κλειδιά που χρησιμοποιούνται για να κρυπτογραφήσουν τα αρχεία ενός συστήματος δεν μπορούν να αλλάξουν συχνά. Μια λύση να είναι να κρυπτογραφηθεί κάθε αρχείο με ένα μοναδικό κλειδί για κάθε αρχείο, και στην συνέχεια να κρυπτογραφηθούν όλα αυτά τα κλειδιά με ένα ιδιωτικό κλειδί. Το ιδιωτικό κλειδί πρέπει έπειτα είτε να απομνημονευθεί είτε να αποθηκευτεί σε μια ασφαλή θέση. Φυσικά, η απώλεια αυτού του κλειδιού θα σήμαινε απώλεια όλων των μεμονωμένων κλειδιών των αρχείων. Τα ιδιωτικά κλειδιά για τις εφαρμογές ενός συστήματος κρυπτογραφίας έχουν διάρκεια ζωής ανάλογα με την εφαρμογή. Ιδιωτικά κλειδιά που χρησιμοποιούνται για τις ψηφιακές υπογραφές και την πιστοποίησης της ταυτότητας μιας οντότητας ενδέχεται να έχουν διάρκεια ζωής κάποιων ετών ή ακόμα και διάρκεια μιας ζωής.

Το μέγεθος των κρυπτογραφικών κλειδιών είναι ακολουθίες από bits και παράγονται με κάποια αυτόματη διαδικασία. Χρησιμοποιούνται «γεννήτριες» τυχαίου-αριθμού για την παραγωγή τους, αλλά αυτό που είναι σημαντικότερο είναι η εκτέλεση αξιολογημένων αλγορίθμων και των βασικών διαδικασιών κρυπτογράφησης.

2.3 Σύγκριση συμμετρικού αλγόριθμου - αλγόριθμου δημοσίου κλειδιού.

Υπάρχουν δυο βασικές μέθοδοι στην κρυπτογραφία: Τα συστήματα μυστικού κλειδιού ή συμμετρικά συστήματα κρυπτογράφησης (symmetric cryptography) και τα μη-συμμετρικά συστήματα ή συστήματα κρυπτογράφησης δημοσίου κλειδιού (public key cryptography).Τα διαφορετικά χαρακτηριστικά αυτών των μεθόδων κρυπτογράφησης καθώς και ο τρόπος λειτουργίας τους εξαρτάται από τους αλγόριθμους που χρησιμοποιούνται. Αντίστοιχα οι δυο κύριες κατηγορίες στις οποίες διαχωρίζονται οι αλγόριθμοι κρυπτογράφησης με διαφορετικά χαρακτηριστικά ,όπως θα δούμε ,αλλά και διαφορετική πορεία μέσα στο χρόνο, αναλύονται παρακάτω.

Οι **αλγόριθμοι μυστικού κλειδιού** ή **συμμετρικοί αλγόριθμοι** (symmetric algorithms) χρησιμοποιούν ένα μόνο κρυπτογραφικό κλειδί , γνώρισμα στο οποίο οφείλουν και την ονομασία τους. Το κρυπτογραφικό κλειδί χρησιμοποιείται τόσο για την διαδικασία κρυπτογράφησης όσο και για την αποκρυπτογράφηση των δεδομένων.. Προφανώς η λειτουργικότητα του αλγορίθμου εξαρτάται από το πόσο θα προστατευτεί το μυστικό κλειδί από υποκλοπή ή τροποποίηση. Το κλειδί πρέπει να είναι γνωστό αποκλειστικά και μόνο στις οντότητες που επικοινωνούν μεταξύ τους.

Οι **μη-συμμετρικοί αλγόριθμοι** ή **αλγόριθμοι δημοσίου κλειδιού** (public key algorithms) υλοποιούν την διαδικασία κρυπτογράφησης χρησιμοποιώντας ένα ζεύγος κρυπτογραφικών κλειδιών. Κάθε οντότητα έχει στην κατοχή της ένα ζευγάρι κλειδιών ,το ένα από τα οποία είναι δημόσια γνωστό (**δημόσιο κλειδί**) ενώ το άλλο κρατείται μυστικό (**ιδιωτικό κλειδί**). Οτιδήποτε πληροφορίες ή δεδομένα κρυπτογραφούνται με την χρήση του ενός κλειδιού ανακτώνται με την γνώση και την χρήση του άλλου. Το δημόσιο κλειδί μπορεί να γίνει γνωστό, πρέπει όμως να απαγορευτεί η τροποποίηση του, ενώ το ιδιωτικό κλειδί πρέπει να είναι γνωστό στην οντότητα μόνο στην οποία και ανήκει .

Με δεδομένο ότι δύο συστήματα με διαφορετικά χαρακτηριστικά κρυπτογραφούν δεδομένα, εύλογα δημιουργείται η ερώτηση, ποιος από τους δύο αλγόριθμους είναι ο καλύτερος; Η ερώτηση για πολλούς, και πολύ σωστά, δεν έχει νόημα. Ο κάθε αλγόριθμος και η κρυπτογράφηση που προσφέρει αξιολογείται και επιλέγεται με βάση τις ανάγκες κάθε οντότητας ή πληροφοριακού συστήματος και προσαρμόζεται στις απαιτήσεις του. Το γεγονός όμως ότι η κρυπτογράφηση δημοσίου κλειδιού εφευρέθηκε και αναπτύχθηκε αργότερα, πολλές προσπάθειες σύγκρισης είναι ιστορικά καταγεγραμμένες. Σε μια τέτοια προσπάθεια για παράδειγμα, πολλοί αναλυτές επισήμαναν το γεγονός ότι το μήκος των κρυπτογραφημένων μηνυμάτων (chipertext) είναι πολύ μεγαλύτερο όταν αυτά κρυπτογραφούνται με ένα δημοσίου κλειδιού αλγόριθμο, από ό,τι με ένα συμμετρικό. Το συμπέρασμά τους ήταν ότι ο συμμετρικός αλγόριθμος ήταν

αποδοτικότερος από τον δημοσίου κλειδιού. Φυσικά αυτή η ανάλυση αγνοεί σημαντικά οφέλη της ασφάλειας της μη συμμετρικής κρυπτογράφησης.

Παρολαυατά, μια σύγκριση των χαρακτηριστικών των δύο αλγορίθμων κρυπτογράφησης, όσον αφορά την ταχύτητα τους, το μήκος των κλειδιών που χρησιμοποιούν, αλλά και το επίπεδο ασφάλειας που προσφέρουν, κρίνεται απαραίτητη από πλευράς κατανόησης του τρόπου λειτουργίας τους.

Η κυριότερη διαφορά των δυο μεθόδων είναι ότι ενώ ένας συμμετρικός αλγόριθμος χρησιμοποιεί ένα μόνο κλειδί για κρυπτογράφηση και αποκρυπτογράφηση, ένας δημοσίου κλειδιού αλγόριθμος υποστηρίζει ένα ζεύγος τιμών. Το χαρακτηριστικό αυτό επιβεβαιώνει την κρίση πως η κρυπτογράφηση δημοσίου κλειδιού είναι ασφαλέστερη. Μην ξεχνάμε πως στην συμμετρική κρυπτογράφηση πρέπει να μεταφερθεί το κλειδί από την μια οντότητα στην άλλη, ενώ αποστολέας και παραλήπτης πρέπει να προστατεύσουν στον ίδιο βαθμό το κρυπτογραφικό κλειδί. Πρακτικά, έχει υπολογιστεί πως ένας συμμετρικός αλγόριθμος είναι πολλαπλάσια πιο γρήγορος από ένα μη-συμμετρικό, σε επίπεδα τιμών που να φτάνει και τις 10.000 . Η ταχύτητα, γενικότερα, στον κλάδο της επιστήμης της πληροφορικής παίζει σημαντικό ρόλο. Ο χαρακτηρισμός της αργής διαδικασίας κρυπτογράφησης που προσφέρει ένας αλγόριθμος δημοσίου κλειδιού καταγράφεται ως μειονέκτημα.

Ο συμμετρικός αλγόριθμος θεωρείται αποδοτικότερος για την κρυπτογράφηση κειμένων και μηνυμάτων σε μια ασφαλή επικοινωνία, και αυτό γιατί είναι πολύ γρηγορότερος και δεν είναι ευαίσθητος σε επιθέσεις που στοχεύουν στην κρυπτανάλυση του ciphertext. Αντίθετα, ο αλγόριθμος δημοσίου κλειδιού είναι κατάλληλος όσον αφορά την διαχείριση του κρυπτογραφικού κλειδιού ,ενώ υποστηρίζει και ένα μεγάλο αριθμό πρωτοκόλλων.

Η ανθεκτικότητα και η αξιολόγηση μιας κρυπτογραφικής εφαρμογής, όπως έχει προαναφερθεί, εξαρτάται από το μέγεθος των κλειδιών που χρησιμοποιούν οι αλγόριθμοι. Έχει αποδειχθεί πως μεγάλου μεγέθους κλειδιά παρέχουν ανθεκτικότερη κρυπτογράφηση. Ως παράδειγμα, αξίζει να αναφέρουμε πως η διαδικασία κρυπτογράφησης 128-bit με τον αλγόριθμο μυστικού κλειδιού RC5 είναι 3078 φορές ανθεκτικότερη από την 40-bit κρυπτογράφηση.

Δεδομένο θεωρείται πως διαφορετικοί αλγόριθμοι απαιτούν εξίσου διαφορετικά μήκη κλειδιών για είναι εφικτό το ίδιο επίπεδο ανθεκτικότητας κρυπτογράφησης. Ένας συμμετρικός αλγόριθμος με μέγεθος κλειδιού 128 bit παρέχει ανθεκτικότερη κρυπτογράφηση από τον αλγόριθμο δημοσίου κλειδιού RSA με ίδιο μήκος κλειδιού. Για να αποδειχθεί ανθεκτική μια κρυπτογράφηση του RSA πρέπει να χρησιμοποιηθεί κλειδί μεγέθους τουλάχιστον 512 bit, ενώ ένας συμμετρικός αλγόριθμος επιτυγχάνει περίπου το ίδιο επίπεδο ανθεκτικότητας με μέγεθος κλειδιού 64 bit. Γενικότερα, αλγόριθμοι δημοσίου κλειδιού υπολογίζουν και κάνουν χρήση κρυπτογραφικών κλειδιών μεγάλου μήκους, για να πετύχουν το επιθυμητό επίπεδο ασφάλειας. Αξιοσημείωτο είναι πως, ο χρόνος ζωής του

ζεύγους κλειδιών μιας μη-συμμετρικής κρυπτογράφησης θεωρείται περισσότερος από τον αντίστοιχο του μυστικού κλειδιού.

2.4 Κρυπτογράφηση υλικού (hardware) και κρυπτογράφηση λογισμικού (software)

Τα κρυπτογραφικά συστήματα διαχωρίζονται σε συστήματα που εφαρμόζονται, υλοποιούνται και υποστηρίζονται από κατασκευασμένο με συγκεκριμένες προδιαγραφές υλικό (hardware), είναι αυτό που ονομάζουμε Hardware Encryption, και αντίστοιχα σε συστήματα λογισμικού (software), όπου στην ορολογία καταγράφεται ως Software Encryption.

Λίγα χρόνια πριν, σχεδόν όλα τα προϊόντα κρυπτογράφησης ήταν υπό μορφή εξειδικευμένου hardware. Όλα αυτά τα πακέτα κρυπτογράφησης ήταν συνδεδεμένα με το δίκτυο επικοινωνίας του συστήματος και κρυπτογραφούσαν όλα τα δεδομένα που μεταφέρονταν εντός αυτής της σύνδεσης. Σήμερα, τα συστήματα κρυπτογράφησης λογισμικού, συμβαδίζοντας με την νέα τεχνολογία, καταγράφονται συνεχώς ως επικρατέστερα, ενώ τα συστήματα υλικού έχουν κυρίως χρήση σε υψηλού επιπέδου ασφάλειας εφαρμογές (εμπορικές εφαρμογές, συστήματα εθνικής άμυνας). Οποιοσδήποτε αλγόριθμος κρυπτογράφησης μπορεί να εφαρμοστεί στο λογισμικό ενός συστήματος, ενώ είναι εφικτή και η ενσωμάτωση τους σε μεγαλύτερες εφαρμογές, όπως για παράδειγμα τα προγράμματα (εφαρμογές) επικοινωνιών.

Ένα χαρακτηριστικό που διαχωρίζει τους δύο τύπους συστημάτων κρυπτογράφησης είναι η ταχύτητα. Παρόλο που μερικοί επιστήμονες έχουν προσπαθήσει να κάνουν τους πιο κοινούς αλγόριθμους καταλληλότερους και ταχύτερους σε εφαρμογές λογισμικού, η hardware κρυπτογράφηση αναδεικνύεται ως η καλύτερη επιλογή σε θέματα ταχύτητας.

Η δεύτερη διαφοροποίηση τους είναι το επίπεδο ασφάλειας που προσφέρουν. Ένας αλγόριθμος κρυπτογράφησης που υλοποιείται σε έναν υπολογιστή προφανώς δεν έχει καμία φυσική προστασία. Κάποια εξουσιοδοτημένη οντότητα μπορεί να εισέλθει στο σύστημα με την αφορμή διόρθωσης ή επεξεργασίας κάποιων εργαλείων και να τροποποιήσει τον αλγόριθμο χωρίς να το αντιληφθεί κανένας. Οι συσκευές υλικού μπορεί να είναι διασφαλισμένες πως δεν υφίσταται τέτοιος κίνδυνος παραποίησης του συστήματος. Ένα πακέτο hardware κρυπτογράφησης είναι πιο εύκολο να αποτρέψει μια τέτοια διαδικασία. Σε μια τέτοια περίπτωση, ένα πλήρως εξειδικευμένο υλικό έχει ενσωματωμένη κάποια χημική ουσία και είναι με τέτοιο τρόπο κατασκευασμένο ώστε οποιαδήποτε προσπάθεια για προσέγγιση στο εσωτερικό του να οδηγήσει στην καταστροφή

του. Η software κρυπτογράφηση προορίζεται κυρίως για να προστατεύσουν οι χρήστες τα μεμονωμένα αρχεία των συστημάτων τους.

Η ηλεκτρομαγνητική ακτινοβολία μπορεί μερικές φορές να αποκαλύψει τι μεταδίδεται μέσα στο πλαίσιο του ηλεκτρονικού εξοπλισμού. Τα υψηλής τεχνολογίας συστήματα κρυπτογράφησης προσφέρουν την διαβεβαίωση ότι δεν διαρρέει καμία πληροφορία. Η κρυπτογράφηση λογισμικού ενδεχομένως δεν έχει τέτοιου είδους δυνατότητα χωρίς ίσως την υποστήριξη κάποιου hardware. Αντίθετα, είναι σημαντικό να είναι πρώτα από όλα το βασικό διοικητικό σχέδιο ασφαλές για να θεωρηθεί μια κρυπτογραφική εφαρμογή λειτουργική.

Ένας άλλος λόγος για την επικράτηση της hardware κρυπτογράφησης είναι η ευκολία της εγκατάστασης. Οι περισσότερες εφαρμογές κρυπτογράφησης δεν περιλαμβάνουν τους υπολογιστές γενικής χρήσης. Συχνά δημιουργείται η επιθυμία να κρυπτογραφηθούν οι τηλεφωνικές συνομιλίες ή τα δεδομένα μιας επικοινωνίας. Είναι φτηνότερο και πιο πρακτικό να εγκαταστήσει κάποιος το ειδικό υλικό κρυπτογράφησης σε μια τηλεφωνική συσκευή ή κάποιο modem, από την εγκατάσταση ενός μικροεπεξεργαστή αλλά και του κατάλληλου λογισμικού. Η κρυπτογράφηση λογισμικού αντιπαραθέτει ως πλεονέκτημα την ευκολία στην διαδικασία βελτίωσης της.

Τα τρία βασικά είδη hardware encryption που διοχετεύονται στην αγορά σήμερα είναι: Ανεξάρτητα μοντέλα κρυπτογράφησης (υποστηρίζουν λειτουργίες όπως πιστοποίηση κωδικού πρόσβασης και διαχείριση κρυπτογραφικών κλειδιών κυρίως για εφαρμογή σε τραπεζικά συστήματα), πακέτα κρυπτογράφησης για συνδέσεις επικοινωνιών και ειδικό υλικό (hardware) για εγκατάσταση και σύνδεση με προσωπικούς υπολογιστές. Σήμερα όλο και περισσότερες επιχειρήσεις αρχίζουν να εγκαθιστούν hardware κρυπτογράφηση στον εξοπλισμό των καναλιών επικοινωνίας τους.

3. Συμμετρική Κρυπτογράφηση

3.1 Εισαγωγή

Όπως προαναφέρθηκε, το σύστημα της **συμμετρικής κρυπτογράφησης** είναι η διαδικασία υλοποίησης κάποιων τεχνικών κρυπτογραφίας που ονομάζονται **αλγόριθμοι μυστικού κλειδιού** ή **συμμετρικοί αλγόριθμοι** (symmetric algorithms). Κατά την διαδικασία αυτή, το ίδιο κρυπτογραφικό κλειδί (μυστικό κλειδί) κρυπτογραφεί και αποκρυπτογραφεί τις πληροφορίες σε μια συγκεκριμένη επαφή μεταξύ δύο υπολογιστών ή στην προσπάθεια εξασφάλισης της ακεραιότητας των δεδομένων ενός αρχείου. Ο συμμετρικός αλγόριθμος δημιουργεί ένα συγκεκριμένο κλειδί, κρυπτογραφεί με αυτό το αρχικό κείμενο και στέλνει στον παραλήπτη το αποτέλεσμα της κρυπτογράφησης, είτε αποθηκεύει το κρυπτογραφημένο κείμενο για μελλοντική του ανάκτηση και επεξεργασία, όταν πρόκειται για ένα αρχείο του συστήματος. Κάθε διαφορετικός αλγόριθμος δημιουργεί με διαφορετικό τρόπο το κλειδί, πράγμα που θα δούμε λεπτομερειακά παρακάτω. Όταν ο παραλήπτης θελήσει να αποκρυπτογραφήσει το chipertext, χρησιμοποιεί το ίδιο κλειδί που είτε το γνώριζε πριν ακόμα λάβει το μήνυμα, είτε το δέχθηκε από κάποιο ασφαλές κανάλι επικοινωνίας.

Όπως είναι φυσικό, η ασφάλεια ενός συμμετρικού αλγορίθμου εξαρτάται κυρίως από την προστασία του ενός και μοναδικού κλειδιού από ενδεχόμενη υποκλοπή του. Σημείο αναφοράς εδώ είναι η καλή διαχείριση του κρυπτογραφικού κλειδιού (key management). Γενικότερα, ένας συμμετρικός αλγόριθμος κρυπτογραφεί δεδομένα μεγάλου μέγεθος και αυτό έχει να κάνει με την ικανοποιητικά μεγάλη ταχύτητα με την οποία μετατρέπει τα αρχικά δεδομένα.

Στη ορολογία της κρυπτογράφησης συναντάται συχνά ο όρος **cipher**, ως ο μαθηματικός τύπος του αλγόριθμου που υλοποιεί μια κρυπτογραφημένη επικοινωνία, αλλά και όχι μόνο. Γενικότερα υπάρχουν δύο βασικοί τύποι συμμετρικών αλγορίθμων: τα **block ciphers** και τα **stream ciphers**. Τα block ciphers λειτουργούν πάνω σε κομμάτια (blocks) του αρχικού και του κρυπτογραφημένου κειμένου κάθε φορά. Συνήθως, τα κομμάτια αυτά έχουν μέγεθος 64 bits αλλά μερικές φορές μπορεί να είναι και μεγαλύτερα. Τα stream ciphers λειτουργούν πάνω ένα bit ή ένα byte των δεδομένων κάθε φορά που κρυπτογραφούν.

Με ένα block cipher, το ίδιο κομμάτι ενός plaintext θα κρυπτογραφείται πάντα σε ένα ίδιο κομμάτι ciphertext, χρησιμοποιώντας φυσικά το ίδιο κλειδί. Αντίθετα, με ένα stream cipher, το ίδιο byte plaintext θα κρυπτογραφείται σε ένα διαφορετικό byte κάθε φορά που χρησιμοποιείται ο συμμετρικός κρυπτογραφικός αλγόριθμος.

Σημείο αναφοράς της ορολογίας είναι και το **cryptographic mode** ,ο τρόπος κρυπτογράφησης ή αλλιώς το σύνολο των λειτουργιών της όλης διαδικασίας. Ένα κρυπτογραφικό mode (τρόπος) συνήθως συνδυάζει το βασικό cipher, τον συμμετρικό αλγόριθμο δηλαδή, με κάποιο είδος ανατροφοδότησης και μερικές απλές λειτουργίες. Οι λειτουργίες αυτές είναι απλές επειδή η ασφάλεια είναι μια ευθύνη της εφαρμογής του αλγορίθμου. Για αυτόν τον λόγο, υπάρχουν κάποια συγκεκριμένα πρότυπα ασφάλειας. Το περιεχόμενο του κειμένου που θα δεχθεί την κρυπτογράφηση πρέπει να παραμείνει μυστικό. Η διαδικασία εισαγωγής του κατά την διάρκεια εφαρμογής του αλγόριθμου θα πρέπει να γίνεται με τυχαία σειρά. Τέλος, η κρυπτογράφηση περισσότερων από ενός μηνυμάτων με το ίδιο κλειδί πρέπει να καταστεί δυνατή.

Σε κάποιες περιπτώσεις, σημαντική θεωρείται και η επιθυμητή ανοχή σε ελαττώματα. Κάποιες εφαρμογές πρέπει να είναι σε θέση να παραλληλίσουν κρυπτογράφηση ή αποκρυπτογράφηση, ενώ άλλες πρέπει να είναι σε θέση να προεπεξεργαστούν τα δεδομένα όσο αυτό φυσικά είναι πιθανό. Ακόμα, είναι σημαντικό η διαδικασία αποκρυπτογράφησης να είναι σε θέση ανακτήσει χαρακτήρες του ciphertext , από λάθος bits είτε από bits που προστέθηκαν κατά την μετάδοση του μέσα από ένα κανάλι επικοινωνίας, συνήθως από ένα δίκτυο. Διαφορετικά modes έχουν διαφορετική επεξεργασία και υλοποίηση όλων αυτών των χαρακτηριστικών.

Ένα ηλεκτρονικό codebook (ECB) είναι ο προφανέστερος τρόπος να χρησιμοποιήσει κάποιος ένα block cipher. Ένα κομμάτι των αρχικών δεδομένων κρυπτογραφείται και έχει ως έξοδο ένα κομμάτι κρυπτογραφημένο κείμενο. Εάν από θεωρητικής πλευράς, το ίδιο κομμάτι του plaintext μετατρέπεται κάθε φορά στο ίδιο περιεχόμενο του chipertext, προφανής είναι και η δημιουργία ενός βιβλίου (codebook) των αρχικών δεδομένων και της αντιστοιχίας τους σε κρυπτογραφημένους χαρακτήρες. Πρακτικά, εάν το μέγεθος του κειμένου είναι 64 bits τότε θα αντιστοιχούν σε αυτό 2^{64} καταχωρήσεις. Είναι λοιπόν αδύνατον να υπολογιστούν εκ των πρότερων και να αποθηκευτούν όλες αυτές οι καταχωρήσεις. Μην ξεχνάμε πως για κάθε διαφορετικό κλειδί πρέπει να υφίσταται και διαφορετικό codebook.

Κάθε block του plaintext κρυπτογραφείται ανεξάρτητα και όχι με γραμμικό τρόπο. Μπορούμε δηλαδή να κρυπτογραφήσουμε πρώτα δέκα κομμάτια στη μέση του κειμένου, στην συνέχεια τα κομμάτια στο τέλος του και έπειτα αυτά στην αρχή του. Αυτό είναι σημαντικό για τα κρυπτογραφημένα αρχεία που προσεγγίζονται τυχαία, όπως για παράδειγμα μια βάση δεδομένων. Στην πραγματικότητα, κάθε κομμάτι του κειμένου μπορεί να εξεταστεί ως χωριστό μήνυμα, κρυπτογραφημένο με το ίδιο κλειδί.

Ένα λάθος bit σε ένα ciphertext, όταν αυτό αποκρυπτογραφείται, ενδεχομένως να προκαλέσει ανακρίβεια στην ανάκτηση του αρχικού block αλλά σίγουρα δεν θα έχει επιπτώσεις στα υπόλοιπα. Εντούτοις, εάν ένα bit του ciphertext χάνεται

τυχαία ή προστίθεται κάποιο άλλο, όλα τα επόμενα κομμάτια θα αποκρυπτογραφηθούν ανακριβώς, εκτός φυσικά αν υπάρχει κάποια δομή πλαισίων για να ευθυγραμμίσει και να ορίσει εκ νέου τα όρια φραγμών των blocks.

Συνήθως τα μηνύματα δεν διαιρούνται ομοιόμορφα σε κομμάτια των 64 bits. Αυτό έχει ως αποτέλεσμα να υπάρχει ένα μικρότερο κομμάτι στο τέλος. Πριν κρυπτογραφηθεί το block υφίσταται μια διαδικασία γεμίσματος με μηδενικά ή κενούς χαρακτήρες ώστε να έχει ίσο μέγεθος με τα υπόλοιπα. Στην συνέχεια κρυπτογραφείται κανονικά όπως όλα τα blocks του κειμένου. Μετά την ενέργεια ανάκτησης των δεδομένων, οι μηδενικοί χαρακτήρες σβήνονται και έτσι παραμένει αναλλοίωτο το περιεχόμενο των δεδομένων.

Ας δούμε την ανάλυση των block ciphers με την βοήθεια της επιστήμης των μαθηματικών. Μην ξεχνάμε πως το πλαίσιο πάνω στο οποίο αναπτύχθηκε η κρυπτογράφηση είναι η λογική των μαθηματικών όρων και κανόνων. Παρακάτω δίνεται η εξισωτική μορφή της διαδικασίας που ακολουθεί ένα block cipher. Το πιο σημαντικό στοιχείο σε μια τέτοια προσπάθεια είναι σαφώς το κρυπτογραφικό κλειδί που εδώ θα το ορίσουμε ως K. Το κλειδί σε κάθε περίπτωση θα κάνει λήψη τιμών από ένα υποσύνολο τιμών $V_K = \{K_1 ... K_i\}$. Θεωρητικά, το κρυπτογραφικό κλειδί υπολογίζεται επιλέγοντας τιμές από αυτό το υποσύνολο. Για κάθε block του plaintext ορίζεται ένα σταθερό μέγεθος της τάξης των n bits. Έχει ήδη αναφερθεί πως το σύνηθες μέγεθος είναι 64 bits. Έτσι εάν ορίσουμε το plaintext P με f blocks τότε το σύνολο των blocks θα είναι: P_1, $P_2 ... P_f$. Η διαδικασία κρυπτογράφησης E θα είναι : $E_K(P) = C$ με την παραγωγή κάθε block σε chipertext ,ειδικότερα, να δίνεται από την εξίσωση : $E_K(P_f) = C_f$, όπου ως C_f ορίζεται κάθε κομμάτι κρυπτογραφημένο κείμενο (chipertext). Η ενέργεια ανάκτησης του κειμένου (αποκρυπτογράφηση), σύμφωνα με τα παραπάνω φαίνεται στον τύπο : $D_K (C_f) = P_f$. Εδώ το D χαρακτηρίζει την διαδικασία αποκρυπτογράφησης.

Υποσύνολο κρυπτογραφικών κλειδιών:
$V_K = \{K_1 ... K_i\}$.
Όπου K το κλειδί του αλγορίθμου.

Κρυπτογράφηση:
$E_K(P_f) = C_f$.
Όπου, κρυπτογράφηση : E_K ,
blocks του plaintext : P_f ,
blocks του chipertext : C_f .

Αποκρυπτογράφηση:
$D_K(C_f) = P_f$
Όπου, αποκρυπτογράφηση : D_K ,
blocks του plaintext : P_f ,
blocks του chipertext : C_f .

Από τους πολλούς συμμετρικούς αλγόριθμους και ειδικότερα από τα block ciphers που είναι διαθέσιμα σήμερα, περισσότερη σημασία σε αυτή την ενότητα θα δοθεί σε αυτούς με την μεγαλύτερη ακτινοβολία, το εντονότερο ιστορικό ενδιαφέρον και αυτούς που έχουν υποστεί την μεγαλύτερη ανάλυση. Αυτό δεν σημαίνει φυσικά πως αυτοί οι συγκεκριμένοι αλγόριθμοι είναι και οι ασφαλέστεροι όλων. Έμφαση θα δοθεί και σε εκείνους με το μεγαλύτερο πρακτικό ενδιαφέρον και της πιο συχνής εφαρμογής τους. Πρέπει επίσης να σημειωθεί πως μετά την ανάπτυξη της καινούργιας φιλοσοφίας που εισήγαγαν οι αλγόριθμοι δημοσίου κλειδιού, οι συμμετρικοί αλγόριθμοι αντανακλούν ολοένα και περισσότερο το ιστορικό ενδιαφέρον των αναλυτών που ασχολούνται με την κρυπτογραφία.

Ασφάλεια των block ciphers

Όσον αφορά τις πρακτικές ασφάλειας, λαμβάνοντας υπόψη και την πολυπλοκότητα των επιθέσεων, καθορίζεται ο βασικός στόχος ενός block cipher. Ο αντικειμενικός αυτός στόχος είναι να παρέχει εμπιστευτικότητα των δεδομένων στους πόρους του συστήματος, οι οποίοι διαχειρίζονται τη διαδικασία κρυπτογράφησης. Ο αντίστοιχος στόχος ενός αντίπαλου είναι να ανακτήσει το plaintext εφόσον έχει στην κατοχή του το ciphertext. Ένας συμμετρικός αλγόριθμος μπορούμε να πούμε πως σπάει ολοκληρωτικά όταν γίνει γνωστό το κλειδί του σε μη εξουσιοδοτημένες οντότητες. Από πρακτικής όμως πλευράς, ένας αλγόριθμος σπάει εάν ένας αντίπαλος είναι σε θέση να ανακτήσει μέρος του αρχικού κειμένου από το ciphertext, χωρίς τη γνώση του κρυπτογραφικού κλειδιού.

Για την αντικειμενική αξιολόγηση της παρεχόμενης ασφάλειας ενός block cipher, γίνεται πάντα η υπόθεση πως ένας μη εξουσιοδοτημένος πόρος:

- έχει πρόσβαση σε όλα τα στοιχεία που διαβιβάζονται μέσα από το κανάλι επικοινωνίας και,
- γνωρίζει όλες τις λεπτομέρειες της διαδικασίας κρυπτογράφησης, εκτός από το μυστικό κρυπτογραφικό κλειδί, αφού επάνω του στηρίζεται εξ ολόκληρου η ασφάλεια του αλγορίθμου.

Το πιο αποτελεσματικό διαθέσιμο μέτρο ασφάλειας των συμμετρικών αλγορίθμων είναι η πολυπλοκότητα των πιο μεθοδικών και περισσότερο χρησιμοποιημένων επιθέσεων. Διάφορες πτυχές της πολυπλοκότητας μπορούν να διακριθούν στα παρακάτω:

1. Πολυπλοκότητα των στοιχείων, είναι ο αναμενόμενος αριθμός από μονάδες δεδομένων εισόδου, που απαιτούνται στην διαδικασία μιας επίθεσης. (π.χ., κομμάτια από το ciphertext).
2. Πολυπλοκότητα αποθήκευσης, είναι αναμενόμενος αριθμός από μονάδες αποθήκευσης που απαιτούνται κατά την διάρκεια της επίθεσης.

3. Πολυπλοκότητα επεξεργασίας, είναι ο αναμενόμενος αριθμός διαδικασιών που απαιτούνται για την επεξεργασία των δεδομένων που αποτέλεσαν την είσοδο και για την αποθήκευση τους σε αρχεία. Πρακτικά, υπολογίζεται σε μονάδα χρόνου ανά μονάδα αποθήκευσης.

Όλα τα παραπάνω προφανώς αποσκοπούν στην πολυπλοκότητα της επίθεσης σε έναν συμμετρικό αλγόριθμο. Η επεξεργασία της πολυπλοκότητας μπορεί να είναι διαιρεμένη σε πολλές διαδικασίες, χωρίς όμως να μειωθεί, μειώνοντας κατά αυτό τον τρόπο το χρόνο που απαιτείται για μια επίθεση.

Λαμβάνοντας υπόψη μια πολυπλοκότητα στοιχείων μεγέθους 2^n , μια επίθεση θα είναι πάντα δυνατή. Όλα αυτά όμως τα διαφορετικά κομμάτια των n bits, σε συνδυασμό με ένα κλειδί σταθερού μήκους k-bit, χαρακτηρίζει τη λειτουργία της κρυπτανάλυσης εξοντωτική για μια μη εξουσιοδοτημένη οντότητα. Ομοίως, λαμβάνοντας υπόψη μια πολυπλοκότητα επεξεργασίας 2^k , μια επίθεση είναι δυνατή μόνο στο πλαίσιο της χρονοβόρας αναζήτησης του μυστικού κλειδιού.

Κατά συνέπεια ως ελάχιστη απαίτηση, το αποτελεσματικό μέγεθος ενός κρυπτογραφικού κλειδιού πρέπει να είναι τόσο μεγάλο, για να αποκλείσει μια εξαντλητική αναζήτηση από έναν αντίπαλο. Παράλληλα, το μέγεθος των blocks απαιτείται να είναι τέτοιο, ώστε να αποκλείσει ή να καταστήσει ανέφικτη μια εξοντωτική ανάλυση των δεδομένων (ciphertext). Ένα block cipher θεωρείται λοιπόν υπολογιστικά ασφαλής, εάν αυτοί οι όροι είναι πρακτικά υλοποιήσιμοι, ορίζοντας παράλληλα ως εφικτή και την πολυπλοκότητα της επεξεργασίας όπως αυτή αναλύθηκε παραπάνω.

3.2 Αλγόριθμος DES

Ιστορική Αναδρομή

Ο **DES** (Data Encryption Standard) είναι ο πιο γνωστός συμμετρικός αλγόριθμος στην ιστορία της κρυπτογράφησης καθορισμένος από το Αμερικανικό Πρότυπο FIPS 46–2. Αναγνωρισμένο παγκοσμίως block cipher όπου αναπτύχθηκε στα μέσα της δεκαετίας του '70 και αποτελούσε πρότυπο για σχεδόν 20 χρόνια. Αν και ομολογουμένως φαίνονται τα σημάδια της «μεγάλης ηλικίας» του, έχει αντέξει στην κρυπτολογική ανάλυση με εντυπωσιακά αποτελέσματα. Θεωρείται και είναι ακόμα ασφαλής απολαμβάνοντας την πιο διαχρονική και εμπορικότερη εφαρμογή στα κρυπτογραφικά συστήματα.

Στις αρχές της δεκαετίας του '70, η μη στρατιωτική κρυπτογραφική έρευνα και ανάπτυξη ήταν τυχαία. Σχεδόν καμία ερευνητική εργασία και προσπάθεια δεν είχε δημοσιευθεί. Οι περισσότεροι ερευνητές ήξεραν ότι η στρατιωτική ηγεσία

χρησιμοποιούσε κάποιον ειδικό εξοπλισμό κωδικοποίησης ως βασικό συστατικό της Εθνικής Ασφάλειας, αλλά λίγοι μπορούσαν να κατανοήσουν την επιστήμη του συστήματος της κρυπτογραφίας.

Διάφορες μικρές επιχειρήσεις πουλούσαν κρυπτογραφικό εξοπλισμό, κυρίως στις κυβερνήσεις των αναπτυγμένων κρατών. Τα χαρακτηριστικά των εξοπλισμών αυτών είχαν μηδαμινές ομοιότητες μεταξύ τους με αποτέλεσμα να μην υποστηρίζεται ούτε η εγκατάσταση καναλιών επικοινωνίας. Κανένας δεν γνώριζε πραγματικά την ασφάλεια που μπορούσαν να παρέχουν αυτά τα συστήματα, καθώς δεν υπήρχε κάποια ανεξάρτητη οντότητα για να τα πιστοποιήσει.

Το 1972, το **Εθνικό Ίδρυμα Προτύπων** (NBS), άρχισε μια προσπάθεια σχεδίασης ενός προγράμματος που θα προστατεύει τα υπολογιστικά και επικοινωνιακά δεδομένα. Ως τμήμα εκείνου του προγράμματος, θέλησαν να αναπτύξουν έναν ενιαίο και τυποποιημένο κρυπτογραφικό αλγόριθμο. Κύριος στόχος της δημιουργίας ενός αλγορίθμου ήταν η πεποίθηση πως θα μπορούσε να επικυρωθεί και να προσφέρει παράλληλα στον κρυπτογραφικό εξοπλισμό που χρησιμοποιούνταν διόδους επικοινωνίας.

Το Μάιο του 1973 το NBS εξέδωσε ένα δημόσιο αίτημα για καταγραφή ερευνητικών προτάσεων ανάπτυξης ενός κρυπτογραφικού αλγορίθμου. Στο περιεχόμενο του υπήρχε και μια σειρά από κριτήρια σχεδίασης. Σύμφωνα με αυτά ο αλγόριθμος έπρεπε :

- ✓ να παρέχει ένα υψηλό επίπεδο ασφάλειας,
- ✓ να είναι κατανοητός,
- ✓ να είναι διαθέσιμος στο σύνολο των χρηστών,
- ✓ να μπορεί να προσαρμοστεί και να υποστηρίζει διαφορετικές εφαρμογές,
- ✓ η διαδικασία εφαρμογής και εκτέλεσης του να είναι οικονομικά αποδεκτή,
- ✓ να είναι αποδοτικός,
- ✓ να είναι σε θέση να επικυρωθεί.

Όσον αναφορά την επιθυμητή ασφάλεια του αλγορίθμου έπρεπε να :

- ✓ εξαρτάται αποκλειστικά και μόνο από την μυστικότητα του κρυπτογραφικού κλειδιού,
- ✓ και όχι από την μυστικότητα του ίδιου του αλγορίθμου.

Η αντίδραση που υπήρξε απέδειξε μεν το ιδιαίτερο ενδιαφέρον για τα ανασφαλή τότε κρυπτογραφικά πρότυπα, αλλά η πείρα των ερευνητών δεν επαρκούσε με αποτέλεσμα καμία πρόταση να μην καλύπτει τις απαιτήσεις.

Τον Αυγούστου του 1974 μετά από μια δεύτερη προτροπή του NBS, εμφανίστηκε μια ελπιδοφόρα πρόταση. Ένας αλγόριθμος βασισμένος σε μία ερευνητική ανάπτυξη και εφαρμογή της IBM, που αναπτύχθηκε στις αρχές της δεκαετίας του '70, γνωστή τότε ως Lucifer. Ο αλγόριθμος, αν και περίπλοκος, χρησιμοποιούσε απλές λογικές διαδικασίες σε ομάδες από bits και μπορούσε να εφαρμοστεί αποτελεσματικά. Το NBS ζήτησε τη βοήθεια της **Αντιπροσωπείας**

Εθνικής Ασφάλειας (NSA) για την αξιολόγηση του αλγορίθμου και τον καθορισμό της καταλληλότητας του ως ομοσπονδιακό πρότυπο. Η IBM είχε ήδη εξαγγείλει δίπλωμα ευρεσιτεχνίας, αλλά ήταν πρόθυμη να διαθέσει τα πνευματικά δικαιώματα σε άλλους για το περιθώριο της κατασκευής και μελλοντικής χρήσης του αλγορίθμου.

Τον Μαρτίου 1975, το NBS δημοσίευσε τις λεπτομέρειες του τρόπου σχεδίασης του αλγορίθμου καθώς και την δήλωση της IBM για χορήγηση άδειας ελεύθερης χρήσης και επεξεργασίας του. Πολλοί χρήστες και κυρίως αναλυτές ήταν ανήσυχοι για την πιστοποίηση του αλγόριθμου καθώς οι τροποποιήσεις της NSA είχαν μειώσει το μέγεθος του κλειδιού από τα 128 bits σε 56-bits. Πολλές από αυτές τις αλλαγές έγιναν σαφείς αργότερα, στην δεκαετία του '90. Στην προσπάθεια αξιολόγησης του προτεινόμενου προτύπου το NBS διοργάνωσε μια επίσημη συνάντηση. Οι σχεδιαστές, κάποιοι αναλυτές και οι προμηθευτές του εξοπλισμού ανέλυσαν τον αλγόριθμο από μαθηματικής οπτικής, ενώ εκφράστηκε η δυνατότητα και η ανάγκη για αύξηση του μήκους του κρυπτογραφικού κλειδιού.

Τελικά, ο αλγόριθμος **DES** (Data Encryption Standard), έτσι όπως ονομάστηκε, υιοθετήθηκε ως ομοσπονδιακό πρότυπο τον Νοεμβρίου του 1976 και εξουσιοδοτήθηκε για χρήση σε όλες τις επικοινωνίες σε κυβερνητικό επίπεδο. Η επίσημη έκθεση για την περιγραφή του προτύπου δημοσιεύθηκε τον Ιανουαρίου του 1977. Τα επόμενα χρόνια εκδόθηκαν αρκετά συγγράμματα για τον λεπτομερέστερο τρόπο λειτουργίας του, καθώς και οδηγίες για την εφαρμογή του.

Όλες αυτές οι ενέργειες ήταν κάτι το πρωτοφανές για την εποχή εκείνη. Δικαιολογημένα κάποιες στιγμές υπήρχε έντονη η ανησυχία για την αποτελεσματικότητα όλων αυτών των διαδικασιών. Η ιστορία όμως δικαίωσε απόλυτα εκείνη την προσπάθεια, αφού ο DES έχει αντικρούσει την κρυπτολογική ανάλυση για πάνω από 2 δεκαετίες, ενώ αποτελεί ακόμα και τώρα μια από τις σημαντικότερες τεχνικές μυστικού κλειδιού των κρυπτογραφικών συστημάτων.

Περιγραφή του DES

Ο DES είναι ένα block cipher και κρυπτογραφεί δεδομένα σε κομμάτια των 64 bits. Αυτό σημαίνει ότι κρυπτογράφηση και αποκρυπτογράφηση έχουν ως έξοδο blocks τού ίδιου μεγέθους (64 bits). Βασικό χαρακτηριστικό του είναι πως ανήκει στην κατηγόρια των συμμετρικών αλγορίθμων. Είναι ο συμμετρικός αλγόριθμος με την μεγαλύτερη ιστορική σημασία. Παράγει ένα κρυπτογραφικό, μυστικό κλειδί το οποίο χρησιμοποιείται τόσο για να κρυπτογραφήσει όσο και να ανακτήσει δεδομένα. Το μήκος του κλειδιού είναι 56 bits, μπορεί να είναι οποιοσδήποτε αριθμός και μπορεί να αλλάξει οποιαδήποτε στιγμή. Συνήθως το κλειδί χαρακτηρίζεται ως ένας αριθμός των 64 bits αλλά κάθε όγδοο bit χρησιμοποιείται για τον έλεγχο ισότητας, για αυτό και αγνοείται.

Στο απλούστερο επίπεδό του, ο αλγόριθμος δεν είναι τίποτα περισσότερο από ένας συνδυασμός των δύο βασικών τεχνικών κρυπτογράφησης, την **διάχυση** (diffusion) και την **σύγχυση** (confusion). Με την διάχυση κάθε ψηφίο του αρχικού κειμένου επεκτείνεται και παράγει πολλά ψηφία με σκοπό την απόκρυψη των στατιστικών χαρακτηριστικών του κάθε block, έτσι ώστε να τα μηδενίσει. Η διαδικασία της σύγχυσης έχει και αυτή σημείο αναφοράς τα ενδεχόμενα στατιστικά χαρακτηριστικά των blocks, εφόσον είναι το πλαίσιο πάνω στο οποίο βασίζεται η κρυπτανάλυση. Με την τεχνική της σύγχυσης χρησιμοποιούνται κάποιοι κρυπτογραφικοί μετασχηματισμοί, που θα δούμε αναλυτικά, οι οποίοι περιπλέκουν την σχέση μεταξύ των στατιστικών στοιχείων του αρχικού κειμένου και του chipertext.

Η θεμελιώδης διαδικασία του DES σε κάθε block, είναι ένα ενιαίος συνδυασμός αυτών των τεχνικών πάνω στο κείμενο χρησιμοποιώντας απλές αριθμητικές και λογικές πράξεις. Κάθε τέτοια ενέργεια στηρίζεται φυσικά στο κλειδί, ενώ είναι γνωστή ως **κύκλος**. Ο DES έχει 16 κύκλους, εφαρμόζει δηλαδή αυτό τον συνδυασμό σε κάθε block του plaintext 16 φορές.

Κάθε κομμάτι των 64 bits που αποτελεί είσοδο, μετά από μια αρχική μεταλλαγή διασπάται σε δυο ισομερή μικρότερα κομμάτια των 32 bits. Το ένα μέρος περιέχει τα πρώτα 32 bits του block και το άλλο τα υπόλοιπα. Στην συνέχεια, υλοποιείται μία μαθηματική συνάρτηση f, η οποία εφαρμόζεται σε 16 **κύκλους** των ίδιων διαδικασιών. Τα δεδομένα, σε κάθε τέτοια εφαρμογή, μετασχηματίζονται με βάση τις τιμές που παίρνει το κλειδί. Μετά τον δέκατο έκτο κύκλο τα δυο μέρη ενώνονται και με μια τελική μεταλλαγή, ως αντιστοιχία της αρχικής, ολοκληρώνεται η διαδικασία κρυπτογράφησης. Η αρχική μεταλλαγή εφαρμόζεται στο block που εισάγεται κάθε φορά στη διαδικασία κρυπτογράφησης. Αυτή η μεταλλαγή και η αντίστοιχη τελική δεν έχουν επιπτώσεις στην ασφάλεια του DES. Σκοπός τους είναι να γίνει ευκολότερη η εισαγωγή των δεδομένων του plaintext και του ciphertext στον αλγόριθμο, με την μορφή ταξινομημένων σε bytes κομματιών.

Για να γίνει πιο κατανοητή η σαφώς ιδιαίτερη λειτουργία του αλγορίθμου καθώς και να καταγραφούν πρακτικά οι λειτουργίες του, δίνονται παρακάτω οι μαθηματικοί τύποι σύμφωνα με τους οποίους υλοποιείται η κρυπτογράφηση.

$L_{i+1} = R_i$
$R_{i+1} = L_i \text{ XOR } f(R_i, K_{i+1})$

Όπου για i= 1 έως 16 ,
L_i : Το αριστερό (πρώτο) κομμάτι του αρχικού block.
R_i : Το δεξιό (δεύτερο) κομμάτι στο οποίο διασπάται το αρχικό block.
L_{i+1}, R_{i+1} : Τα επόμενα κομμάτια που δημιουργούνται από την διαδικασία.
K_{i+1} : Το κρυπτογραφικό κλειδί του αλγορίθμου.
XOR : Διαδικασία συνδυασμού (not or)

f : Η συνάρτηση που συνδυάζει το δεξιό κομμάτι του αρχικού block με το κρυπτογραφικό κλειδί. Οι λειτουργίες που επιτελεί η συνάρτηση f είναι :

1. **Μεταλλαγή συμπίεσης** (compression permutation), κατά την οποία τα bits του κλειδιού K_{i+1} μετατοπίζονται και επιλέγονται τελικά τα 48 από τα 56.
2. **Μεταλλαγή επέκτασης** (expansion permutation), κατά την οποία το κομμάτι των αρχικών δεδομένων R_i επεκτείνεται στα 48 bits.
3. **Αντικατάσταση S-Box** (S-box substitution), κατά την οποία το K_{i+1} και το R_i συνδυάζονται με ένα XOR και το αποτέλεσμα συμπιέζεται σε ένα block μεγέθους 32 bits. Αυτές οι τρεις λειτουργίες αναλύονται λεπτομερέστερα παρακάτω.

Στον πίνακα που δίνεται καταγράφονται όλοι οι πιθανοί συνδυασμοί από bits του L_i και της f καθώς και το αποτέλεσμα που θα δώσει το XOR :

L_i	0	0	1	1
f	0	1	0	1
XOR	**1**	**0**	**0**	**0**

1. **Μεταλλαγή συμπίεσης** (compression permutation).

Όπως αναφέρθηκε το κρυπτογραφικό κλειδί είναι ένας αριθμός μεγέθους 64 bits. Κατά την διάρκεια της εφαρμογής του αλγορίθμου κάθε όγδοο bit αγνοείται μειώνοντας έτσι το κλειδί του DES στα 56 bits. Αργότερα, αυτά τα bits χρησιμεύουν ως έλεγχος ισότητας για να εξασφαλιστεί ότι το κλειδί δεν περιέχει λάθος χαρακτήρες. Στην συνέχεια, το κλειδί μεταλλάσσεται (permutation) παράγοντας για κάθε κύκλο (από τους 16) ένα διαφορετικό 48-bits υπό-κλειδί (subkey). Αυτά τα subkeys καθορίζονται με τον ακόλουθο τρόπο στην αρχή κάθε κύκλου:

- Τα 56 bits διασπώνται σε δυο κομμάτια των 28 bits.
- Το κάθε κομμάτι μετατοπίζεται στη φορά του ρολογιού (προς τα αριστερά σε φορά ενός κύκλου), είτε ένα είτε δύο bits. Αυτό εξαρτάται από τον κύκλο που πρόκειται να εφαρμοστεί. Ενώ για παράδειγμα στον πρώτο κύκλο έχουμε μετατόπιση ενός bit στον δέκατο και τον δέκατο πέμπτο έχουμε μετατόπιση δυο bits.
- Μετά την μετατόπιση, επιλέγονται τελικά τα 48 από τα 56 bits για την δημιουργία του subkey.

Εξαιτίας της μετατόπισης είναι κατανοητό πως διαφορετικό υποσύνολο του αρχικού κλειδιού χρησιμοποιείται σε κάθε διαδικασία ενός κύκλου. Αυτό που έχει ξεχωριστή σημασία είναι ότι κάθε bit του κλειδιού χρησιμοποιείται τελικά στα 14 περίπου από τα 16 subkeys. Επειδή η όλη διαδικασία μεταλλάσσει την σειρά των

bits του κλειδιού, ενώ επιλέγει και ένα υποσύνολο των bits, καλείται **μεταλλαγή συμπίεσης** (compression permutation).

2. **Μεταλλαγή επέκτασης** (expansion permutation)

Αυτή η λειτουργία επεκτείνει το δεξιό κομμάτι των δεδομένων R_i από 32 bits μέγεθος που έχει αρχικά σε 48 bits. Κατά την διάρκεια αυτής της λειτουργίας υλοποιούνται οι δυο ακόλουθοι στόχοι:

- Μεταβάλλεται το μέγεθος του R_i σε ίσο με αυτό του κλειδιού (48 bits), για να είναι δυνατή η διαδικασία του XOR.
- Παράγεται ένα μεγαλύτερο αποτέλεσμα που μπορεί να συμπιεστεί κατά την διάρκεια της διαδικασίας αντικατάστασης.

Ωστόσο κανένας από αυτούς δεν είναι ο κεντρικός σκοπός της κρυπτογράφησης.

Για κάθε κομμάτι των 4-bit που αποτελεί είσοδο, το πρώτο και το τέταρτο κατά σειρά bit αντιπροσωπεύονται ως δύο bits στο κομμάτι που παράγεται μετά την διαδικασία. Με αυτό το τρόπο τα παραγόμενα κομμάτια θα έχουν μέγεθος 6 bits, το οποίο τελικά δημιουργεί και την επιθυμητή επέκταση (expansion). Αξιοσημείωτο είναι πως κάθε αρχικό κομμάτι εξάγει κάποιο άλλο μοναδικό κομμάτι.

Ειδικότερα, κάθε bit που βρίσκεται στην θέση 1 παράγει τον εαυτό του μεταβιβάζοντας τον στο τέλος του αμέσως προηγούμενου κομματιού. Ενώ διατηρεί την παρουσία του στο παραγόμενο αποτέλεσμα. Κάθε bit που βρίσκεται στην θέση 4 παράγει τον εαυτό του και μεταβιβάζεται στην αρχή του αμέσως επόμενου κομματιού, διατηρώντας φυσικά και αυτό την θέση του. Εύλογο είναι πως τα bits που βρίσκονται στις θέσεις 2 και 3 δεν μεταβάλλονται, ούτε φυσικά μετατρέπονται. Το παρακάτω παράδειγμα θα μπορούσε ενδεχομένως να είναι πιο περίπλοκο, αλλά εδώ ο στόχος είναι να κατανοήσουμε όσο πιο απλά την διαδικασία επέκτασης του αλγορίθμου. Έστω ότι οι αριθμοί 1 έως 8 εκφράζουν την σειρά των bits των αρχικών δεδομένων. Τα κομμάτια [1 2 3 4] και [5 6 7 8] κατά την διαδικασία επέκτασης παράγουν τα ακόλουθα κομμάτια: [8 1 2 3 4 5] και [4 5 6 7 8 1]. Είναι σαφές πως το μέγεθος του αποτελέσματος αυξάνει κατά ένα δεύτερο σε σχέση με το αρχικό. Με πιο μαθηματικούς όρους μετά την επέκταση το κομμάτι του plaintext R_i θα έχει μέγεθος ίσο με :$1.5^* R_i = 1.5^*32$ bits, δηλαδή 48 bits.

Επειδή αυτή η λειτουργία αλλάζει τη σειρά των bits και επαναλαμβάνει την παρουσία ορισμένων από αυτά, καλείται **μεταλλαγή επέκτασης** (expansion permutation).

3. **Αντικατάσταση S-Box** (S-box substitution)

Το συμπιεσμένο πια κλειδί και το block που επεκτάθηκε με την προηγούμενη λειτουργία συνδυάζονται με ένα XOR. Το αποτέλεσμα μεγέθους 48 bits μετέχει σε μία διαδικασία αντικατάστασης με στόχο να παραχθεί ένα block των 32 bits. Η

λειτουργία αυτή της αντικατάστασης εκτελείται από 8 **κιβώτια αντικατάστασης (substitution boxes)** τα οποία χάριν της κρυπτογραφικής ορολογίας στο εξής θα αναφέρονται ως **S-boxes**. Το σημαντικότερο ίσως χαρακτηριστικό τους είναι ότι κάθε S-box έχει ως είσοδο 6 bits και παράγει κομμάτια των 4 bits. Η συνολική μνήμη που απαιτείται για τα 8 S-boxes είναι της τάξης των 256 bytes.

Στην συνέχεια αναλύεται λεπτομερέστερα η διαδικασία με τη οποία λαμβάνει χώρα η αντικατάσταση. Ειδικότερα, τα 48 bits διαιρούνται σε 8 υπό-blocks των 6 bits όπου σε κάθε ένα χρησιμοποιείται το αντίστοιχο S-box. Στο πρώτο block χρησιμοποιείται το S-box 1, στο δεύτερο το S-box 2 και ου τω καθεξής. Το κάθε S-box αποτελεί ένα πίνακα 4 σειρών και 16 στηλών με 64 αριθμούς των 4 bits οι οποίοι μπορούν να επαναλαμβάνονται. Η διαδικασία έχει ως μοναδικό σκοπό να επιλέγει ο αριθμός που θα αποτελέσει την έξοδο, από αυτόν τον πίνακα. Η επιλογή γίνεται με συγκεκριμένο τρόπο και εξαρτάται όπως θα δούμε από την μορφή των υπό-blocks. Είναι προφανές ότι ο αριθμός που θα επιλέγει έχει μέγεθος 4 bits οπότε και ο συνδυασμός τους θα δώσει στο τέλος ένα ενιαίο block των 32 bits.

Κάθε S-box λειτουργεί, σε συνδυασμό φυσικά με τα bits εισόδου του, με τρόπο πολύ ιδιαίτερο. Ορίζουμε τα 6 bits εισόδου ως b1, b2, b3, b4, b5, b6. Τα b1 και b2 συνδυάζονται για να διαμορφώσουν έναν αριθμό των 2 bits που αντλεί τιμές από 0 έως 3, ο οποίος και αντιστοιχεί σε μια σειρά του πίνακα. Τα b2 μέχρι και b5 διαμορφώνουν έναν αριθμό ο οποίος θα ορίσει την στήλη του πίνακα και θα παίρνει τιμές από : {0,...,15}. Για παράδειγμα ας υποθέσουμε ότι το κομμάτι των 6 bits που έχει ως είσοδο ένα S-box είναι 110011. Το πρώτο και το τελευταίο bit συνδυασμένα μας δίνουν 11, δηλαδή στο δεκαδικό σύστημα τον αριθμό 3. Τα υπόλοιπα 4 bits με την δυαδική μορφή 1001, αντιστοιχούν στον αριθμό 9. Έτσι επιλέγεται ο αριθμός που βρίσκεται στην σειρά 3 και στην στήλη 9. Μην ξεχνάμε όμως πως σε αυτή την περίπτωση η μέτρηση των στηλών και των σειρών αρχίζει από το 0 και όχι από το 1.

Η αντικατάσταση S-box είναι ουσιαστικά το κρίσιμο βήμα μέσα στον DES. Οι άλλες λειτουργίες του αλγορίθμου μπορούν να χαρακτηριστούν γραμμικές και είναι εύκολο να αναλυθούν. Η διαδικασία των S-boxes είναι μη γραμμική και ουσιαστικά προσφέρει, περισσότερο από οποιαδήποτε άλλη, την ασφάλεια στον αλγόριθμο DES.

Ως τελική εργασία της συνάρτησης f υφίσταται μια τελική μεταλλαγή στο αποτέλεσμα της S-Box αντικατάστασης. Κάθε bit εισαγωγής χαρτογραφεί ένα bit εξόδου καθώς κανένα δεν αγνοείται, είτε χρησιμοποιείται πάνω από μία φορές. Η μεταλλαγή αυτή υλοποιείται με συγκεκριμένη διαδικασία όπου για παράδειγμα, πάντα το bit στην θέση 21 μεταφέρεται στο bit 4 και το bit που υπάρχει αρχικά στην θέση 4 του block μετακινείται στην θέση 31. Τελικά, το παραγόμενο κομμάτι της συνάρτησης συνδυάζεται με το πρώτο αριστερό κομμάτι (L_i), στο οποίο διασπάσθηκε το αρχικό block, με ένα not or (XOR). Είναι η τελευταία πράξη του μαθηματικού τύπου : $R_{i+1} = L_i$ XOR f (R_i , K_{i+1}).

Φυσικά όταν τελειώνει πια η διαδικασία του πρώτου **κύκλου** ξεκινάει ο δεύτερος, με τις λειτουργίες τις οποίες στοιχειοθετήσαμε παραπάνω. Στο χρονικό σημείο όπου ολοκληρώνεται και ο τελευταίος **κύκλος**, τα κομμάτια L_{16} και R_{16} συνδέονται για μια τελική μεταλλαγή (permutation) της κρυπτογράφησης του αλγορίθμου.

Αποκρυπτογράφηση του DES

Μετά τις λειτουργίες της αντικατάστασης (substitution), της μεταλλαγής (permutations) και των μετατοπίσεων το πιο προφανές θα ήταν η διαδικασία αποκρυπτογράφησης των blocks να είναι εντελώς διαφορετική, με εξίσου όμως ιδιαίτερες λειτουργίες και ίσως άλλη φιλοσοφία. Αντίθετα, οι διάφορες διαδικασίες του DES επιλέχθηκαν από τους σχεδιαστές του με τρόπο τέτοιο ώστε να προσφέρουν ή αν θέλετε να παράγουν μια εξαιρετικά χρήσιμη ιδιότητα : Ο ίδιος ο αλγόριθμος ουσιαστικά «δουλεύει» και για την κρυπτογράφηση αλλά και για την ανάκτηση των αρχικών δεδομένων.

Στον DES χρησιμοποιείται η ίδια πορεία των διαδικασιών, είτε για να κρυπτογραφήσει και για να αποκρυπτογραφήσει έναν block. Το μόνο διαφορετικό στοιχείο είναι ότι τα κλειδιά πρέπει να χρησιμοποιηθούν σε αντίστροφη φορά από αυτή που ήδη χρησιμοποιήθηκε στην κρυπτογράφηση. Έτσι, εάν τα κλειδιά κρυπτογράφησης για κάθε κύκλο έχουν την σειρά : K_1 , K_2 , K_3 ,..., K_{16} τότε τα κλειδιά αποκρυπτογράφησης θα έχουν, με σειρά αρχικοποίησης, την μορφή : K_{16} , K_{15} , K_{14} ,..., K_1 . Συνεπώς, ο DES μπορεί να χαρακτηριστεί ως ένας κυκλικός αλγόριθμος. Θυμηθείτε πως κατά την λειτουργία της **μεταλλαγής συμπίεσης** το κάθε κομμάτι του κρυπτογραφικού κλειδιού (subkey) μετατοπιζόταν προς τα αριστερά στην φορά ενός κύκλου. Είναι προφανές πως κατά την αποκρυπτογράφηση η μετατόπιση των sybkeys θα γίνεται προς τα δεξιά.

Ασφάλεια του DES

Η προσπάθεια κρυπτανάλυσης του DES έκανε πολλούς αναλυτές να ξοδέψουν πολύτιμο χρόνο σε αυτό το εγχείρημα. Στόχος της ανάλυσης της λειτουργίας του αλγορίθμου ήταν συνήθως το μέγεθος του κλειδιού, ο αριθμός των κύκλων καθώς και το πρότυπο σχεδιασμού των S-boxes. Η βασική προσέγγιση των σχεδιαστών του DES ήταν να εντοπίσουν μια ισχυρή αντικατάσταση (substitution) και μια μεταλλαγή (permutation) οι οποίες και θα εκμηδενίζουν τα στατιστικά στοιχεία των χαρακτήρων στα εισερχόμενα δεδομένα. Όπως γίνεται αντιληπτό λοιπόν, όλες οι οροθετημένες λειτουργίες της συνάρτησης f, αλλά και όχι μόνο, έχουν στοιχείο αναφοράς αυτό τον σκοπό. Με βάση την παραπάνω διαπίστωση, πολλές προτάσεις αλλά και αναφορές κρυπτανάλυσης εμφανίστηκαν, στο πέρασμα των χρόνων.

Η προφανέστερη μέθοδος επίθεσης στον DES είναι μια διαδικασία εξαντλητικής αναζήτησης στο πλαίσιο όλων των πιθανών κρυπτογραφικών κλειδιών. Η γλώσσα των αριθμών δείχνει την δυσκολία αυτού του εγχειρήματος, καθώς κατά μέσο όρο χρειάζονται 2^{55} βήματα αναζήτησης. Αναλυτές και ερευνητές προσπάθησαν με κάποιες τεχνικές να κρυπταναλύσουν τον αλγόριθμο, κάμπτοντας το επίπεδο ασφαλείας του. Η πιο ενδιαφέρουσα σκέψη ήταν η δημιουργία ενός υπολογιστικού υλικού αναζήτησης (hardware), ειδικά κατασκευασμένο, το οποίο θα ολοκλήρωνε την διαδικασία σε λογικό χρονικό διάστημα.

Όλες αυτές οι κινήσεις ήταν λογικό να ενθαρρύνουν τις αμφιβολίες, που προϋπήρχαν, για την ασφάλεια του DES. Παρά τις υποψίες όμως, κανένας εφικτός τρόπος, μέχρι τώρα, δεν ανακαλύφθηκε για να «σπάσει» τον αλγόριθμο γρηγορότερα από μια εξαντλητική αναζήτηση. Αυτή η κατάληξη που είχαν οι κατά τα άλλα οργανωμένες «επιθέσεις» στον DES δεν είναι καθόλου τυχαία. Παρακάτω αναλύονται τα ιδιαίτερα γνωρίσματα του (κρυπτογραφικό κλειδί, αριθμός των **κύκλων** κ.α.) και το πώς αυτά βοηθούν στο να χαρακτηρίζεται ακόμα ο DES ασφαλής.

Ορισμένες τιμές που μπορεί να πάρουν τα διαφορετικά, για κάθε λειτουργία κρυπτογράφησης, κλειδιά μπορεί να τα χαρακτηρίσει αδύναμα και κατά συνέπεια να κάνει τρωτή την ασφάλεια του DES. Σε μια τέτοια περίπτωση, όταν τα bits του κλειδιού είναι εξ ολοκλήρου 0, είτε εξ ολοκλήρου 1 στο δυαδικό σύστημα, τα subkeys που παράγονται θα είναι τα ίδια σε κάθε ένα **κύκλο** της κρυπτογράφησης. Κάποια άλλα κλειδιά παράγουν μόνο δύο ή μόνο τέσσερα διαφορετικά sybkeys, από το σύνολο των 16, κατά την διαδικασία παραγωγής τους. Είναι σαφές, πως οι συγκεκριμένες πιθανές τιμές των κλειδιών ορίζονται ως αδυναμία στην γενικότερη λειτουργία του αλγορίθμου. Το ευχάριστο είναι πως οι πιθανότητες για να γίνει η επιλογή τους από το σύνολο τιμών των κρυπτογραφικών κλειδιών είναι αμελητέες έως και μηδαμινές.

Πολύς λόγος έγινε για τον συγκεκριμένο αριθμό των **κύκλων** κατά την εφαρμογή του αλγορίθμου. Γιατί να είναι ακριβώς 16 και όχι λιγότεροι ή ίσως και περισσότεροι. Διαπιστώθηκε, πως μετά τον όγδοο κύκλο τα κρυπτογραφημένα πια bits ήταν ουσιαστικά μια εντελώς τυχαία παραγωγή σε σχέση με τα αρχικά bits του plaintext. Μηδενίζονται δηλαδή οποιαδήποτε στατιστικά στοιχεία που ενδεχομένως να χρησιμοποιούνταν από τους κρυπταναλυτές. Στην κρυπτογραφική ορολογία το αποτέλεσμα αυτό καλείται επίδραση της χιονοστιβάδας. Είναι εύλογο λοιπόν το ερώτημα, το γιατί να μην σταματά η διαδικασία μετά τον όγδοο κύκλο.

Με το πέρασμα των χρόνων, κάποιες παραλλαγές του DES με μειωμένο αριθμό κύκλων ήταν τρωτές και δέχονταν εύκολα μια επίθεση. Οι Biham και Shamir , γνωστοί στην κρυπτογραφική κοινότητα, το 1990 έκαναν μια διαπίστωση όσον αφορά τον αριθμό των κύκλων που χρησιμοποιεί ο αλγόριθμος. Αυτή ανέφερε πως ο DES με οποιοδήποτε αριθμό κύκλων λιγότερο

από 16, θα μπορούσε να «σπάσει» πιο αποτελεσματικά με μια επίθεση όπου θα ήταν γνωστό μέρος του plaintext, από μια εξαντλητική αναζήτηση. Προφανώς, δεν υπήρχε κανένας ουσιαστικός λόγος οι σχεδιαστές του αλγορίθμου να αλλάξουν τον αρχικό αριθμό των κύκλων που ήταν 16.

Τα κριτήρια σχεδίασης των S-boxes στόχευαν στην ύπαρξη και ενσωμάτωση αλγεβρικών δομών. Μέσα από μία ανάλυση τους, γίνεται ίσως εύκολα κατανοητό πως τα S-boxes έχουν περισσότερα κοινά χαρακτηριστικά γνωρίσματα με έναν γραμμικό μετασχηματισμό από μια τυχαία επιλεγμένη διαδικασία μετασχηματισμού, όπως κάποιοι ενδεχομένως θα ανέμεναν. Η ιδιαίτερη λειτουργία αντικατάστασης έγινε για καιρό πόλος έλξης πολλών ερευνητών με διαφορετικά αλλά και ενδιαφέροντα συμπεράσματα: "Οι αλγεβρικές δομές που βρέθηκαν και καταγράφηκαν στα S-boxes είναι αναμφισβήτητο ότι ενισχύουν το κρυπτοσύστημα ενάντια σε ορισμένους τύπους επιθέσεων".

Αναλυτές ανέφεραν συχνά πως είχαν διαπιστώσει και χαρακτηριστικά γνωρίσματα των προτύπων σχεδιασμού συγκεκριμένων S-boxes, χωρίς όμως να επωφεληθούν ποτέ από αυτά στην προσπάθεια ανάλυσης της διαδικασίας αντικατάστασης των S-box. Η πιο κρίσιμη λειτουργία της κρυπτογράφησης που προσφέρει το επιθυμητό επίπεδο ασφάλειας στον DES, είναι χωρίς αμφισβήτηση η αντικατάσταση S-box. Οι λειτουργίες της επέκτασης και της συμπίεσης μπορούν πιο εύκολα να οριοθετηθούν, καθώς αποτελούν απλές μαθηματικές διαδικασίες.

Σε όλη αυτή την ατμόσφαιρα που είχε αναπτυχθεί, υπήρχαν όπως ήταν φυσικό οι αντιδράσεις των σχεδιαστών, με επίσημες ενέργειες ανάπτυξης της λειτουργίας του DES από την IBM – ουσιαστικά τον σχεδιαστή του αλγορίθμου. Μια έκθεση εκείνης της εποχής διαβεβαίωνε πως δεν υπήρχε καμία αλλαγή στο σχεδιασμό των διαδικασιών και λειτουργιών του αλγορίθμου, αλλά σκοπός ήταν ο εντοπισμός και η διόρθωση πιθανών αδυναμιών, όπως κάποια μη ταξινομημένα στοιχεία.

Χρησιμότητα του DES

Ο αλγόριθμος μπορεί να χρησιμοποιηθεί για κρυπτογραφημένη επικοινωνία απλών χρηστών. Μεγάλη είναι η χρήση του σε περιπτώσεις όπου γίνεται αποθήκευση αρχείων σε σκληρό δίσκο σε κρυπτογραφημένη μορφή. Για κρυπτογραφημένη επικοινωνία χρηστών με μεγάλες απαιτήσεις σε επίπεδο ασφάλειας των πληροφοριών, σίγουρα παρουσιάζει αρκετά μειονεκτήματα. Η καλύτερη επιλογή προφανώς είναι ένα σύστημα δημοσίου κλειδιού.

Το πιο σημαντικό και πρακτικό ζήτημα είναι ίσως το πόσο χρήσιμος μπορεί να είναι ο αλγόριθμος σήμερα και εάν η εφαρμογή του δεν εγκυμονεί κινδύνους. Μια μηχανή εξαντλητικής αναζήτησης, που θα εφαρμοστεί ειδικά για το «σπάσιμο»

του αλγορίθμου, μπορεί να ανακτήσει το κλειδί σε κάτι περισσότερο από τρεισήμισι ώρες, με λειτουργικό κόστος μερικά εκατομμύρια δολάρια.

Υποθετικά, υπάρχει μια σειρά τεχνικών που ενδεχομένως να μειώσουν το μέγεθος της πολυπλοκότητας μια εξαντλητικής αναζήτησης και παράλληλα τους πιο πάνω αριθμούς. Πολλοί ερευνητές θεωρούν ότι είναι σχεδόν βέβαιο πως έχει αναπτυχθεί μια νεώτερη τεχνική κρυπτανάλυσης που μπορεί να εφαρμοστεί στον DES. Το σίγουρο είναι πως δεν έχει καταγράφει κανένα τέτοιο γεγονός, παρόλο που οι φήμες είναι πολύ έντονες.

Έχει επίσης ειπωθεί, ανεπίσημα βέβαια, από το NSA πως αν οι εμπειρογνώμονες του έχουν στην κατοχή τους ένα μεγάλο μέρος του plaintext και του ciphertext, μπορούν να εφαρμόσουν κάποιο στατιστικό υπολογισμό και να ανακτήσουν έτσι με πραγματικά μικρό κόστος το κρυπτογραφικό κλειδί. Φανταστείτε τι μεγάλο πλήγμα θα ήταν αυτό για την χρησιμότητα αλλά και την ιστορία του DES.

Εμείς δεν έχουμε κανένα λόγο να συμφωνήσουμε είτε να διαφωνήσουμε με οποιαδήποτε τέτοια γνώμη. Εξάλλου, υπάρχουν ήδη πολλές αντικρουόμενες απόψεις στην κρυπτογραφική κοινότητα. Σκοπός μας είναι να καταγράψουμε με όσο πιο κατανοητό τρόπο τα χαρακτηριστικά γνωρίσματα του αλγορίθμου και τις επιπτώσεις στην αδιαμφισβήτητη διαχρονικότητα του.

3.3 Αλγόριθμος IDEA

Ιστορική Αναδρομή

Από τους πιο γνωστούς και εφαρμόσιμους συμμετρικούς αλγορίθμους είναι ο **IDEA** (International Data Encryption Algorithm). Η ιδέα και τα κριτήρια πάνω στα οποία βασίστηκε ο σχεδιασμός του αλγορίθμου και αργότερα το πρότυπο εφαρμογής του ως ένα block cipher, ανήκει αποκλειστικά στους Xuejia Lai and James Massey, οι οποίοι ουσιαστικά είναι και οι ενσαρκωτές του. Πρωτοεμφανίστηκε στα μέσα του 1990 και αρχικά έγινε γνωστός ως PES (Proposed Encryption Standard). Ένα χρόνο αργότερα οι Biham και Shamir συνέταξαν και δημοσίευσαν ένα πλάνο κρυπτανάλυσης του PES, αναγκάζοντας ουσιαστικά τους σχεδιαστές του να ενισχύσουν την λειτουργία του με νέες βελτιωμένες διαδικασίες κρυπτογράφησης. Το νέο cipher ονομάστηκε IPES (Improved Proposed Encryption Standard), καταδεικνύοντας την πεποίθηση για ανανέωση και ενδυνάμωση. Τελικά, το 1992 ο αλγόριθμος υιοθετήθηκε ως ένα αναγνωρισμένο πρότυπο και μετονομάστηκε σε **IDEA** (International Data Encryption Algorithm).

Ο **IDEA** είναι βασισμένος σε κάποια πραγματικά εντυπωσιακά θεωρητικά θεμέλια και παρόλο που οι κρυπταναλυτές έχουν σημειώσει σημαντική πρόοδο, σε κάποιες παραλλαγές υλοποίησης και εφαρμογής του, φαίνεται πως είναι ακόμα αρκετά ισχυρός. Δεν λίγοι ενδεχομένως αυτοί, είτε αναλυτές είτε εμπειρογνώμονες, που αναγνωρίζουν τον **IDEA** ως τον καλύτερο και ασφαλέστερο συμμετρικό αλγόριθμο που είναι διαθέσιμος στους χρηστές αυτή την στιγμή.

Το βραχυπρόθεσμο μέλλον του στον κόσμο της κρυπτογράφησης ενδεχομένως να μην δείχνει αρκετά ξεκάθαρο. Δεν υπάρχει καμία βιασύνη ορισμού του και οριοθέτησης του ως αυτός ο αλγόριθμος που θα αντικαταστήσει τον «γερασμένο» DES, αν και υφίσταται αυτή η προοπτική. Κυρίως γιατί δεν είναι αναγνωρισμένο παγκόσμια με χορήγηση άδειας για μεγάλες εμπορικές εφαρμογές και πληροφοριακά συστήματα και δεν είναι απολύτως σίγουρο αν θα μπορέσει να αντέξει στην μακροχρόνια κρυπτολογική ανάλυση. Το δεδομένο είναι πως μέχρι τώρα έχει δείξει πολύ ισχυρός σκορπώντας αισιοδοξία στους κρυπτογραφικούς κύκλους.

Περιγραφή του IDEA

Ο αλγόριθμος **IDEA**, ως ένα block cipher, λειτουργεί κρυπτογραφώντας δεδομένα σε κομμάτια (blocks) του plaintext των 64-bit. Το κρυπτογραφικό μυστικό του κλειδί έχει μέγεθος 128 bits και είναι προφανές πως η εφαρμογή του αλγόριθμου χρησιμοποιείτε τόσο κατά την διαδικασία κρυπτογράφησης, όσο και αυτής της ανάκτησης των αρχικών δεδομένων (αποκρυπτογράφηση). Όπως και ο DES αλλά και αρκετά αλλά block ciphers, ο IDEA χρησιμοποιεί τις μαθηματικές λειτουργίες της **σύγχυσης** (confusion) και της **διάχυσης** (diffusion). Το πρότυπο και η φιλοσοφία σχεδίασης του αλγορίθμου καταγράφεται ως μια μίξη, ένα «πάντρεμα» από διαδικασίες διαφορετικών αλγεβρικών ομάδων και λειτουργιών. Οι τρεις αλγεβρικές διαδικασίες που χρησιμοποιούνται και εφαρμόζονται εύκολα τόσο σε ένα λογισμικό του IDEA, όσο και σε ένα hardware πακέτο, είναι:

- Ο μαθηματικός συνδυασμός του XOR (not or)
- Προσθήκη 2^{16}
- Πολλαπλασιασμός $2^{16} + 1$ (Αυτή η διαδικασία μπορεί να χαρακτηριστεί και ως η αντικατάσταση S-box του IDEA).

Όλες αυτές οι λειτουργίες, οι οποίες είναι και οι μόνες λειτουργίες του αλγορίθμου, χρησιμοποιούνται σε υπό-blocks (sub-blocks) μεγέθους 16-bit. Κατά την εφαρμογή αυτών των διαδικασιών, δεν υπάρχει κάποιου είδους μεταλλαγή στο επίπεδο του μεγέθους των bits, όπως συμβαίνει στο αλγόριθμο DES. Ο IDEA είναι αποδοτικός ακόμα και πάνω σε επεξεργαστές (processors) των 16-bit.

Παρακάτω θέτουμε σε μια αναλυτική διάσταση τον τρόπο λειτουργίας του αλγόριθμου. Πως δηλαδή κρυπτογραφεί τα αρχικά δεδομένα και πληροφορίες σε

κομμάτια των 64 bits, εξάγοντας αυτό που καλούμε ciphertext και φυσικά πως στην συνεχεία το αποκρυπτογραφεί ολοκληρώνοντας την όλη διαδικασία. Όπως και ο DES έτσι και ο αλγόριθμος IDEA χρησιμοποιεί **κύκλους** (rounds) διαδικασιών οι οποίοι στο συνόλω τους είναι οκτώ.

Αρχικά, το κάθε block των 64 bits διαιρείται σε 4 ισόποσα sub-blocks με μέγεθος 16 bits το κάθε ένα και ορίζονται ως: X_1, X_2, X_3, και X_4 . Αυτά τα τέσσερα sub-blocks αποτελούν την είσοδο στην διαδικασία του πρώτου κύκλου. Σε κάθε κύκλο τα κομμάτια των δεδομένων συνδυάζονται με στατιστικούς συνδυασμούς XOR, προσθέτονται μεταξύ τους και πολλαπλασιάζονται με ένα από τα έξι υπό-κλειδιά (subkeys) των 16 bits, στα οποία διασπάται το αρχικό κρυπτογραφικό κλειδί. Κατά το πέρασμα των κύκλων, σε κάποια δεδομένη στιγμή, το δεύτερο και το τρίτο sub-block ανταλλάσσουν τους εαυτούς τους. Τελικά, τα υπό-blocks συνδυάζονται με τέσσερα από τα υπό-κλειδιά σε ένα τελικό μετασχηματισμό παραγωγής του ciphertext. Σε κάθε έναν δεδομένο κύκλο η ακολουθία των διαδικασιών ακολουθεί τα παρακάτω βήματα:

1. Πολλαπλασιασμός του X_1 με το πρώτο subkey.
2. Πρόσθεση του υπό-block X_2 με το δεύτερο subkey.
3. Πρόσθεση του X_3 με το τρίτο subkey.
4. Πολλαπλασιασμός του X_4 με το τέταρτο subkey.
5. Συνδυασμός XOR (not or) των αποτελεσμάτων των βημάτων (1) και (3).
6. Συνδυασμός XOR (not or) των αποτελεσμάτων των βημάτων (2) και (4).
7. Πολλαπλασιασμός του αποτελέσματος που εξάγει το βήμα (5) με το πέμπτο subkey.
8. Πρόσθεση των αποτελεσμάτων των βημάτων (6) και (7).
9. Πολλαπλασιασμός του αποτελέσματος από το βήμα (8) με το έκτο subkey.
10. Πρόσθεση των αποτελεσμάτων που έχουν εξαχθεί από τα βήματα (7) και (9).
11. Συνδυασμός XOR (not or) των αποτελεσμάτων των βημάτων (1) και (9).
12. Συνδυασμός XOR (not or) των αποτελεσμάτων των βημάτων (3) και (9).
13. Συνδυασμός XOR (not or) των αποτελεσμάτων των βημάτων (2) και (10).
14. Συνδυασμός XOR (not or) των αποτελεσμάτων των βημάτων (4) και (10).

Όπως είναι προφανές τα παραγωγικά στοιχεία του κύκλου είναι 4 sub-blocks, αποτελέσματα των συνδυασμών από τα τέσσερα τελευταία βήματα (11), (12), (13), (14). Στο τέλος κάθε κύκλου γίνεται μια ανταλλαγή των θέσεων των δυο εσωτερικών sub-blocks. Αυτά τα κομμάτια θα αποτελέσουν στην συνέχεια την εισαγωγή στην διαδικασία του επόμενου κύκλου ως τα νέα X_1, X_2, X_3, και X_4.

Στο τέλος του τελευταίου (όγδοου) κύκλου η παραπάνω ανταλλαγή δεν ολοκληρώνεται. Μετά το πέρας της διαδικασίας των κύκλων, υπάρχει ένας τελικός μετασχηματισμός με τις παρακάτω τέσσερις λειτουργίες μαθηματικής κλίμακας:

1. Πολλαπλασιασμός του τελικού X_1 με το πρώτο subkey.

2. Πρόσθεση του τελικού X_2 με το δεύτερο subkey.
3. Πρόσθεση του τελικού X_3 με το τρίτο subkey.
4. Πολλαπλασιασμός του τελικού X_4 με το τέταρτο subkey.

Το ciphertext τελικά παράγεται από την συνένωση των τεσσάρων τελικών υπό-blocks σε ένα block των 64 bits, των αποτελεσμάτων δηλαδή των παραπάνω μαθηματικών πράξεων.

Η διενέργεια δημιουργίας από το αρχικό, μυστικό κρυπτογραφικό κλειδί των υπό-κλειδιών (subkeys) τα οποία χρησιμοποιούνται στους κύκλους είναι ιδιαίτερη και παράλληλα αρκετά εύκολη. Ουσιαστικά ο αλγόριθμος κάνει χρήση 52 διαφορετικών υπό-κλειδιών. Έξι για κάθε έναν από τους οκτώ κύκλους διαδικασιών όπως είδαμε παραπάνω και τέσσερα για την τελική μεταλλαγή κρυπτογράφησης. Το αρχικό κρυπτογραφικό κλειδί των 128-bit διαιρείτε σε 8 subkeys των 16 bits. Αυτά αποτελούν και τα πρώτα οκτώ τα οποία χρησιμοποιεί ο IDEA. Στην συνέχεια, τα bits του κλειδιού ολοκληρώνουν μια αριστερή περιστροφή της τάξεως των 25 bits, για να διαιρεθεί ξανά σε οκτώ ισομερή subkeys. Όταν ο αλγόριθμος κάνει χρήση και αυτών των υπό-κλειδιών, επαναλαμβάνεται η παραπάνω περιστροφή, για να συνεχιστεί έως ότου ολοκληρωθεί η όλη λειτουργία της κρυπτογράφησης.

Ο IDEA αποκρυπτογραφεί τα δεδομένα με τον ίδιο τρόπο που κρυπτογραφεί καθώς κατά την ανάκτηση του αρχικού plaintext ακολουθούνται ακριβώς οι ίδιες διαδικασίες. Αυτά που διαφέρουν στην αποκρυπτογράφηση είναι τα subkeys, στα οποία υφίσταται μια αντίθετη, σε σχέση με την αρχική, περιστροφή.

Ασφάλεια του IDEA

Η ασφάλεια του IDEA στηρίζεται κατά κύριο λόγο στην χρήση που κάνει των τριών ασυμβίβαστων τύπων από αριθμητικές και μαθηματικές διαδικασίες σε πολύ μικρά κομμάτια δεδομένων, όπως είδαμε, μεγέθους μόνο 16 bits. Ένα από τα βασικά κριτήρια πάνω στα οποία βασίστηκαν οι σχεδιαστές του αλγορίθμου ήταν η ενδυνάμωση ενάντια στην διαφορική (differential) κρυπτανάλυση. Επιπλέον, κανενός είδους επίθεση γραμμικής κρυπτανάλυσης δεν έχει επισήμως καταγράφει, που σημαίνει πως δεν έχει ακόμη εντοπιστεί κάποια αλγεβρική αδυναμία στην δομή σχεδιασμού του IDEA.

Η σημαντικότερη και ίσως εντυπωσιακότερη ανακάλυψη από την ανάλυση στην οποία υποβλήθηκε ο αλγόριθμος ανήκει στον Daemen. Έκανε γνωστό πως εντόπισε μια μεγάλη κατηγορία αδύναμων κρυπτογραφικών κλειδιών μεγέθους 2^{51}, όπου η χρήση ενός τέτοιου κλειδιού κατά τη διάρκεια της κρυπτογράφησης θα μπορούσε να ανιχνευθεί και να οριοθετηθεί από μη εξουσιοδοτημένους χρηστές, κάνοντας παράλληλα δυνατή την ανάκτηση του. Εντούτοις, εφόσον τα πιθανά μυστικά κρυπτογραφικά κλειδιά είναι της τάξης των 2^{128}, ένα τέτοιο

συμπέρασμα δεν ασκεί καμία ουσιαστική αρνητική επίδραση στην πρακτική ασφάλεια της λειτουργίας του αλγορίθμου.

Άξιο αναφοράς είναι το γεγονός πως ο αλγόριθμος IDEA έχει γίνει αντικείμενο πολλών αναλύσεων και σημείο αναφοράς μακροχρόνιων ερευνών. Δεν είναι τυχαίο βέβαια πως έχει ορισθεί, σε θεωρητική αρχικά βάση, η ανάπτυξη του αλγορίθμου, ως προετοιμασία για την ενίσχυση της δομής σχεδίασης του.

Κρυπτανάλυση του IDEA

Το μέγεθος του κρυπτογραφικού κλειδιού του IDEA έχει μέγεθος 128 bits, δύο φορές μεγαλύτερο από το κλειδί DES. Υποθέτοντας ότι μια εξαντλητική αναζήτηση της τιμής του κλειδιού είναι η αποδοτικότερη επίθεση κρυπτανάλυσης, θα απαιτούνταν σίγουρα όχι λιγότερο από 2^{128} (περίπου 10^{38}) προσπάθειες για την ανάκτηση του. Σχεδιάζοντας μια εφαρμογή, η οποία να είχε την δυνατότητα να εξετάσει περίπου ένα δισεκατομμύριο πιθανά κλειδιά ανά δευτερόλεπτο, ένας κρυπταναλυτής θα χρειαζόταν 10^{13} χρόνια για να ανακτήσει το κλειδί και να μπορέσει «σπάσει» έτσι τον αλγόριθμο. Εξωφρενικά μεγάλο χρόνο, ίσως περισσότερο και από την ηλικία ολόκληρης της ανθρωπότητας. Μια τέτοια διαπίστωση χαρακτηρίζει, αν θέλετε, την σημαντικότητα της επιστήμης της κρυπτογραφίας και τον πρωταρχικό ρόλο που έχει στην ασφάλεια των ηλεκτρονικών πληροφοριών και δεδομένων.

Οι σχεδιαστές του αλγορίθμου έχουν πραγματικά δημιουργήσει ένα cipher άνοσο στη διαφορική κρυπτολογική ανάλυση. Οι διαδικασίες κρυπτανάλυσης καθώς και οι έρευνες που έχουν έως τώρα δημοσιευθεί, έχουν δείξει και κάτι παραπάνω. Πως η αντίσταση του IDEA στην ενδεχόμενη διαφορική ανάλυση μπορεί να διαμορφωθεί και να οριοθετηθεί. Βασικό χαρακτηριστικό που μπορεί να οδηγήσει στην περαιτέρω ενίσχυση του αλγορίθμου ενάντια σε τέτοιου είδους κρυπτολογικές επιθέσεις. Κάπως έτσι αναβαθμίσθηκε ο αρχικός αλγόριθμος PES, που αναφέρθηκε στην αρχή του κεφαλαίου, για την τελική μετατροπή του στον IDEA. Μια λεπτομερή σύγκριση ανάμεσα στην δομή τους εξάγει μια ιδιαίτερη διαπίστωση: πως μερικές, λεπτές, με χειρουργική ακρίβεια αλλαγές μπορούν να κάνουν μια τέτοια μεγάλη διάφορα ανάμεσα στα δυο ciphers.

Ανάμεσα στις έρευνες που έλαβαν χώρα κατά το παρελθόν και είχαν στόχο την κρυπτολογική ανάλυση του αλγορίθμου, υπήρξαν κατά καιρούς μερικές σημαντικές ανακαλύψεις.

Ο Joan Daemen ανακάλυψε μια κατηγορία αδύναμων κλειδιών για την λειτουργία του IDEA. Αυτή η κατηγορία δεν χαρακτηρίζεται βέβαια αδύναμη με την έννοια που έχει μια ομάδα κλειδιών του DES και αναλύθηκαν σε κάποιο προηγούμενο σημείο. Απλά, σε μία τέτοια περίπτωση, η χρησιμοποίηση ενός αδύναμου κρυπτογραφικού κλειδιού μπορεί να προσδιορισθεί και να επιφέρει αρνητικές επιπτώσεις, με την προϋπόθεση ότι ο κρυπταναλυτής διενεργεί μια

επίθεση όπου είναι γνωστό ένα κομμάτι του plaintext. Σε κάθε περίπτωση όμως, η πιθανότητα επιλογής ενός από αυτά τα αδύνατα κλειδιά είναι πολύ μικρή: ένα προς 296. Όπως είναι λοιπόν προφανές, δεν υπάρχει κανένας άμεσος κίνδυνος εάν η επιλογή των κρυπτογραφικών κλειδιών γίνεται με τυχαία διαδικασία.

Ένας άλλος αναλυτής, ο Willi Meier εξέτασε τις τρεις αλγεβρικές διαδικασίες του αλγορίθμου, και αν πεπεισμένος ότι είναι ασυμβίβαστες, διαπίστωσε πως υπάρχουν περιπτώσεις όπου μπορεί να απλουστευθεί η κρυπτανάλυση με απώτερο σκοπό την μείωση του απαιτούμενου χρόνου αναζήτησης. Τελικά, συμπέρανε πως μια επίθεση με τα συγκεκριμένα χαρακτηριστικά είναι αποδοτικότερη μόνο δύο φορές από μια διαδικασία εξαντλητικής αναζήτησης.

Το σίγουρο είναι πως θα συνεχίσουν να υπάρχουν πολλές προσπάθειες κρυπτολογικής ανάλυσης του IDEA. Το ποια πιθανά αποτελέσματα μπορεί να έχουν αυτές οι ανακαλύψεις παραμένει σίγουρα άγνωστο. Αυτό που μπορούμε όμως να πούμε με βεβαιότητα για τον αλγόριθμο IDEA, είναι ότι το μέλλον του ανήκει στα πλαίσια της συμμετρικής κρυπτογράφησης, έστω και ως σημείο αναφοράς ερευνών και αναλύσεων.

3.4 Αλγόριθμος RC5

Περιγραφή του RC5

Ο αλγόριθμος **RC5** είναι ένα block cipher αρκετά γρήγορο σε πραγματικούς χρόνους που κρυπτογραφεί, αλλά και αποκρυπτογραφεί δεδομένα . Είναι ένας από τους πιο γνωστούς συμμετρικούς αλγορίθμους, αναπτύχθηκε και σχεδιάστηκε από τον γνωστό στην ευρύτερη κρυπτογραφική κοινότητα εμπειρογνώμονα Ron Rivest για την RSA Data Security (RSA Security). Προσαρμόστηκε στην τελική του μορφή πριν από μερικά χρόνια, το 1994 και πήρε το όνομα του από τον ίδιο τον σχεδιαστή του, "**Rivest Cipher**". Τον Μάιο του 1997 τελικά χορηγήθηκε στον RC5 δίπλωμα ευρεσιτεχνίας (patent).

Ο **RC5** είναι ένας αλγόριθμος με ιδιαίτερα γνωρίσματα, καθώς έχει ποικίλες παραμέτρους: μεταβλητό μέγεθος κομματιών (blocks) του αρχικού plaintext, μεταβλητό μέγεθος του κρυπτογραφικού κλειδιού και μεταβλητό αριθμό κύκλων (rounds). Οι επιτρεπόμενες τιμές για κάθε μια από αυτές τις παραμέτρους είναι οι εξής:

1. Τα block μπορούν να έχουν μέγεθος 32 bits (για λόγους πειραματισμού και αξιολόγησης μόνο), 64 bits ή 128 bits.
2. Ο αριθμός των κύκλων μπορεί να κυμανθεί από 0 έως και 255.
3. Το μυστικό κρυπτογραφικό κλειδί έχει μέγεθος που κυμαίνεται από 0 έως και 2048 bits.

Όπως είναι προφανές αυτές οι προσαρμόσιμες τιμές των παραμέτρων έχουν αναφορά στα επίπεδα ασφάλειας και αποδοτικότητας του αλγορίθμου. Επίσης, η δυνατότητα των μεταβλητών μεγεθών προσφέρει ευελιξία στην όλη διαδικασία κρυπτογράφησης.

Οι κύριες διαδικασίες του αλγορίθμου είναι τρεις, η προσθήκη, οι περιστροφές και ο μαθηματικός συνδυασμός του XOR (not or). Η λειτουργία της περιστροφής είναι μια διαδικασία σταθερού χρόνου και βασίζεται στο κρυπτογραφικό κλειδί και στα δεδομένα (plaintext), από κοινού.

Για να γίνει πιο κατανοητή η λειτουργία του RC5, παρόλο που το μέγεθος των blocks είναι μεταβλητό, θα εστιάσουμε σε ένα 64-bit block δεδομένων. Πριν την κρυπτογράφηση υπάρχει αρχικά μια επέκταση του παρεχόμενου μυστικού κλειδιού, το μέγεθος του οποίου εξαρτάται από τον αριθμό των κύκλων (rounds). Συνήθως οι τιμές του κλειδιού είναι 64-bit ή 128-bit ή 160-bit. Πρακτικά, χρησιμοποιείται ένα κρυπτογραφικό κλειδί μεγέθους $2*r + 2$, όπου η τιμή r δηλώνει των αριθμό των κύκλων που θα ολοκληρωθούν. Παρακάτω υπάρχει η αναλυτική διαδικασία βάση της οποίας υπολογίζονται οι τιμές του πίνακα του κρυπτογραφικού κλειδιού.

Η δημιουργία του πίνακα του κλειδιού είναι περίπλοκη, αλλά ταυτόχρονα και αρκετά απλή. Αρχικά, τοποθετούμε τα bytes του κλειδιού σε έναν πίνακα L, από c ψηφιολέξεις των 32 bits. Εάν κριθεί απαραίτητο, γεμίζουμε με μηδέν την τελευταία ψηφιολέξη. Στην συνέχεια δημιουργούμε έναν πίνακα S, χρησιμοποιώντας μια γραμμική γεννήτρια παραγωγής:

For i=1 to $2*(r + 1) -1$, οι τιμές των S διαμορφώνονται
$S_i = (S_{i-1} + Q) \bmod 2^{32}$,
με $S_0 = P$.

Όπου, για τις παραπάνω πράξεις συμβολίζουμε με r τον αριθμό των κύκλων, Q = 0x9e3779b9 και P = 0xb7e15163 με τις Q και P σταθερές να είναι η δυαδική απεικόνιση των σταθερών e και p = 3.014 αντίστοιχα. Η πράξη $\bmod 2^{32}$ έχει ως αποτέλεσμα το υπόλοιπο της διαίρεσης της τιμής της παρένθεσης $(S_{i-1} + Q)$ με τον αριθμό 2^{32} .

Τελικά, για την ολοκλήρωση της επέκτασης του κρυπτογραφικού κλειδιού γίνεται μια διενέργεια μίξης του πίνακα L στον S, για τον υπολογισμό ενός νέου πίνακα S :
$A = S_i = (S_i + A + B) <<< 3$.
$B = L_f = (L_f + A + B) <<< (A + B)$, όπου
$i = (i +1) \bmod 2*(r +1)$ και
$f = (f+1) \bmod c$

Το σύμβολο ">>>" δηλώνει μια κυκλική μετατόπιση των bits προς τα δεξιά, ενώ η όλη διαδικασία γίνεται 3*n φορές, όπου n είναι η μεγαλύτερη τιμή μεταξύ των αριθμών c και 2*(r +1). Τα τελικά προϊόντα της επέκτασης του μυστικού κλειδιού είναι οι τιμές : S_0 , S_1, S_2 ,..., S_{2r+1} .

Αρχίζοντας η διαδικασία κρυπτογράφησης, το κάθε block διαιρείται σε δύο ίσα μικρότερα κομμάτια των 32 bits, τα οποία ορίζονται ως A και B. Τα A και B δίνουν παράλληλα τιμές στις παραπάνω πράξεις υπολογισμού του πίνακα τιμών του κλειδιού. Η κρυπτογράφηση του RC5 χρησιμοποιεί τα A και B καθώς και τις τιμές του πίνακα του μυστικού κρυπτογραφικού κλειδιού. Οι τιμές των blocks στο τέλος κάθε κύκλου υπολογίζονται:
$A = A + S_0$.
$B = B + S_1$.

Ενώ η διαδικασία των κύκλων δίνεται με την παρακάτω μαθηματική μορφή:
For i = 1 to r,
$A = ((A*B) <<< B) + S_{2i}$
$B = ((B*A) <<< A) + S_{2i+1}$

Τα παραγόμενα κομμάτια είναι τα A και B όταν πια ολοκληρωθεί και ο τελευταίος κύκλος. Η διαδικασία αποκρυπτογράφησης είναι το ίδιο εύκολη. Διαιρείται το block του chipertext σε δυο κομμάτια των 32 bits, A και B. Έτσι, η λειτουργία της ανάκτησης των δεδομένων ολοκληρώνεται σε r κύκλους με:
For i = r down to 1,
$B = ((B - S_{2i+1}) >>> A) *A$
$A = ((A - S_{2i}) >>> B) * B$.

Ασφάλεια του RC5

Η αντίσταση του αλγορίθμου έχει αναφορά ένα βασικό ιδιαίτερο γνώρισμα του. Το γεγονός ότι ο RC5 προσαρμόζει ανάλογα το μέγεθος των συστατικών του και ιδιαίτερα η παρεχόμενη μεταβλητότητα του μεγέθους του κρυπτογραφικού κλειδιού, αυξάνει την ενδεχόμενη προσπάθεια αλλά και τον απαιτούμενο χρόνο της ανάκτησης του. Η εξέταση όλων των πιθανών μυστικών κλειδιών είναι γνωστή ως επίθεση εξαντλητικής αναζήτησης. Υπολογίζεται πως μία υπολογιστική μηχανή αξίας ενός εκατομμυρίου δολαρίων θα μπορέσει να «σπάσει» τον αλγόριθμο RC5 με ένα 128-bit κλειδί, ανακτώντας το σε περίπου 10^{18} χρόνια.

Η εξαιρετική απλότητα του RC5 τον καθιστά εύκολα να εφαρμόσιμο και αναλύσιμο. Η χρήση των εξαρτώμενων από τα ίδια τα δεδομένα (plaintext), περιστροφών και η μίξη διαφορετικών διαδικασιών είναι τα στοιχεία που ουσιαστικά παρέχουν την ασφάλεια στον RC5. Ειδικότερα, η χρήση αυτών των περιστροφών βοηθάει στην αντίσταση του αλγορίθμου στην γραμμική κρυπτολογική ανάλυση.

Όπως είναι φυσικό έχουν υπάρξει πολυάριθμες μελέτες για την ασφάλεια του RC5. Κάθε μια από αυτές τις μελέτες έδινε μια παραπάνω διαπίστευση στο ότι η δομή και τα συστατικά του αλγορίθμου συμβάλλουν εξολοκλήρου στην ασφάλεια του.

Το 2002, μια παγκόσμια συντονισμένη ομάδα προγραμματιστών με την ενσωμάτωση περίπου 331.000 εθελοντών, ανέκτησε (βρήκε) το μυστικό κλειδί για ένα μήνυμα το οποίο κρυπτογραφήθηκε από το RC5 cipher με κλειδί 64-bit. Ήταν μια αποδοχή της πρόκλησης που τέθηκε στα μέσα του 1997 από την RSA Security. Για την επίλυση της όλης πρόκλησης, χρησιμοποιήθηκε η μη απασχολούμενη υπολογιστική ισχύς για μια αναζήτηση περίπου 10^{19} πιθανών κρυπτογραφικών κλειδιών η οποία διαρκούσε για σχεδόν τέσσερα ολόκληρα χρόνια.

Μετά από μια τέτοιου περιεχομένου δημοσίευση άρχισαν, όπως είναι φυσικό, να δημιουργούνται έντονες αμφιβολίες για την ασφάλεια των δεδομένων που προστατεύονται από τον RC5. Τα οφέλη όμως, ενδεχομένως να θεωρηθούν περισσότερα. Αρχικά, δίνεται η δυνατότητα στους αναλυτές να επιβεβαιώσουν τις καθαρά θεωρητικές εκτιμήσεις. Παράλληλα, μέσω αυτής της σταθερής αξιολόγησης, τα στελέχη των βιομηχανιών ηλεκτρονικού εμπορίου παραινούνται για να συνεχίσουν να βελτιώνουν τα υψηλά επίπεδα ασφάλειας τους.

Ο ίδιος ο σχεδιαστής (Ron Rivest) έσπευσε να διαβεβαιώσει, πως η εφαρμογή του αλγορίθμου RC5 με πιο μεγάλο μέγεθος κρυπτογραφικού κλειδιού, σίγουρα καθιστά πιο δύσκολη την διαδικασία κρυπτανάλυσης, παρέχοντας μεγάλα επίπεδα ασφάλειας. Εξάλλου, το 1996 ο Ron Rivest ήταν αυτός που μαζί με μία ομάδα από άλλους αναλυτές πρότειναν στους χρηστές να χρησιμοποιούν κρυπτογραφικά κλειδιά μεγέθους τουλάχιστον 90 bits για συμμετρικά κρυπτογραφικά συστήματα όπως ο RC5.

Χρησιμότητα του RC5

Πριν από 4 χρόνια, η RSA Security σε συνεργασία με το WAP Forum διοργάνωσε ένα συνέδριο για την ανάπτυξη της ασύρματης τεχνολογίας. Ίσως να πρόκειται για μια απλή καταγραφή των γεγονότων που όμως αναδεικνύει αναμφισβήτητα την χρησιμότητα του αλγόριθμου RC5, αλλά και γενικότερα της κρυπτογραφικής τεχνολογίας σε σύγχρονες εφαρμογές μίας ή και περισσοτέρων διαστάσεων.

«Η RC5 κρυπτογράφηση προορίζεται να παρέχει τη μυστικότητα, τον προσδιορισμό, την ελεγμένη ακεραιότητα των μηνυμάτων καθώς και την μη-αποκήρυξη, που απαιτούνται για την ασφάλεια σε ηλεκτρονικές συναλλαγές εμπορίου στα ασύρματα περιβάλλοντα. Το πρότυπο σχεδιασμού του αλγόριθμου υποστηρίζει ασύρματες εφαρμογές με την ενσωμάτωση ενός αποδοτικού

πρωτοκόλλου και συντηρεί παράλληλα την υπάρχουσα δύναμη της μνήμης και της επεξεργασίας. Είναι ευχάριστο το γεγονός ότι η τεχνολογία ανάπτυξης του RC5 θα είναι ένα σημαντικό στοιχείο στην παροχή της κρίσιμης ασύρματης ασφάλειας».

Φυσικά, μέσα στα επόμενα χρόνια η RSA Security συνέχισε να παρέχει λύσεις στο κρίσιμο θέμα της ασφάλειας στις ασύρματες τεχνολογίες, βοηθώντας την ανάπτυξη και την επέκταση τους. Το WAP Forum είναι μια ένωση βιομηχανίας που περιλαμβάνει εκατοντάδες μέλη, έχοντας αναπτύξει τα παγκόσμια πρότυπα για τις ασύρματες πληροφορίες και υπηρεσίες τηλεφωνίας στα ψηφιακά κινητά τηλέφωνα καθώς και σε αλλά ασύρματα τερματικά.

4. Κρυπτογράφηση Δημοσίου Κλειδιού

4.1 Εισαγωγή

Η σύγχρονη κρυπτογραφία, η οποία περικλείει τις σύγχρονες τεχνικές κρυπτογράφησης δεδομένων, έχει γίνει πια συνώνυμη με το σύνολο των μη-συμμετρικών εφαρμογών και τεχνικών. Αυτό το σύνολο είναι γνωστό ως μη-συμμετρικό σύστημα ή **σύστημα κρυπτογράφησης δημοσίου κλειδιού** (public key cryptography). Η κρυπτογράφηση δημοσίου κλειδιού είναι η διαδικασία εφαρμογής κάποιων τεχνικών-αλγορίθμων, που ονομάζονται **μη-συμμετρικοί αλγόριθμοι** ή **αλγόριθμοι δημοσίου κλειδιού** (public key algorithms).

Οι αλγόριθμοι δημοσίου κλειδιού υλοποιούν την διαδικασία κρυπτογράφησης κάνοντας χρήση ενός ζεύγους κρυπτογραφικών κλειδιών, σε μια δεδομένη επαφή δυο υπολογιστών ή αν θέλετε δυο οντοτήτων. Έχουμε ήδη αναφερθεί σε αυτό το ζεύγος κλειδιών, αλληλένδυτων και αλληλοεξαρτώμενων, όσον αφορά τον υπολογισμό των τιμών τους. Ο διαχωρισμός αυτών των κλειδιών γίνεται με βάση την δημοσίευση τους στις μη εξουσιοδοτημένες οντότητες ή όχι. Έχει επικρατήσει, αυτό το κύριο γνώρισμα των κλειδιών να τα ονομάζει σε **δημόσιο κλειδί** (public key) και **ιδιωτικό κλειδί** (private key). Το δημόσιο κλειδί είναι το κλειδί του αλγόριθμου κρυπτογράφησης το οποίο μπορεί να γίνει δημόσια γνωστό χωρίς να κλονιστεί η ασφάλεια του συστήματος κρυπτογράφησης, προστατευόμενο όμως από ενδεχόμενη τροποποίηση του. Το ιδιωτικό κλειδί είναι γνωστό μόνο στην οντότητα στην οποία και ανήκει, κρατείτε μυστικό και προστατεύεται από υποκλοπή καθώς είναι αυτό που προσφέρει την ασφάλεια σε ολόκληρη την διαδικασία κρυπτογράφησης.

Κάθε οντότητα, κάθε ένα μέρος από αυτά που επικοινωνούν έχουν στην κατοχή τους ένα δημόσιο και ένα ιδιωτικό κλειδί. Οποιεσδήποτε πληροφορίες ή δεδομένα που κρυπτογραφούνται με την χρήση του ενός κλειδιού ανακτώνται μόνο με την γνώση και την χρήση του άλλου. Είναι προφανές πως ο υπολογισμός τους γίνεται με συγκεκριμένη διαδικασία, διαφορετική ασφαλώς για κάθε αλγόριθμο και η παραγωγή του ενός είναι εξίσωση της τιμής του αλλού.

Στα συμμετρικά συστήματα κρυπτογράφησης, στην «κλασική κρυπτογραφία» το ένα και μοναδικό κλειδί παραμένει μυστικό. Ο αποστολέας, η οντότητα που κρυπτογραφεί τα δεδομένα, χρησιμοποιεί ένα κλειδί ή έναν τύπο για την ολοκλήρωση της διαδικασίας και ο παραλήπτης τον ίδιο ή έναν συναφή τύπο για να τα αποκρυπτογραφήσει. Για να επικοινωνήσουν λοιπόν οι δυο οντότητες ουσιαστικά «μοιράζονται» το ίδιο κλειδί. Εδώ βρίσκεται ομολογουμένως το αδύνατο σημείο της συμμετρικής τεχνολογίας κρυπτογράφησης, καθώς ο δίαυλος επικοινωνίας μέσω του οποίου θα μεταφερθεί το κλειδί πρέπει να είναι

ασφαλής. Η δημιουργία του συστήματος κρυπτογράφησης δημοσίου κλειδιού είχε ως πρωταρχικό στόχο την αντιμετώπιση αυτού του προβλήματος.

Οι αλγόριθμοι δημοσίου κλειδιού έχουν χαρακτηριστεί ως αρκετά αργοί, σε σύγκριση βεβαίως με τις τεχνικές της συμμετρικής κρυπτογράφησης. Η χρήση τους είναι αναγκαία, όταν πρόκειται για δεδομένα που διακινούνται ή υπάρχει το ενδεχόμενο να εκτεθούν και θεωρούνται υψίστης ασφαλείας. Για αρκετά μεγάλου μεγέθους δεδομένα και πληροφορίες, συνήθως γίνεται επιλογή ενός αλγορίθμου μυστικού κλειδιού καθώς ένα σύστημα δημοσίου κλειδιού δεν υποστηρίζει την μαζική κρυπτογράφηση δεδομένων.

Εδώ φυσικά θα πρέπει να γίνει αναφορά στο σύστημα αυτό που συνδυάζει την ταχύτητα των συμμετρικών αλγορίθμων με την ασφάλεια των αλγορίθμων δημοσίου κλειδιού (υβριδικό σύστημα κρυπτογράφησης). Ένα υβριδικό σύστημα δεν είναι κάτι νέο, κάτι διαφορετικό και σίγουρα δεν έχει ιδιαιτερότητες. Κατά την διαδικασία υλοποίησης ενός τέτοιου συστήματος, ένας συμμετρικός αλγόριθμος κρυπτογραφεί τα δεδομένα (plaintext) με ένα συγκεκριμένο μυστικό κλειδί. Στην συνέχεια ένα αλγόριθμος δημοσίου κλειδιού κρυπτογραφεί το ίδιο το κλειδί για να γίνει αργότερα η μεταφορά του με ασφάλεια.

Η κρυπτογράφηση δημοσίου κλειδιού εμφανίστηκε στα μέσα της δεκαετίας του '70 ως η καινοτομία που θα επαναπροσδιόριζε την μέχρι τότε φιλοσοφία της κρυπτολογικής τεχνολογίας. Οι Whitfield Diffie και Martin Hellman ήταν αυτοί που πρώτοι παρουσίασαν τα χαρακτηριστικά αυτής της έννοιας το 1976 σε μια συνδιάσκεψη, δημοσιεύοντας λίγο καιρό αργότερα την έρευνα τους «Νέες κατευθύνσεις στο σύστημα της κρυπτογραφίας». Ήταν πραγματικά σταθμός στην ιστορία της κρυπτογράφησης, ήταν η πρώτη αναφορά στην έννοια της κρυπτογράφησης δημοσίου κλειδιού, όπου όπως όλες οι καινοτομίες δέχθηκε, αρχικά, έντονη αρνητική και αποκρουστική κριτική.

Ο αρχικός στόχος της τεχνικής αυτής ήταν η πεποίθηση ότι τα κρυπτογραφικά κλειδιά θα μπορούσαν να παραχθούν και να οριστούν σε ζευγάρια. Ένα κλειδί κρυπτογράφησης και ένα άλλο αποκρυπτογράφησης. Πολλοί τότε θεώρησαν, ότι είναι απραγματοποίητο να υπολογιστεί ένα κλειδί με την συμβολή ενός άλλου και να χρησιμοποιηθούν αργότερα ως ένα αδιαίρετο ζεύγος. Όλες αυτές οι απόψεις άρχισαν να υποχωρούν σιγά σιγά, όπως ήταν φυσικό, και η κρυπτογραφική κοινότητα συνειδητοποίησε ότι βρίσκεται μπροστά σε μια πρόκληση που επαναπροσδιόριζε τα δεδομένα και παράλληλα θα ανέβαζε τον πήχη της ανάγκης για ανάπτυξη ασφαλέστερων τεχνικών κρυπτογράφησης. Από εκείνη την εποχή υπήρχαν ήδη πολλοί αλγόριθμοι που ήταν προτεινόμενοι. Προφανώς λίγοι ήταν αυτοί που μπορούσαν να χαρακτηριστούν αφενός πρακτικοί και αφετέρου ασφαλείς.

Ασφάλεια των αλγορίθμων δημοσίου κλειδιού

Δεδομένου ότι ένας κρυπταναλυτής έχει πρόσβαση στο δημόσιο κλειδί, όπως φυσικά συμβαίνει και με το θεωρητικό σύνολο των χρηστών, μπορεί πάντα να επιλέξει για την κρυπτολογική ανάλυση οποιοδήποτε μήνυμα το οποίο κρυπτογραφείτε. Αναφέρθηκε νωρίτερα, πως οι αλγόριθμοι δημοσίου κλειδιού χρησιμοποιούνται πολύ συχνά στην κρυπτογράφηση του μοναδικού μυστικού κλειδιού μιας συμμετρικής κρυπτογράφησης. Με δεδομένο αυτό, ένας κρυπταναλυτής μπορεί, ενδεχομένως, εύκολα να υποθέσει την τιμή του μυστικού κλειδιού (plaintext), εφόσον ο αριθμός των πιθανών τιμών του είναι αρκετά μικρός λόγω φυσικά του μικρού μεγέθους του. Αυτό το πρόβλημα εμφανίζεται συχνά σε εφαρμογές κρυπτογράφησης. Λύνεται με μια διαδικασία γεμίσματος του αρχικού plaintext με τυχαία bits που μετά την αποκρυπτογράφηση θα είναι ανούσια για την οντότητα που θα το δεχθεί (παραλήπτης) και θα αποκρουστούν. Με αυτή την τεχνική δίνεται το πλεονέκτημα ότι το ίδιο μικρού μεγέθους plaintext μπορεί να κρυπτογραφηθεί σε πολλά διαφορετικά ciphertext, μηδενίζοντας τις πιθανότητες για μια πρακτική αναζήτηση της τιμής του.

Οι αλγόριθμοι δημοσίου κλειδιού σχεδιάστηκαν για να αντισταθούν σε επιθέσεις, όπου ο κρυπταναναλυτής μπορεί να εξάγει πληροφορίας παίρνοντας το chipertext από επιλεγμένα από τον ίδιο πειραματικής σημασίας μηνύματα (chosen-ciphertext attack). Ο κρυπταναλυτής επωφελείται από τις στατιστικές πληροφορίες που ενδεχομένως να λάβει. Τέτοιου τύπου επιθέσεις ανήκουν παραδοσιακά, στην κατηγορία υψηλού κίνδυνου. Πολλά συστήματα δημοσίου κλειδιού είναι ακόμα ιδιαίτερα ευαίσθητα σε αυτές τις επιθέσεις, αλλά υπάρχει σαφώς η δυνατότητα για συνεχή βελτίωση και αναβάθμιση.

Για την αξιολόγηση της ασφάλειας ενός συστήματος μη συμμετρικής κρυπτογράφησης, δεν υφίσταται κάποιος αξιόπιστος τρόπος μέτρησης, ούτε προφανώς έχει την δυνατότητα ο δημιουργός του να γνωρίζει εκ των προτέρων ότι έχει κατασκευάσει έναν αδιαπέραστο αλγόριθμο. Ο μοναδικός τρόπος ίσως για να κερδίσει ο αλγόριθμος την αξιοπιστία και το επιθυμητό επίπεδο ασφάλειας είναι η εκτίμηση των επιδόσεων του στη διάρκεια του χρόνου. Η αξιοπιστία του αυξάνεται όσο αυξάνεται ο αριθμός των αναλυτών που προσπάθησαν να «σπάσουν» τον αλγόριθμο ανακτώντας το ιδιωτικό κλειδί του και απέτυχαν.

Ειδικότερα, η ασφάλεια των αλγορίθμων δημόσιου κλειδιού βασίζεται σε δύο χαρακτηριστικά τους γνωρίσματα. Αφενός στην δυσκολία που υπάρχει στο να εξαχθούν συμπεράσματα για την ενδεχόμενη τιμή του ιδιωτικού κλειδιού από την τιμή του γνωστού στο ευρύτερο κοινό δημοσίου κλειδιού και αφετέρου στην αδυναμία υπολογισμού του plaintext από το ciphertext. Τα δημόσιου κλειδιού πρωτόκολλα σχεδιάστηκαν έτσι ώστε τα διάφορα συμβαλλόμενα μέρη να μην έχουν την δυνατότητα να ανακτήσουν αυθαίρετα μηνύματα που κρυπτογραφούνται από την οντότητας με την οποία επικοινωνούν. Σημαντικό στοιχείο, γιατί βεβαιώνεται ο στόχος του να υπάρχει από την αρχή η δυνατότητα

για αποκρυπτογράφηση ενός μηνύματος μόνο σε αυτή την οντότητα στην οποία ανήκει το ιδιωτικό κλειδί του αλγορίθμου.

Ο τομέας της ασφάλειας των συστημάτων δημοσίου κλειδιού έχει ένα παραπάνω κρίσιμο σημείο το οποίο φανερώνει και την βαρύτητα του. Όπως είναι προφανές, σε πολλές περιπτώσεις μη συμμετρικοί αλγόριθμοι χρησιμοποιούνται για μια ασφαλέστερη και λειτουργικότερη διαχείριση του κρυπτογραφικού κλειδιού (key management), ότι δηλαδή έχει να κάνει με την μυστικότητα, την μεταφορά αλλά και την κράτηση του κλειδιού. Αν και ένα τέτοιο δεδομένο είναι αντιφατικό με την γνώμη ενός αξιόλογου αναλυτή, του Whitfield Diffie: « Είναι πρακτικότερο να δούμε την κρυπτογράφηση δημοσίου κλειδιού σαν μια νέα μορφή κρυπτογραφικών συστημάτων, παρά σαν μια μορφή απλής διαχείρισης κλειδιών», η βάση για την κριτική των αλγορίθμων δημοσίου κλειδιού έχει ήδη οριοθετηθεί στις κλίμακες της ασφάλειας και της απόδοσης τους.

Ψηφιακές υπογραφές (digital signatures)

Η ανάγκη επιβεβαίωσης ότι αυτός με τον οποίο επικοινωνείς είναι πράγματι αυτός που ισχυρίζεται ότι είναι, ήταν ένα παραπάνω ζήτημα που έπρεπε η τεχνολογία της κρυπτογράφησης να αναπτύξει, να διαμορφώσει και να δώσει λύσεις. Η ανάγκη ύπαρξης μιας υπογραφής, απαραίτητης για τον έλεγχο της αυθεντικότητας του μηνύματος αλλά και για τις εμπορικές συναλλαγές που λαμβάνουν χώρα στον κόσμο του διαδικτύου, βρίσκει αναφορά σε συστήματα κρυπτογράφησης δημοσίου κλειδιού. Η τεχνολογία κρυπτογράφησης σήμερα εξασφαλίζει ότι η υπογραφή αυτή δε θα μπορεί να πλαστογραφηθεί βεβαιώνοντας την ανάγκη για πιστοποίηση (authentication).

Η χρήση των γνωστών και παράλληλα ευέλικτων συστημάτων δημοσίου κλειδιού υποστηρίζει την δημιουργία και την χρήση μιας ψηφιακής υπογραφής (digital signature) μιας οντότητας. Μια ηλεκτρονική υπογραφή είναι ένας κρυπτογραφικός μηχανισμός που λειτουργεί όπως ακριβώς και η γραπτή υπογραφή ενός ατόμου.

Σε μια περίπτωση όπου η δημιουργία μιας τέτοιας υπογραφής κρίνεται αναγκαία, χρησιμοποιείται ένας αλγόριθμος δημοσίου κλειδιού. Ο αποστολέας; η οντότητα που θα δημιουργήσει την υπογραφή της, χρησιμοποιεί το ιδιωτικό της κλειδί για την κρυπτογράφηση μίας «σύνοψης του μηνύματος». Η «σύνοψη» αυτή είναι ένα κομμάτι του plaintext με μέγεθος περίπου τα 128 bits και αποτελεί την ψηφιακή υπογραφή. Ουσιαστικά, αντιπροσωπεύει το αρχικό μήνυμα ενώ μπορεί να χρησιμοποιηθεί για να ανιχνευθούν τυχόν αλλαγές που αυτό έχει υποστεί κατά τη μεταφορά του μέσα από δίαυλους επικοινωνίας.

Η οντότητα που θα λάβει το μήνυμα μπορεί να επιβεβαιώσει αρχικά την υπογραφή αυτή, χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα για να την αποκρυπτογραφήσει, πιστοποιώντας με αυτό τον τρόπο την ταυτότητα του

ατόμου που απέστειλε το μήνυμα. Αποδεικνύεται φυσικά ότι το σύνολο του μηνύματος δεν έχει υποστεί καμία μετατροπή κατά την μεταφορά του, εφόσον απαιτείται για αυτό η χρήση και η γνώση του ιδιωτικού κλειδιού, το οποίο και παραμένει μυστικό. Ένα εξίσου σημαντικό χαρακτηριστικό μιας τέτοιας εφαρμογής είναι ίσως ότι ο ίδιος ο αποστολέας του μηνύματος δεν μπορεί να αρνηθεί την εγκυρότητα της υπογραφής του.

Υπάρχουν αλγόριθμοι που υποστηρίζουν την ανάπτυξη μια ψηφιακής υπογραφής, αλλά ο πιο γνωστός και λειτουργικός είναι ο DSA (Digital Signature Algorithm). Η χρήση του είναι αποκλειστικά και μόνο αυτή και φυσικά θα αναφερθεί παρακάτω.

4.2 Αλγόριθμος RSA

Ιστορική Αναδρομή

Από το 1976 πολλοί αλγόριθμοι κρυπτογράφησης δημόσιου κλειδιού ήταν προτεινόμενοι, από τους οποίους αρκετοί ήταν ασφαλείς. Από εκείνους που θεωρούνται ακόμα ασφαλής, οι πιο πολλοί δεν είναι ενδεχομένως πρακτικοί. Είτε έχουν ένα πάρα πολύ μεγάλο κλειδί, χαρακτηριστικό που τους κάνει μη λειτουργικούς, είτε το ciphertext είναι κατά πολύ μεγαλύτερο από το αρχικό μήνυμα (plaintext). Μόνο μερικοί αλγόριθμοι δημοσίου κλειδιού μπορούν να χαρακτηριστούν τόσο ασφαλείς όσο και πρακτικοί. Άλλοι είναι κατάλληλοι για την κρυπτογράφηση και κατ' επέκταση για την διαχείριση του κλειδιού και άλλοι είναι μόνο χρήσιμοι για τις ψηφιακές υπογραφές.

Ο πρώτος ολοκληρωμένος αλγόριθμος που κρίθηκε κατάλληλος για τις εργασίες της κρυπτογράφησης αλλά και της ψηφιακής υπογραφής είναι ο **RSA**, που δημοσιεύτηκε τον Απρίλιο 1997. Από όλους τους δημοσίου κλειδιού αλγόριθμους, οι οποίοι προτάθηκαν κατά την διάρκεια των ετών, ο RSA είναι κατά πολύ ευκολότερος στην κατανόηση του και στην εφαρμογή του. Απολαμβάνει την αμέριστη εμπιστοσύνη της κρυπτογραφικής κοινότητας, κατακτώντας τον τίτλο του δημοφιλέστερου συστήματος δημοσίου κλειδιού. Πήρε το όνομα του από τους τρεις εμπνευστές του: Ron **R**ivest, Adi **S**hamir, και Leonard **A**dlema.

Από τον πρώτο καιρό, ο αλγόριθμος RSA έλαβε Δίπλωμα ευρεσιτεχνίας (RSA patent). Σε πολύ μικρό χρονικό διάστημα έγινε πρότυπο εφαρμογής για τα κρυπτογραφικά συστήματα και αναγνωρίστηκε ευρέως η χρησιμότητα του. Υιοθετήθηκε στο πιο πολυχρησιμοποιημένο πρόγραμμα κρυπτογράφησης για τις ηλεκτρονικές επικοινωνίες που κυκλοφορεί σήμερα στο Internet, PGP (Pretty Good Privacy), καθώς είναι ο αλγόριθμος πάνω στον οποίο βασίστηκε η δομή

σχεδίασης αλλά και η λειτουργία του. Αξίζει εδώ να αναφερθεί ότι ο εμπνευστής της διαδικασίας κρυπτογράφησης που χρησιμοποιεί το PGP, Phil Zimmermann «σύρθηκε», ουσιαστικά, στα δικαστήρια με την κατηγορία της παράνομης εξαγωγής όπλων, αφού στις Η.Π.Α. η ισχυρή κρυπτογραφία θεωρείται όπλο. Τελικά, δεν καταδικάστηκε γιατί το δικαστήριο δεν μπόρεσε να οριοθετήσει σαφώς την έννοια της εξαγωγής στα πλαίσια του Internet.

Περιγραφή του RSA

Ο αλγόριθμος RSA οφείλει το πραγματικά μεγάλο επίπεδο ασφάλειας του στην επιλογή μεγάλων πρώτων αριθμών. Πρώτος αριθμός κατά την μαθηματική ορολογία είναι ο αριθμός αυτός που έχει πολλαπλάσια του μόνο τον εαυτό του και την μονάδα. Βέβαια, την σημαντικότητα αυτού του συστατικού για τον RSA θα την καταγράψουμε παρακάτω.

Η παραγωγή ή ο υπολογισμός, αν θέλετε, του δημοσίου και του ιδιωτικού κλειδιού είναι λειτουργίες που εξαρτώνται από ένα ζευγάρι μεγάλων πρώτων αριθμών. Για χάρη της τυποποίησης της διαδικασίας κρυπτογράφησης θα τους ορίσουμε ως: p και q. Συνήθως, αυτοί οι αριθμοί έχουν μέγεθος 100 έως 200 ψηφία ή ακόμα και περισσότερα. Είναι προφανές πως επιλέγονται τυχαία, χωρίς να προϋπάρχει κάποια φόρμουλα επιλογής και φυσικά παραμένουν μυστικοί για το ευρύτερο σύνολο των χρηστών.

Αρχικά, λοιπόν, επιλέγονται οι πρώτοι αριθμοί p και q όπου για λόγους μεγιστοποίησης της ασφάλειας, σχεδόν πάντα, έχουν το ίδιο μέγεθος. Στην συνέχεια, υπολογίζεται το γινόμενο τους: n = p*q. Το δημόσιο κλειδί του αλγορίθμου είναι ένας εξίσου πρώτος αριθμός που επιλέγεται και αυτός τυχαία και ορίζουμε ως e. Η επιλογή του δημοσίου κλειδιού θα πρέπει να εξαντλεί δύο σημαντικές προϋποθέσεις. Το e θα πρέπει να είναι μικρότερο από την τιμή του αριθμού n και σχετικά πρώτο με το γινόμενο (p - 1)*(q - 1). Για να γίνει πιο κατανοητή η δεύτερη προϋπόθεση, αρκεί να πούμε πως πρέπει το δημόσιο κλειδί e και το γινόμενο (p - 1)*(q - 1), να μην έχουν κανένα κοινό παράγοντα εκτός φυσικά από την μονάδα.

Για την παραγωγή του ιδιωτικού κλειδιού (d), ο αλγόριθμος χρησιμοποιεί μια μαθηματική διαδικασία. Το ιδιωτικό κλειδί είναι ουσιαστικά το υπόλοιπο μιας διαίρεσης. Εδώ, η «πράξη» του υπολοίπου της διαίρεσης θα οριστεί ως mod. Ο μαθηματικός τύπος βάση του οποίου υπολογίζεται το ιδιωτικό κλειδί του RSA έχει την μορφή: d = e^-1 mod ((p - 1)*(q - 1)) ή d = 1/e mod ((p - 1)*(q - 1)). Παρατηρούμε πως η τιμή του d εξαρτάται τόσο από το δημόσιο κλειδί (e), όσο και από τους δυο πρώτους αριθμούς. Φυσικά, θα πρέπει να σημειώσουμε πως το ιδιωτικό κλειδί και ο αριθμός n είναι και αυτοί σχετικά πρώτοι αριθμοί. Μετά την ολοκλήρωση της διαδικασίας, οι πρώτοι αριθμοί p και q δεν χρειάζονται και καταστρέφονται ή απλά απορρίπτονται, σε καμία όμως περίπτωση, ποτέ, δεν αποκαλύπτεται η τιμή τους.

Πριν ξεκινήσει η διαδικασία κρυπτογράφησης των αρχικών δεδομένων, διαιρούμε το plaintext σε αριθμητικά κομμάτια (blocks) μικρότερα από τον αριθμό n. (Για την δυαδική μορφή των δεδομένων αρκεί να πούμε πως επιλέγουμε την μεγαλύτερη δύναμη του 2, η οποία είναι μικρότερη από το n). Το plaintext ορίζεται ως m. Εάν οι p και q είναι αριθμοί 100 αριθμητικών ψηφίων, τότε προφανώς το n θα έχει λίγο παρακάτω από 200 ψηφία και το κάθε block του αρχικού κειμένου (m_i) θα πρέπει να έχει λίγα λιγότερα από 200 ψηφία. Εάν χρειαστεί γεμίζουμε με μηδενικά στοιχεία κάποιο κομμάτι προσθέτοντας τα στο αριστερό μέρος του. Ο τύπος κρυπτογράφησης είναι απλός: $c_i = m_i \text{ ^ } e \bmod n$, όπου ως c_i ορίζουμε κάθε κομμάτι του κρυπτογραφημένου πια κειμένου. Το σύμβολο (^) δηλώνει την δύναμη στην οποία θα υψωθεί το m_i. Το πιο σημαντικό χαρακτηριστικό του παραπάνω τύπου, πέρα από τις όποιες τυποποιημένες μεθόδους που χρησιμοποιούνται, είναι ότι η κρυπτογράφηση ολοκληρώνεται μόνο με την γνώση και φυσικά την χρήση του δημοσίου κλειδιού e. Σε καμία άλλη περίπτωση αυτό δεν θα ήταν δυνατό.

Το κρυπτογραφημένο κείμενο (c) θα αποτελείται από blocks δεδομένων που θα έχουν περίπου το ίδιο μέγεθος με τα blocks του plaintext. Το σύνολο των κομματιών αυτών αποτελούν το chipertext. Για να αποκρυπτογραφήσει κάποιος τα δεδομένα χρησιμοποιεί κάθε κομμάτι του c και ανακτά το m: $m_i = c_i \text{ ^ } d \bmod n$. Παρατηρούμε πως η ανάκτηση των αρχικών δεδομένων γίνεται μόνο με την χρήση του ιδιωτικού κλειδιού d. Εδώ τελικά βρίσκεται και η ουσία της όλης προσπάθειας περιγραφής του αλγορίθμου, δείχνοντας την διαφορά του τρόπου που λειτουργεί σε σχέση με έναν συμμετρικό αλγόριθμο.

Θα μπορούσε κάλλιστα στην παραπάνω περιγραφή του αλγορίθμου RSA να κρυπτογραφηθεί ένα μήνυμα με το ιδιωτικό κλειδί d και να αποκρυπτογραφηθεί αργότερα με το δημόσιο κλειδί e, στοχεύοντας στη πιστοποίηση της οντότητας που θα το κρυπτογραφήσει, αφού μόνο αυτή έχει στην κατοχή της το d. Η επιλογή είναι αυθαίρετη και εξαρτάται από τις οντότητες που επικοινωνούν μεταξύ τους.

Καλό είναι να παραθέσουμε ένα απλό αριθμητικό παράδειγμα της όλης λειτουργίας κρυπτογράφησης του RSA, με εξαιρετικά μικρούς πρώτους αριθμούς. Φυσικά, μια τέτοια κρυπτογράφηση δεν είναι λειτουργική, αλλά θα βοηθήσει στην ανάλυση του αλγορίθμου.

Ξεκινώντας με τα βήματα της διαδικασίας επιλέγουμε δυο πρώτους αριθμούς. Όπου p = 47 και q = 71. Υπολογίζουμε το γινόμενο τους:
n = p*q = 47*71 = 3337

Επιλέγουμε σαν δημόσιο κλειδί την τιμή e = 79. Ελέγχουμε εάν το e και το γινόμενο (q-1)*(q-1) = 3220 έχουν κοινό παράγοντα εκτός του 1, προϋπόθεση που ισχύει. Σε αυτή την περίπτωση το ιδιωτικό κλειδί θα είναι :
d = 79 ^ -1 mod 3220 = 1019.

Η τιμή αυτή υπολογίζεται χρησιμοποιώντας τον αλγόριθμο Euclidean. Πρακτικά, ψάχνουμε μια τιμή d τέτοια ώστε η τιμή (q-1)*(q-1) = 3220 να διαιρείτε από το e*d-1 = 79*d-1.

Έστω ότι το μήνυμα που θα κρυπτογραφήσουμε είναι το m=6882326879666683. Αρχικά, το σπάμε σε μικρότερα blocks. Στην περίπτωση που εξετάζουμε blocks των τριών ψηφίων είναι η καλύτερη επιλογή. Όποτε το m σπάει σε έξι κομμάτια: m1=688, m2=232, m3=687, m4=966, m5=668 και m6=003 (θυμηθείτε ότι γεμίζουμε με μηδενικά στοιχεία το τελευταίο block για να έχει το ίδιο μέγεθος με τα υπόλοιπα). Το πρώτο block όταν κρυπτογραφηθεί θα μας δώσει:
c1 = m1 ^ e mod n = 688 ^ 79 mod 3337 = 1570.

Η εκτέλεση της ίδιας λειτουργίας στα επόμενα κομμάτια παράγει το κρυπτογραφημένο κείμενο:
c=1570 2756 2091 2276 2423 158.
Η αποκρυπτογράφηση του c απαιτεί την ίδια διαδικασία χρησιμοποιώντας όμως ως κλειδί αποκρυπτογράφησης το ιδιωτικό κλειδί d = 1019:
m1 = c1 ^ d mod n = 1570 ^ 1019 mod 3337 = 688 = m1.
Το υπόλοιπο των αρχικών δεδομένων μπορεί βεβαίως να ανακτηθεί με αυτόν ακριβώς τον τρόπο.

Παρακάτω δύνεται πιο συνοπτικά ο τρόπος λειτουργίας του RSA, πως παράγονται και επιλέγονται τα κλειδιά αλλά και πως αυτά χρησιμοποιούνται στην κωδικοποίηση των δεδομένων.

Δημόσιο κλειδί: e
Επιλέγουμε δυο πρώτους αριθμούς, p και q οι οποίοι πρέπει να παραμείνουν μυστικοί. Υπολογίζουμε το γινόμενο τους:
Όπου n=p*q
Επιλέγουμε τυχαία ένα πρώτο αριθμό e, όπου e < n και e, (p - 1)*(q - 1) σχετικά πρώτοι αριθμοί.

Ιδιωτικό κλειδί: d
Όπου : d=e^-1 mod ((p - 1)*(q - 1))
Δηλαδή d=1/e mod ((p - 1)*(q - 1))

Κρυπτογράφηση:
Το m είναι το αρχικό μήνυμα
και το c το κρυπτογραφημένο μήνυμα που για κάθε κομμάτι τους παράγεται:
$c_i = m_i$ ^ e mod n
Είναι εφικτό μόνο όταν ξέρουμε το δημόσιο κλειδί e.

Αποκρυπτογράφηση:
Το c αποτελεί τα κρυπτογραφημένα δεδομένα που λαμβάνουμε,
το d το ιδιωτικό κλειδί και

το m_i το αρχικό κομμάτι που θα ανακτήσουμε:
$m_i = c_i \wedge d \bmod n$.
Είναι εφικτό μόνο εάν γνωρίζουμε το ιδιωτικό κλειδί d.

Ταχύτητα του RSA

Όπως ειπώθηκε, οι ταχύτητες εφαρμογής των μη συμμετρικών συστημάτων κρυπτογράφησης είναι κατά πολύ μεγαλύτερες από αυτές των αντίστοιχων συμμετρικών συστημάτων. Είναι φυσικά το μεγαλύτερο μειονέκτημα που χαρακτηρίζει τους αλγόριθμους δημοσίου κλειδιού. Σε επίπεδο hardware, έχει δειχθεί πως ο RSA είναι περίπου 1.000 φορές πιο αργός από τον συμμετρικό αλγόριθμο DES. Η γρηγορότερη εφαρμογή hardware για τον RSA έχει μια απόδοση 128 kilobits ανά δευτερόλεπτο. Οι κατασκευαστές έχουν προγραμματίσει εφαρμογές του RSA για τις έξυπνες κάρτες (smart cards). Οι εφαρμογές αυτές είναι φυσικά πιο αργές λόγω της μεγάλης απαίτησης σε ασφάλεια. Προφανώς, η ταχύτητα και η ασφάλεια του RSA είναι αντίθετα συμμετρικά στοιχεία. Όσο αυξάνεται το ένα συστατικό, μειώνεται το άλλο.

Σε επίπεδο λογισμικού, ο αλγόριθμος DES είναι περίπου 100 φορές γρηγορότερος από τον δημοσίου κλειδιού RSA. Αυτοί οι αριθμοί μπορούν να αλλάξουν, ως αποτέλεσμα του συνεχώς αυξανόμενου ρυθμού με τον οποίο αναπτύσσεται η τεχνολογία. Το μόνο σίγουρο είναι πως ο RSA,αλλά και τα υπόλοιπα συστήματα δημοσίου κλειδιού, δεν θα πλησιάσουν ποτέ την ταχύτητα που έχουν οι συμμετρικοί αλγόριθμοι.

Ταχύτητες λογισμικού RSA με διαφορετικά μήκη συντελεστών (δημόσιο κλειδί 8-bit)

	512 bits	768 bits	1024 bits
Κρυπτογράφηση	0.03 sec	0.05 sec	0.08 sec
Αποκρυπτογράφηση	0.16 sec	0.48 sec	0.93 sec
Έλεγχος	0.02 sec	0.07 sec	0.08 sec

Το παραπάνω παράδειγμα σε μορφή πίνακα, μας δείχνει τις ταχύτητες σε πραγματικό χρόνο που ο αλγόριθμος κρυπτογραφεί, αποκρυπτογραφεί και ελέγχει, με μήκος δημόσιου κλειδιού 8 bits. Οι τιμές αυτές είναι ενδεικτικές και

χρησιμοποιούνται εδώ για λόγους ανάλυσης και μόνο. Άξιο αναφοράς είναι ο πολλαπλάσιος χρόνος που χρειάζεται ο RSA να αποκρυπτογραφήσει και να ανακτήσει ένα αρχικό κείμενο, σε σύγκριση με τον χρόνο που απαιτείται για την κρυπτογράφηση του. Τα μήκη συντελεστών αφορούν το μέγεθος των πρώτων αριθμών που επιλέγονται κατά την διαδικασία παραγωγής των δυο κλειδιών. Ενδεικτικά μεγέθη εδώ παρουσιάζονται τα 512 bits, τα 768 bits και τα 1024 bits.

Ασφάλεια του RSA

Η ασφάλεια του RSA εξαρτάται ολοκληρωτικά από το πρόβλημα της εξεύρεσης μεγάλων πρώτων αριθμών, η οποία από μαθηματικής πλευράς είναι δύσκολη έως και αδύνατη. Εάν αυτό ήταν εφικτό τότε κάποιος κρυπταναλυτής γνωρίζοντας το γινόμενο των πρώτων αριθμών n, θα μπορούσε να υπολογίσει (ανακτήσει) το αρχικό κείμενο (m) από το δημόσιο κλειδί e και από το κρυπτογραφημένο κείμενο (chipertext c). Ενδεχομένως, θα είχε ανακαλυφθεί ένας εξ ολοκλήρου διαφορετικός τρόπος κρυπτανάλυσης του RSA. Εντούτοις, εάν αυτός ο νέος τρόπος επιτρέπει σε έναν κρυπτναλυτή να υπολογίσει το ιδιωτικό κλειδί d, θα μπορούσε κάλλιστα να χρησιμοποιηθεί ως νέος τρόπος εξεύρεσης των μεγάλων πρώτων αριθμών. Πολλοί ερευνητές είναι αυτοί που αφιερώνουν πολύ χρόνο στην προσπάθεια ανακάλυψης νέων πρώτων αριθμών με δεκάδες ψηφία. Ο υπολογισμός, λοιπόν, του συντελεστή n είναι ο προφανέστερος τρόπος κρυπτανάλυσης. Η τεχνολογία «επιβάλει» αυτή την περίοδο έναν συντελεστή με περισσότερα από 220 ψηφία.

Μια άλλη συνηθισμένη επίθεση στον αλγόριθμο RSA είναι η εικασία της τιμής της παράστασης (p - 1)*(q - 1). Αυτή η προσπάθεια κρυπτανάλυσης βέβαια έχει δειχθεί πως δεν είναι ευκολότερη από την εξεύρεση των πρώτων αριθμών. Οι περισσότερες κοινές τεχνικές υπολογισμού των πρώτων αριθμών δεν μπορούν να χαρακτηριστούν παρά πιθανολογικές. Είναι βεβαίως δυνατόν, για κάποιον αναλυτή να δοκιμάσει κάθε πιθανή τιμή του ιδιωτικού κλειδιού, για να καταλήξει στη σωστή που θα του δώσει την δυνατότητα να αναστήσει τα αρχικά δεδομένα. Μια τέτοια προσπάθεια θα ήταν αποδοτικότερη από τον πιθανό υπολογισμό του n, αλλά η εξαντλητική αναζήτηση προφανώς θα χρειαζόταν μια τεραστία χρονική περίοδο για να τεθεί υπό επιτυχία.

Η επιλογή των δύο πρώτων αριθμών, συστατικό ασφάλειας για τον αλγόριθμο, είναι μια ιδιαίτερη διαδικασία. Οι αριθμοί αυτοί, υπήρχε αρχικά η πεποίθηση, πως θα πρέπει να είναι «ισχυροί». «Ισχυροί» πρώτοι αριθμοί καλούνται αυτοί με ορισμένες ιδιότητες οι οποίες καθιστούν το γινόμενο τους (n = p*q), σκληρό ενάντια σε συγκεκριμένες μεθόδους εξεύρεσης του. Εντούτοις, οι πρόοδοι στην διάρκεια των τελευταίων χρόνων έχουν καταστήσει επισφαλές το πλεονέκτημα των «ισχυρών» πρώτων αριθμών. Επομένως, η επιλογή ενός παραδοσιακού «ισχυρού» ζευγαριού των p και q από μόνο του δεν αυξάνει σημαντικά την ασφάλεια στην εφαρμογή του RSA. Ενδεχομένως δεν υπάρχει κάποιο πρόβλημα στο να επιλέγονται όλο και μεγαλύτεροι πρώτοι αριθμοί. Πιο πάνω, εξάλλου,

αναφέραμε πως οι αριθμοί αυτοί συνήθως έχουν μέγεθος έως και 200 ψηφία. Είναι σχεδόν σίγουρο πως στο άμεσο μέλλον η κρυπτογραφική τεχνολογία να «απαιτεί» ακόμα μεγαλύτερους πρώτους αριθμούς. Η χρήση τους στην κρυπτογραφική διαδικασία του RSA θα είναι πάντα αναγκαία και σημαντική.

Το κυριότερο πρόβλημα, ίσως, στην λειτουργία του RSA έχει να κάνει επίσης με τους μεγάλους πρώτους αριθμούς. Μια ρεαλιστική αντιμετώπιση της όλης διαδικασίας θα όριζε σημαντικό το ενδεχόμενο οι πρώτοι αριθμοί που χρησιμοποιούνται (p και q), ακριβώς γιατί είναι μεγάλοι, να είναι σύνθετοι αριθμοί. Ποιο μπορεί να ήταν λοιπόν το πρόβλημα σε μια τέτοια περίπτωση; Αρχικά, πρέπει να εξαντληθούν όλες οι πιθανότητες για να μην συμβεί αυτό. Σε μία όμως αντίθετη περίπτωση, το σίγουρο θα ήταν ότι το σύνολο των διαδικασιών της κρυπτογράφησης και της αποκρυπτογράφησης δεν θα λειτουργούσαν κατάλληλα. Έχει αποδειχθεί πως υπάρχουν κάποιοι πρώτοι αριθμοί, που η χρησιμοποίηση τους θα φέρει σε αποτυχία το σύστημα κρυπτογράφησης του RSA. Οι πρώτοι αριθμοί πρέπει να πούμε πως επιλέγονται συνήθως μέσα από κάποιες πιθανολογικές μεθόδους και τεχνικές. Η ανίχνευση αυτών των σύνθετων πρώτων αριθμών δεν είναι δυνατή, μέσα από τέτοιες τεχνικές. Βεβαίως και οι αριθμοί αυτοί είναι επισφαλείς, αλλά σίγουρα είναι και αρκετά σπάνιοι.

Κατά διαστήματα, πολλοί υποστηρίζουν ότι έχουν βρει εύκολους τρόπους να «σπάσουν» τον RSA ανακτώντας το ιδιωτικό του κλειδί, αλλά καμία τέτοια άποψη δεν πλησίασε την πραγματικότητα. Το 1998 ο William Payne πρότεινε μια μέθοδο βασισμένη στο θεώρημα Fermat. Αυτή η μέθοδος ήταν τελικά πιο αργή ακόμα και από την διαδικασία «παραγωγής» του συντελεστή n. Ο αλγόριθμος RSA έχει αντέξει στην πολύπλευρη κρυπτανάλυση που έχει δεχθεί, κερδίζοντας την εμπιστοσύνη όχι μόνο των αναλυτών της κρυπτογραφικής κοινότητας. Είναι εξάλλου αποδεδειγμένο πως ακόμη και η ανάκτηση ορισμένων κομματιών από τις πληροφορίες του κρυπτογραφημένου μηνύματος, είναι τόσο δύσκολη όσο η αποκρυπτογράφηση ολόκληρου του μηνύματος.

Για την λειτουργικότητα και πόσο μάλλον για την διατήρηση του επιπέδου ασφάλειας που προσφέρει ο RSA, κάποια σημαντικά στοιχεία λαμβάνονται πάντα υπόψη. Ένας συντελεστής n δεν θα πρέπει σε καμία περίπτωση να είναι είτε να θεωρείται κοινός. Σε μία κρυπτογραφημένη επικοινωνία μέσω ενός δικτύου, ίσως η χρήση του να επιφέρει αρνητικές επιπτώσεις. Δεν είναι όμως αρκετό να υπάρχει και να εφαρμόζεται ένας ασφαλής κρυπτογραφικός αλγόριθμος, όπως ο RSA. Ολόκληρο το κρυπτογραφικό σύστημα και το κρυπτογραφικό πρωτόκολλο πρέπει να είναι ασφαλείς. Μια αποτυχία σε οποιαδήποτε από αυτές τις τρεις περιοχές καθιστά το γενικότερο σύστημα προβληματικό.

Το μήκος των κλειδιών (δημόσιο και ιδιωτικό) που χρησιμοποιεί ο RSA έχει γίνει κατά καιρούς σημείο αναφοράς και απαίτησης. Ένα κλειδί 512 bits δεν θεωρείται πλέον ασφαλές. Εάν χρησιμοποιηθεί ένα 768-bit κλειδί αναμφισβήτητα μειώνεται κατά πολύ η πιθανότητα ανάκτησης του. Η απαίτηση όμως της RSA

Security είναι η χρήση κλειδιών μήκους 1024 bits. Θεωρείται πως μια διαδικασία κρυπτογράφησης του RSA με ένα 1024-bit κλειδί θα είναι για μερικά χρόνια ακόμα ασφαλής. Μια μεγαλύτερη τιμή κλειδιού (2048 bits ή ακόμα και 4096 bits) είναι αυτή που θα καταγραφεί ως εξαιρετικά ασφαλής, αλλά ο χρόνος που θα χρειασθεί για να κρυπτογραφηθεί και να αποκρυπτογραφηθεί το αρχικό μήνυμα σίγουρα δεν χαρακτηρίζει το σύστημα πρακτικό.

Ο μεγαλύτερος όμως κίνδυνος στην χρησιμοποίηση ενός πολύ μεγάλου κλειδιού είναι η ψεύτικη αίσθηση ασφάλειας που παρέχει στους χρήστες. Μια 4096-bit ασφάλεια σε ένα σύστημα, αντηχεί εντυπωσιακά σε μια προσπάθεια μάρκετινγκ, αλλά εάν το ιδιωτικό κλειδί δεν προστατεύεται επαρκώς ή η τυχαία γεννήτρια παραγωγής πρώτων αριθμών δεν είναι και τόσο τυχαία, προφανώς η ύπαρξη ενός μεγάλου κρυπτογραφικού κλειδιού είναι άχρηστη.

Χρησιμότητα του RSA

Σε μια προσπάθεια να οριοθετήσουμε επαρκώς την χρησιμότητα του αλγορίθμου RSA σήμερα, αρκεί να πούμε πως είναι ο αλγόριθμος εκείνος που θεωρείται ευρέως πρότυπο κρυπτογράφησης και η τεχνολογία ανάπτυξης του είναι εξασφαλίζει την ύπαρξη της πλειοψηφίας των εφαρμογών e-business στον κόσμο του διαδικτύου.

Σε συνέδριο που διοργάνωσε τον Σεπτέμβριο του 2000 η RSA security, η αρχική πεποίθηση ήταν η καθησύχαση της κοινότητας, μετά από την παραπληροφόρηση που είχε υπήρχε σχετικά με την λήξη του διπλώματος ευρεσιτεχνίας του RSA. Το U.S. patent που είχε χορηγηθεί στον RSA το Σεπτέμβριο του 1983, έληγε 17 χρόνια μετά. Εκτός από την επίσημη θέση της RSA security σχετικά με το δίπλωμα ευρεσιτεχνίας, διατυπώθηκαν πολύ σημαντικά συμπεράσματα.

Για σχεδόν δυο δεκαετίες, περισσότερες από 800 επιχειρήσεις που επεκτείνονται στην αναπτυσσόμενη ηλεκτρονική αγορά έχουν αποδείξει την εμπιστοσύνη τους στην ασφάλεια του RSA. Εμπιστοσύνη για έναν αλγόριθμο που μπορεί να παρέχει το επιθυμητό επίπεδο στο κρίσιμο σημείο της ασφάλειας, με χρόνο-λειτουργικές εφαρμογές και πόρους κρυπτογράφησης. Όλο αυτό τον καιρό η RSA security είχε κάνει τροποποιήσεις στον σχεδιασμό και την βάση πάνω στην οποία ο αλγόριθμος εφαρμόζεται, συμπεριλαμβάνοντας διάφορες βελτιώσεις απόδοσης, μη απεικονισμένες στο αρχικό δίπλωμα ευρεσιτεχνίας. Αυτές οι τροποποιήσεις είχαν στόχο ένα ευρύ φάσμα εφαρμογών λογισμικού και λειτουργικών συστημάτων.

Η τεχνολογία κρυπτογράφησης έχει αναδιαμορφώσει ένα εξ ολοκλήρου νέο επίπεδο σπουδαιότητας στον κόσμο των επιχειρήσεων και στην ανάπτυξη του ηλεκτρονικού εμπορίου. Εκεί, η τεχνολογία σχεδίασης του αλγορίθμου RSA συνεχίζει να διατηρεί έναν ηγετικό ρόλο. Όπως είναι φυσικό, οριοθετήθηκαν νέα

θεσμικά πλαίσια και κανόνες για την αναπτυσσόμενη ηλεκτρονική αγορά. Μέσα σε αυτό το πλαίσιο, η νομοθεσία ηλεκτρονικών υπογραφών ως κανονισμός και απαίτηση διεξαγωγής διατραπεζικών συναλλαγών και όχι μόνο, βρίσκει εφαρμογή στην χρήση του RSA και άλλων βεβαίως αλγορίθμων-τεχνικών δημοσίου κλειδιού. Όπως γίνεται εύκολα κατανοητό, η RSA κρυπτογράφηση θα διαδραματίζει έναν βασικό ρόλο στην περαιτέρω επέκταση των πρωτοβουλιών ηλεκτρονικού εμπορίου.

Ανεξάρτητα από τα αλλά επίσημα πρότυπα, η ύπαρξη προτύπων όπως το κρυπτοσύστημα RSA είναι εξαιρετικά σημαντική για την ανάπτυξη μιας ψηφιακής οικονομίας. Εάν ένα σύστημα δημοσίου κλειδιού χρησιμοποιείται παντού για επικύρωση των οντοτήτων, τα ψηφιακά υπογεγραμμένα έγγραφα μπορούν κατόπιν να ανταλλαχθούν μεταξύ των χρηστών, σε διαφορετικά μέρη του κόσμου χρησιμοποιώντας διαφορετικό λογισμικό σε διαφορετικές πλατφόρμες. Αυτή η διαλειτουργικότητα είναι αδιαμφισβήτητα απαραίτητη για να αναπτυχθεί μία πραγματικά μεγάλη ψηφιακή οικονομία. Η υιοθέτηση του κρυπτογραφικού συστήματος RSA έχει αυξήσει σημαντικά την πεποίθηση για την επίτευξη ενός τέτοιου στόχου. Φυσικά, η αποδοχή ενός και μόνο παγκόσμιου προτύπου να εξαρτάται και από άλλους παράγοντες, το ευχάριστο όμως είναι ότι ο RSA περικλείει το σύνολο των ενδεχόμενων απαιτήσεων.

Ο αλγόριθμος RSA χρησιμοποιείται σε πολλά λογισμικά εμπορικών προϊόντων και σχεδιάζεται να χρησιμοποιηθεί σε πολύ περισσότερα. Εκτός αυτών, ο RSA εφαρμόζεται στα τρέχοντα λειτουργικά συστήματα των Microsoft, Apple και Sun. Σε επίπεδο hardware, μπορεί να «βρεθεί» στην ασφάλεια των ασύρματων τηλεφώνων, στις κάρτες δικτύου Ethernet, καθώς και στην τεχνολογία ανάπτυξης των έξυπνων καρτών (smart cards).

Επιπλέον, ο αλγόριθμος έχει ενσωματωθεί σε όλα τα σημαντικά πρωτόκολλα ασφάλειας της επικοινωνίας μέσω του διαδικτύου συμπεριλαμβανομένου και του SSL (Secure Sockets Layer). Το SSL πρωτόκολλο αναπτύχθηκε από την Netscape Communications Corporation για να παρέχει την ασφάλεια και τη μυστικότητα των πληροφοριών που ανταλλάσσονται μέσω του Διαδικτύου. Το πρωτόκολλο υποστηρίζει server και client επικύρωση, ενώ είναι σε θέση να διαπραγματευτεί τα κλειδιά κρυπτογράφησης. Υποστηρίζει το κρυπτοσύστημα RSA, καθώς διατηρεί την ασφάλεια και την ακεραιότητα του καναλιού μετάδοσης με τη χρησιμοποίηση και την εφαρμογή της κρυπτογράφησης.

Όταν οι κύριοι χρηματοδοτικοί οργανισμοί της αμερικανικής οικονομικής βιομηχανίας ανέπτυσσαν τα πρότυπα για τις ψηφιακές υπογραφές, υιοθέτησαν το ANSI X9.31, το οποίο εφαρμόζει την τεχνολογία ψηφιακών υπογραφών του RSA. Μια ψηφιακή υπογραφή είναι το ακριβές εργαλείο που είναι απαραίτητο, για να μετατραπούν τα πιο ουσιαστικά έγγραφα σε ψηφιακής μορφής δεδομένα. Η χρήση της ψηφιακής υπογραφής του RSA προσφέρει πολλά πλεονεκτήματα, κυρίως σε ταχύτητα επαλήθευσης της υπογραφής και βρίσκει εφαρμογή σε μεγάλα εμπορικά συστήματα ακόμα και σήμερα.

Μερικές επιχειρήσεις θεωρούν ότι, με την κρυπτογράφηση των στοιχείων, λύνουν τα περισσότερα προβλήματα ασφάλειας και δεν φροντίζουν να αποτρέψουν στους επιτιθεμένους το «σπάσιμο» των συστημάτων επειδή τα δεδομένα θα είναι άχρηστα σε αυτούς, εφόσον είναι κρυπτογραφημένα. Καλό είναι οι χρήστες να μην βασίζονται σε μια ψεύτικη αίσθηση της ασφάλειας και να στηριχθούν εκεί χωρίς να δώσουν την απαραίτητη προσοχή στην ασφάλεια δικτύων και λειτουργικών συστημάτων. Ένας από τους σχεδιαστές του RSA,ο Ron Rivest, διατύπωσε πως η κρυπτογράφηση δεν είναι μια λύση στις ανησυχίες ασφάλειας αλλά ένας τρόπος να μεταφερθεί το πρόβλημα: «Αντί της διαχείρισης 100 MB των κρίσιμων δεδομένων, αρκεί μόνο να διαχειριστείτε ένα κρυπτογραφικό κλειδί, που είναι πολύ μικρότερο στο μέγεθος».

4.3 Αλγόριθμος DSA

Ιστορική Αναδρομή

Τον Αύγουστο του 1991, το Εθνικό Ίδρυμα Προτύπων και Τεχνολογίας (**NIST**) πρότεινε το **DSA** (**D**igital **S**ignature **A**lgorithm) ως ένα Πρότυπο Ψηφιακών Υπογραφών (**DSS**). Το προτεινόμενο πρότυπο είναι ένας αλγόριθμος δημοσίου κλειδιού κατάλληλος μόνο για ψηφιακές εφαρμογές υπογράφων. Ο αλγόριθμος κάνει χρήση ενός δημοσίου κλειδιού, με το οποίο ο παραλήπτης ενός μηνύματος ελέγχει την ακεραιότητα των στοιχείων και φυσικά την ταυτότητα του αποστολέα. Μπορεί επίσης να χρησιμοποιηθεί από μια τρίτη οντότητα, για μια διαδικασία εξακρίβωσης της αυθεντικότητας μιας υπογραφής, αλλά και των δεδομένων που συνδέονται με αυτήν.

Το 1987 το NIST, σε μια προσπάθεια ανάπτυξης προτύπων ασφάλειας, είχε εκδώσει την εξής ανακοίνωση προς τους αναλυτές και ερευνητές της κρυπτογραφικής κοινότητας: «Αναζητάμε την οικονομικώς αποδεκτή ασφάλεια και μυστικότητα των ομοσπονδιακών πληροφοριών σε μια επιλογή με τα πιο επιθυμητά χαρακτηριστικά λειτουργίας και χρήσης». Ως επιλογή χαρακτηρίστηκε ένας αλγόριθμος που θα ανταποκρίνεται στις οικονομικές και λειτουργικές απαιτήσεις που είχαν οριοθετηθεί. Μεταξύ των παραγόντων που εξετάστηκαν κατά τη διάρκεια αυτής της διαδικασίας ήταν το παρεχόμενο επίπεδο ασφάλειας, η ευκολία της εφαρμογής, ο αντίκτυπος στην εθνική ασφάλεια και τα νομοθετικά πλαίσια και το επίπεδο αποδοτικότητας της ψηφιακής υπογραφής αλλά και των διαδικασιών επαλήθευσης.

Η ανακοίνωση του NIST δημιούργησε μια δίνη κριτικών και κατηγοριών. Η RSA Security ήταν ο πιο σκληρός επικριτής καθώς, απολύτως φυσιολογικά, η

επιθυμία της ήταν να χρησιμοποιείται ο αλγόριθμος RSA ως πρότυπο και όχι κάποιος άλλος. Πολλές μεγάλες επιχειρήσεις λογισμικού που είχαν χορηγήσει άδεια ήδη στον αλγόριθμο RSA στράφηκαν ενάντια στον DSA. Επιχειρήσεις όπως η IBM, η Apple, η Microsoft, η DEC και η Sun είχαν ήδη ξοδέψει μεγάλα ποσά εφαρμόζοντας την ψηφιακή υπογραφή (digital signature) του RSA και προφανώς δεν ήταν διατεθειμένες να χάσουν αυτή την επένδυση.

Τελικά, τον Μάιο του 1994 εκδόθηκε στην τελική μορφή του το πρότυπο του DSA και καθορίστηκε άμεσα ως το ψηφιακό πρότυπο επικύρωσης της κυβέρνησης των Ηνωμένων Πολιτειών. Η ανακοίνωση του Εθνικού Ιδρύματος Προτύπων και Τεχνολογίας (NIST) ήταν σαφής. «Ο αλγόριθμος DSA και όλα τα προτεινόμενα πρότυπα ψηφιακών υπογραφών ισχύουν σε όλα τα ομοσπονδιακά τμήματα και τις αντιπροσωπείες για την προστασία των αταξινόμητων πληροφοριών. Επίσης, η υιοθέτηση τους είναι διαθέσιμη σε ιδιωτικές και εμπορικές εταιρίες στο πλαίσιο της ανάγκης ύπαρξης ψηφιακών υπογραφών».

Η κριτική προς τον αλγόριθμο συνεχίστηκε και μετά την έκδοση του. Φυσικά ήταν βασισμένη και είχε εστιάσει σε μερικά όντως κύρια ζητήματα. Αρχικά, ο αλγόριθμος στερείται τη βασική ικανότητα ανταλλαγής των κρυπτογραφικών κλειδιών. Το κρυπτογραφικό σύστημα ήταν πάρα πολύ πρόσφατο και υπόκειται σε λίγη διερεύνηση για τους χρήστες, για να είναι βέβαιοι της δύναμής του. Η επαλήθευση των υπογραφών με εφαρμογή του DSA είναι συγκριτικά πολύ αργή. Ενδεχομένως το πιο σημαντικό ζήτημα που θα συνεχίζει να απασχολεί είναι η ύπαρξη δεύτερων προτύπων επικύρωσης, που είχε προκαλέσει δυσκολία σε προμηθευτές λογισμικού και υλικού, οι όποιοι είχαν ήδη στηριχθεί επάνω στην τεχνολογία του RSA. Τέλος, έγινε λόγος για τις συνθήκες κάτω από τις οποίες το NIST επέλεξε τον DSA, καθώς η διαδικασία χαρακτηρίσθηκε μυστικοπαθής και αυθαίρετη. Φυσικά η επιλογή ενός προτύπου και ποσό μάλλον οι λεπτομέρειες σχεδίασης του δεν μπορεί παρά μόνο να γίνεται κάτω από μυστικότητα και ασφάλεια.

Περιγραφή του DSA

Ο DSA είναι μια παραλλαγή των αλγορίθμων δημοσίου κλειδιού Schnorr και ElGamal. Ο αλγόριθμος χρησιμοποιεί έναν αριθμό από παραμέτρους. Η λειτουργία παραγωγής των κλειδιών αλλά και η ολοκλήρωση της διαχείρισης της ψηφιακής υπογραφής αναλύεται παρακάτω.

Δημόσιο κλειδί: y
p: τυχαίος πρώτος αριθμός μεγέθους 512-bit έως 1024-bit, όπου μπορεί να γνωστοποιηθεί σε μια ομάδα χρηστών.
q: σχετικά πρώτος αριθμός με την τιμή p-1, μεγέθους 160-bit. Μπορεί να γνωστοποιηθεί σε μια αμάδα χρηστών.

$g = h^{(p-1)/q} \bmod p$, όπου ο h έχει τιμή μικρότερη από το p-1. Μπορεί να γνωστοποιηθεί σε μια ομάδα χρηστών .
$y = g^x \bmod p$

Βλέπουμε πως το δημόσιο κλειδί παράγεται από τυχαίες τινές πρώτων ή σχετικά πρώτων αριθμών. Το μέγεθος του δημόσιου κλειδιού y είναι ίσο με το μέγεθος του πρώτου αριθμού p (μεγέθους 512-bit έως 1024-bit).

Ιδιωτικό κλειδί: x
$x < q$: τυχαίος αριθμός μεγέθους 160-bit

Υπογραφή:
k: τυχαίος αριθμός, μικρότερος από την τιμή του q.
r (υπογραφή) = $(g^k \bmod p) \bmod q$.
s (υπογραφή) = $(k^{-1} (H(m) + xr)) \bmod q$.

Για την υπογραφή ενός μηνύματος m ακολουθείται η παραπάνω διαδικασία όπου H(m) είναι αυτό που ονομάζουμε σύνοψη του μηνύματος. Οι παράμετροι r και s που παράγονται είναι η ψηφιακή υπογραφή. Παρατηρούμε πως η οντότητα που θα παράγει την μοναδική ψηφιακή υπογραφή της, έχει την δυνατότητα να το κάνει μόνο με την χρήση του ιδιωτικού κλειδιού x.

Επαλήθευση της υπογραφής:
$w = s^{-1} \bmod q$.
$u1 = (H(m) * w) \bmod q$.
$u2 = (rw) \bmod q$.
$v = ((g^{u1} * y^{u2}) \bmod p) \bmod q$.
Εάν η τιμή v = r τότε η υπογραφή επαληθεύεται.

Ο παραλήπτης του μηνύματος ελέγχει την ορθότητα της υπογραφής υπολογίζοντας τις παραπάνω τιμές, έτσι ώστε να φτάσει στην ισότητα της επαλήθευσης (v = r). Οι παράμετροι r και s, ως ψηφιακή υπογραφή, χρησιμοποιούνται για την παραγωγή του συντελεστή v.

Στην DSA κρυπτογράφηση, η παραγωγή της υπογραφής είναι γρηγορότερη από την διαδικασία επαλήθευσης της. Με τον αλγόριθμο RSA αντίθετα, η επαλήθευση είναι κατά πολύ γρηγορότερη από την λειτουργία της δημιουργίας και χρήσης μιας ψηφιακής υπογραφής. Σίγουρα είναι θετικό το γεγονός ότι ο DSA κατά την διαδικασία της παραγωγής είναι πολύ γρήγορος, αλλά δεδομένου ότι σε πολλές εφαρμογές ένα κομμάτι των ψηφιακών πληροφοριών υπογράφεται μία φορά, αλλά ελέγχεται συχνά, μπορούμε να πούμε ότι ο αλγόριθμος μειονεκτεί στα επιθυμητά επίπεδα ταχύτητας. Πολλοί ερευνητές θεωρούν ότι με βάση τις αναπτυσσόμενες τεχνικές, είναι εφικτό να βελτιωθεί η αποδοτικότητα του DSA μέσα στα επόμενα έτη.

Ασφάλεια του DSA

Η φιλοσοφία σχεδίασης του DSA είναι βασισμένη στην δομή υλοποίησης που είχαν προτείνει οι ερευνητές Schnorr και ElGamal. Γενικά, ο αλγόριθμος θεωρείται ασφαλής όταν το μέγεθος του δημόσιου κρυπτογραφικού κλειδιού είναι αρκετά μεγάλο. Το δημόσιο κλειδί έχει μέγεθος από 512 bits έως 1024 bits σε κάποια τιμή πολλαπλάσια των 64 bits. Το κλιμακούμενο μέγεθος του εξαρτάται από την μέθοδο επιλογής και το αντίστοιχο μέγεθος του πρώτου αριθμού και συντελεστή p. Η 512-bits εφαρμογή του DSA δεν είναι αρκετά ισχυρή για μακροπρόθεσμη ασφάλεια. Η αρχική πρόταση του NIST ήταν αυτή, αλλά μετά από μια περίοδο έντονης κριτικής και αμφισβήτησης, το Ίδρυμα αναθεώρησε την άποψη του επιτρέποντας την χρήση κλειδιών μέχρι και 1024 bits μέγεθος.

Κάποιοι ερευνητές κατέγραψαν την ύπαρξη μια «καταπακτής» στον σχεδιασμό του DSA, η οποία δίνει την δυνατότητα σε κάποιον κρυπταναλυτή, έχοντας πρόσβαση μέσω αυτής, να ανακτήσει δεδομένα του μηνύματος χωρίς την γνώση του αποστολέα. «Καταπακτή» ονομάζουμε ένα ευαίσθητο σημείο στη δομή ενός αλγορίθμου που μπορεί κάποια τρίτη οντότητα να εκμεταλλευτεί μέσα από την κρυπτολογική ανάλυση. Το δεδομένο είναι ότι ο DSA δεν κρυπτογραφεί κάποια δεδομένα. Η χρήση του είναι οπωσδήποτε διαφορετική. Το πραγματικό, λοιπόν, ζήτημα είναι εάν η σχεδίαση του είναι ευαίσθητη στην δυνατότητα σφυρηλάτησης της ψηφιακής υπογραφής, που σίγουρα θα αποφέρει δυσφήμιση ολόκληρου του συστήματος. Αυτή η πιθανότητα αποφεύγεται εύκολα εάν ακολουθούνται οι κατάλληλες διαδικασίες παραγωγής των κρυπτογραφικών κλειδιών.

5.Στεγανογραφία (Steganography)

5.1 Ιστορική Αναδρομή

Σε όλη τη διαδρομή της ιστορίας, ο άνθρωπος συνεχώς ανακάλυπτε νέες μεθόδους και τεχνικές που του επέτρεπαν να κρύψει κάποια πολύτιμη πληροφορία. Ένα από τα πρώτα κείμενα που περιγράφουν και ορίζουν τη στεγανογραφία (steganography) έρχεται από τον Ηρόδοτο. Στην αρχαία Ελλάδα, τα κείμενα συνήθως γράφονταν σε πίνακες καλυμμένους με κερί. Σε μια αφήγηση ιστορικού γεγονότος αναφέρεται ότι ο Δημάρατος ήθελε να ειδοποιήσει τη Σπάρτη, πως ο Ξέρξης είχε την πρόθεση να εισβάλει στην Ελλάδα. Για να αποφύγει λοιπόν την κλοπή του μηνύματος, έγραψε το μήνυμά του σε ξύλινη πινακίδα, αφού έξυσε το κερί που αυτή είχε και την οποία μετά κάλυψε πάλι με κερί. Οι πινακίδες φαίνονταν λευκές και αχρησιμοποίητες. Με αυτό τον τρόπο το μήνυμα πέρασε από κάθε έλεγχο και έδωσε σε εμάς το πρώτο καταγεγραμμένο ντοκουμέντο χρήσης στεγανογραφικής τεχνικής.

Μια άλλη κοινή μορφή αόρατης γραφής επιτυγχάνεται με τη χρήση αόρατου μελανιού. Τέτοιου είδους μελάνια χρησιμοποιήθηκαν με επιτυχία μέχρι και στο δεύτερο παγκόσμιο πόλεμο. Ένα αθώο, κατά τα φαινόμενα, γράμμα μπορεί να περιείχε ένα πολύ διαφορετικό μήνυμα γραμμένο ανάμεσα στις γραμμές από χαρακτήρες που γινόταν ορατές. Την εποχή του δευτέρου παγκοσμίου πολέμου, η τεχνολογία της στενογραφίας αποτελείτο κυρίως από τέτοια αόρατα μελάνια. Κάποια συστατικά, αναμεμειγμένα, σκουραίνουν όταν θερμαίνονται και αυτό τους το χαρακτηριστικό εκμεταλλεύτηκε η στεγανογραφία της εποχής. Με την ανάπτυξη βεβαίως της τεχνολογίας ανακαλύφθηκαν νέα, χημικά, υλικά που υλοποιούσαν ακριβώς την ίδια αόρατη τεχνική, αλλά η ανάκληση τους ήταν δυνατή μόνο κάτω από συγκεκριμένες προϋποθέσεις.

Άλλή μια μέθοδος που χρησιμοποιήθηκε κατά το παρελθόν είναι αυτή των «Null ciphers», μη κρυπτογραφημένων μηνυμάτων. Υπήρχε τότε, όπως και σήμερα, η τεχνική της ανίχνευσης υπόπτων μηνυμάτων μέσω κάποιων ειδικών φίλτρων μιας αυτοματοποιημένης διαδικασίας. Ωστόσο, τα «αθώα» μηνύματα περνούσαν ανενόχλητα. Το μόνο που είχε να κάνει κάποιος, ο οποίος ήθελε να μεταφέρει κάποια κρυφή πληροφορία, ήταν να την κάνει να φαίνεται όσο το δυνατόν πιο αθώα. Έτσι, έγραφε ένα τυχαίο κείμενο στο οποίο η πληροφορία βρισκόταν σε κάθε δεύτερο, για παράδειγμα, γράμμα των λέξεων που περιείχε το κείμενο.

Καθώς, όμως η τεχνολογία συνέχισε να αναπτύσσεται, βρέθηκαν νέοι τρόποι διακίνησης μεγαλύτερου όγκου πληροφορίας και με ακόμα πιο αόρατο τρόπο. Οι Γερμανοί ανέπτυξαν τη τεχνολογία των μικροτελειών (microdots). Οι μικροτελείες

είναι ουσιαστικά φωτογραφίες υψηλής ανάλυσης, ασήμαντου όμως μεγέθους (τελείες). Αυτή η τεχνική χρησιμοποιήθηκε από Γερμανούς κατάσκοπους για την μεταφορά απόρρητων δεδομένων κατά την διάρκεια του δευτέρου παγκοσμίου πόλεμου.

5.2 Ορισμοί - Ιδιότητες

Όπως μπορούμε να αντιληφθούμε και από το όνομά της, η **στεγανογραφία (steganography)** είναι η τέχνη, που στις μέρες μας έχει εξελιχθεί και σε τεχνική, που υλοποιεί μια διαδικασία επικοινωνίας, κατά τρόπο τέτοιο ώστε να κρύβεται η ίδια η ύπαρξη αυτής της επικοινωνίας. Σε αντίθεση με τη κρυπτογράφηση, όπου επιτρέπεται σε μια «τρίτη οντότητα» να ανιχνεύσει και να παρεμβληθεί ή ακόμα και να αιχμαλωτίσει τη πληροφορία, ο στόχος της στεγανογραφίας είναι να κρύψει την πληροφορία μέσα σε μια άλλη «αθώα» πληροφορία, με τέτοιο τρόπο που δεν δίνεται η δυνατότητα να ανιχνευθεί η ύπαρξή της.

Αυτή είναι η πιο διακριτή και σημαντική διαφορά της με την κρυπτογράφηση, χωρίς αυτό να σημαίνει ότι τελικά η φιλοσοφία τους έχει πολλά κοινά στοιχεία. Όμως, και οι δυο είναι τεχνικές που διατηρούν και προσφέρουν ασφάλεια στα δεδομένα και τους πόρους που διαχειρίζονται.

Η ύπαρξη και η εφαρμογή μιας μεθόδου που βασίζεται στις αρχές της στεγανογραφίας, εξαρτάται από ιδιαίτερες προϋποθέσεις και σίγουρα υλοποιείται μέσα σε στενά και συγκεκριμένα όρια. Ένα καλό και λειτουργικό στεγανογραφικό σύστημα πρέπει να εκπληρώνει τις προδιαγραφές που έθεσε η «Αρχή του Kerckhoff» στην κρυπτογραφία: «Η ασφάλεια ενός συστήματος πρέπει να βασίζεται στο δεδομένο ότι ο «εχθρός» έχει πλήρη γνώση των σχεδιαστικών λεπτομερειών αλλά και της υλοποίησης ενός κρυπτογραφικού συστήματος». Η μόνη πληροφορία που λείπει από τον «εχθρό» και που πρέπει να κρατηθεί μυστική, είναι ένας μικρός και εύκολα ανταλλάξιμος τυχαίος αριθμός, το κρυπτογραφικό κλειδί. Χωρίς αυτή την πληροφορία δεν είναι δυνατόν να γνωρίζει εάν στο κανάλι επικοινωνίας διενεργείται κρυφή επικοινωνία. Η πληροφορία που πρέπει να κρατηθεί μυστική για είναι βιώσιμο ένα στεγανογραφικό σύστημα είναι αυτή της ίδιας της ύπαρξης του.

Η στεγανογραφία σχετίζεται άμεσα με το πρόβλημα των «κρυμμένων καναλιών» στο σχεδιασμό ενός ασφαλούς περιβάλλοντος επικοινωνίας. Ένας ορισμός που αναφέρεται σε όλα τα μέσα επικοινωνίας που δεν μπορούν εύκολα να περιοριστούν από κάποιους μηχανισμούς ελέγχου. Παράδειγμα, δύο εφαρμογές-διαδικασίες που επικοινωνούν διαμορφώνοντας και μετρώντας το φόρτο της CPU.

Η στεγανογραφία σχετίζεται επιπλέον και με τη τεχνική εκπομπής ευρέως φάσματος, η οποία επιτρέπει την λήψη μηνυμάτων που είναι εκατό φορές πιο αδύνατα από τον ατμοσφαιρικό θόρυβο. Τα περισσότερα κανάλια επικοινωνιών, όπως οι τηλεφωνικές γραμμές και οι εκπομπές ράδιο, εκπέμπουν σήματα που συνοδεύονται πάντα από κάποιου μεγέθους θόρυβο. Αυτός ο θόρυβος μπορεί να αντικατασταθεί από κάποιο μυστικό σήμα, που έχει τη μορφή θορύβου, για κάποιον που δεν γνωρίζει το μυστικό κλειδί.

Εδώ φαίνεται η βασική σχεδιαστική αρχή των στεγανογραφικών συστημάτων. Υπάρχουν, όπως είναι φυσικό, πολλά προγράμματα που υλοποιούν κάποιου είδους στεγανογραφικό μηχανισμό. Ωστόσο, η πραγματικά καλή εφαρμογή της στεγανογραφίας είναι πολύ δύσκολη υπόθεση. Για αυτό ακριβώς το λόγο η ανίχνευση της ύπαρξης και χρήσης της από μηχανισμούς ανάλυσης, αποδίδει όταν πρόκειται για απλή εφαρμογή της. Η ανίχνευση αυτή στηρίζεται στα χαρακτηριστικά των αναλογικών συστημάτων. Ο θόρυβος των αναλογικών συστημάτων έχει ένα μεγάλο αριθμό ιδιοτήτων που είναι πολύ χαρακτηριστικές και ιδιαίτερες, τόσο για το κανάλι όσο και για τον εξοπλισμό του επικοινωνιακού συστήματος. Ένα λειτουργικό στεγανογραφικό σύστημα πρέπει να παρακολουθεί το κανάλι, να χτίζει ένα μοντέλο του θορύβου που είναι παρόν και μετά να προσαρμόζει τις παραμέτρους των δικών του αλγορίθμων και τεχνικών. Έτσι η αντικατάσταση του θορύβου του καναλιού με τον κατάλληλο τεχνητό θόρυβο, ο οποίος θα περιέχει την μυστική πληροφορία προς μετάδοση θα είναι επιτυχής. Το κατά πόσο το στεγανογραφικό σύστημα είναι ασφαλές, εξαρτάται από τους μηχανισμούς ανάλυσης του θορύβου που μπορεί να έχει στην διάθεση της μια τρίτη οντότητα. Όπως γίνεται προφανές, η λέξη κλειδί για ένα στεγανογραφικό σύστημα είναι αυτή της προσαρμογής. Προσαρμογή της εφαρμογής στα συγκεκριμένα χαρακτηριστικά του καναλιού επικοινωνίας και τις παραμέτρους που ισχύουν σε αυτό.

Εάν κάποιος ήθελε να εξετάσει ένα αρχείο με κρυμμένες πληροφορίες θα μπορούσε εύκολα να τις βρει. Στη χειρότερη περίπτωση, θα μπορούσε να καταλάβει ότι αυτές υπάρχουν έστω και αν δεν τις έβλεπε. Εάν οι κρυμμένες πληροφορίες είναι κρυπτογραφημένες, τότε σίγουρα θα φτάσει μέχρι αυτό το σημείο και θα σταματήσει. Εάν ωστόσο, δεν είναι κρυπτογραφημένες τότε θα είναι σε θέση να εξετάσει το σύνολο των κρυμμένων δεδομένων. Για το λόγο αυτό, δεν θα πρέπει να θεωρούμε τη στεγανογραφία σαν αντικαταστάτη της κρυπτογραφίας. Σαν μια μέθοδο που κατακτά τους ίδιους στόχους στο ευαίσθητο ζήτημα της ασφάλειας των δεδομένων ψηφιακής μορφής. Χωρίς αμφισβήτηση και οι δύο τεχνολογίες μπορούν να χαρακτηριστούν ως μέθοδοι ασφάλειας. Η στεγανογραφία πρέπει όμως να θεωρηθεί σαν η τεχνική εκείνη που θα μπορούσε να χρησιμεύσει σαν ένα συμπλήρωμά της κρυπτογράφησης.

5.3 Τεχνικές και ανάλυση της στεγανογραφίας

Η στεγανογραφία βασίζει την ασφάλειά της στο γεγονός ότι κάποιος δεν μπορεί να ψάξει για κάτι που δεν γνωρίζει εάν υπάρχει. Η άγνοια ύπαρξης ενός, στεγανογραφικά, ενσωματωμένου μηνύματος αποτελεί την προϋπόθεση για την επιτυχή παράδοση του. Επιπλέον, όλες τις μετακινήσεις του ανυπολόγιστα τεράστιου όγκου δεδομένων που λαμβάνουν χώρα καθημερνά στο Διαδίκτυο είναι ένα μεγάλο πλεονέκτημα. Κανείς ίσως δεν έχει την απαιτούμενη υπολογιστική ισχύ για να περάσει από ανίχνευση το σύνολο των δεδομένων, των εικόνων και γενικότερα των εφαρμογών πολυμέσων τα οποία διακινούνται.

Πολλές διαφορετικές στεγανογραφικές μέθοδοι έχουν προταθεί κατά τη διάρκεια της τελευταίας δεκαετίας. Υπάρχουν διάφορες προσεγγίσεις στην ταξινόμηση αυτών των συστημάτων. Μια ταξινόμηση μπορεί να γίνει σύμφωνα με τις τροποποιήσεις κάλυψης που συμβαίνουν στο αρχικό σήμα, εφαρμόζοντας την διαδικασία ενσωμάτωσης των μυστικών πληροφοριών. Προσεγγίζοντας αυτή την ταξινόμηση, μπορούμε να διαχωρίσουμε τις στεγανογραφικές μεθόδους στις ακόλουθες κατηγορίες, αν και σε μερικές περιπτώσεις μια ακριβής ταξινόμηση δεν είναι δυνατή:

Τα **συστήματα αντικατάστασης** (substitution systems) με την εφαρμογή των οποίων αντικαθιστώνται περιττά μέρη ενός σήματος, με τα bits από ένα μυστικό μήνυμα. Η αντικατάσταση γίνεται στα λιγότερο σημαντικά bits του σήματος. Ο δέκτης μπορεί να εξαγάγει τις πληροφορίες εάν έχει τη γνώση από τις θέσεις όπου οι μυστικές πληροφορίες έχουν ενσωματωθεί. Δεδομένου ότι μόνο κάποιες δευτερεύουσες τροποποιήσεις γίνονται με την διαδικασία ενσωμάτωσης, ο αποστολέας υποθέτει ότι δεν θα παρατηρηθούν από μια παθητική οντότητα. Η αλλαγή αυτών των bits προκαλεί ανεπαίσθητες αλλαγές στη μορφή του σήματος, στοιχείο που προσδίδει την ασφάλεια στα συστήματα αντικατάστασης.

Διάφορες μέθοδοι υπάρχουν για το κρύψιμο των πληροφοριών στα διάφορα μέσα. Η σειρά αυτών των μεθόδων ορίζεται από την κωδικοποίηση LSB, με απλό χειρισμό μιας εικόνας ή χρήση αλγορίθμων συμπίεσης, με σκοπό την τροποποίηση κάποιων ιδιοτήτων του σήματος, όπως για παράδειγμα τη φωτεινότητα. Οι τεχνικές τροποποίησης LSB είναι πρακτικά εύκολοι τρόποι ενσωμάτωσης των μυστικών πληροφοριών. Το κυριότερο μειονέκτημα τους είναι ότι εμφανίζονται ιδιαίτερα τρωτές, ακόμη και σε μικρού μεγέθους τροποποιήσεις κάλυψης.

Οι **τεχνικές μετατροπής περιοχών** (transform domain techniques) ενσωματώνουν τις μυστικές πληροφορίες σε ένα διάστημα μετατροπής του σήματος. Παράδειγμα σε μια περιοχή συχνότητας. Έχει σημειωθεί τα τελευταία χρόνια αξιόλογη ανάπτυξη των στεγανογραφικών συστημάτων, που ενσωματώνουν πληροφορίες στη περιοχή συχνότητα ενός σήματος.

Μια τέτοια τεχνική είναι και η χρήση της μετατροπής wavelet (wavelet transform). Κατά την διαδικασία μιας wavelet μετατροπής χρησιμοποιούνται κάποιες μαθηματικές λειτουργίες, οι οποίες και εφαρμόζονται στα σήματα μεταφοράς. Σήματα μιας ή και περισσοτέρων διαστάσεων, όπως εφαρμογές ήχου, βίντεο, είτε και ψηφιακών εικόνων. Η μέθοδος των wavelets έχει την ιδιότητα να αποσυνθέτει το σήμα στις τάσεις και τις λεπτομέρειες του. Σε μια εφαρμογή αυτής της τεχνικής, αρχικά κάποιος θα χρησιμοποιούσε τα wavelets για να αποσυνθέσει το σήμα. Κατόπιν, θα τα ξαναχρησιμοποιούσε για να κρύψει το μυστικό μήνυμα στο αποσυντεθειμένο ήδη σήμα.

Η τεχνική ενσωμάτωσης, στεγανογραφικά, κρυμμένων πληροφοριών σε μέσα ψηφιακών εικόνων καταδεικνύουν ιδιαίτερη πειραματική ανάλυση τα τελευταία χρόνια. Μερικές ευαίσθητες πληροφορίες, συνδυάζονται «σιωπηρά» με ένα κομμάτι από δεδομένα διαμορφώνοντας ένα σύνθετο σήμα (στεγανο-εικόνα). Μια μέθοδος στεγανογραφιάς εικόνας που εμφανίζεται εξαιρετικά γερή είναι η ενσωμάτωση των πληροφοριών σε εικόνα με JPEG συμπίεση. Η μέθοδος αυτή βασίζεται σε wavelet μετατροπή δυο διαστάσεων.

Οι εικόνες συμπιέζονται συνήθως πριν από τη μετάδοση ή την αποθήκευση τους. Έτσι η ενσωμάτωση των πληροφοριών σε ένα συμπιεσμένο στοιχείο χαρακτηρίζεται ως η καλύτερη επιλογή. Δεδομένου ότι σε πολλές εικόνες εφαρμόζεται συμπίεση JPEG2000 και ο αριθμός αυτός θα πολλαπλασιάζεται στο άμεσο μέλλον, αξίζει να αναφερθεί ο τρόπος με τον οποίο ενσωματώνεται αποτελεσματικά ένας μεγάλος όγκος δεδομένων.

Η ψηφιακή εικόνα υποβάλλεται αρχικά σε μια μετατροπή (wavelet transform). Στην συνέχεια οι παραγόμενοι wavelet συντελεστές κβαντοποιούνται και κωδικοποιούνται. Ένας στατιστικός έλεγχος εφαρμόζεται κατά την διάρκεια του βήματος της κωδικοποίησης, προκειμένου να επιτευχθεί η ανίχνευση μηδενικών bits .Οι κρυμμένες πληροφορίες μπορούν να ενσωματωθούν ακόμα και σε μηδενικά bit λάθους. Η διαδικασία της ανάκτησης ουσιαστικά αντιστρέφει τις λειτουργίες, με αποκωδικοποίηση και απο-κβαντοποιήση των bits και τέλος την εφαρμογή του αντιστρόφου της αρχικής μετατροπής της εικόνας για την αναδημιουργία της.

Οι **στατιστικές μέθοδοι** (statistical methods), όπου κωδικοποιούνται οι μυστικές πληροφορίες με την αλλαγή διάφορων στατιστικών ιδιοτήτων ενός σήματος και εφαρμόζουν μια διαδικασία δοκιμής (test) κατά την λειτουργία της εξαγωγής. Οι στατιστικές τεχνικές στεγανογραφίας χρησιμοποιούν την ύπαρξη στεγανογραφικών σχεδίων των «1-bit», τα οποία ενσωματώνουν ένα bit από πληροφορίες σε έναν ψηφιακό μεταφορέα (σήμα). Το σύνολο των ενσωματωμένων bits αυτού του μεταφορέα αποτελεί το μυστικό στεγανό-μήνυμα. Αυτό γίνεται με την τροποποίηση του σήματος, κατά τρόπο τέτοιο ώστε κάποια στατιστικής φύσεως χαρακτηριστικά να μετατρέπονται σημαντικά, εάν διαβιβάζεται bit με τιμή «1». Διαφορετικά, εάν η τιμή είναι το «0», το σήμα

αφήνεται ουσιαστικά αμετάβλητο. Έτσι ο δέκτης πρέπει να είναι σε θέση να διακρίνει τα σήματα χωρίς τροποποιήσεις από τα τροποποιημένα.

Πιο συγκεκριμένα, αρχικά διαιρείται το σήμα σε ισόποσα blocks. Ένα μυστικό bit παρεμβάλλεται με την τοποθέτηση του χαρακτήρα «1» εάν η τιμή είναι bit = 1. Διαφορετικά το block δεν αλλάζει κατά την διαδικασία ενσωμάτωσης. Η ανίχνευση ενός συγκεκριμένου κομματιού (block) γίνεται μέσω μιας λειτουργίας δοκιμής που διακρίνει και διαχωρίζει τα τροποποιημένα blocks. Η λειτουργία αυτή περιλαμβάνει ένα τεστ στατιστικής υπόθεσης, λόγος που χαρακτηρίζει τις μεθόδους της κατηγορίας στατιστικές.

Το σήμα στο οποίο ενσωματώνονται οι πληροφορίες του στεγανό-μηνύματος μπορεί να είναι ένα κείμενο με χαρακτήρες, μια εικόνα, ένα αρχείο ήχου ή οποιοσδήποτε ψηφιακός κώδικας. Παρακάτω θα αναφερθεί ακόμα πιο απλά ως «μέσο μεταφοράς». Συνήθως, στην στεγανογραφική ορολογία, μπορεί να βρεθεί και ως «κάλυψη» (cover). Οποιαδήποτε λέξη και να το χαρακτηρίσει, αυτό το μέσο μεταφοράς, το σημαντικότερο είναι ότι ο ρόλος του στην εφαρμογή ενός στεγανογραφικού συστήματος είναι τέτοιος που αποσκοπεί στην επιτυχή παράδοση των μυστικών δεδομένων.

Η στεγανογραφία γίνεται όλο και πιο σημαντική στον Κυβερνοχώρο, εξαιτίας του ότι οι κυβερνήσεις αρκετών χωρών απαγορεύουν τη χρήση ισχυρής κρυπτογράφησης από ιδιώτες, χαρακτηρίζοντας την μη αποδεκτή νομικά. Τέτοιες χώρες είναι η Γαλλία και η Ρωσία. Η εφαρμογή ενός στεγανογραφικού συστήματος είναι ίσως πιο πρακτική για έναν χρηστή, εφόσον μπορεί κάλλιστα να αρνηθεί την αποστολή ενός κρυπτογραφημένου και κρυμμένου, στεγανογραφικά, μηνύματος από το να το κάνει για ένα απλά κρυπτογραφημένο. Εάν κάποιος κρύψει πληροφορία σε μια εικόνα για παράδειγμα, μπορεί εύκολα να το αρνηθεί, καθώς είναι πραγματικά δύσκολο για την αρχή που διενεργεί τον έλεγχο να αποδείξει το αντίθετο.

5.4 Στεγανάλυση (steganalysis)

Η **στεγανάλυση** (steganalysis) είναι η τεχνική της ανίχνευσης της κρυμμένης, στεγανογραφικά, πληροφορίας. Η στεγανογραφία διαβιβάζει την κρυμμένη αυτή πληροφορία μέσω των, προφανώς, αβλαβών σημάτων σε μια προσπάθεια να κρυφτεί η ύπαρξη της. Τα εργαλεία της στεγανάλυσης τα οποία εξετάζουν την ικανότητα επιβίωσης των στεγανογραφικών εφαρμογών, είναι ουσιαστικά η βάση για την εξέλιξη ισχυρότερων τεχνικών. Χρησιμοποιώντας τις μεθόδους στεγανάλυσης, οι ερευνητές αποσκοπούν στο να κατανοήσουν πόσο μεγαλύτερη προσπάθεια απαιτείται για να καταστήσουν τις ενσωματωμένες πληροφορίες δυσανάγνωστες.

Κάθε σήμα μπορεί κάλλιστα να τροποποιηθεί με στόχο τη καταστροφή κάποιας κρυμμένης πληροφορίας που πιθανόν να υπάρχει μέσα της. Η απόσπαση, καταστροφή του σήματος είναι μια διαδικασία έκτακτης ανάγκης και δεν προτείνεται. Εξάλλου, η ανίχνευση της ύπαρξης ενδεχόμενης κρυμμένης πληροφορίας εξοικονομεί χρόνο από τη διαδικασία καταστροφής. Η ανάκτηση του κρυμμένου μηνύματος είναι και αυτή χρονοβόρα αλλά γίνεται μόνο όταν η πληροφορία έχει βρεθεί.

Η ορολογία των στεγαναλυτικών τεχνικών είναι παρόμοια με αυτή των τεχνικών κρυπτανάλυσης, υπάρχουν ωστόσο και σημαντικές διαφορές. Ισχύει η, περιγραφική της λειτουργίας του συστήματος, εξίσωση :

μέσο μεταφοράς + μήνυμα + στεγανο-κλειδί = στεγανο-μέσο.

Όπου:

- Το μέσο μεταφοράς αποτελεί εικόνα, ήχο, κείμενο ή κάποιο άλλο ψηφιακό κώδικα.
- Το μήνυμα είναι το σύνολο των πληροφοριών που θέλουμε να κρύψουμε. Μαζί με το μέσο μεταφοράς αποτελούν το στεγανο-φορέα (stego-carrier).
- Το στεγανο-κλειδί αποτελεί την επιπλέον πληροφορία ασφάλειας, με την χρήση της οποίας ανακτώνται οι πληροφορίες του μηνύματος.

Στην στεγανάλυση ενός σήματος γίνονται συγκρίσεις ανάμεσα στο αρχικό μέσο μεταφοράς και το στεγανο-μέσο που αποτελεί την έξοδο της διαδικασίας ενσωμάτωσης του μηνύματος. Όπως ακριβώς η κρυπτανάλυση εφαρμόζει διάφορες τεχνικές με σκοπό την αποκρυπτογράφηση της πληροφορίας, έτσι και η στεγανάλυση εφαρμόζοντας δικές της τεχνικές στοχεύει στην ανίχνευση και στην συνέχεια την ανάκτηση της κρυμμένης πληροφορίας.

Ο στεγαναλυτής χρησιμοποιεί τεχνικές επίθεσης και ανίχνευσης ανάλογα με το τι είδους πληροφορία μπορεί να έχει στην κατοχή του ή απλά να γνωρίζει.

Μία μορφή επίθεσης είναι η «στεγανο-αποκλειστική» επίθεση (stego-only attack) όπου διαθέσιμο για ανάλυση είναι μόνο το στεγανογραφικά ενσωματωμένο σήμα (στεγανο-μέσο). Η διαδικασία προφανώς είναι αρκετά πολύπλοκη και υλοποιείται όταν γίνεται προσέγγιση σε ορατά σημάδια της κρυμμένης πληροφορίας, είτε η στεγανογραφική εφαρμογής έχει σημαντικές αδυναμίες. Στα τωρινό επίπεδα στεγανογραφιάς η επιτυχία μιας τέτοιος επίθεσης φαντάζει αδύνατη.

Εάν τόσο το αρχικό μέσο μεταφοράς όσο και το στεγανο-μέσο που περιέχει την κρυμμένη πληροφορία είναι διαθέσιμα, τότε έχουμε την δεύτερη μορφή επίθεσης στεγανάλυσης. Η επίθεση «γνωστού μέσου» (known cover attack) είναι πρακτική για έναν αναλυτή όταν το στεγανο-μέσο αποκαλυφθεί κάποια στιγμή

μετά την παράδοση και ανάκτηση του κρυμμένου μηνύματος. Στόχος του είναι η ανάλυση του για την περίπτωση μελλοντικών επιθέσεων.

Η επίθεση «γνωστού μηνύματος» (known message attack) είναι από τις πιο πολυεφαρμοσμένες και αποτελεσματικές προσπάθειες στεγανάλυσης. Σε ένα μέρος του μόνο, το κρυμμένο μήνυμα μπορεί να γίνει γνωστό στον αναλυτή. Αυτό δεν σημαίνει απαραίτητα ότι μπορεί να ανακτηθεί και το σύνολο του. Η λειτουργία ανάλυσης του στεγανο-μέσου για τα σχέδια που χρησιμοποιήθηκαν κατά την ενσωμάτωση του, μπορεί όμως να φανεί χρήσιμη σε επόμενες επιθέσεις στεγανάλυσης.

Μια άλλη μορφή επίθεσης είναι η «επιλεκτική στεγανο-επίθεση» (chosen stego attack). Σε αυτήν τόσο το εργαλείο (αλγόριθμος) που χρησιμοποιήθηκε για τη στεγανογράφηση, όσο και το στεγανο-μέσο είναι γνωστά. Μια επίθεση επιλεγμένου μέσου είναι αυτή κατά την οποία ο στεγαναλυτής αναλύει το στεγανο-μέσο που δημιουργήθηκε από κάποιο συγκεκριμένο στεγανογραφικό εργαλείο ή αλγόριθμο. Ο στόχος μιας τέτοιας επίθεσης είναι ο καθορισμός συγκεκριμένων ιδιοτήτων του στεγανο-μέσου οι οποίες διαμορφώνονται με την χρήση κάποιου στεγανογραφικού αλγορίθμου ή εργαλείου.

Ακόμη και η «καλύτερη» εναλλακτική λύση να υπάρχει για τον επιτιθέμενο, το ενσωματωμένο μήνυμα μπορεί να παραμένει δύσκολο να εξαχθεί. Μερικές φορές, η πιο κατάλληλη προσέγγιση δεν είναι η επίθεση και η ανάλυση στην τεχνική ή την μέθοδο στεγανογράφησης που εφαρμόστηκε. Η γνώση ή η ανάκτηση της επιπρόσθετης πληροφορίας, του στεγανο-κλειδιού, είναι πολλές φορές επιτυχής.

Ευρετήριο-Ορισμοί

Αλγόριθμος κρυπτογράφησης (algorithm encryption), μέθοδος που υλοποιεί τις διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης και συμπεριλαμβάνει ένα σύνολο μαθηματικών τύπων.
(σελ. 13).

Αλγόριθμοι κρυπτογράφησης, συμμετρικοί (symmetric algorithms), αλγόριθμοι που χρησιμοποιούν ένα μόνο κρυπτογραφικό κλειδί κατά τις διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης των δεδομένων.
(σελ. 17, 21).

Αλγόριθμοι κρυπτογράφησης, δημοσίου κλειδιού (public key algorithms), αλγόριθμοι που χρησιμοποιούν ένα ζεύγος κρυπτογραφικών κλειδιών κατά τις διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης των δεδομένων.
(σελ. 17, 45).

Αντικατάσταση S-Box (S-box substitution), λειτουργία κατά την εφαρμογή του αλγορίθμου κρυπτογράφησης DES.
(σελ. 29).

Αποκρυπτογράφηση (decryption), η διεργασία ανάκτησης του αρχικού μηνύματος σε αναγνώσιμη μορφή από μια έκδοση που έχει παραχθεί κατά την διαδικασία κρυπτογράφησης.
(σελ. 5).

Διαχείριση κρυπτογραφικού κλειδιού (key management), οι διαδικασίες της παραγωγής, μεταφοράς, χρησιμοποίησης, αποθήκευσης και τελικά καταστροφής ενός κρυπτογραφικού κλειδιού.
(σελ. 15).

Κείμενο, αρχικό (plaintext), το σύνολο των δεδομένων που αποτελούν την είσοδο σε μια διεργασία κρυπτογράφησης.
(σελ. 5).

Κείμενο, κρυπτογραφημένο (chipertext), το αποτέλεσμα της εφαρμογής μιας κρυπτογραφικής τεχνικής ή ενός αλγόριθμου κρυπτογράφησης πάνω στο αρχικό κείμενο.
(σελ. 5).

Κλειδί, δημόσιο (public key), το κρυπτογραφικό κλειδί ενός αλγόριθμου που μπορεί να γίνει δημόσια γνωστό χωρίς να κλονιστεί η ασφάλεια του συστήματος κρυπτογράφησης.
(σελ. 15, 45).

Κλειδί, κρυπτογράφησης (encryption key), μια τιμή από μια μεγάλη λίστα τιμών που χρησιμοποιείται από τις διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης.
(σελ. 14).

Κλειδί ιδιωτικό (private key), το κρυπτογραφικό κλειδί ενός αλγόριθμου που κρατείτε μυστικό και προστατεύεται από υποκλοπή ή τροποποίηση του.
(σελ. 15, 45).

Κρυπτανάλυση (cryptanalysis), η διεργασία αποκρυπτογράφησης από μία μη εξουσιοδοτημένη οντότητα.
(σελ. 5).

Κρυπτογραφία (encryption), διεργασία μετασχηματισμού ενός μηνύματος σε μια ακατανόητη μορφή, με την χρήση ενός κρυπτογραφικού αλγορίθμου, έτσι ώστε αυτό να μην είναι αναγνώσιμο μη εξουσιοδοτημένες οντότητες .
(σελ. 5).

Κρυπτολογία (cryptology), ο κλάδος των μαθηματικών που καλύπτει την κρυπτογραφία και την κρυπτολογική ανάλυση .
(σελ. 6).

Μεταλλαγή επέκτασης (expansion permutation), λειτουργία κατά την εφαρμογή του αλγορίθμου κρυπτογράφησης DES.
(σελ. 29).

Μεταλλαγή συμπίεσης (compression permutation), λειτουργία κατά την εφαρμογή του αλγορίθμου κρυπτογράφησης DES.
(σελ. 29).

Περιορισμένοι αλγόριθμοι, αλγόριθμοι κρυπτογράφησης των οποίων η ασφάλεια εξαρτάται εξ ολοκλήρου από το αν αυτός παραμείνει κρυφός ή όχι.
(σελ. 14).

Στατιστικές μέθοδοι (statistical methods), κατηγορία στεγανογραφικών μεθόδων.
(σελ. 66).

Στεγανάλυση (steganalysis), η τεχνική της ανίχνευσης της κρυμμένης, στεγανογραφικά, πληροφορίας.
(σελ. 67).

Στεγανογραφία (steganography), η τεχνική που υλοποιεί μια διαδικασία επικοινωνίας, κατά τρόπο τέτοιο ώστε να κρύβεται η ίδια η ύπαρξη αυτής της επικοινωνίας.
(σελ. 63).

Συστήματα αντικατάστασης (substitution systems), κατηγορία στεγανογραφικών μεθόδων.
(σελ. 65).

Τεχνικές μετατροπής περιοχών (transform domain techniques), κατηγορία στεγανογραφικών μεθόδων.
(σελ. 65).

Ψηφιακές υπογραφές (digital signatures), κρυπτογραφικοί μηχανισμοί που λειτουργούν όπως ακριβώς και οι γραπτές υπογραφές ενός ατόμου.
(σελ. 48, 58).

Block cipher, τύπος κρυπτογραφικού αλγορίθμου που εφαρμόζεται πάνω σε κομμάτια (blocks) του αρχικού και του κρυπτογραφημένου κειμένου κάθε φορά.
(σελ. 21).

Cryptographic mode, το σύνολο των λειτουργιών της όλης διαδικασίας κρυπτογράφησης.
(σελ. 22).

DES (Data Encryption Standard), συμμετρικός αλγόριθμος κρυπτογράφησης.
(σελ. 25, 53)

DSA (Digital Signature Algorithm), αλγόριθμος κρυπτογράφησης δημοσίου κλειδιού.
(σελ. 58).

IDEA (International Data Encryption Algorithm), συμμετρικός αλγόριθμος κρυπτογράφησης.
(σελ. 35).

NBS (Εθνικό Ίδρυμα Προτύπων).
(σελ. 26).

NIST (Εθνικό Ίδρυμα Προτύπων και Τεχνολογίας)
(σελ. 58).

NSA (Αντιπροσωπεία Εθνικής Ασφάλειας).
(σελ. 27, 35).

RC5, συμμετρικός αλγόριθμος κρυπτογράφησης.
(σελ. 40).

RSA, αλγόριθμος κρυπτογράφησης δημοσίου κλειδιού.
(σελ. 49, 50).

RSA Security
(σελ. 40, 56, 58).

Stream cipher, τύπος κρυπτογραφικού αλγόριθμου που εφαρμόζεται πάνω σε ένα bit ή ένα byte των δεδομένων κάθε φορά.
(σελ. 21).

SSL (Secure Sockets Layer), πρωτόκολλο ασφαλής επικοινωνίας μέσω του Διαδικτύου.
(σελ. 57).

Βιβλιογραφία

Συγγράμματα:

- "Applied Cryptography - Protocols, Algorithms, and Source Code", Bruce Schneier, 1996.
- "Artech House Information Hiding Techniques for Steganography and Digital Watermarking", Stefan Katzenbeisser, Fabien A. P. Petitcolas, London 2000.
- "Handbook of Applied Cryptography", A. Menezes, P. van Oorschot, S. Vanstone, 1997.
- "Introduction to Cryptography", David Bishop, 2003.

Δικτυακοί τόποι:

- http://www.cryptography.com/newsevents/news_articles.html
- http://www.cryptography.com/
- http://www.nsa.gov/
- http://www.rsasecurity.com/