ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ

ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Αλγόριθμοι Κρυπτογράφησης και υλοποίηση του αλγορίθμου RSA με λογισμικό Matlab

i) Γεωργαλάς Στυλιανός

ii) Κορώνης Λάμπρος

Α.Μ : i) 2097
ii) 2146

Επιβλέπων Καθηγητής : Ασημακόπουλος Γεώργιος

Πάτρα Ιανουάριος 2020

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή

Πάτρα, Ημερομηνία

ΕΠΙΤΡΟΠΗ ΑΞΙΟΛΟΓΗΣΗΣ

1. Ονοματεπώνυμο, Υπογραφή

2. Ονοματεπώνυμο, Υπογραφή

3. Ονοματεπώνυμο, Υπογραφή

Υπεύθυνη Δήλωση Φοιτητή

Βεβαιώνω ότι είμαι συγγραφέας αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επίσης βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τη συγκεκριμένη εργασία.

Η έγκριση της διπλωματικής εργασίας από το Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Πανεπιστημίου Πελοποννήσου δεν υποδηλώνει απαραιτήτως και αποδοχή των απόψεων του συγγραφέα εκ μέρους του Τμήματος.

Ευχαριστίες

Αρχικά θα θέλαμε να εκφράσουμε τις ευχαριστίες μας στον Καθηγητή κ. Ασημακόπουλο Γεώργιο για την δυνατότητα που μας έδωσε να πραγματοποιήσουμε την πτυχιακή μας εργασία και για το πολύτιμο χρόνο που διέθεσε για την περάτωση της.

Θα θέλαμε να ευχαριστήσουμε ακόμα, όλους του καθηγητές του Τμήματος Μηχανικών Πληροφορικής Δυτικής Ελλάδος για τις πολύτιμες γνώσεις που μας προσέφεραν όλα αυτά τα χρόνια των σπουδών.

Τέλος, θέλαμε να εκφράσουμε ένα τεράστιο ευχαριστώ στην οικογένεια μας, για την στήριξη και την εμπιστοσύνη που μας έδειξε όλα αυτά τα χρόνια των σπουδών μας. Πέραν όμως από την πολύτιμη αυτή στήριξη, μας έδωσαν όλα τα εφόδια ώστε να γίνουμε καλύτεροι Άνθρωποι και αυτό είναι κάτι που δεν μαθαίνεται, αλλά μεταδίδεται.

Περιεχόμενα

Ευχαριστίες 3
Περίληψη 6
Summary 7
ΚΕΦΑΛΑΙΟ 1 : ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ 8
1.1 Εισαγωγή 8
1.2 Ιστορική Αναδρομή 9
1.2.1 Από την Αρχαιότητα έως την Αναγέννηση 9
1.2 Ύστερη Αναγέννηση(19ος -20ος Αιώνας) 10
1.3 Enigma : "Η μεγάλη Ώρα του Alan Turung" 11
1.4 Σύγχρονη κρυπτογραφία 12
1.4.1 21ος αιώνας 13
ΚΕΦΑΛΑΙΟ 2ο: ΚΛΑΣΣΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ 14
2.1 Μονοαλφαβητικά Συστήματα Αντικατάστασης 15
2.1.1 Κώδικας του Καίσαρα (Caesar's Cipher) 15
2.2 Πολυαλφαβητικά Συστήματα Αντικατάστασης 16
2.2.1 Κρυπτοσύστημα VIGENÉRE 16
2.2.2 Ο κώδικας Vernam (one-time pad) 18
ΚΕΦΑΛΑΙΟ 3ο : ΣΥΓΧΡΟΝΑ ΣΥΣΤΗΜΑΤΑ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ 19
3.1 Είδη Κρυπτογραφίας 20
3.1.1 Ασύμμετρη Κρυπτογραφία 20
3.1.2 Συμμετρική Κρυπτογραφία 21
3.1.3 Μειονεκτήματα και Πλεονεκτήματα 22
3.2 Κρυπτογραφικά Εργαλεία 23
3.2.1 Κώδικες Τμήματος 23
3.2.2 Τρόποι Λειτουργίας 24
3.2.3 Κώδικες Ροής 28
3.2.4 One-time Pads 28
3.2.5 Συναρτήσεις Κατακερματισμού 30
3.2.6 Message Authentication Code (MAC) 31
3.2.7 Μηχανισμοί Διαχείρισης και Ανταλλαγής Κλειδιών 32
3.3 Απλές Εφαρμογές της Κρυπτογραφίας 32
3.3.1 Διαφύλαξη του Απορρήτου και Κρυπτογράφηση 32

3.3.2 Πιστοποίηση Ταυτότητας και Ψηφιακές Υπογραφές 33
ΚΕΦΑΛΑΙΟ 4ο : ΑΛΓΟΡΙΘΜΟΙ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ 35
4.1 Αλγόριθμοι Ασύμμετρης Κρυπτογραφίας 35
4.2 Αλγόριθμοι Συμμετρικής Κρυπτογραφίας 36
4.3 Συναρτήσεις Κατακερματισμού 39
4.4 Αλγόριθμοι Ανταλλαγής Κλειδιών 40
4.5 Αρχές Έκδοσης Πιστοποιητικών 42
ΚΕΦΑΛΑΙΟ 5ο : ΑΛΓΟΡΙΘΜΟΣ RSA 45
5.1 Ιστορική Αναδρομή 45
5.2 Περιγραφή του RSA 46
5.3 Ταχύτητα του RSA 47
5.4 Ασφάλεια του RSA 48
5.5 Χρησιμότητα του RSA 50
ΚΕΦΑΛΑΙΟ 6ο : ΠΕΙΡΑΜΑΤΙΚΟ ΜΕΡΟΣ 53
ΠΑΡΑΡΤΗΜΑ Α 58
ΠΑΡΑΡΤΗΜΑ Β 59
ΒΙΒΛΙΟΓΡΑΦΙΑ 60

Περίληψη

Αντικείμενο της συγκεκριμένης πτυχιακής εργασίας είναι η Κρυπτογραφία και η εξέλιξη της. Ειδικότερα, θα μελετηθεί η ιστορική αναφορά της εμφάνισης της κρυπτογραφίας με έμφαση στην σύγχρονη εποχή και στους κώδικες κρυπτογράφησης στις τηλεπικοινωνίες .

Η εργασία ξεκινά με μία εκτενής ιστορική αναδρομή για να δούμε την εξέλιξη της μέσα στους αιώνες, πως ξεκίνησε, με ποια μέσα μπόρεσε και εξελίχθηκε καθώς επίσης και τις διαφορετικές εφαρμογές μέσα στον χρόνο.

Στην συνέχεια γίνεται αναφορά στις κατηγορίες των αλγορίθμων κρυπτογράφησης καθώς και λεπτομερής αναφορά στους σημαντικότερους εξ αυτών.

Τέλος, στην εργασία θα παρουσιαστεί το πειραματικό μέρος όπου θα αναπτυχθεί με τη χρήση του λογισμικού πακέτου Matlab με κώδικα προσομοίωσης ενός από τους σημαντικότερους αλγορίθμους κρυπτογράφησης, του RSA.

Summary

The subject of this thesis is Cryptography and its evolution. In particular, the historical reference to the emergence of cryptography will be studied, with emphasis on the modern era and the codes of encryption in telecommunications.

The thesis begins with an extensive historical overview to see its evolution over the centuries, how it began, with what means it has been able and evolved as well as the different applications over time.

In addition, the categories of the encryption algorithms are then referred to in detail giving emphasis to the most important of them.

Finally, in thesis will presented an experimental part where it will be developed using the Matlab software package with simulation code of one of the most important encryption algorithms, the RSA.

ΚΕΦΑΛΑΙΟ 1 : ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ

1.1 Εισαγωγή

Η κρυπτολογία, ως ο κλάδος που ασχολείται με ζητήματα ασφάλειας των επικοινωνιών, έχει μία πλούσια ιστορία χιλιάδων ετών, όσων δηλαδή και οι διάφοροι τρόποι επικοινωνίας: ξεκινάει με την εμφάνιση πρωτόλειων μορφών κρυπτογράφησης, που βασίζονται σε απλές αντικαταστάσεις των συμβόλων του μεταδιδόμενου μηνύματος, και συνεχίζεται μέχρι σήμερα όπου έχει αναπτυχθεί μια πληθώρα πολύπλοκων αλγορίθμων κρυπτογράφησης αλλά και σύνθετων πρωτοκόλλων που στηρίζονται στην απόκρυψη πληροφορίας.

Ιδιαίτερα στις τελευταίες δεκαετίες, η ραγδαία άνθηση των τηλεπικοινωνιών (με κυριότερο εκφραστή αυτής το διαδίκτυο) έχει καταστήσει τη διασφάλιση του απορρήτου των επικοινωνιών απόλυτη ανάγκη, φέρνοντας την κρυπτολογία στο επίκεντρο των τεχνολογικών εξελίξεων. Η κρυπτολογία αποτελεί πλέον αντικείμενο έντονης ερευνητικής δραστηριότητας, η οποία την έχει μετατρέψει από μορφή τέχνης σε επιστήμη, με αυστηρούς ορισμούς και αποδείξεις. Τυπικά με τον όρο ‘κρυπτολογία’ αναφερόμαστε τόσο στην κρυπτογραφία όσο και στην κρυπτανάλυση: η κρυπτογραφία ασχολείται με τον σχεδιασμό κρυπτοσυστημάτων, ενώ η κρυπτανάλυση μελετά το σπάσιμό τους. Καταχρηστικά, ο όρος ‘κρυπτολογία’ έχει “απορροφηθεί” από τον όρο ‘κρυπτογραφία’.

1.2 Ιστορική Αναδρομή

1.2.1 Από την Αρχαιότητα έως την Αναγέννηση

Η κρυπτογραφία εμφανίζεται με τη μορφή τέχνης από τα πρώτα χρόνια που ο άνθρωπος άρχισε να γράφει. Χαρακτηριστικό παράδειγμα ο δίσκος της Φαιστού που θεωρείται το αρχαιότερο έντυπο στην ιστορία του ανθρώπου. Για το κείμενο του δίσκου, που χρονολογείται γύρω στον 17ο π.Χ. αιώνα έχουν δοθεί πολλές ερμηνείες, παρ' όλα αυτά καμία δε θεωρείται αξιόπιστη και η αποκρυπτογράφησή του παραμένει άλυτο πρόβλημα

Στην αρχαία Ελλάδα, οι έφοροι της Σπάρτης επικοινωνούσαν με τους στρατηγούς χρησιμοποιώντας μακριές και στενές κορδέλες τις οποίες τύλιγαν γύρω από μια σκυτάλη (στενός ξύλινος κύλινδρος). Για να διαβάσει κάποιος το μήνυμα, έπρεπε να έχει μια παρόμοια σκυτάλη με αυτή που είχε χρησιμοποιηθεί από τον δημιουργό του και να τυλίξει την κορδέλα γύρω από τη σκυτάλη με τον ίδιο τρόπο. Αυτό το σύστημα (διπλής κατεύθυνσης) κρυπτογραφίας είναι ένα κλασικό σύστημα με ένα κλειδί (τη σκυτάλη).

Ο Ιούλιος Καίσαρας επικοινωνούσε με τους συνεργάτες του αντικαθιστώντας κάθε γράμμα με ένα άλλο, το οποίο προ έκυπτε με ολίσθηση κατά k βήματα στο αλφάβητο. Αυτό είναι ένα από τα πιο απλά, εύκολα αλλά ανασφαλή κρυπτοσυστήματα που έχουν προταθεί.

Οι Βενετοί ήταν οι πρώτοι που χρησιμοποίησαν κρυπτογραφία συστηματικά, από το 13ο αιώνα, για διπλωματική αλληλογραφία. Οι πρώτες δημοσιεύσεις (στα λατινικά) περί κρυπτογραφίας φάνηκαν το 1500 (”Στεγανογραφία”) και το 1518 από τον αββά Ιωάννη Τριθέμιο όπου έγραψε την πρώτη εκδιδόμενη εργασία κρυπτογραφίας που την ονόμασε “Polygraphia” . Αργότερα δημοσιεύτηκε το ”Περί κρυπτικών συμβόλων και γραμμάτων” από τον J. B. Porta (1538 - 1615, Ιταλό φυσικό και μαθηματικό). Από τότε η κρυπτογραφία έγινε αντικείμενο ιδιαίτερου ενδιαφέροντος και απέκτησε εφαρμογές.

Οι αλχημιστές χρησιμοποιούσαν σύμβολα για να κρυπτογραφήσουν τους τύπους τους, αλλά και πολλοί φιλόσοφοι ενδιαφέρθηκαν για την κρυπτογραφία: Ο Sir Francis Bacon (1561 - 1626) επινόησε ένα σύστημα κρυπτογράφησης όπου κάθε γράμμα αντικαθίσταται με μια λέξη πέντε γραμμάτων και ο Leonardo Da Vinci (1452 - 1519) χρησιμοποιούσε μια μέθοδο κρυπτογράφησης με καθρέπτη.

1.2 Ύστερη Αναγέννηση(19ος -20ος Αιώνας)

Ο Edgar Allan Poe (1809-1849) στο κλασικό διήγημα ”Το χρυσό έντομο” (”The Gold Bug”) που δημοσίευσε το 1843, εξηγεί τις βασικές αρχές παραβίασης των κωδικών και υποστηρίζει την άποψη ότι ο ανθρώπινος νους μπορεί να σπάσει οποιοδήποτε κρυπτογραφημένο κείμενο που η ανθρώπινη ευρηματικότητα μπορεί να επινοήσει. Ακόμη περιγράφει ένα σύστημα με το οποίο κάθε κρυπτογραφημένο κείμενο που προέρχεται από μια ευρωπαϊκή γλώσσα μπορεί να αποκρυπτογραφηθεί, αν έχει κρυπτογραφηθεί με αντικατάσταση, μετρώντας τη συχνότητα των γραμμάτων της γλώσσας, τεχνική που πρώτοι συνέλαβαν οι Άραβες. Ίσως από τα διασημότερα κρυπτογραφήματα, το σημείωμα του Zimmerman (the Zimmerman Note) όπου ώθησε τις ΗΠΑ στον πρώτο παγκόσμιο πόλεμο. Όταν το κρυπτογράφημα αποκρυπτογραφήθηκε το 1917, οι Αμερικανοί έμαθαν ότι η Γερμανία είχε προσπαθήσει να πείσει το Μεξικό να μπει στον πόλεμο με το μέρος της, υποσχόμενη παραχωρήσεις εδαφών των ΗΠΑ στο Μεξικό.

Τον ίδιο περίπου καιρό, ο Gilbert S. Vernam της AT&T ανέπτυξε τον πρώτο πραγματικά άθραυστο κώδικα που ονομάστηκε βέβαια κρυπτόγραμμα Vernam (The Vernam Cipher). Μια ξεχωριστή ιδιότητα αυτού του κώδικα είναι η απαίτηση για ένα κλειδί με μήκος όσο και το μήνυμα που πρέπει να μεταδοθεί και το οποίο δεν επαναχρησιμοποιείται για την αποστολή άλλου μηνύματος. Η κρυπτογράφηση Vernam είναι γνωστή επίσης και ως κρυπτογράφηση με μπλοκάκι μιας χρήσης (onetime-pad) από την πρακτική της προμήθειας κατασκόπων με το κείμενο-κλειδί γραμμένο σε ένα μπλοκάκι του οποίου κάθε κομμάτι χρησιμοποιείται μια φορά και μετά καταστρέφεται.

Η ανακάλυψη του συστήματος αυτού δεν εκτιμήθηκε ιδιαίτερα εκείνη την εποχή, πιο πολύ επειδή δεν είχε αποδειχτεί ακόμη ότι είναι άθραυστος κώδικας και επειδή η απαίτηση για πολλά και μεγάλα κλειδιά την έκαναν μη πρακτική για γενική χρήση. Αξίζει να αναφερθεί ότι το 1967, όταν ο στρατός της Βολιβίας συνέλαβε και εκτέλεσε τον επαναστάτη Che Guevara, όπου βρήκαν στην κατοχή του ένα χαρτί που έδειχνε πως προετοίμαζε ένα μήνυμα για αποστολή στον Κουβανό πρόεδρο Fidel Castro. Ο Che Guevara χρησιμοποιούσε τον άσπαστο κώδικα του Vernam. Εξαιτίας των μη πρακτικών απαιτήσεων της κρυπτογράφησης Vernam, άλλες (πιο αδύναμες) μέθοδοι συνέχισαν να χρησιμοποιούνται ευρέως. Έτσι, κατά το δεύτερο παγκόσμιο πόλεμο, οι Σύμμαχοι ήταν σε θέση να αποκρυπτογραφούν τα περισσότερα από τα μυστικά μηνύματα που στέλνονταν από τους Γερμανούς. Η εγγενής δυσκολία του σπασίματος των ολοένα και πιο περίπλοκων κρυπτογραφικών μεθόδων ήταν μάλιστα ένας από τους παράγοντες που προώθησε την ανάπτυξη των ηλεκτρονικών υπολογιστών.

1.3 Enigma : “Η μεγάλη Ώρα του Alan Turung”

Η περίφημη Μηχανή-Αίνιγμα (Enigma) που χρησιμοποιήθηκε από τους Γερμανούς κατά το δεύτερο παγκόσμιο πόλεμο για κρυπτογράφηση ραδιοτηλεπικοινωνιών ήταν ίσως το πλέον εξελιγμένο κρυπτοσύστημα της εποχής και πυροδότησε μια από τις πιο έντονες προσπάθειες αποκρυπτογράφησης στην ιστορία. Ο κώδικας Αίνιγμα θυμίζει έναν παλιότερο κώδικα (τύπου Vigenére) αλλά είναι πολύ πιο πολύπλοκος. Μια βασική ιδιότητα της μηχανής αυτής ήταν η αυτο-αντιστροφή: εάν το κωδικοποιημένο κείμενο δινόταν ως είσοδος στη μηχανή, τότε η έξοδος θα ήταν το αρχικό μήνυμα (αν φυσικά η μηχανή είχε την ίδια αρχική κατάσταση με τη μηχανή που είχε κάνει την κωδικοποίηση). Παρόλο που αυτό αποτελούσε τρομερή ευκολία για τους χειριστές της μηχανής, αποδείχτηκε ότι ήταν και μεγάλη αδυναμία του κώδικα Αίνιγμα.

Πριν τον πόλεμο, η γαλλική αντικατασκοπεία είχε αποκτήσει αντίγραφα των εντολών της μηχανής Αίνιγμα και έδωσε την πληροφορία αυτή στους Πολωνούς που υπέκλεπταν και ανέλυαν τις γερμανικές ράδιο-επικοινωνίες. Με τη βοήθεια των εντολών αυτών, οι Πολωνοί κρυπταναλυτές μπόρεσαν να συμπεράνουν τη συνδεσμολογία (καλωδίωση της μηχανής), οπότε έγινε δυνατό να διαβάζονται τα κρυπτογραφημένα κείμενα, αρκεί να είναι γνωστή η αρχική κατάσταση της μηχανής. Παρόλο που οι Βρετανοί τα έμαθαν όλα αυτά από τους Πολωνούς, είχαν μικρή αξία γι’ αυτούς επειδή οι Γερμανοί έκαναν κάποιες τροποποιήσεις στη μηχανή πριν τον πόλεμο. Οι Βρετανοί συγκέντρωσαν μια ομάδα κρυπταναλυτών και μαθηματικών, με επικεφαλής τον Alan Turing, σε μια βικτωριανή έπαυλη στο Buckinghamshire που ονομαζόταν Bletchley Park. Χρησιμοποιώντας τις πληροφορίες των Πολωνών, η ομάδα βάσισε τις προσπάθειές της στη λεγόμενη μέθοδο πιθανής λέξης. Η μέθοδος αυτή βασίζεται στο γεγονός ότι σε κάποιες περιπτώσεις μια συγκεκριμένη ακολουθία συμβόλων σχεδόν σίγουρα αντιπροσωπεύει μια γνωστή λέξη. Μαντεύοντας σωστά μερικές από τις κρυπτογραφημένες λέξεις του κρυπτοκειμένου, μπορούσαν να καθορίζουν τη συνδεσμολογία της μηχανής, δοκιμάζοντας όλες τις πιθανές συνδεσμολογίες και προσδιορίζοντας ποια είχε ως αποτέλεσμα τα υποτιθέμενα ζευγάρια κρυπτογραφημένων/αποκρυπτογραφημένων λέξεων.

Ο Turing αντιλήφθηκε ότι μόνο μια αυτόματη και σχετικά γρήγορη μηχανή θα μπορούσε να τα βγάλει πέρα με τις δοκιμές, όποτε και οδηγήθηκε στην κατασκευή ενός εξομοιωτή της μηχανής-Αίνιγμα με το όνομα Bombe (Βόμβα). Με την ανακάλυψη της «Βόμβας» από τον Turing και την υποκλοπή των σημάτων του Γερμανικού Ναυτικού (και όχι μόνο) , οι Βρετανοί ήταν πλέον σε θέση να ελαχιστοποιήσουν τις απώλειες τους σε τροφοδοσία από την άλλη άκρη του Ατλαντικού , αποφεύγοντας τα τρομερής αποτελεσματικότητας U-Boats (Γερμανικά Υποβρύχια) του Χιτλερ και να κερδίσουν την Μάχη του Ατλαντικού.

1.4 Σύγχρονη κρυπτογραφία

Η σημερινή μορφή των κρυπτογραφικών συστημάτων έχει καθοριστεί σε πολύ μεγάλο βαθμό από δύο κεφαλαιώδους σημασίας για την κρυπτογραφία και της επικοινωνίας γενικότερα, επιστημονικές εργασίες Kerchoffs και Shannon, που δημοσιεύτηκαν το 1883 και 1949 αντίστοιχα .

Στην πρώτη, ο Kerchoffs έθεσε τη βασική σχεδιαστική αρχή που έκτοτε διέπει κάθε κρυπτογραφικό σύστημα, σύμφωνα με την οποία η ασφάλεια ενός συστήματος πρέπει να έγκειται μόνο στη μυστικότητα του κλειδιού και να μην εξαρτάται από τη μυστικότητα του αλγορίθμου κρυπτογράφησης.

Η δεύτερη εργασία ανήκει στο θεμελιωτή της Θεωρίας Πληροφορίας Claude Shannon. Στην εργασία αυτή η κρυπτογραφία μετατρέπεται σε αυστηρό επιστημονικό πεδίο, όπου ορίζεται η έννοια του κρυπτοσυστήματος και η απόλυτη ασφάλεια. Η εργασία αυτή του Shannon αποτέλεσε ισχυρή κινητήρια δύναμη για την ταχεία εξέλιξη της έρευνας στο χώρο της κρυπτογραφίας, η οποία έλαβε χώρα στο δεύτερο μισό του εικοστού αιώνα και συνεχίζεται μέχρι σήμερα. Όλοι οι σύγχρονοι κρυπτογραφικοί αλγόριθμοι σχεδιάζονται υπό το πρίσμα των εννοιών που εισήγαγε ο Shannon.

Σημαντική τομή επίσης στο χώρο της κρυπτογραφίας αποτέλεσε η εργασία των Diffie-Hellman το 1976, όπου προτάθηκε μία επαναστατική τεχνική η οποία επιλύει το πρόβλημα της ανταλλαγής κλειδιού από απόσταση, χωρίς να απαιτείται άμεση επαφή, θέτοντας έτσι τις βάσεις για την κρυπτογραφία δημοσίου κλειδιού. Πράγματι, το 1977 οι Ronald L. Rivest, Adi Shamir και Leonard M. Adleman (τότε στο MIT) πρότειναν ένα ιδιαίτερα επιτυχημένο (έως και σήμερα) κρυπτοσύστημα δημοσίου κλειδιού, γνωστό ως RSA. Οι παραπάνω εργασίες καθώς και η δουλειά ερευνητών στην δεκαετία του 1980, όπως η Shafi Goldwasser, ο Silvio Micali ,κ.ά., οδήγησαν στην Σύγχρονη Κρυπτογραφία, στην οποία κεντρικό ρόλο διαδραματίζει η έννοια της αποδείξιμης ασφάλειας και ο κλάδος της υπολογιστικής πολυπλοκότητας με τα οποία θα ασχοληθούμε εκτενώς στην τρέχων πτυχιακή διατριβή. Εκτός από την παραπάνω αλλαγή, η σύγχρονη κρυπτογραφία έχει επεκτείνει σημαντικά το πεδίο εφαρμογής της πέρα από την ιδιωτική επικοινωνία. Οι μέθοδοί της επιτρέπουν τον έλεγχο της ακεραιότητας μηνυμάτων, την μη αποποίηση αποστολής ή λήψης τους, την χρονική τους σήμανση, και πλήθος άλλων ιδιοτήτων.

Επιπλέον μπορεί να χρησιμοποιηθεί για την απόδειξη της ταυτότητας κάποιου χρήστη (αυθεντικοποίηση) και την παροχή εξουσιοδότησης για την πραγματοποίηση συγκεκριμένων λειτουργιών. Από την άλλη μπορεί να παρέχει ανωνυμία και δυνατότητα άρνησης σε περίπτωση εκβιασμού. Σε ακόμα πιο υψηλό επίπεδο η κρυπτογραφία δρα ως καταλύτης για την

οικοδόμηση εμπιστοσύνης μεταξύ οντοτήτων με διαφορετικά και συχνά αντικρουόμενα συμφέροντα, τα οποία αλληλοεπιδρούν από απόσταση, μια πολύ σημαντική λειτουργία στο σημερινό πολλαπλά συνδεδεμένο κόσμο.

1.4.1 21ος αιώνας

Κατά τον 21ο αιώνα, οι κρυπτογραφικές εφαρμογές, πρωτόκολλα και τεχνικές παίζουν κομβικό ρόλο στη σύγχρονη τεχνολογία, ειδικά στους τομείς της ασφαλούς επικοινωνίας, της ασφαλούς πρόσβασης, των ηλεκτρονικών ψηφοφοριών, της ανάκτησης και διαχείρισης ευαίσθητων δεδομένων, και των ηλεκτρονικών συναλλαγών, με πρόσφατη σημαντικότατη εξέλιξη την ανάπτυξη του κρυπτονομίσματος Bitcoin, και αρκετών ήδη διαδόχων του, με κυρίαρχο χαρακτηριστικό την απουσία κεντρικού ελέγχου.

Οι παραπάνω εφαρμογές, και πολλές άλλες που δεν αναφέρθηκαν, μπόρεσαν να πραγματοποιηθούν χάρη στην αλματώδη ανάπτυξη επαναστατικών ιδεών και αλγορίθμων, όπως η τέλεια μυστικότητα, η κρυπτογραφία δημοσίου κλειδιού, η ασφαλής ανταλλαγή κλειδιού από απόσταση, οι ψηφιακές υπογραφές, τα διαλογικά συστήματα αποδείξεων και οι αποδείξεις μηδενικής γνώσης, οι γεννήτριες ψευδοτυχαιότητας, η σύνθεση πρωτοκόλλων, οι συναρτήσεις σύνοψης χωρίς συγκρούσεις, η υπολογιστική πολυπλοκότητα και πολλά άλλα. Κοινό χαρακτηριστικό των παραπάνω μεθόδων είναι ότι η ασφάλειά τους εδράζεται όλο και περισσότερο, σε αυστηρές μαθηματικές αποδείξεις.

Για παράδειγμα, είμαστε πλέον σε θέση να διενεργούμε ηλεκτρονικές ψηφοφορίες που παρέχουν αποδείξεις ορθότητας για διάφορες φάσεις της λειτουργίας τους ή να διενεργούμε συναλλαγές χωρίς κεντρική αρχή, μέσω του Bitcoin ή άλλων κρυπτονομισμάτων, με απόδειξη εγκυρότητας για κάθε συναλλαγή, που επικυρώνεται συλλογικά!

Τα κρυπτονομίσματα είναι μια επανάσταση σε εξέλιξη, ανοίγοντας δρόμους για αποκεντρωμένη και αποδεδειγμένα ασφαλή ψηφιακή υλοποίηση λειτουργιών που μέχρι σήμερα απαιτούσαν την ύπαρξη κάποιας αρχής, όπως για παράδειγμα τη σύναψη συμβολαίων, αλλά και ηλεκτρονικών ψηφοφοριών. Τα μαθηματικά γίνονται για άλλη μια φορά επίκαιρα, βοηθώντας στην εμπέδωση εμπιστοσύνης σε κρίσιμες λειτουργίες, και μέσω αυτής στο άνοιγμα της κρυπτογραφίας στο πλατύ κοινό. Τα περισσότερα κρυπτοσυστήματα είναι πλέον εντελώς ανοιχτά (ο τρόπος λειτουργίας είναι γνωστός), και η ασφάλειά τους βασίζεται αποκλειστικά σε αριθμητικούς αλγορίθμους που μας επιτρέπουν να εκτελούμε αποδοτικά πράξεις με αριθμούς χιλιάδων ψηφίων, ώστε η υπολογιστική δυσκολία (πολυπλοκότητα) των αντίστροφων πράξεων να είναι τεράστια.

Η κρυπτογραφία έχει φύγει οριστικά από τα στεγανά των μυστικών υπηρεσιών και τη στρατιωτική χρήση και είναι έτοιμη να προσφέρει ακόμη περισσότερο τις υπηρεσίες της στο σύνολο

της ανθρωπότητας πλέον, προάγοντας τη δημοκρατία, τον σεβασμό της ιδιωτικής ζωής, και τελικά την ενεργό και ισότιμη συμμετοχή όλων στο οικονομικό, πολιτικό, και κοινωνικό γίγνεσθαι.

ΚΕΦΑΛΑΙΟ 2ο: ΚΛΑΣΣΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ

Στην κλασική κρυπτογραφία, οι αλγόριθμοι κρυπτογράφησης και αποκρυπτογράφησης είναι γνωστοί σε όλους, και το ίδιο κλειδί χρησιμοποιείται και για τις δύο κατευθύνσεις (κρυπτογράφηση-αποκρυπτογράφηση). Με άλλα λόγια, στα κλασικά συστήματα, η αποκρυπτογράφηση είναι εύκολη αν το κλειδί κρυπτογράφησης είναι γνωστό. Αντίθετα, στην κρυπτογραφία δημοσίου κλειδιού το κλειδί κρυπτογράφησης k μπορεί με ασφάλεια να δημοσιοποιηθεί χωρίς να αποκαλυφθεί το κλειδί αποκρυπτογράφησης k′.

Για αυτό το λόγο τα κλασικά συστήματα αναφέρονται επίσης και ως συμμετρικά ή διπλής κατεύθυνσης συστήματα, και τα συστήματα δημοσίου κλειδιού ως μη-συμμετρικά ή μονής κατεύθυνσης συστήματα (αυτό σημαίνει ότι η διαδικασία κρυπτογράφησης είναι μονής κατεύθυνσης - δεν μπορεί εύκολα να αντιστραφεί). Μία κεντρική ιδέα που διέπει τα συμμετρικά συστήματα είναι ότι οι συμμετέχοντες μπορούν να ανταλλάξουν το κλειδί με ασφάλεια (μέσω κάποιου διαφορετικού δίαυλου επικοινωνίας) κάτι που φυσικά δεν ισχύει στα ασύμμετρα.

Μια (πολύ παλιά) κατηγοριοποίηση των κλασικών κρυπτοσυστημάτων είναι σε συστήματα αντικατάστασης (substitution) και μετάθεσης (permutation) (ή αναδιάταξης (transposition)).

Στα συστήματα αντικατάστασης (substitution ciphers), τα γράμματα του αρχικού κειμένου αντικαθίστανται από άλλα τα οποία διατηρούνται στην ίδια διάταξη όπως και τα πρωτότυπα τους στο αρχικό κείμενο. Αν οι αντικαταστάτες παραμένουν οι ίδιοι σε όλο το κείμενο (κάθε γράμμα του αρχικού κειμένου αναπαρίσταται πάντοτε από το ίδιο σύμβολο-αντικαταστάτη) τότε το σύστημα ονομάζεται μονοαλφαβητικά. Αν το αρχικό κείμενο είναι σε κάποια φυσική γλώσσα, η κρυπτανάλυση είναι πάντοτε εφικτή βασιζόμενη στη στατιστική κατανομή των γραμμάτων.

Στα πολυαλφαβητικά συστήματα αντικατάστασης κάθε γράμμα του αρχικού κειμένου μπορεί να έχει πολλούς αντικαταστάτες και κάθε φορά χρησιμοποιείται διαφορετικός. Στα συστήματα μετάθεσης (ή αναδιάταξης) τα γράμματα του αρχικού κειμένου αναδιατάσσονται. Αυτή η μέθοδος είναι υπερβολικά απλή, οπότε θα πρέπει να συνδυαστεί με κάποια άλλη ιδέα .

Μια άλλη κατηγοριοποίηση των κρυπτοσυστημάτων θα μπορούσε να είναι σε συστήματα αντικατάστασης χωρίς συμφραζόμενα (context-free) και σε συστήματα αντικατάστασης με συμφραζόμενα (context-sensitive) : Στα συστήματα χωρίς συμφραζόμενα κάθε γράμμα κωδικοποιείται ξεχωριστά ενώ σε εκείνα με συμφραζόμενα η κωδικοποίηση γίνεται ανά ομάδες (blocks).

2.1 Μονοαλφαβητικά Συστήματα Αντικατάστασης

Ένα κρυπτοσύστημα ονομάζεται μονοαλφαβητικό αν κάθε γράμμα του αρχικού κειμένου αναπαρίσταται πάντοτε από το ίδιο σύμβολο-αντικαταστάτη (κάθε εμφάνιση ενός συμβόλου του αρχικού κειμένου κρυπτογραφείται με τον ίδιο πάντα αντικαταστάτη).

2.1.1 Κώδικας του Καίσαρα (Caesar's Cipher)

Το κρυπτοσύστημα του Καίσαρα είναι από τα πρώτα κρυπτογραφικά σχήματα που χρησιμοποιήθηκαν. Είναι επίσης πολύ απλό, και μπορεί κανείς να το σπάσει πολύ εύκολα. Το σύστημα του Καίσαρα βασίζεται σε αντικαταστάσεις με ολίσθηση κατά k θέσεις, δηλαδή κάθε γράμμα αντικαθίσταται με άλλο, προχωρώντας k θέσεις στο αλφάβητο modulo το μέγεθος του αλφαβήτου. (k = 1; : : : ; 25). Δηλαδή για k = 3 έχουμε:
Τα γράμματα του αρχικού κειμένου: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Οι αντικαταστάτες του κρυπτοκειμένου: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Έτσι το αρχικό κείμενο I LOVE MATH κρυπτογραφείται ως LORYH PDWK. Η μέθοδος κρυπτογράφησης Ek είναι ολίσθηση μπροστά κατά k βήματα στο αλφάβητο, και η μέθοδος αποκρυπτογράφησης είναι ολίσθηση πίσω κατά Dk βήματα στο αλφάβητο. Παρακάτω δίνονται κάποιες προφανείς ιδιότητες των Ek και Dk:

$$E_i\, D_j = D_j\, E_i \qquad \text{(αντιμεταθετική ιδιότητα)}$$
$$D_k = E_{26-k},$$
$$D_k\, E_k = D_0 = E_0 = D_{26} = E_{26}.$$

Αν το αρχικό κείμενο ανήκει σε μια γνωστή φυσική γλώσσα, η κρυπτανάλυση αυτού του συστήματος είναι πολύ εύκολη: από τη στιγμή που ο συνολικός αριθμός των δυνατών κλειδιών είναι αρκετά μικρός (25 στην προκειμένη όσα τα γράμματα της αλφαβήτου) μπορεί κανείς απλά να τα δοκιμάσει όλα σε ένα μικρό μέρος του κρυπτοκειμένου και να δει ποιο από όλα οδηγεί σε αρχικό κείμενο που έχει νόημα. Επίσης, όπως και όλα τα μονοαλφαβητικά

συστήματα αντικατάστασης, το σύστημα του Καίσαρα μπορεί να το σπάσει κανείς υπολογίζοντας τις συχνότητες εμφάνισης των γραμμάτων.

2.2 Πολυαλφαβητικά Συστήματα Αντικατάστασης

Στα πολυαλφαβητικά κρυπτοσυστήματα αντικατάστασης, ένα γράμμα δεν αντικαθίσταται από το ίδιο σύμβολο παντού στο κείμενο: η χρήση των αντικαταστατών ποικίλει στα διάφορα μέρη του απλού κειμένου. Για παράδειγμα στη γερμανική μηχανή Αίνιγμα μετά από κάθε γράμμα του κειμένου, τα γρανάζια γυρίζουν, δίνοντας ένα νέο πρότυπο κρυπτογράφησης.

2.2.1 Κρυπτοσύστημα VIGENÉRE

Το σύστημα του Vigenére (Blaise de Vigenére 1523-1596)) είναι από τα πιο παλιά και τα πιο γνωστά πολυαλφαβητικά κρυπτοσυστήματα (στην πραγματικότητα ο κώδικας Αίνιγμα και ο κώδικας Vernam είναι Vigenére συστήματα). Αρχικά αντιστοιχίζουμε σε κάθε γράμμα του αλφαβήτου έναν αριθμό (A-0,B -1,…Z - 25). Το VIGENÉRE μπορεί να θεωρηθεί ένα σύστημα του Καίσαρα στο οποίο το κλειδί αλλάζει από βήμα σε βήμα. Το κλειδί στο σύστημα VIGENÉRE είναι ένα διάνυσμα rx χαρακτήρων k = (k-0; k-1… kr-1). Αυτό το διάνυσμα έχει μορφή μιας λέξη-κλειδί, και μπορεί να είναι οποιαδήποτε λέξη ή φράση (επαναλήψεις γραμμάτων επιτρέπονται). Ο αριθμός r λέγεται περίοδος του συστήματος. Το αρχικό κείμενο διαιρείται σε blocks μεγέθους r και κάθε block κρυπτογραφείται χρησιμοποιώντας τη λέξη-κλειδί ως εξής: γράφουμε τη λέξη-κλειδί κάτω από το block του αρχικού κειμένου και κρυπτογραφούμε κάθε γράμμα του κειμένου χρησιμοποιώντας ένα σύστημα του Καίσαρα με το k να ισούται με τον αριθμό που αντιστοιχεί στο γράμμα της λέξης-κλειδί που είναι γραμμένη από κάτω. Με μαθηματικό συμβολισμό η αντικατάσταση VIGENÉRE για κάθε σύμβολο του αρχικού κειμένου ορίζεται ως:

$$ci = E_K(x_i) = (x_i + k_i \bmod r) \bmod 26, \quad 0 < i \_ < n - 1$$

Για την αποκρυπτογράφηση φυσικά έχουμε:

$$xi = D_K(c_i) = (c_i - k_i \bmod r) \bmod 26, \quad 0 < i \_ < n - 1$$

Οι διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης μπορούν να εκτελεστούν και χωρίς υπολογιστή χρησιμοποιώντας έναν πίνακα παρόμοιο με τον παρακάτω, στον οποίο κάθε

στήλη μπορεί να θεωρηθεί ως ένα σύστημα του Καίσαρα. Για να χρησιμοποιήσουμε αυτόν τον πίνακα διαβάζουμε το κείμενο από την πρώτη στήλη, το κλειδί από την πρώτη γραμμή και το κρυπτοκείμενο είναι το γράμμα που βρίσκεται στην τομή τους. Για την αποκρυπτογράφηση, βρίσκουμε το γράμμα του κρυπτοκειμένου στη στήλη που υποδεικνύεται από το κλειδί και διαβάζουμε το αντίστοιχο γράμμα του αρχικού κειμένου από την πρώτη στήλη της γραμμής στην οποία βρίσκεται το γράμμα του κρυπτοκειμένου. (Σημειώνεται ότι ο ρόλος των γραμμών και των στηλών μπορεί να αλλαχθεί)

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
B C D E F G H I J K L M N O P Q R S T U V W X Y Z A
C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
F G H I J K L M N O P Q R S T U V W X Y Z A B C D E
G H I J K L M N O P Q R S T U V W X Y Z A B C D E F
H I J K L M N O P Q R S T U V W X Y Z A B C D E F G
I J K L M N O P Q R S T U V W X Y Z A B C D E F G H
J K L M N O P Q R S T U V W X Y Z A B C D E F G H I
K L M N O P Q R S T U V W X Y Z A B C D E F G H I J
L M N O P Q R S T U V W X Y Z A B C D E F G H I J K
M N O P Q R S T U V W X Y Z A B C D E F G H I J K L
N O P Q R S T U V W X Y Z A B C D E F G H I J K L M
O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
P Q R S T U V W X Y Z A B C D E F G H I J K L M N O
Q R S T U V W X Y Z A B C D E F G H I J K L M N O P
R S T U V W X Y Z A B C D E F G H I J K L M N O P Q
S T U V W X Y Z A B C D E F G H I J K L M N O P Q R
T U V W X Y Z A B C D E F G H I J K L M N O P Q R S
U V W X Y Z A B C D E F G H I J K L M N O P Q R S T
V W X Y Z A B C D E F G H I J K L M N O P Q R S T U
W X Y Z A B C D E F G H I J K L M N O P Q R S T U V
X Y Z A B C D E F G H I J K L M N O P Q R S T U V W
Y Z A B C D E F G H I J K L M N O P Q R S T U V W X
Z A B C D E F G H I J K L M N O P Q R S T U V W X Y

Η κρυπτογράφηση του αρχικού κειμένου χρειάζεται μια λέξη-κλειδί μήκους r η οποία επαναλαμβάνεται για να καλύψει όλο το αρχικό κείμενο. Τέτοια πολυαλφαβητικά συστήματα, όπου τα αλφάβητα των αντικαταστατών επαναλαμβάνονται περιοδικά συνήθως ονομάζονται περιοδικά. Αν γνωρίζουμε την περίοδο κάποιου περιοδικού πολυαλφαβητικού συστήματος, τότε η κρυπτανάλυση του μπορεί να αναχθεί στην κρυπτανάλυση ενός μονοαλφαβητικά συστήματος: Θεωρούμε ότι η περίοδος είναι r. Διατάσσουμε τα γράμματα του κρυπτοκειμένου σε γραμμές με r στήλες σε κάθε γραμμή (γράφουμε r γράμματα σε κάθε γραμμή). Δύο εμφανίσεις του ίδιου γράμματος στην ίδια στήλη αντιπροσωπεύουν το ίδιο αρχικό γράμμα. Οπότε μπορούμε να αποκρυπτογραφήσουμε κάθε στήλη με μέτρηση συχνοτήτων. Αν η περίοδος που χρησιμοποιείται σε ένα περιοδικό σύστημα τύπου VIGENÉRE είναι άγνωστη, μπορεί (ίσως) να βρεθεί με την μέθοδο του Kasiski (F.W. Kasiski, 1860): Αυτή η μέθοδος υπολογίζει την περίοδο ψάχνοντας τις εμφανίσεις της ίδιας λέξης στο κρυπτοκείμενο. Υποθέτουμε ότι μια συγκεκριμένη λέξη εμφανίζεται δύο φορές στο κρυπτοκείμενο, και ότι μεσολαβούν m γράμματα μεταξύ των εμφανίσεων αυτών (δηλαδή από την αρχή της πρώτης μέχρι την αρχή της δεύτερης).

2.2.2 Ο κώδικας Vernam (one-time pad)

Μία ακραία περίπτωση ενός πολυαλφαβητικού συστήματος είναι ένα σύστημα όπου το κλειδί έχει ίσο μήκος με το αρχικό κείμενο. Ο κώδικας Vernam, ή αλλιώς ”μπλοκάκι μιας χρήσης” (One-Time Pad (OTP)) είναι ένα κρυπτοσύστημα μυστικού κλειδιού όπου το κλειδί έχει το ίδιο μήκος με το κείμενο προς κρυπτογράφηση. Επιπλέον, το κλειδί το χρησιμοποιούμε μόνο μια φορά και μετά το ”πετούμε”, δεν το ξαναχρησιμοποιούμε. Το αρχικό κείμενο M αναπαρίσταται ως δυαδική ακολουθία, όπως επίσης και το κλειδί K. Το κρυπτοκείμενο C προκύπτει από τη αποκλειστική διάζευξη ανά bit (XOR) (ή πρόσθεση modulo 2) του αρχικού κειμένου με το κλειδί:

$$C = M \oplus K.$$

Η αποκρυπτογράφηση δίνεται από την ίδια πράξη:

$$M = C \oplus K.$$

Αποδεικνύεται ότι είναι αδύνατο για τον κρυπταναλυτή να σπάσει τον κώδικα που χρησιμοποιεί μπλοκάκι μιας χρήσης: Οποιοδήποτε κρυπτοκείμενο C δεν αποκαλύπτει καμία πληροφορία για το αρχικό κείμενο P αφού κάθε μήνυμα M θα μπορούσε να παραγάγει το C, αν το κλειδί K ήταν ίσο με $K = C \oplus M$. Η κρυπτογράφηση με μπλοκάκι μιας χρήσης είναι αποδεδειγμένα ασφαλής με πληροφοριοθεωρητική έννοια, αφού ο υποκλοπέας δεν έχει ποτέ αρκετή πληροφορία για να αποκρυπτογραφήσει το κρυπτοκείμενο και κανένα μέγεθος υπολογιστικής

δύναμης δεν μπορεί να τον βοηθήσει. Από την άλλη πλευρά, το μπλοκάκι μιας χρήσης δεν είναι πρακτικό αφού ένα μεγάλο κλειδί πρέπει να δημιουργηθεί, να διανεμηθεί και να αποθηκευτεί.

ΚΕΦΑΛΑΙΟ 3ο : ΣΥΓΧΡΟΝΑ ΣΥΣΤΗΜΑΤΑ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ

Κρυπτογραφία (cryptography) είναι η μελέτη τεχνικών που βασίζονται σε μαθηματικά προβλήματα δύσκολο να λυθούν, με σκοπό την εξασφάλιση της ασφάλειας (εμπιστευτικότητα, ακεραιότητα, αυθεντικότητα) των δεδομένων. Κρυπτανάλυση (cryptanalysis) είναι η μελέτη μαθηματικών τεχνικών για την προσβολή κρυπτογραφικών τεχνικών ή υπηρεσιών ασφάλειας και κρυπτολογία (cryptology) είναι ο συνδυασμός της κρυπτογραφίας και κρυπτανάλυσης σε ένα ενιαίο επιστημονικό κλάδο. Εφαρμογή της κρυπτογραφίας είναι η κρυπτογράφηση. Κρυπτογράφηση είναι ο μετασχηματισμός δεδομένων σε μορφή που να είναι αδύνατον να διαβαστεί χωρίς τη γνώση της σωστής ακολουθίας bit. Η ακολουθία bit καλείται "κλειδί" και χρησιμοποιείται σε συνδυασμό με κατάλληλο αλγόριθμο/συνάρτηση.

Η αντίστροφη διαδικασία είναι η αποκρυπτογράφηση και απαιτεί γνώση του κλειδιού. Σκοπός της κρυπτογράφησης είναι να εξασφαλίσει το απόρρητο των δεδομένων κρατώντας τα κρυφά από όλους όσους έχουν πρόσβαση σε αυτά. Η κρυπτογράφηση και η αποκρυπτογράφηση απαιτούν, όπως είπαμε, τη χρήση κάποιας μυστικής πληροφορίας, το κλειδί. Για μερικούς μηχανισμούς χρησιμοποιείται το ίδιο κλειδί και για την κρυπτογράφηση και για την αποκρυπτογράφηση, για άλλους όμως τα κλειδιά που χρησιμοποιούνται διαφέρουν.

Η κρυπτογραφία παρέχει μηχανισμούς για διαδικασίες ασφάλειας, όπως η ψηφιακή υπογραφή, η οποία συνδέει ένα έγγραφο με τον κάτοχο ενός κλειδιού, έτσι ώστε όλοι όσοι είναι σε θέση να το αναγνώσουν, να είναι σίγουροι για το ποιος το έχει γράψει. Επίσης, μία ψηφιακή χρονοσφραγίδα (digital timestamp) συνδέει ένα έγγραφο με την ώρα δημιουργίας του. Τέτοιοι μηχανισμοί μπορούν να χρησιμοποιηθούν για έλεγχο πρόσβασης σε ένα σκληρό δίσκο, για ασφαλείς συναλλαγές μέσω του Διαδικτύου ή ακόμα και για σύνδεση με καλωδιακή τηλεόραση.

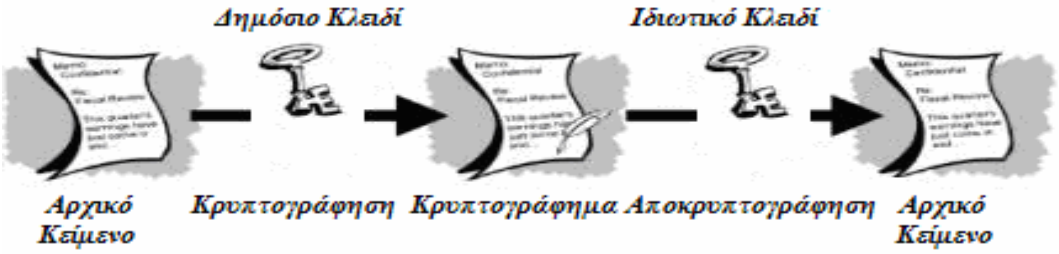
3.1 Είδη Κρυπτογραφίας

3.1.1 Ασύμμετρη Κρυπτογραφία

Η ασύμμετρη κρυπτογραφία (Public Key Cryptography) χρησιμοποιεί δύο διαφορετικά κλειδιά για την κρυπτογράφηση και αποκρυπτογράφηση. Κάθε χρήστης έχει στην κατοχή του ένα ζεύγος κλειδιών, το ένα καλείται δημόσιο κλειδί (public key) και το άλλο καλείται ιδιωτικό κλειδί (private key). Το δημόσιο κλειδί δημοσιοποιείται, ενώ το ιδιωτικό κλειδί κρατείται πάντοτε μυστικό. Το ιδιωτικό κλειδί δεν μεταδίδεται ποτέ στο δίκτυο και όλες οι επικοινωνίες βασίζονται στο δημόσιο κλειδί. Η ανάγκη ο αποστολέας και ο παραλήπτης να μοιράζονται το ίδιο κλειδί εξαφανίζεται και μαζί και πολλά προβλήματα που θα δούμε παρακάτω. Η μόνη απαίτηση της ασύμμετρης κρυπτογραφίας είναι η διαπιστευμένη και επιβεβαιωμένη συσχέτιση των δημόσιων κλειδιών με τους κατόχους τους, ώστε να μην είναι δυνατή η σκόπιμη ή μη πλαστοπροσωπία.

Η ασύμμετρη κρυπτογράφηση μπορεί να χρησιμοποιηθεί όχι μόνο για κρυπτογράφηση, αλλά και για παραγωγή ψηφιακών υπογραφών. Το ιδιωτικό κλειδί είναι μαθηματικά συνδεδεμένο με το δημόσιο κλειδί. Τυπικά, λοιπόν, είναι δυνατόν να "σπάσει" ένα τέτοιο κρυπτοσύστημα ανακτώντας το ιδιωτικό κλειδί από το δημόσιο.

Η κρυπτογράφηση με χρήση της ασύμμετρης κρυπτογραφίας γίνεται ως εξής: όταν ο χρήστης Α θέλει να στείλει ένα μυστικό μήνυμα στο χρήστη Β, χρησιμοποιεί το δημόσιο κλειδί του Β για να κρυπτογραφήσει το μήνυμα και έπειτα το στέλνει στον Β. Ο χρήστης Β, αφού παραλάβει το μήνυμα, κάνει χρήση του ιδιωτικού του κλειδιού για να το αποκρυπτογραφήσει. Κάποιος που παρακολουθεί τη σύνδεση, δεν μπορεί να αποκρυπτογραφήσει το μήνυμα. Όποιος έχει το δημόσιο κλειδί του Β, μπορεί να του στείλει μήνυμα, ενώ μόνο ο Β μπορεί να το διαβάσει, γιατί είναι ο μόνος που γνωρίζει το ιδιωτικό κλειδί.

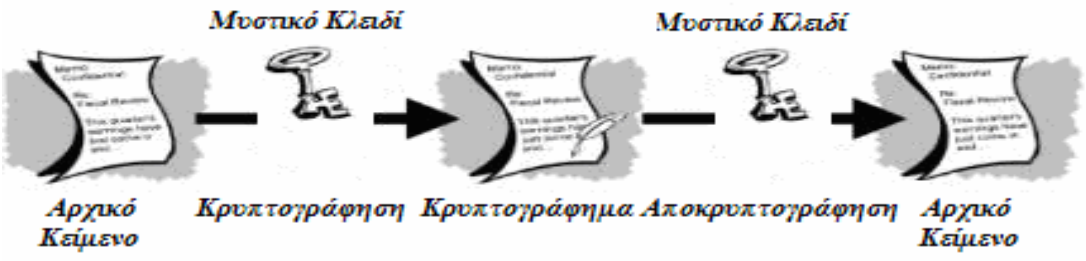


Εικόνα 1. Ασύμμετρη Κρυπτογραφία

Όταν ο Α θέλει να χρησιμοποιήσει την ασύμμετρη κρυπτογραφία για να υπογράψει ένα μήνυμα, τότε πραγματοποιεί ένα υπολογισμό που απαιτεί το ιδιωτικό του κλειδί και το ίδιο το μήνυμα. Το αποτέλεσμα του υπολογισμού καλείται ψηφιακή υπογραφή και μεταδίδεται μαζί με το μήνυμα. Για να επαληθεύσει την υπογραφή ο Β πραγματοποιεί ανάλογο υπολογισμό χρησιμοποιώντας το δημόσιο κλειδί του Α, το μήνυμα και την υπογραφή. Εάν το αποτέλεσμα είναι θετικό, τότε η υπογραφή είναι αυθεντική. Διαφορετικά η υπογραφή είναι πλαστή ή το μήνυμα έχει τροποποιηθεί.

3.1.2 Συμμετρική Κρυπτογραφία

Στη συμμετρική κρυπτογραφία (Symmetric Cryptography ή Secret-Key Cryptography) ο αποστολέας και ο παραλήπτης ενός μηνύματος γνωρίζουν και χρησιμοποιούν το ίδιο μυστικό κλειδί (secret key). Ο αποστολέας χρησιμοποιεί το μυστικό κλειδί για να κρυπτογραφήσει το μήνυμα και ο παραλήπτης χρησιμοποιεί το ίδιο κλειδί για να αποκρυπτογραφήσει το μήνυμα. Αυτή η μέθοδος καλείται συμμετρική κρυπτογραφία ή κρυπτογραφία μυστικού κλειδιού. Η συμμετρική κρυπτογραφία χρησιμοποιείται όχι μόνο για κρυπτογράφηση, άλλα και για πιστοποίηση ταυτότητας. Μία τέτοια τεχνική είναι η Message Authentication Code (MAC).



Εικόνα 2. Συμμετρική Κρυπτογραφία

Το κύριο πρόβλημα της συμμετρικής κρυπτογραφίας είναι η συνεννόηση του αποστολέα και του παραλήπτη στο κοινό μυστικό κλειδί που θα κρυπτογραφεί και αποκρυπτογραφεί όλη τη διακινούμενη πληροφορία, χωρίς κάποιον άλλο να λάβει γνώση αυτού. Πλεονέκτημα της είναι ότι είναι ταχύτερη από την ασύμμετρη κρυπτογραφία.

3.1.3 Μειονεκτήματα και Πλεονεκτήματα

Το μεγαλύτερο πρόβλημα της συμμετρικής κρυπτογραφίας, όπως αναφέραμε περιληπτικά προηγουμένως, είναι η συνεννόηση και ανταλλαγή του κλειδιού, χωρίς κάποιος τρίτος να μάθει για αυτό. Η μετάδοση μέσα από το Διαδίκτυο δεν είναι ασφαλής, γιατί οποιοσδήποτε γνωρίζει για τη συναλλαγή μπορεί να καταγράψει όλη την επικοινωνία μεταξύ αποστολέα και παραλήπτη και να αποκτήσει το κλειδί. Έπειτα, μπορεί να διαβάσει, να τροποποιήσει και να πλαστογραφήσει όλα τα μηνύματα που ανταλλάσσουν οι δύο ανυποψίαστοι χρήστες. Βέβαια, μπορούν να βασισθούν σε άλλο μέσο επικοινωνίας για τη μετάδοση του κλειδιού (π.χ. τηλεφωνία), αλλά ακόμα και έτσι δεν μπορεί να εξασφαλιστεί ότι κανείς δεν παρεμβάλλεται μεταξύ της γραμμής επικοινωνίας των χρηστών.

Η ασύμμετρη κρυπτογραφία δίνει λύση σε αυτό το πρόβλημα, αφού σε καμία περίπτωση δεν μεταφέρονται στο δίκτυο οι εν λόγω ευαίσθητες πληροφορίες με την αρχική τους μορφή. Άλλο ένα ακόμα πλεονέκτημα των ασύμμετρων κρυπτοσυστημάτων είναι ότι μπορούν να παρέχουν ψηφιακές υπογραφές που δεν μπορούν να αποκηρυχθούν από την πηγή τους. Η πιστοποίηση ταυτότητας μέσω συμμετρικής κρυπτογράφησης απαιτεί την κοινή χρήση του ίδιου κλειδιού και πολλές φορές τα κλειδιά αποθηκεύονται σε υπολογιστές που κινδυνεύουν από εξωτερικές επιθέσεις. Σαν αποτέλεσμα, ο αποστολέας μπορεί να αποκηρύξει ένα πρωτύτερα υπογεγραμμένο μήνυμα, υποστηρίζοντας ότι το μυστικό κλειδί είχε κατά κάποιον τρόπο αποκαλυφθεί. Στην ασύμμετρη κρυπτογραφία δεν επιτρέπεται κάτι τέτοιο, αφού κάθε χρήστης έχει αποκλειστική γνώση του ιδιωτικού του κλειδιού και είναι δικιά του ευθύνη η φύλαξή του.

Μειονέκτημα της ασύμμετρης κρυπτογραφίας είναι η ταχύτητα. Κατά κανόνα, οι διαδικασίες κρυπτογράφησης και πιστοποίησης ταυτότητας με συμμετρικό κλειδί είναι σημαντικά ταχύτερες από την κρυπτογράφηση και ψηφιακή υπογραφή με ζεύγος ασύμμετρων κλειδιών. Η ιδιότητα αυτή καλείται διασφάλιση της μη αποκήρυξης της πηγής (non-repudiation). Επίσης, τεράστιο μειονέκτημα της ασύμμετρης κρυπτογραφίας είναι η ανάγκη για πιστοποίηση και επαλήθευση των δημόσιων κλειδιών από οργανισμούς Πιστοποίησης (Certificate Authority) ώστε να διασφαλίζεται η κατοχή των νόμιμων χρηστών. Όταν κάποιος επιτήδειος κατορθώσει και ξεγελάσει τον οργανισμό, μπορεί να συνδέσει το όνομά του με το δημόσιο κλειδί ενός νόμιμου χρήστη και να προσποιείται την ταυτότητα αυτού του νόμιμου χρήστη. Σε μερικές περιπτώσεις, η ασύμμετρη κρυπτογραφία δεν είναι απαραίτητη και η συμμετρική κρυπτογραφία από μόνη της είναι αρκετή. Τέτοιες περιπτώσεις είναι περιβάλλοντα κλειστά (π.χ. στρατός), που δεν έχουν σύνδεση με το Διαδίκτυο.

Ένας υπολογιστής μπορεί να κρατά τα μυστικά κλειδιά των χρηστών που επιθυμούν να εξυπηρετηθούν από αυτόν, μιας και δεν υπάρχει ο φόβος για κατάληψη της μηχανής από εξωτερικούς παράγοντες. Επίσης, στις περιπτώσεις που οι χρήστες μπορούν να συναντηθούν και

να ανταλλάξουν τα κλειδιά ή όταν η κρυπτογράφηση χρησιμοποιείται για τοπική αποθήκευση κάποιων αρχείων, η ασύμμετρη κρυπτογραφία δεν είναι απαραίτητη. Τα δύο κρυπτοσυστήματα μπορούν να εφαρμοστούν μαζί, συνδυάζοντας τα καλά τους χαρακτηριστικά και εξαλείφοντας τα μειονεκτήματα τους.

3.2 Κρυπτογραφικά Εργαλεία

Μέχρι τώρα αναφερθήκαμε στα δύο σημαντικότερα κρυπτοσυστήματα που ευρέως εφαρμόζονται σήμερα. Περιγράψαμε τις αρχές που τα διέπουν και το είδος των κλειδιών που χρησιμοποιούν (συμμετρικά ή ασύμμετρα). Στις ακόλουθες παραγράφους θα ασχοληθούμε με τους μηχανισμούς με τους οποίους εφαρμόζεται η κρυπτογραφία γενικότερα.

3.2.1 Κώδικες Τμήματος

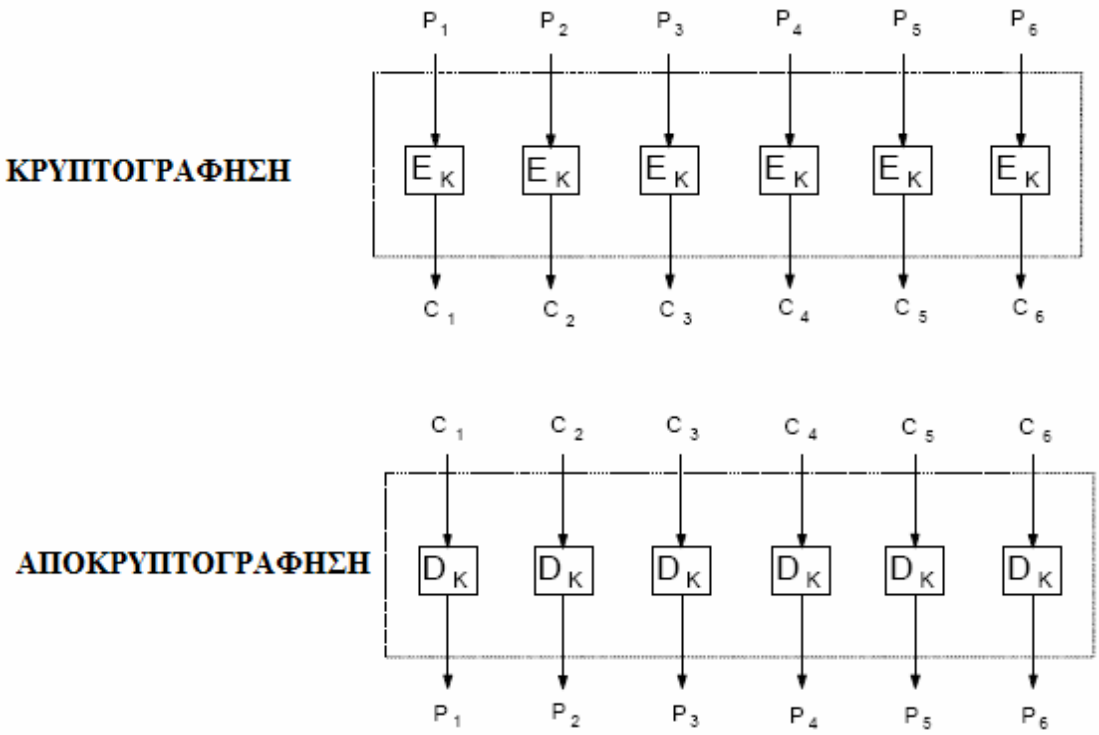
Ο Κώδικας Τμήματος (Block Cipher) είναι ένας τύπος αλγόριθμου συμμετρικής κρυπτογράφησης που μετατρέπει ένα τμήμα (block) μη κρυπτογραφημένου καθορισμένου μήκους κειμένου (plaintext), σε τμήμα (block) κρυπτογραφημένου (ciphertext). Αυτός ο μετασχηματισμός πραγματοποιείται με την βοήθεια ενός μυστικού κλειδιού που δίνεται από το χρήστη. Η αποκρυπτογράφηση γίνεται με την εφαρμογή του αντίστροφου μετασχηματισμού στο κρυπτογραφημένο κείμενο χρησιμοποιώντας το ίδιο μυστικό κλειδί. Το καθορισμένο μήκος καλείται μήκος τμήματος (block size) (64,128,196... bits). Κάθε κείμενο δίνει διαφορετικό κρυπτογραφημένο κείμενο (ciphertext). Οι κώδικες τμήματος (block ciphers) λειτουργούν επαναληπτικά, κρυπτογραφώντας ένα τμήμα διαδοχικά αρκετές φορές. Σε κάθε γύρο, ο ίδιος μετασχηματισμός εφαρμόζεται στα δεδομένα χρησιμοποιώντας ένα υποκλειδί (subkey). Το σύνολο των υποκλειδιών προέρχεται από το μυστικό κλειδί που παρείχε ο χρήστης, με ειδική συνάρτηση. Το σύνολο των υποκλειδιών καλείται σχεδιασμός κλειδιών (key schedule).

Ο αριθμός των επαναλήψεων του επαναληπτικού κρυπτοσυστήματος εξαρτάται από το επίπεδο της επιθυμητής ασφάλειας και την απόδοση του συστήματος. Στις περισσότερες περιπτώσεις, ο αυξημένος αριθμός επαναλήψεων βελτιώνει την προσφερόμενη ασφάλεια, αλλά για μερικά κρυπτοσυστήματα ο αριθμός των επαναλήψεων για να επιτευχθεί ικανοποιητική ασφάλεια θα είναι πολύ μεγάλος για να πραγματοποιηθεί. Τα Feistel κρυπτοσυστήματα είναι ειδικές περιπτώσεις επαναληπτικών κρυπτοσυστημάτων όπου το κρυπτογραφημένο κείμενο υπολογίζεται ως εξής: το κείμενο χωρίζεται στο μισό. Η συνάρτηση f εφαρμόζεται στο ένα μισό με χρήση ενός υποκλειδιού και η έξοδος της f περνάει από λογική πράξη X-OR με το άλλο μισό.

Έπειτα, το αποτέλεσμα της λογικής πράξης γίνεται είσοδος της f και το προηγούμενο μισό το οποίο μετασχηματίστηκε γίνεται μία από τις εισόδους της επόμενης XOR. Η άλλη είσοδος της XOR είναι το αποτέλεσμα του δεύτερου μετασχηματισμού, ο οποίος χρησιμοποιεί νέο υποκλειδί. Ο αλγόριθμος συνεχίζεται με το ίδιο τρόπο. Στο τέλος της τελευταίας επανάληψης, τα δύο κρυπτογραφημένα μισά συνενώνονται. Ένα σημαντικό χαρακτηριστικό του Feistel είναι ότι η αποκρυπτογράφηση είναι δομικά ταυτόσημη με την κρυπτογράφηση. Τα υποκλειδιά χρησιμοποιούνται σε αντίστροφη σειρά στην αποκρυπτογράφηση.

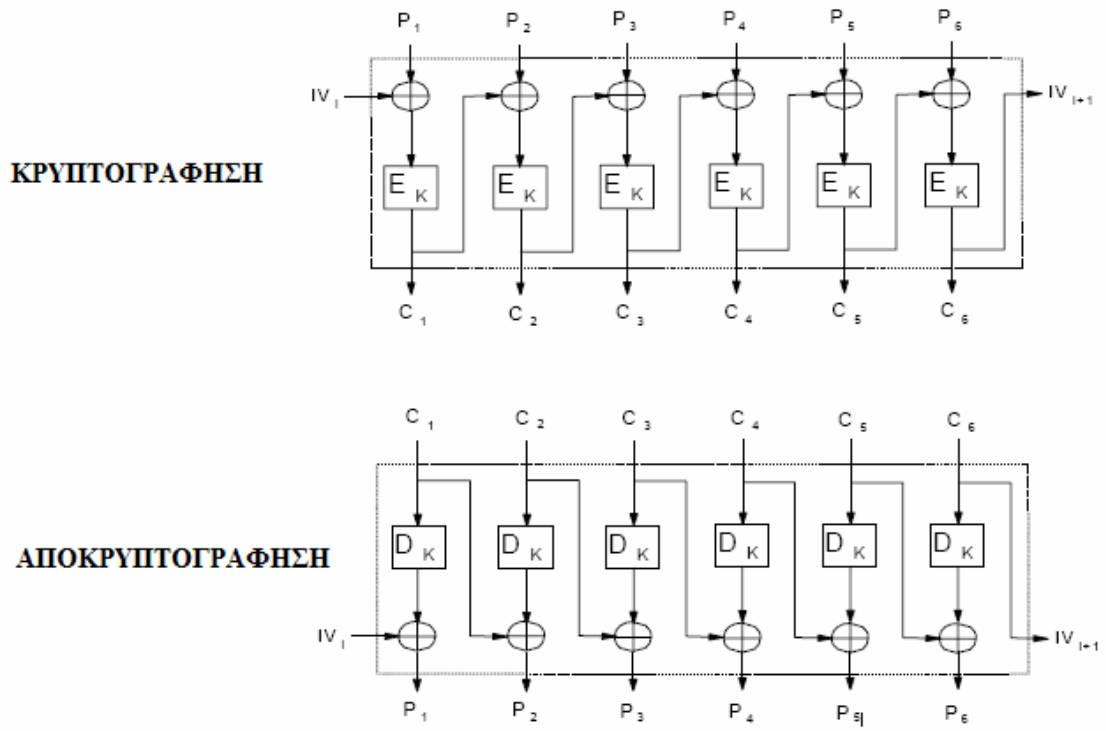
3.2.2 Τρόποι Λειτουργίας

Ένας αλγόριθμος τύπου κώδικα τμήματος έχει διάφορους τρόπους λειτουργίας. Κάθε τρόπος λειτουργίας μπορεί να έχει τις δικές του ιδιότητες εκτός από αυτές που κληρονομεί από τον βασικό κρυπτοσυστήματος. Οι βασικοί τρόποι λειτουργίας είναι: ο Electronic Code Book (ECB), ο Cipher Block Chaining (CBC), ο Cipher Feedback (CFB) και ο Output Feedback (OFB).



Εικόνα 3. Electronic Code Book (ECB)

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

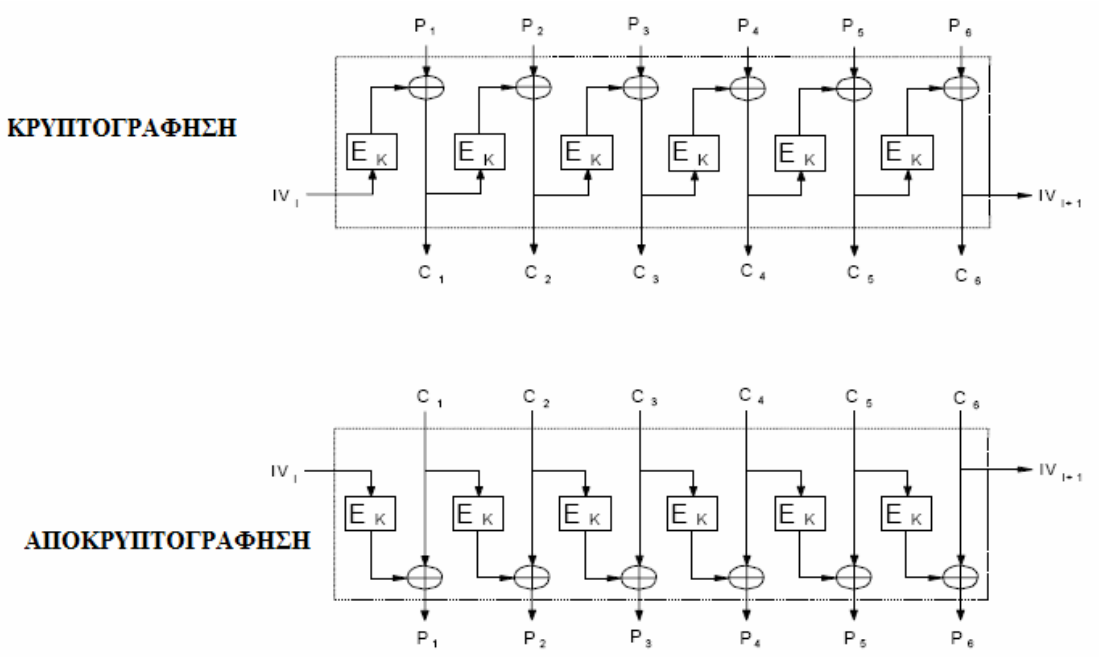


Εικόνα 4. Cipher Block Chaining (CBC)

Σε CBC mode, κάθε μη κρυπτογραφημένο block συνδυάζεται μέσω της λογικής πράξης XOR με το πρωτύτερα κρυπτογραφημένο block. Το αποτέλεσμα κρυπτογραφείται. Απαιτείται μια αρχική τιμή για την πρώτη XOR πράξη που καλείται Διάνυσμα Αρχικοποίησης (Initialization Vector), c_0. Τα όμοια αρχικά τμήματα καλύπτονται με την χρήση της λογικής πράξης και αυξάνεται η ασφάλεια του αλγόριθμου. Η ταχύτητα της κρυπτογράφησης είναι ίδια

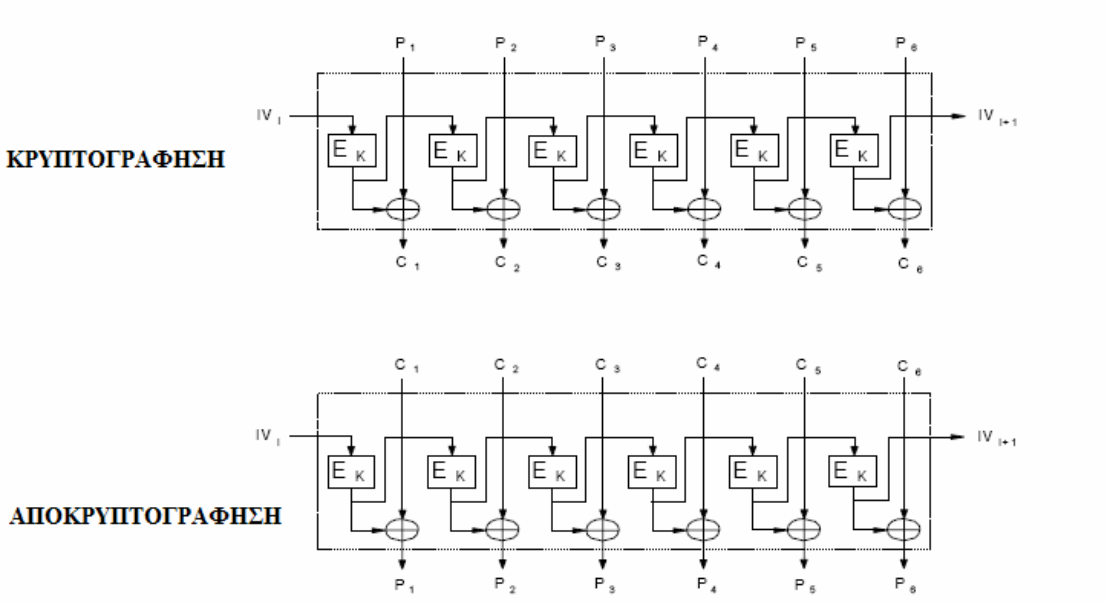
με αυτή του κώδικα τμήματος, αλλά η διαδικασία δεν μπορεί να πραγματοποιηθεί παράλληλα παρ' όλο που η αποκρυπτογράφηση μπορεί.

Σε CFB mode, το προηγούμενο κρυπτογραφημένο τμήμα κρυπτογραφείται και το αποτέλεσμα που παράγεται συνδυάζεται με το επόμενο αρχικό τμήμα με χρήση μιας XOR. Η έξοδος της XOR αποτελεί το νέο κρυπτογραφημένο τμήμα που θα κρυπτογραφηθεί, συνεχίζοντας την διαδικασία. Γίνεται η ποσότητα που χρησιμοποιείται για ανάδραση (feedback) να μην είναι ένα πλήρες τμήμα. Απαιτείται ένα Διάνυσμα Αρχικοποίησης c_0 για την πρώτη XOR πράξη.



Εικόνα 5. Cipher Feedback (CFB)

Με αυτόν τον τρόπο καλύπτονται πιθανές ομοιότητες στα αρχικά τμήμα-τα μέσω της XOR. Γίνεται, όμως, στην πλήρη ανάδραση τα c_i και c_{i-1} να είναι ταυτόσημα. Σαν συνέπεια και το επόμενο ζεύγος κρυπτογραφημένων block θα είναι ταυτόσημα μεταξύ τους. Αυτό το πρόβλημα λύνεται με την χρήση μερικής ανάδρασης. Η ταχύτητα της κρυπτογράφησης είναι ίδια με αυτή του block cipher και δεν επιτρέπεται παράλληλη επεξεργασία.



Εικόνα 6. Output Feedback (OFB)

Σε OFB mode, η διαδικασία είναι παρόμοια με αυτήν του CFB mode, με την διαφορά ότι η ποσότητα που συνδυάζεται με XOR με κάθε αρχικό τμήμα παράγεται ανεξάρτητα από τα αρχικά και κρυπτογραφημένα. Ένας Διάνυσμα Αρχικοποίησης s_0 χρειάζεται για να ξεκινήσει την διαδικασία και κάθε τμήμα si προκύπτει από την κρυπτογράφηση του προηγούμενου s_{i-1}. Η κρυπτογράφηση του αρχικού τμήματος γίνεται με τον συνδυασμό κάθε αρχικού τμήματος μέσω μιας XOR, με το κρυπτογραφημένο s. Ο OFB mode έχει το εξής πλεονέκτημα σε σχέση με τον CFB. Τα πιθανά λάθη μετάδοσης δεν πολλαπλασιάζονται κατά την αποκρυπτογράφηση και έτσι δεν την επηρεάζουν. Το κείμενο, όμως, μπορεί εύκολα να αλλοιωθεί με την αφαίρεση, πρόσθεση ή και ανακατάταξη όμοιων κρυπτογραφημένων τμημάτων. Δεν είναι δυνατή η παράλληλη επεξεργασία, αλλά η διαδικασία μπορεί να επιταχυνθεί με την παραγωγή των κρυπτογραφημένων s πριν τα δεδομένα να είναι διαθέσιμα για κρυπτογράφηση.

Άλλος ένας τρόπος λειτουργίας είναι ο Propagating Cipher Block Chaining (PCBC). Χρησιμοποιείται με πρωτόκολλα όπως το Kerberos version 4, ενώ δεν έχει επίσημα τυποποιηθεί ούτε χαίρει παγκόσμιας αναγνώρισης. Είναι παρόμοιος με το CBC και έχει σχεδιασθεί με σκοπό να αναπαράγει το πιθανό λάθος μετάδοσης, έτσι ώστε να γίνεται αντιληπτό και το κείμενο που προκύπτει να απορρίπτεται.

3.2.3 Κώδικες Ροής

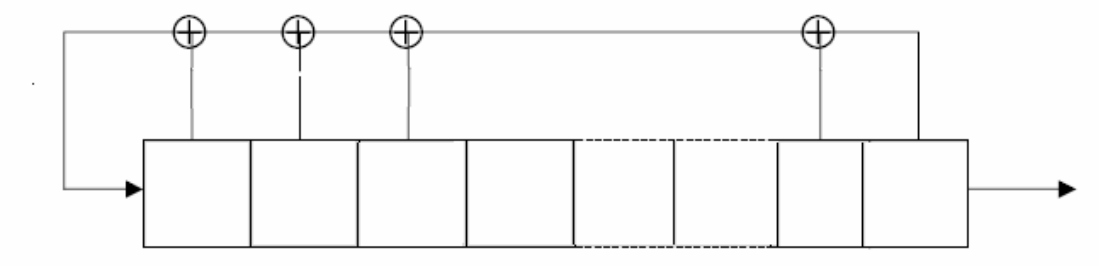
Ο Κώδικας Ροής (stream cipher) είναι ένας τύπος αλγόριθμου συμμετρικής κρυπτογράφησης. Είναι εξαιρετικά ταχείς αλγόριθμοι, κατά πολύ ταχύτεροι από τους κώδικες τμήματος. Σε αντίθεση με τους κώδικες τμήματος που λειτουργούν με μεγάλα κομμάτια δεδομένων (blocks), οι κώδικες ροής τυπικά λειτουργούν με μικρότερες μονάδες απλού κειμένου, συνήθως με bits. Η κρυπτογράφηση ενός συγκεκριμένου κειμένου με έναν κώδικα τμήματος θα καταλήγει πάντα στο ίδιο αποτέλεσμα όταν χρησιμοποιείται το ίδιο κλειδί. Με έναν κώδικα ροής, ο μετασχηματισμός των μικρότερων αυτών μονάδων θα ποικίλει, ανάλογα με πότε αντιμετωπίζονται κατά την διάρκεια της κρυπτογράφησης. Ένας κώδικας ροής παράγει μια ακολουθία από bits που χρησιμοποιείται σαν κλειδί και καλείται keystream. Η κρυπτογράφηση επιτυγχάνεται με τον συνδυασμό του keystream με το αρχικό μη κρυπτογραφημένο κείμενο, συνήθως μέσω της XOR πράξης. Η παραγωγή του keystream μπορεί να είναι ανεξάρτητη του αρχικού κειμένου και του κρυπτογραφήματος (συγχρονισμένοι κώδικες ροής (synchronous stream cipher)) ή μπορεί να εξαρτάται από αυτά (ασύγχρονοι κώδικες ροής (self-synchronizing stream cipher)).

3.2.4 One-time Pads

Οι κώδικες ροής βασίζονται στις θεωρητικές ιδιότητες ενός one-time pad. One-time pads (καμιά φορά καλούνται και Vernam κρυπτοσυστήματα) είναι τα κρυπτοσυστήματα που χρησιμοποιούν μια ακολουθία bits (keystream) που παράγεται τελείως στην τύχη.

Η ακολουθία των bits είναι του ίδιου μήκους με το μη κρυπτογραφημένο κείμενο και συνδυάζεται μέσω μιας XOR πράξης με το αυτό για την παραγωγή του κρυπτογραφήματος. Επειδή η ακολουθία των bits είναι τελείως τυχαία και είναι του ίδιου μήκους με το αρχικό κείμενο, η εύρεση του κειμένου είναι αδύνατη ακόμα και με τη διάθεση τεράστιας υπολογιστικής ισχύος. Ένα τέτοιο κρυπτοσύστημα προσφέρει τέλεια μυστικότητα και ασφάλεια και έχει χρησιμοποιηθεί σε μεγάλη κλίμακα σε καιρό πολέμου για τη διασφάλιση διπλωματικών καναλιών. Το γεγονός, όμως, ότι το μυστικό κλειδί (δηλαδή το keystream), που χρησιμοποιείται μόνο μία φορά, είναι του ίδιου μήκους με το μήνυμα, εισάγει σημαντικό πρόβλημα στη διαχείριση του κλειδιού. Παρ' όλη την ασφάλεια που προσφέρει, ο one-time pad δεν μπορεί να εφαρμοστεί στην πράξη. Οι κώδικες ροής αναπτύχθηκαν σαν μια προσέγγιση της λειτουργίας ενός one-time pad. Βέβαια, παρά το γεγονός ότι δεν είναι σε θέση να παρέχουν τη θεωρητική ασφάλεια ενός time-pad, είναι τουλάχιστον πρακτικοί.

Ο πιο ευρέως χρησιμοποιούμενος κώδικας ροής είναι ο RC4. Ενδιαφέρον παρουσιάζει το γεγονός ότι συγκεκριμένοι τρόποι λειτουργίας ενός block cipher προσομοιάζουν ένα κώδικα ροής όπως για παράδειγμα ο DES σε CFB και OFB modes. Ακόμα και έτσι, οι αυθεντικοί κώδικες ροής είναι αρκετά ταχύτεροι.



Εικόνα 7. Γραμμικός Καταχωρητής Ολίσθησης

Ένας μηχανισμός για την παραγωγή του keystream είναι ο Γραμμικός Καταχωρητής Ολίσθησης (Linear Feedback Shift Register (LFSR)). Ο καταχωρητής αποτελείται από μία σειρά κελιών (cells) το καθένα από τα οποία αποτελείται από ένα bit. Τα περιεχόμενα των κελιών καθορίζονται από ένα Διάνυσμα Αρχικοποίησης (Initialization Vector) που λειτουργεί σαν το μυστικό κλειδί. Το keystream δεν αποτελεί πλέον το μυστικό κλειδί (όπως στους one-time pads) λόγω του μεγέθους του. Η συμπεριφορά του καταχωρητή ρυθμίζεται από ένα ρολόι και σε κάθε χρονική στιγμή τα bits μετακινούνται μία θέση δεξιά, την στιγμή που το XOR αποτέλεσμα μερικών από αυτών τοποθετείται στο αριστερότερο κελί. Κάθε αλλαγή του ρολογιού δίνει ένα bit εξόδου.

Η κατασκευή των LFSR είναι εύκολη τόσο υπό μορφή λογισμικού (software) όσο και υπό μορφή υλικού (hardware), ενώ η λειτουργία τους είναι ταχύτατη. Οι ακολουθίες bit, όμως, που δημιουργούνται από ένα και μοναδικό LFSR δεν είναι ασφαλείς, καθ' ότι τον τελευταίο καιρό έχει αναπτυχθεί δυνατή μαθηματική φόρμουλα που επιτρέπει την ανάλυση του μηχανισμού και εύρεση του keystream. Απαιτείται, λοιπόν, η συνδυασμένη χρήση πολλών LFSRs. Ένας Shift Register Cascade αποτελεί ένα σύνολο από LFSRs που συν-δέονται μεταξύ τους με τέτοιο τρόπο ώστε η συμπεριφορά του ενός να εξαρτάται από την συμπεριφορά του άλλου. Αυτό επιτυγχάνεται συνήθως με τη χρήση του ενός LFSR να ελέγχει το ρολόι του άλλου. Άλλο παράδειγμα τέτοιου συνδυασμού είναι ο Shrinking Generator που αναπτύχθηκε από τους Coppersmith, Krawczyk και Mansour. Βασίζεται στην αλληλεπίδραση των εξόδων δύο LFSRs. Τα bits της μιας εξόδου χρησιμοποιούνται για να καθορίσουν, μέσω κατάλληλης τεχνικής, εάν τα bits της δεύτερης εξόδου θα συμπεριληφθούν στο keystream. Είναι απλός και έχει καλά χαρακτηριστικά ασφαλείας.

3.2.5 Συναρτήσεις Κατακερματισμού

Ο όρος συνάρτηση κατακερματισμού (hash function) h υποδηλώνει ένα μετασχηματισμό που παίρνει ως είσοδο ένα μήνυμα m οποιουδήποτε μήκους και επιστρέφει στην έξοδο μία ακολουθία χαρακτήρων h(m) περιορισμένου μήκους που καλείται τιμή κατακερματισμού (hash value). Οι συναρτήσεις κατακερματισμού είναι συναρτήσεις με τις εξής ιδιότητες:

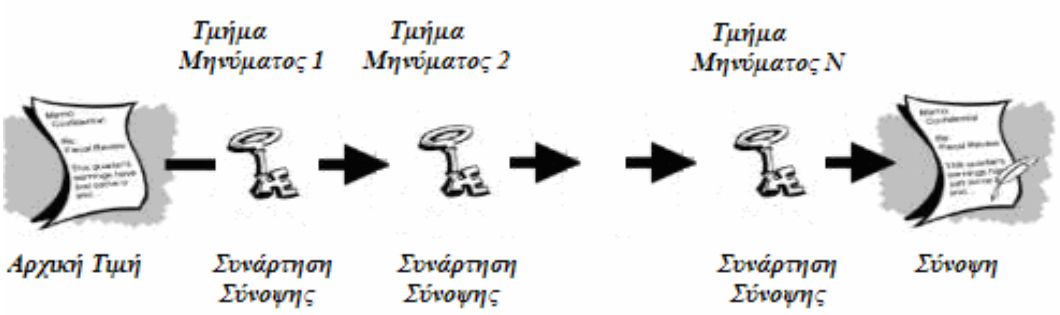
- Η είσοδος είναι οποιουδήποτε μήκους.
- Η έξοδος έχει περιορισμένο μήκος.
- Δεδομένου του m, ο υπολογισμός του h(m) είναι εύκολος.
- Η h είναι μη αντιστρέψιμη.
- Η h δεν είναι αμφιμονοσήμαντη (ένα προς ένα συνάρτηση).

Η τιμή κατακερματισμού παρουσιάζει συνοπτικά το μεγαλύτερο μήνυμα ή έγγραφο, για αυτό καλείται και σύνοψη μηνύματος (message digest). Μπορούμε να φανταστούμε τη σύνοψη του μηνύματος σαν "ψηφιακό αποτύπωμα" ("digital fingerprint") του εγγράφου. Παραδείγματα γνωστών συναρτήσεων κατακερματισμού είναι οι MD2, MD5 και SHA.

Εικόνα 8. Συνάρτηση Κατακερματισμού (hash function)

Η ψηφιακή υπογραφή των μηνυμάτων παράγεται με την εφαρμογή κρυπτογραφικών διαδικασιών στη σύνοψη του μηνύματος, το οποίο είναι πιο μικρό και εύκολο στη διαχείριση. Επιπλέον ένα μήνυμα σύνοψης μπορεί να δημοσιοποιηθεί χωρίς να αποκαλύπτει τα περιεχόμενα του αυθεντικού κειμένου. Οι Damgard και Merkle εισήγαγαν την έννοια του συναρτήσεων συμπίεσης (compression function). Αυτές οι συναρτήσεις παίρνουν είσοδο καθορισμένου μήκους και δίνουν έξοδο μικρότερου, περιορισμένου μήκους. Δεδομένης μίας συνάρτησης κατακερματισμού, μια συνάρτηση συμπίεσης μπορεί να πραγματοποιηθεί με την επανειλημμένη εφαρμογή της συναρτήσεων σύνοψης, έως ότου ολόκληρο το μήνυμα έχει επεξεργαστεί.

Πιο αναλυτικά, το μήνυμα τεμαχίζεται σε τμήματα (blocks), των οποίων το μέγεθος εξαρτάται από τη συνάρτηση σύνοψης και συμπληρώνεται (padded) για λόγους ασφαλείας, ώστε το μήκος του μηνύματος να είναι πολλαπλάσιο του μήκους του block. Το παρακάτω σχήμα επιδεικνύει τη λογική της διαδικασίας.



Εικόνα 9. Συνάρτηση Συμπίεσης

3.2.6 Message Authentication Code (MAC)

Message Authentication Code είναι ένα κώδικας (καλείται και άθροισμα ελέγχου-checksum) που συνοδεύει το μήνυμα και πιστοποιεί την ταυτότητα του αποστολέα και την ακεραιότητα του μηνύματος. Για την παραγωγή τους εφαρμόζεται στο μήνυμα ένα από τα προαναφερθέντα κρυπτογραφικά εργαλεία σε συνδυασμό με ένα μυστικό κλειδί. Σε αντίθεση με τις ψηφιακές υπογραφές, τα MACs υπολογίζονται και επαληθεύονται με το ίδιο κλειδί, έτσι ώστε να μπορούν να επαληθευθούν μόνο από τον προοριζόμενο παραλήπτη. Υπάρχουν τέσσερις τύποι MAC: (1) τα άνευ όρων ασφαλή, (2) τα βασιζόμενα σε συναρτήσεις κατακερματισμού, (3) τα βασιζόμενα σε κώδικες ροής και (4) τα βασιζόμενα σε κώδικες τμημάτων.

1. Οι Simmons και Stinson πρότειναν έναν άνευ όρων ασφαλή MAC βασισμένο στην κρυπτογράφηση με ένα one-time pad. Όπως είπαμε, όμως, επειδή το κλειδί ενός one-time pad είναι πολύ μεγάλο, δεν χρησιμοποιούνται στην πράξη, γι' αυτό το λόγο δεν θα προχωρήσουμε σε περαιτέρω ανάλυσή τους.

2. Τα MACs που βασίζονται σε συναρτήσεις κατακερματισμού χρησιμοποιούν ένα μυστικό κλειδί σε συνδυασμό με μια συνάρτηση κατακερματισμού για να παράγουν το άθροισμα ελέγχου που συνοδεύει το μήνυμα. Το κλειδί χρησιμοποιείται για να κρυπτογραφήσει τη σύνοψη μηνύματος. Ο παραλήπτης του μηνύματος, που μοιράζεται με τον αποστολέα το ίδιο κλειδί, αποκρυπτογραφεί το μήνυμα σύνοψης (message digest) και έπειτα το συγκρίνει με ένα μήνυμα σύνοψης που παράγει ο ίδιος από το μήνυμα. Εάν η σύγκριση είναι επιτυχής, τότε ο παραλήπτης σιγουρεύεται ότι τα δεδομένα δεν έχουν αλλοιωθεί. Ένα παράδειγμα είναι ο keyed-MD5.

3. Τα MACs που βασίζονται σε κώδικες ροής αναπτύχθηκαν από τους Lai, Rueppel και Woolven. Στο αλγόριθμο που ανέπτυξαν, ένας αποδεδειγμένα ασφαλής κώδικα ροής,

χρησιμοποιείται για να χωρίσει το μήνυμα σε δύο substreams καθένα από τα οποία τροφοδοτείται σε ένα LFSR. Το άθροισμα ελέγχου αποτελεί την τελική κατάσταση των δύο LFSRs.
4. Τέλος, τα MAC μπορούν να δημιουργηθούν από κώδικες τμήματος, όπως τον DES-CBC. Σε αυτήν τη μέθοδο, το μήνυμα κρυπτογραφείται με εφαρμογή του αλγόριθμου κώδικα τμήματος. Το τελευταίο κρυπτογραφημένο τμήμα που δίνει ο αλγόριθμος αποτελεί το άθροισμα ελέγχου του μηνύματος.

3.2.7 Μηχανισμοί Διαχείρισης και Ανταλλαγής Κλειδιών

Οι μηχανισμοί διαχείρισης κλειδιών (key management) και ανταλλαγής κλειδιών (key exchange), ασχολούνται με την ασφαλή παραγωγή, διανομή και αποθήκευση των κλειδιών κρυπτογράφησης. Η εύρεση απρόσβλητων μεθόδων διαχείρισης και ανταλλαγή κλειδιών είναι πολύ σημαντική στη διατήρηση της ασφάλειας της επικοινωνίας. Η έννοια της διαχείρισης κλειδιών αναφέρεται στα ασύμμετρα κρυπτοσυστήματα. Τα χαρακτηριστικά που πρέπει να έχει ένας μηχανισμός διαχείρισης κλειδιών είναι τα ακόλουθα. Οι χρήστες πρέπει να είναι σε θέση να μπορούν να αποκτήσουν με ασφάλεια ένα ζεύγος δημόσιου – ιδιωτικού κλειδιού που θα ικανοποιεί τις ανάγκες τους για προστατευμένη επικοινωνία. Πρέπει να υπάρχει τρόπος αποθήκευσης και δημοσιοποίησης των δημόσιων κλειδιών, ενώ παράλληλα θα είναι δυνατή η ανάκτησή τους όποτε χρειάζεται. Επίσης τα δημόσια κλειδιά θα πρέπει να συσχετίζονται με σίγουρο τρόπο με την ταυτότητα του νόμιμου κατόχου. Έτσι, δεν θα μπορεί κάποιος να παρουσιάζεται σαν κάποιος άλλος, επιδεικνύοντας ένα ψεύτικο δημόσιο κλειδί. Τέλος οι χρήστες πρέπει να έχουν τη δυνατότητα να φυλάσσουν τις ιδιωτικές τους κλείδες με ασφάλεια, οι οποίες θα είναι έγκυρες μόνο για συγκεκριμένο χρονικό διάστημα. Η ανταλλαγή κλειδιών εφαρμόζεται στα συμμετρικά κρυπτοσυστήματα όπου οι δύο επικοινωνούντες χρήστες πρέπει να αποφασίσουν για το κοινό μυστικό κλειδί και έπειτα να αποκτήσουν από ένα αντίγραφο αυτού, χωρίς κανένας άλλος να μάθει για αυτό.

3.3 Απλές Εφαρμογές της Κρυπτογραφίας

3.3.1 Διαφύλαξη του Απορρήτου και Κρυπτογράφηση

Η πιο φανερή εφαρμογή της κρυπτογραφίας είναι η εξασφάλιση του απορρήτου (privacy) μέσω της κρυπτογράφησης. Οι ευαίσθητες πληροφορίες κρυπτογραφούνται με κατάλληλο αλγόριθμο που εξαρτάται από τις ανάγκες της επικοινωνίας. Για να μπορέσει κάποιος να επαναφέρει τα κρυπτογραφημένα δεδομένα στην αρχική τους μορφή πρέπει να κατέχει το κλειδί που

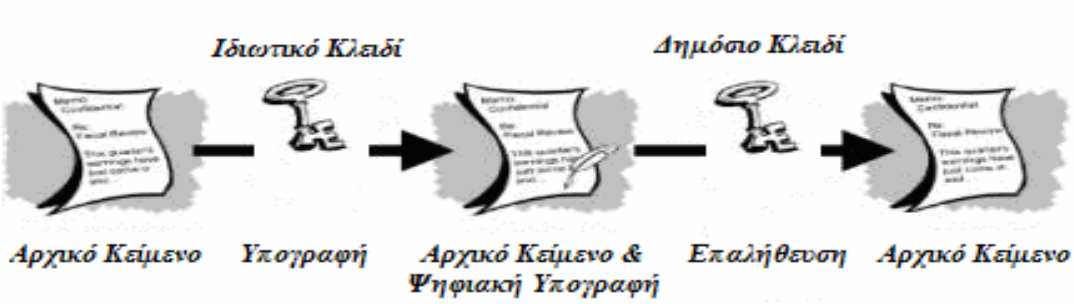
χρησιμοποιήθηκε για την κρυπτογράφησή τους, εάν μιλάμε για συμμετρική κρυπτογράφηση ή το ιδιωτικό κλειδί που αντιστοιχεί στο δημόσιο κλειδί που το κρυπτογράφησε, εάν μιλάμε για ασύμμετρη κρυπτογράφηση. Αξίζει να σημειώσουμε ότι υπάρχουν περιπτώσεις όπου οι πληροφορίες δεν πρέπει να είναι απροσπέλαστες από όλους και γι' αυτό αποθηκεύονται με τέτοιο τρόπο, ώστε η αντιστροφή της κρυπτογραφικής διαδικασίας που έχει εφαρμοστεί, να είναι αδύνατη.

Για παράδειγμα, σε ένα τυπικό περιβάλλον πολλών χρηστών, κανένας δεν πρέπει να έχει γνώση του αρχείου που περιέχει τους κωδικούς όλων των χρηστών. Συχνά, λοιπόν, αποθηκεύονται οι συνόψεις (hash values) των πληροφοριών (στην προηγούμενη περίπτωση θα ήταν οι κωδικοί) αντί για τις ίδιες τις πληροφορίες. Έτσι, οι χρήστες είναι σίγουροι για το απόρρητο των κωδικών τους, ενώ μπορούν να αποδεικνύουν την ταυτότητα τους με την παροχή του κωδικού τους. Ο υπολογιστής που έχει αποθηκευμένες τις τιμές κατακερματισμού των κωδικών, σε κάθε εισαγωγή κωδικού υπολογίζει την τιμή κατακερματισμού του και τη συγκρίνει με το αποθηκευμένο που αντιστοιχεί στον χρήστη που προσπαθεί να πιστοποιήσει τον εαυτό του.

3.3.2 Πιστοποίηση Ταυτότητας και Ψηφιακές Υπογραφές

Η ψηφιακή υπογραφή είναι ένα εργαλείο που παρέχει ακεραιότητα (integrity) των δεδομένων και πιστοποίηση ταυτότητας (authentication). Η έννοια πιστοποίηση ταυτότητας περιλαμβάνει όλες εκείνες τις διαδικασίες που είναι απαραίτητες για την επαλήθευση συγκεκριμένων ευαίσθητων πληροφοριών, όπως την ταυτότητα του αποστολέα ενός μηνύματος, την αυθεντικότητα ενός εγγράφου, ακεραιότητα δεδομένων (integrity) και την ταυτότητα ενός υπολογιστή. Οι ψηφιακές υπογραφές επιτυγχάνουν την πιστοποίηση ταυτότητας, παράγοντας ένα σύνολο πληροφοριών που βασίζεται στο έγγραφο και σε ιδιωτικά στοιχεία του αποστολέα. Το σύνολο αυτό δημιουργείται μέσω μιας συνάρτηση κατακερματισμού και του ιδιωτικού κλειδιού του αποστολέα. Ας δούμε πως λειτουργεί μία ψηφιακή υπογραφή. Έστω δύο χρήστες, ο Α και ο Β. Όταν ο Α θέλει να στείλει ένα υπογεγραμμένο έγγραφο στον Β. Το πρώτο βήμα είναι η παραγωγή της σύνοψης του μηνύματος. Η σύνοψη είναι κατά κανόνα μικρότερο σε μέγεθος από το αρχικό μήνυμα. Στο δεύτερο βήμα, ο Α κρυπτογραφεί τη σύνοψη με το ιδιωτικό του κλειδί. Τέλος, στέλνει τη κρυπτογραφημένη σύνοψη στον Β μαζί με το έγγραφο. Για να μπορέσει ο Β να επαληθεύσει την υπογραφή πρέπει να γνωρίζει το δημόσιο κλειδί του Α και την συνάρτηση κατακερματισμού που χρησιμοποίησε ο Α. Πρώτα θα αποκρυπτογραφήσει τη σύνοψη με το δημόσιο κλειδί του Α και θα πάρει τη σύνοψη που είχε παράγει ο Α. Έπειτα, θα υπολογίσει τη

σύνοψη του εγγράφου ξανά και θα το συγκρίνει με το παραληφθέν. Εάν τα δύο είναι ταυτόσημα τότε η υπογραφή επαληθεύτηκε επιτυχώς. Εάν δεν ταιριάζουν τότε ή κάποιος προσποιείται ότι είναι ο Α ή το μήνυμα τροποποιήθηκε κατά την μεταφορά του ή προέκυψε λάθος κατά την μετάδοση. Οποιοσδήποτε που γνωρίζει το δημόσιο κλειδί του Α, τη συνάρτηση κατακερματισμού και τον αλγόριθμο κρυπτογράφησης που χρησιμοποιήθηκε, μπορεί να επιβεβαιώσει το γεγονός ότι το μήνυμα προέρχεται από τον Α και ότι δεν αλλοιώθηκε μετά την υπογραφή του.



Εικόνα 10. Ψηφιακή Υπογραφή

Για να έχει αποτέλεσμα η παραπάνω μέθοδος, πρέπει να τηρούνται δύο προϋποθέσεις: (α) η συνάρτηση κατακερματισμού πρέπει να είναι όσο το δυνατόν περισσότερο μη αντιστρέψιμη και (β) τα ζεύγη δημόσιου – ιδιωτικού κλειδιού να είναι συσχετισμένα με τους νόμιμους κατόχους τους. Για την εξασφάλιση της δεύτερης προϋπόθεσης υπάρχουν ψηφιακά έγγραφα που καλούνται πιστοποιητικά (certificates) και συνδέουν ένα άτομο με ένα συγκεκριμένο δημόσιο κλειδί.

ΚΕΦΑΛΑΙΟ 4ο : ΑΛΓΟΡΙΘΜΟΙ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ

4.1 Αλγόριθμοι Ασύμμετρης Κρυπτογραφίας

RSA

Το σύστημα RSA είναι ένα σύστημα ασύμμετρης κρυπτογραφίας που προσφέρει τεχνικές κρυπτογράφησης και ψηφιακές υπογραφές. Αναπτύχθηκε το 1977 από τους Ron Rivest, Adi Shamir και Leonard Adleman. Από τα αρχικά των επιθέτων τους προέρχεται το ακρωνύμιο RSA. Το RSA λειτουργεί ως εξής: παίρνουμε δύο μεγάλους πρώτους αριθμούς p,q και υπολογίζουμε το γινόμενο τους n = pq. Το n καλείται modulus. Διαλέγουμε ένα αριθμό e μικρότερο του n και τέτοιο, ώστε e και (p-1)(q-1) να μην έχουν κοινούς διαιρέτες εκτός του 1. Βρίσκουμε έναν άλλο αριθμό d, ώστε (ed-1) να διαιρείται από το (p-1)(q-1). Τα ζευγάρια (n,e) και (n,d) καλούνται δημόσιο κλειδί και ιδιωτικό κλειδί, αντίστοιχα.

Είναι δύσκολο να βρεθεί το ιδιωτικό κλειδί d από το δημόσιο κλειδί e. Αυτό θα απαιτούσε την εύρεση των διαιρετέων του πρώτου αριθμού n, δηλαδή των αριθμών p και q. Ο n είναι πολύ μεγάλος και επειδή είναι πρώτος, θα έχει μόνο δύο πρώτους διαιρέτες. Άρα η εύρεση των διαιρετέων είναι πολύ δύσκολη έως και αδύνατη. Στο άλυτο αυτού του προ-βλήματος βασίζεται το σύστημα RSA. Η ανακάλυψη μιας εύκολης μεθόδου επίλυσης του προβλήματος, θα αχρήστευε το RSA. Με το RSA η κρυπτογράφηση και η πιστοποίηση ταυτότητας πραγματοποιούνται χωρίς την κοινή χρήση ιδιωτικών κλειδιών. Ο καθένας χρησιμοποιεί μόνο το δικό του ιδιωτικό κλειδί ή το δημόσιο κλειδί οποιουδήποτε άλλου. Όλοι μπορούν να στείλουν ένα κρυπτογραφημένο μήνυμα ή να επαληθεύσουν μια υπογραφή, αλλά μόνο ο κάτοχος του σωστού ιδιωτικού κλειδιού μπορεί να αποκρυπτογραφήσει ή να υπογράψει ένα μήνυμα.

Κρυπτογράφηση με το RSA

Έστω ο χρήστης Α που θέλει να στείλει κρυπτογραφημένο στο χρήστη Β ένα έγγραφο. Ο Α κρυπτογραφεί το έγγραφο με την εξής εξίσωση: c = me mod n, όπου (n,e) είναι το δημόσιο κλειδί του Β. Ο Β, όταν παραλάβει το μήνυμα θα εφαρμόσει την εξής εξίσωση: m = cd mod n, όπου (n,d) το ιδιωτικό κλειδί του Β. Η μαθηματική σχέση που το e και το d εξασφαλίζει το γεγονός ότι ο Β αποκρυπτογραφεί το μήνυμα. Αφού μόνο ο Β ξέρει το d, μόνο αυτός μπορεί να αποκρυπτογραφήσει το μήνυμα.

Ψηφιακές Υπογραφές με το RSA

Ας υποθέσουμε, τώρα, ότι ο Α θέλει να στείλει μήνυμα στον Β με τέτοιο τρόπο, ώστε ο Β να είναι σίγουρος ότι το μήνυμα είναι αυθεντικό και δεν έχει μεταβληθεί. Ο Α υπογράφει το έγγραφο ως εξής: s = md mod n, ό-που d και n είναι το ιδιωτικό κλειδί του Α. Για να

επαληθεύσει την υπογραφή ο Β εκτελεί την πράξη: m = se mod n, όπου e και n το δημόσιο κλειδί του Α.

4.2 Αλγόριθμοι Συμμετρικής Κρυπτογραφίας

DES (Data Encryption Standard)

Αντιπροσωπεύει την τυποποίηση Federal Information Processing Standard (FIPS) 46-1 που επίσης περιγράφει τον Data Encryption Algorithm (DEA). Αρχικά αναπτύχθηκε από την IBM, ενώ σημαντικό ρόλο στην ανάπτυξη του έπαιξε η NSA και το National Institute of Standards and Technology (NIST). Είναι ο πιο γνωστός και παγκόσμια χρησιμοποιούμενος συμμετρικός αλγόριθμος. Ο DES είναι block cipher, πιο συγκεκριμένα Feistel cipher, με μέγεθος block 64 bit. Χρησιμοποιεί κλειδί 64 bits από τα οποία τα 8 αποτελούν bits ισοτιμίας. Όταν χρησιμοποιείται για την επικοινωνία, αποστολέας και παραλήπτης μοιράζονται το ίδιο κλειδί. Ο DES, εκτός από κρυπτογράφηση, μπορεί να χρησιμοποιηθεί στην παραγωγή MACs (σε CBC mode). Επίσης, μπορεί να χρησιμοποιηθεί για κρυπτογράφηση αρχείων αποθηκευμένα σε σκληρό δίσκο σε περιβάλλοντα ενός χρήστη. Για την διανομή των κλειδιών σε περιβάλλον πολλών χρηστών, συνδυάζεται με ασύμμετρο κρυπτοσύστημα.

Triple-DES

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

- DES-EEE3 (Encrypt-Encrypt-Encrypt): πραγματοποιούνται τρεις συνεχόμενες κρυπτογραφήσεις με το τρία διαφορετικά κλειδιά.
- DES-EDE3 (Encrypt-Decrypt-Encrypt): το μήνυμα διαδοχικά κρυπτογραφείται, αποκρυπτογραφείται και τέλος κρυπτογραφείται με χρήση τριών διαφορετικών κλειδιών.
- DES-EEE2: είναι η ίδια με την πρώτη διαδικασία εκτός του ότι απαιτούνται δύο διαφορετικά κλειδιά.
- DES-EDE2: είναι η ίδια με την δεύτερη διαδικασία εκτός του ότι απαιτούνται δύο κλειδιά.

Τα επιπλέον κλειδιά δημιουργούνται από το κοινό μυστικό κλειδί με κατάλληλο αλγόριθμο. Από αυτούς τους τρόπους, ο πιο ασφαλής είναι ο DES-EEE3, με την τριπλή κρυπτογράφηση και τα τρία διαφορετικά κλειδιά.

DESX

Ο DESX είναι μια άλλη παραλλαγή του DES. Η διαφορά του DES και του DESX είναι ότι η είσοδος στο DESX περνάει από μια XOR πράξη με ένα επιπλέον κλειδί 64 bits και ομοίως η έξοδος της κρυπτογράφησης. Η αιτία ανάπτυξης του DESX είναι η δραματική αύξηση της αντοχής του DES σε γνωστές επιθέσεις.

AES (Advanced Encryption Standard)

Είναι ένας block cipher που προορίζεται να γίνει τυποποίηση του FIPS και να αντικαταστήσει τον DES.

DSS (Digital Signature Algorithm)

Το National Institute of Standards and Technology (NIST) δημοσιοποίησε το Digital Signature Algorithm (DSS), που είναι μέρος του Capstone Project της κυβέρνησης των Ηνωμένων Πολιτειών, τον Μάιο του 1994. Έχει καθιερωθεί σαν το επίσημο αλγόριθμο παραγωγής ψηφιακών υπογραφών της κυβέρνησης των Η.Π.Α. Βασίζεται στο πρόβλημα του διακριτού λογαρίθμου και χρησιμοποιείται μόνο για παραγωγή ψηφιακών υπογραφών.

Η διαφορά από τις υπογραφές του RSA είναι, ότι ενώ στο DSA η παραγωγή των υπογραφών είναι πιο γρήγορη από την επιβεβαίωσή τους, στο RSA συμβαίνει το αντίθετο: η επιβεβαίωση είναι ταχύτερη από την υπογραφή. Παρ' όλο που μπορεί να υποστηριχθεί ότι η γρήγορη παραγωγή υπογραφών αποτελεί πλεονέκτημα, επειδή ένα μήνυμα υπογράφεται μία φορά αλλά η υπογραφή του μπορεί να επαληθευτεί πολλές φορές, κάτι τέτοιο δεν ανταποκρίνεται στην πραγματικότητα. Το DSS έχει ολοκληρωθεί σε πολλά συστήματα ασφαλείας, αν και έχει λάβει πολλές άσχημες κριτικές. Τα κυριότερα θέματα κριτικής είναι η έλλειψη ευελιξίας, η αργή επαλήθευση των υπογραφών, η αδυναμία συνεργασίας με άλλο πρωτόκολλο πιστοποίησης ταυτότητας και τέλος ότι ο αλγόριθμος δεν είχε αποκαλυφθεί.

RC2, RC4, RC5

Ο RC2 είναι ένας block cipher με κλειδί μεταβλητού μήκους που σχεδιάστηκε από τον Ron Rivest για την RSA Inc. Τα αρχικά σημαίνουν "Ron's Code" ή "Rivest's Cipher". Είναι γρηγορότερος από τον DES και στόχος της σχεδίασης ήταν να λειτουργήσει για αντικατάσταση του DES. Μπορεί να γίνει περισσότερο ή λιγότερο ασφαλής από τον DES, ανάλογα με το μήκος του κλειδιού. Έχει μέγεθος block ίσο με 64 bits και είναι έως και τρεις φορές ταχύτερος από τον DES. Ο RC4 είναι ένας κώδικας ροής που σχεδιάστηκε πάλι από την Ron Rivest για

λογαριασμό της RSA Inc. Έχει μεταβλητό μήκος κλειδιού και λειτουργεί στο επίπεδο του byte. Θεωρείται εξαιρετικά ασφαλής και οι υλοποιήσεις του σε λογισμικό τρέχουν πολύ γρήγορα. Χρησιμοποιείται για κρυπτογράφηση τοπικά αποθηκευμένων αρχείων και για την διασφάλιση της επικοινωνίας μεταξύ δύο απομακρυσμένων σημείων μέσω του πρωτοκόλλου SSL. Ο RC5 είναι ένας γρήγορος block cipher που αναπτύχθηκε από τον Ron Rivest για λογαριασμό της RSA Inc το 1994. Έχει πολλούς παραμέτρους: μεταβλητό μήκος κλειδιού, μεταβλητό μέγεθος block και μεταβλητό αριθμό επαναλήψεων. Τυπικές επιλογές για το μέγεθος του block είναι 32 bits (για πειραματικές εφαρμογές), 64 bits (για αντικατάσταση του DES) και 128 bits. Ο αριθμός των επαναλήψεων μπορεί να είναι από 0 έως και 255. Ο RC5 είναι πολύ απλός στην λειτουργία, πράγμα που τον κάνει εύκολο στην ανάλυση.

IDEA (International Data Encryption Algorithm)

Ο IDEA είναι ένας block cipher που αναπτύχθηκε από τους Lai και Massey. Χρησιμοποιεί block μεγέθους 64 bits και κλειδιά 128 bits. Η διαδικασία της κρυπτογράφησης απαιτεί 8 σύνθετες επαναλήψεις. Παρ' όλο που δεν έχει την κατασκευή ενός Feistel κρυπτοσυστήματος, η αποκρυπτογράφηση γίνεται με τον ίδιο τρόπο που γίνεται και η κρυπτογράφηση. Έχει σχεδιαστεί για να είναι εύκολα εφαρμόσιμος τόσο σε υλικό (hardware) όσο και σε λογισμικό (software). Μερικές, όμως, αριθμητικές διεργασίες που χρησιμοποιεί ο IDEA καθιστούν τις εφαρμογές αργές, παρόμοιες σε ταχύτητα με τον DES. Ο IDEA αποτελεί ένα πολύ δυνατό αλγόριθμο που είναι απρόσβλητος από τα περισσότερα είδη επιθέσεων.

Blowfish

Ο Blowfish είναι ένας block cipher που κατασκευάστηκε από τον Schneier. Είναι ένας Feistel cipher με μέγεθος block 64 bits και μεταβλητό μήκος κλειδιού, με μέγιστο μήκος 448 bits. Όλες οι διεργασίες βασίζονται σε XOR πράξεις και προσθέσεις λέξεων των 32 bits. Από το κλειδί παράγεται πίνακας με τα subkeys που χρησιμοποιούνται σε κάθε γύρο επανάληψης της κρυπτογράφησης. Έχει σχεδιασθεί για 32-bit μηχανές και είναι σημαντικά ταχύτερος από τον DES. Παρ' όλες τις αδυναμίες που έχουν ανακαλυφθεί καθ' όλη την διάρκεια της ύπαρξης του, θεωρείται ακόμα ασφαλής αλγόριθμος.

4.3 Συναρτήσεις Κατακερματισμού

SHA και SHA-1 (Secure Hash Algorithm)

Ο SHA, όπως και SHA-1, αναπτύχθηκε από το NIST. Ο SHA-1 αποτελεί επανέκδοση του SHA που διόρθωνε μια ατέλεια του τελευταίου. Ο SHA-1 είδε το φως της δημοσιότητας το 1994 και η δομή και λειτουργία του είναι παρόμοια με την αντίστοιχη του MD4 που αναπτύχθηκε από τον Ron Rivest. Είναι και αυτός μέρος του Capstone Project. Ο SHA-1 παίρνει είσοδο μήνυμα μήκους μικρότερο από 264 bits και παράγει σύνοψη 160 bits. Είναι ελαφρά πιο αργός από τον MD5, αλλά η μεγαλύτερη σύνοψη που παράγει τον κάνουν πιο ασφαλή απέναντι σε προσπάθειες αντιστροφής του.

MD2, MD4, MD5 (Message Digest)

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

Ο MD2 αναπτύχθηκε το 1989. Το μήνυμα αρχικά συμπληρώνεται με κατάλληλο αριθμό bytes, ώστε το μήκος του σε bytes να είναι διαιρέσιμο από το 16. Ένα αρχικό άθροισμα ελέγχου (checksum) των 16 bits προστίθεται στο τέλος του μηνύματος και η τελική σύνοψη παράγεται από το αποτέλεσμα της προηγούμενης ενέργειας. Η κρυπτανάλυση του MD2 έδειξε ότι είναι δυνατόν να υπάρχουν μηνύματα που παράγουν την ίδια σύνοψη, αν και μόνο αν παραλείπεται το βήμα πρόσθεσης του 16-byte checksum.

Ο MD4 αναπτύχθηκε το 1990. Το μήκος του μηνύματος συμπληρώνεται με κατάλληλο αριθμό bits, ώστε να το μήκος του σε bits συν 448 να είναι διαιρέσιμο από το 512. Μια δυαδική αναπαράσταση του μηνύματος των 64 bits προστίθεται στο μήνυμα και το αποτέλεσμα επεξεργάζεται με τη συνάρτηση σύνοψης. Τα τμήματα που διαχειρίζεται η συνάρτηση σύνοψης έχουν μήκος 512 bits και κάθε τμήμα επεξεργάζεται πλήρως σε τρεις διακριτούς επαναληπτικούς γύρους. Ο MD4 έχει επανειλημμένα αναλυθεί με διάφορους τρόπους και δεν πρέπει να θεωρείται πλέον ασφαλής. Συγκεκριμένα, έχει αποδειχθεί ότι μπορεί να αντιστραφεί η διαδικασία και ότι υπό ορισμένες συνθήκες δεν είναι αμφιμονοσήμαντος.

Ο MD5 αναπτύχθηκε το 1991. Είναι μια κατά πολύ βελτιωμένη έκδοση του MD4, γι' αυτό είναι και λίγο πιο αργός. Η μόνη διάφορα είναι η χρήση τεσσάρων επαναλήψεων κατά

την επεξεργασία του κάθε τμήματος. Οι απαιτήσεις σε μέγεθος τμήματος και μήκος μηνύματος παραμένουν οι ίδιες. Η κρυπτανάλυση του MD5 συνεχίζεται ακόμα, αλλά οι πρώτες εκτιμήσεις δείχνουν ότι έχει αρκετές αδυναμίες.

4.4 Αλγόριθμοι Ανταλλαγής Κλειδιών

Diffie-Hellman

Το πρωτόκολλο Diffie-Hellman είναι ένας μηχανισμός ανταλλαγής κλειδιών και αναπτύχθηκε από τους Diffie και Hellman το 1976. Επιτρέπει σε δύο χρήστες να ανταλλάσσουν ένα μυστικό κλειδί μέσα από ένα μη ασφαλές δίκτυο. Το πρωτόκολλο έχει δύο παραμέτρους: p και g. Είναι και οι δύο δημοσιοποιημένοι και μπορούν να χρησιμοποιηθούν από όλους τους χρήστες του συστήματος. Η παράμετρος p είναι ένας πρώτος αριθμός και η παράμετρος g είναι ένας ακέραιος με την εξής ιδιότητα: για οποιοδήποτε ακέραιο αριθμό n στο διάστημα [1, p-1], υπάρχει αριθμός k τέτοιος ώστε gk = n mod p. Ας υποθέσουμε τώρα ότι δύο χρήστες, ο Α και ο Β, θέλουν να συμφωνήσουν για ένα μυστικό κλειδί. Πρώτα, ο Α παράγει μία τυχαία ιδιωτική τιμή a και ο Β μία τυχαία ιδιωτική τιμή b. Οι τιμές a και b διαλέγονται από το σύνολο [1, p-1]. Έπειτα δημιουργούν τις δημόσιες τιμές τους χρησιμοποιώντας τις παραμέτρους p και g και τις ιδιωτικές τους τιμές. Η δημόσια τιμή του Α είναι ga mod p και του Β είναι gb mod p. Στην συνέχεια ανταλλάσσουν τις δημόσιες τιμές τους. Τέλος, ο Α κάνει τον υπολογισμό gab = (gb)a mod p και Β κάνει με την σειρά του τον υπολογισμό gba = (ga)b mod p. Επειδή gab = gba = k, ο Α και Β έχουν τώρα ένα κοινό μυστικό κλειδί. Το πρωτόκολλο εξαρτάται από το γεγονός ότι είναι αδύνατον να υπολογιστεί το κ από τις δημόσιες τιμές ga mod p και gb mod p χωρίς τη γνώση των a και b και όταν ο p είναι πολύ μεγάλος.

Οι πρώτες εκδόσεις του μηχανισμού Diffie-Hellman ήταν ευάλωτες σε επιθέσεις ενδιάμεσου (man-in-the-middle). Σε αυτή την επίθεση ο χρήστης C παρεμβάλλεται στην επικοινωνία των Α και Β και όταν ανταλλάσσουν τις δημόσιες τιμές τους, τις αντικαθιστά με τις δικές του. Δηλαδή όταν ο Α μεταδίδει τη δημόσια τιμή του στον Β, ο C την αντικαθιστά με τη δικιά του και τη στέλνει στον Β. Ομοίως, όταν ο Β στέλνει τη δημόσια τιμή του στον Α. Σαν συνέπεια, οι C και Α συμφωνούν για ένα μυστικό κλειδί και οι C και Β συμφωνούν για ένα άλλο κλειδί. Έτσι ο C μπορεί να διαβάσει τα μηνύματα που μεταδίδουν ο Α στον Β και πιθανώς να τα τροποποιήσει πριν τα προωθήσει σε έναν από τους δύο. Το 1992 αναπτύχθηκε μία ανανεωμένη έκδοση από τους Diffie, Van Oorschot και Wiener που υποστήριζε την πιστοποίηση της ταυτότητας των δύο πλευρών και είχε σαν σκοπό να καταπολεμήσει την επίθεση ενδιάμεσου (man-in-the-middle). Τα μηνύματα ανταλλάσσονται υπογεγραμμένα με τις ιδιωτικές κλείδες των Α και Β, ενώ χρησιμοποιούνται και πιστοποιητικά (βλέπε παρακάτω) για την απόκτηση των

σωστών δημοσίων κλειδιών. Ο C ακόμα και αν είναι σε θέση να παρακολουθεί την επικοινωνία των A και B, δεν μπορεί να πλαστογραφήσει τα μηνύματα.

Ψηφιακοί Φάκελοι (Digital Envelopes)

Ο μηχανισμός των ψηφιακών φακέλων βρίσκει εφαρμογή στην ανταλλαγή μυστικών κλειδιών που χρησιμοποιούνται σε συμμετρικά κρυπτοσυστήματα. Ο ψηφιακός φάκελος αποτελείται από ένα μήνυμα κρυπτογραφημένο με ένα συμμετρικό κλειδί και το συμμετρικό κλειδί κρυπτογραφημένο με άλλο κλειδί.

Συνήθως η κρυπτογράφηση του συμμετρικού κλειδιού γίνεται με το δημόσιο κλειδί της αντίθετης πλευράς, αλλά αυτό δεν είναι απαραίτητο. Μπορεί κάλλιστα να χρησιμοποιηθεί και ένα προ-συμφωνημένο συμμετρικό κλειδί. Ας υποθέσουμε ότι ο χρήστης B θέλει να στείλει μήνυμα στον χρήστη B. Ο A διαλέγει ένα συμμετρικό κλειδί και κρυπτογραφεί το μήνυμα με αυτό. Έπειτα κρυπτογραφεί το μυστικό συμμετρικό κλειδί με το δημόσιο κλειδί του B. Στέλνει στον B το κρυπτογραφημένο μήνυμα συνοδευόμενο από το κρυπτογραφημένο κλειδί. Όταν ο B θελήσει να διαβάσει το μήνυμα, χρησιμοποιεί το ιδιωτικό του κλειδί για να ανακτήσει το συμμετρικό κλειδί και μετά αποκρυπτογραφεί το μήνυμα με το μυστικό συμμετρικό κλειδί. Στην περίπτωση που το μήνυμα έχει παραπάνω του ενός παραλήπτες, το μυστικό συμμετρικό κλειδί κρυπτογραφείται ξεχωριστά με το δημόσιο κλειδί του κάθε παραλήπτη. Και πάλι μεταδίδεται μόνο ένα κρυπτογραφημένο μήνυμα. Οι χρήστες μπορούν να αλλάζουν κλειδιά όσο συχνά θέλουν, γεγονός που αυξάνει κατακόρυφα την ασφάλεια του συστήματος.

Επίσης, οι ψηφιακοί φάκελοι όχι μόνο λύνουν το πρόβλημα της ανταλλαγής κλειδιών, αλλά βελτιώνουν και την απόδοση του συστήματος καθ' ότι η ασύμμετρη κρυπτογράφηση από μόνη της απαιτεί εξαιρετικά χρονοβόρα επεξεργασία. Ο πιο συνηθισμένος συνδυασμός είναι το ασύμμετρο κρυπτοσύστημα RSA με το συμμετρικό DES.

Πιστοποιητικά

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

Ας υποθέσουμε ότι ο A χρειάζεται το δημόσιο κλειδί του B για να μπορέσει να εγκαταστήσει μία ασφαλή συναλλαγή. Το να ζητήσει από τον B να του στείλει το δημόσιο κλειδί του, μπορεί να θέσει την όλη επικοινωνία σε κίνδυνο. Εκτός από την παρακολούθηση της συναλλαγής και αντικατάστασης του δημόσιου κλειδιού του B με το δημόσιο κλειδί κάποιου άλλου

(επίθεση man-in-the-middle), μπορεί οποιοσδήποτε να ξεγελάσει τον Α, όταν ο Α δεν γνωρίζει και δεν μπορεί να επικοινωνήσει τηλεφωνικά με τον Β, λέγοντας πως είναι ο Β και παρουσιάζοντας ένα ψεύτικο δημόσιο κλειδί. Δηλαδή, έστω ότι ο Β υποστηρίζει ότι είναι ο πρωθυπουργός της Ελλάδος. Τότε ο Α θα νομίζει ότι συνδιαλέγεται με τον πρωθυπουργό της Ελλάδος και χρησιμοποιεί το δημόσιο κλειδί που του παρουσίασε ο Β για να στείλει στον δήθεν πρωθυπουργό εμπιστευτικά έγγραφα.

Ένα πιστοποιητικό περιέχει τις ακόλουθες πληροφορίες:

• το όνομα του κατόχου,

• το όνομα της του εκδοτικού οργανισμού – CA (βλέπε παρακάτω),

• το δημόσιο κλειδί του ονόματος που αναγράφεται στο πιστοποιητικό,

• την ημερομηνία λήξης του πιστοποιητικού,

• ένα σειριακό αριθμό (serial number),

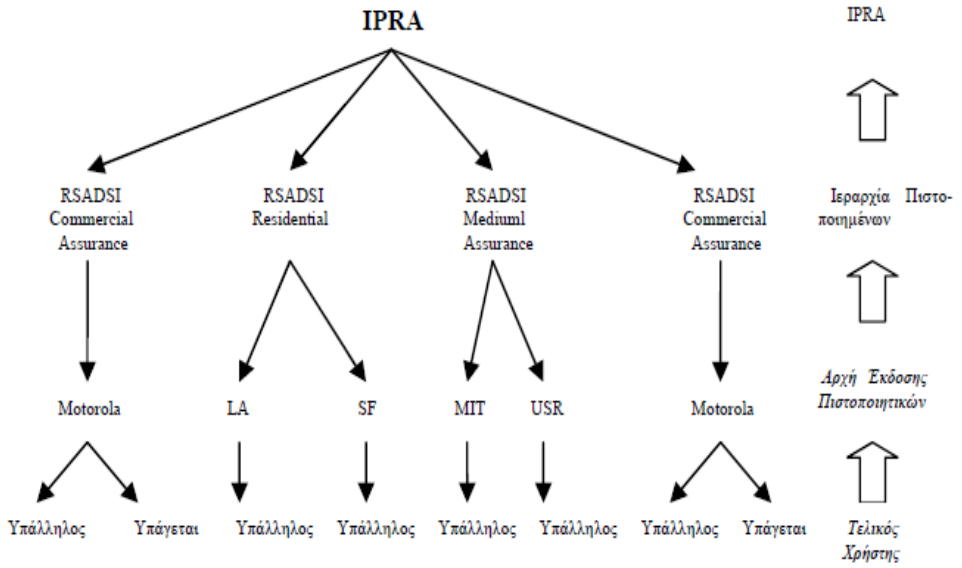
• την ψηφιακή υπογραφή του εκδοτικού οργανισμού.

Το πιστοποιητικό μεταφέρεται, συνήθως, μαζί με την ψηφιακή υπογραφή. Για την επαλήθευση της ψηφιακής υπογραφής ο παραλήπτης πρέπει να έχει το σωστό δημόσιο κλειδί του αποστολέα. Επίσης, το πιστοποιητικό στέλνεται κατά την εγκαθίδρυση μιας σύνδεσης μεταξύ δύο άκρων, για την γνωστοποίηση του δημόσιου κλειδιού κάθε πλευράς στην άλλη πλευρά και για την χρήση της στην κρυπτογράφηση της επικοινωνίας. Το πιστοποιητικό δεν χρειάζεται να αποστέλλεται κάθε φορά που ξεκινά μία συναλλαγή. Αρκεί να σταλεί μία φορά κατά την έναρξη της σύνδεσης.

4.5 Αρχές Έκδοσης Πιστοποιητικών

Τα πιστοποιητικά εκδίδονται από τις Αρχές Έκδοσης Πιστοποιητικών (Certification Authorities – CA), που μπορεί να είναι οποιοσδήποτε άξιος εμπιστοσύνης οργανισμός ικανός να εγγυηθεί για την ταυτότητα αυτών για τους οποίους εκδίδει πιστοποιητικά. Ένας οργανισμός μπορεί να εκδίδει πιστοποιητικά για τους υπάλληλους του ή ένα Πανεπιστήμιο για τους σπουδαστές του ή ακόμα και μια πόλη για τους κατοίκους της. Η CA πρέπει να κατέχει ένα ζεύγος ιδιωτικού – δημόσιου κλειδιού. Με το ιδιωτικό της κλειδί υπογράφει ψηφιακά τα πιστοποιητικά που εκδίδει, ενώ την εγκυρότητα του δημόσιου κλειδιού πρέπει να επικυρώνει εκδοτικός οργανισμός σε υψηλότερη θέση στην ιεραρχία των CAs. Η ιεραρχική κατάταξη που βλέπουμε στο ακόλουθο σχήμα, έχει στην κορυφή της τον οργανισμό Internet Policy Registration

Authority (IRPA) και αμέσως μετά ακολουθούν οι Policy Certification Authorities (PCAs) που δημοσιοποιούν πολιτικές ασφάλισης και έκδοσης πιστοποιητικών. Ανάλογα με το είδος των πιστοποιητικών και περιορισμών που ασκούν όσο αναφορά την χρήση τους, οι Αρχές Έκδοσης Πιστοποιητικών (CAs) που τα εκδίδουν κατατάσσονται σε μία από τις υψηλότερες σε επίπεδο, PCAs. Τέλος, έρχονται οι τελικοί χρήστες που ανάλογα με τις ανάγκες τους επιλέγουν την CA που θα πιστοποιήσει το δημόσιο κλειδί τους. Οι ανάγκες κάθε χρήστη καθορίζονται στο αν το κλειδί θα χρησιμοποιηθεί για εμπορικές συναλλαγές, για υπογραφή κυβερνητικών εγγράφων, για την απλή ανταλλαγή ηλεκτρονικού ταχυδρομείου ή ακόμα για την διασφάλιση τεχνολογικών επιτευγμάτων.



Εικόνα 11. Ιεραρχική Κατάταξη

Σ' αυτήν της ιεραρχία, οι οργανισμοί κάθε επιπέδου πιστοποιούν το δημόσιο κλειδί και ταυτότητα του χαμηλότερου επιπέδου. Έτσι, πολλές φορές το πιστοποιητικό για έναν χρήστη μπορεί να συνοδεύεται από μία αλυσίδα πιστοποιητικών (certificates chain) που φθάνουν ως την κορυφή της ιεραρχίας. Σε κάθε πιστοποιητικό περιέχεται η υπογραφή του ανώτερου εκδοτικού οργανισμού που έχει δημιουργηθεί με το ιδιωτικό κλειδί αυτού. Από το σχήμα καταλαβαίνουμε ότι μια τέτοια ιεραρχική δομή μπορεί να εφαρμοστεί και στο εσωτερικό μεγάλων εταιριών. Το δημόσιο κλειδί του ανώτερου εκδοτικού οργανισμού δεν μπορεί να πιστοποιηθεί από κανέναν. Ο οργανισμός εκδίδει πιστοποιητικό για τον εαυτό του που περιέχει το δημόσιο κλειδί του και την υπογραφή του με το ιδιωτικό του κλειδί, το οποίο καλείται αρχικό πιστοποιητικό (root

certificate). Αυτονόητο είναι, λοιπόν, ότι αυτός ο οργανισμός πρέπει να είναι απόλυτα έμπιστος. Ο χρήστης που επιθυμεί να αποκτήσει ένα πιστοποιητικό, θα δημιουργήσει πρώτα ένα ζεύγος ιδιωτικού – δημόσιου κλειδιού και θα αποστείλει σε μία CA το δημόσιο κλειδί μαζί με πληροφορίες που προσδιορίζουν την ταυτότητα του χρήστη. Η CA αφού επαληθεύσει την ταυτότητα του χρήστη και σιγουρευτεί ότι η αίτηση έκδοσης πιστοποιητικού προέρχεται από τον πραγματικό χρήστη, απαντά στον χρήστη με χρήστη το πιστοποιητικό του μαζί με τα ιεραρχικά δεμένα πιστοποιητικά που επιβεβαιώνουν την αυθεντικότητα του δημόσιου κλειδιού της CA.

Λίστες Ανάκλησης Πιστοποιητικών (Certificate Revocation Lists)

Μία λίστα ανάκλησης πιστοποιητικών περιέχει πιστοποιητικά που έχουν ακυρωθεί πριν από την προγραμματισμένη ημερομηνία λήξης. Υπάρχουν αρκετοί λόγοι γιατί ένα πιστοποιητικό μπορεί να ανακληθεί. Για παράδειγμα το μυστικό κλειδί που ορίζεται στο πιστοποιητικό να έχει κοινοποιηθεί καθιστώντας αυτόματα την χρήση του πιστοποιητικού μη ασφαλή ή το άτομο για το οποίο εκδόθηκε το πιστοποιητικό να μην έχει πια την δικαιοδοσία να το χρησιμοποιεί. Ας φανταστούμε την περίπτωση όπου ένας υπάλληλος μια εταιρείας έχει πιστοποιητικό που έχει εκδώσει για λογαριασμό του η εταιρεία.

Εάν ο υπάλληλος απολυθεί, η εταιρεία θα ακυρώσει το πιστοποιητικό, ώστε να μην έχει τη δυνατότητα να υπογράφει έγγραφα με αυτό το κλειδί. Κατά την επαλήθευση μιας υπογραφής, πρέπει κάθε χρήστης να συμβουλεύεται μία CRL για να διαπιστώσει εάν το εν λόγω πιστοποιητικό δεν έχει αποσυρθεί. Το αν αξίζει τον κόπο να πραγματοποιήσει τέτοιο έλεγχο, εξαρτάται από τη σημασία του εγγράφου. Οι λίστες διατηρούνται και ανανεώνονται από τις CA, και κάθε CA διαχειρίζεται τις λίστες που παρέχουν πληροφορίες για τα ανακληθέντα πιστοποιητικά που είχαν εκ-δοθεί από την ίδια. Επίσης, οι λίστες περιέχουν τα πιστοποιητικά των οποίων δεν έχει περάσει η ημερομηνία λήξης. Αυτά τα πιστοποιητικά δεν γίνονται δεκτά σε καμία περίπτωση.

ΚΕΦΑΛΑΙΟ 5ο : ΑΛΓΟΡΙΘΜΟΣ RSA

5.1 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 Rivest, Adi Shamir, και Leonard Adlema. 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.

5.2 Περιγραφή του RSA

Ο αλγόριθμος RSA οφείλει το πραγματικά μεγάλο επίπεδο ασφάλειας του στην επιλογή μεγάλων πρώτων αριθμών. 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: ρ και q. 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 ρ 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 ή και σχετικά πρώτο με το γινόμενο (ρ - 1)*(q - 1). Για να γίνει πιο κατανοητή η δεύτερη προϋπόθεση, αρκεί να πούμε πως πρέπει το δημόσιο κλειδί e και το γινόμενο (ρ - 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 μις 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 = eA-1 mod ((ρ - 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. Μετά την ολοκλήρωση της διαδικασίας, οι πρώτοι αριθμοί ρ 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 η (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 ρ και q είναι αριθμοί 100 αριθμητικών ψηφίων, τότε προφανώς το η θα έχει λίγο παρακάτω από 200 ψηφία και το κάθε block του αρχικού κειμένου 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: q = ιτη Λ e mod n, όπου ως q ορίζουμε κάθε κομμάτι του κρυπτογραφημένου πια κειμένου. Το σύμβολο (Λ) δηλώνει την δύναμη στην οποία θα υψωθεί το nrij. 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.

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, = q Λ d mod 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.

5.3 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.

	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 ης 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.

5.4 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 η, 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 κρυπταναλυτή 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 η 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 (ρ - 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 η, 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 ρ 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 (ρ 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 η. 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 η 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.

5.5 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 σχεδίασμά 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(Windows), Apple(Macintosh) και Sun(Solaris). 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».

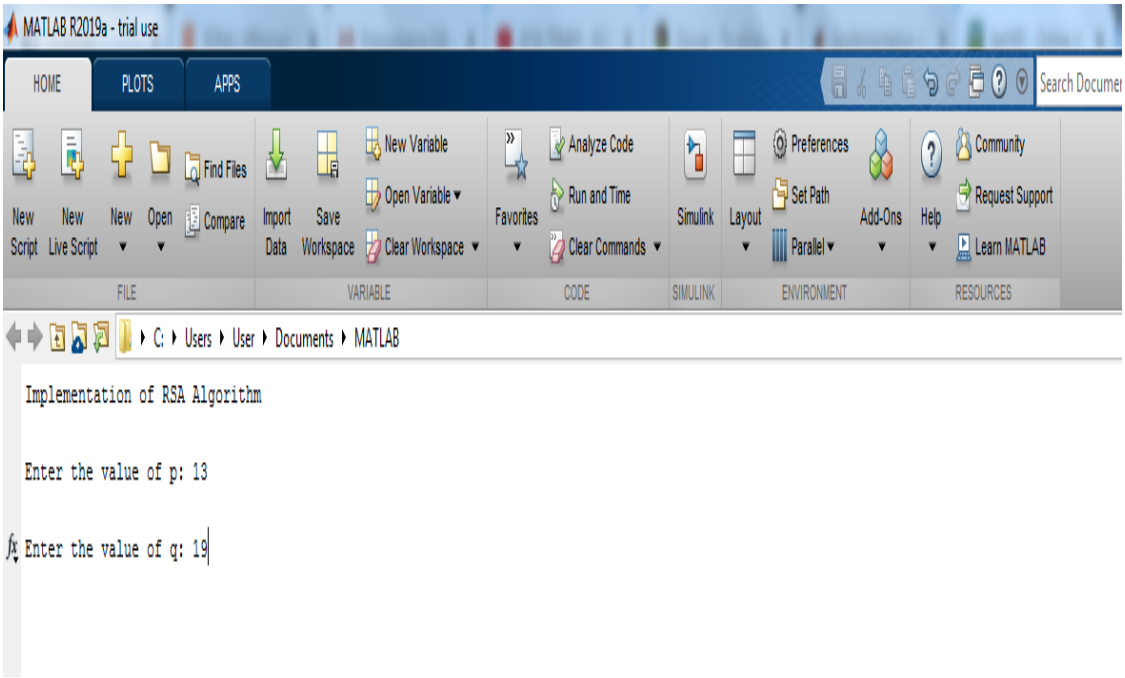
ΚΕΦΑΛΑΙΟ 6ο : ΠΕΙΡΑΜΑΤΙΚΟ ΜΕΡΟΣ

Στα πλαίσια του πειραματικού μέρους της εργασίας προσομοιώσαμε την λειτουργία του αλγορίθμου κρυπτογράφησης RSA με τη χρήση του λογισμικού πακέτου Matlab (Έκδοση 2019a).

Ο αλγόριθμος δέχεται από τον χρήστη δύο πρώτους αριθμούς και υπολογίζει την συνάρτηση του Euler, Φ(n) καθώς και το ιδιωτικό κλειδί. Με βάση αυτά τα δεδομένα ζητείται από το χρήστη να δώσει ένα μήνυμα σε αλφαριθμητική μορφή και η εφαρμογή υπολογίζει το κρυπτοκείμενο σε μορφή ASCII καθώς και την αποκρυπτογράφησή του στην ίδια μορφή.

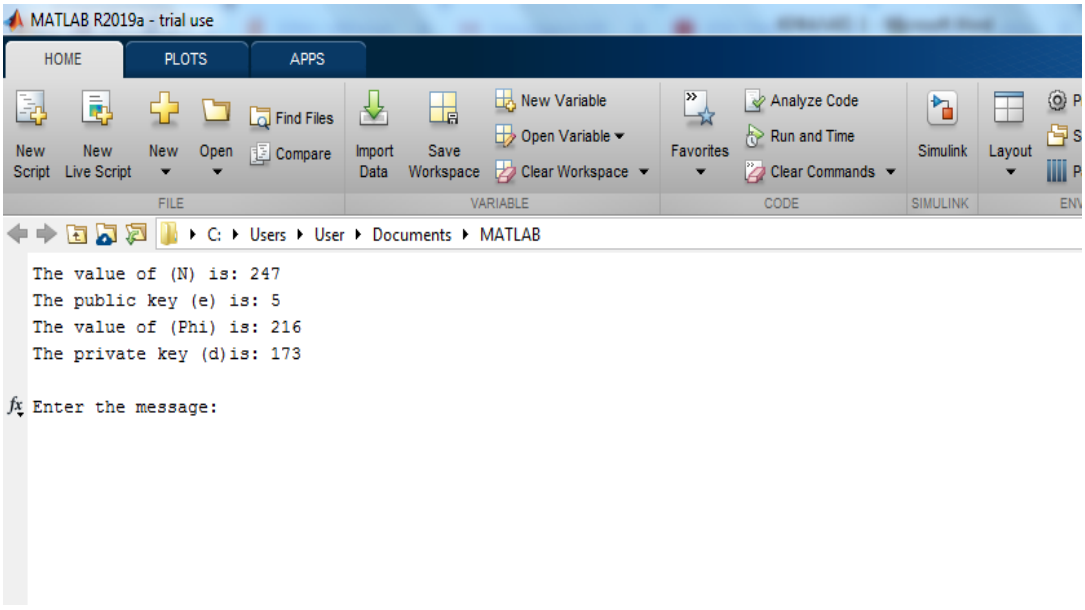
Για την προσομοίωση ο κώδικας χρησιμοποιεί τρεις συναρτήσεις και το κυρίως πρόγραμμα. Η συνάρτηση **initialize.m** υπολογίζει τις ποσότητες Pk(public key) , την τιμή Phi (της συνάρτησης Φ(n)) και τα δύο κλειδιά , το ιδιωτικό κλειδί (d). Με αυτές τις τιμές ως εισόδους η συνάρτηση **crypt.m** υπολογίζει την κρυπτογράφηση του μηνύματος καθώς και την αποκρυπτογράφηση εφόσον ο τύπος υπολογισμού και των δύο είναι αποτέλεσμα της ίδιας πράξης (mod), με εναλλαγή φυσικά των ρόλων του κρυπτοκειμένου και του αρχικού μηνύματος. Για την μετατροπή των αριθμών που βρίσκονται στην καρδιά του κώδικα σε μορφή αλφαριθμητικών μέσω του κώδικα ASCII χρησιμοποιείται η συνάρτηση **dec2bin.m**. Τέλος μέσω του κυρίου προγράμματος RSA.m όλες οι προαναφερθείσες συναρτήσεις καλούνται με τα ορίσματα που δίνει ο χρήστης.

Ακολουθεί μία επίδειξη της προσομοίωσης, ενώ ο πλήρης κώδικας παρατίθεται στο Παράρτημα. Αρχικά το πρόγραμμα μας καλεί να θέσουμε τιμές , δύο πρώτους αριθμούς (p και q)



Στο παράδειγμά μας θέσαμε τις τιμές p=11 και q=19

Στο επόμενο βήμα εκτέλεσης , παρουσιάζονται οι υπολογισθείσες τιμές για το ιδιωτικό και το δημόσιο κλειδί , την συνάρτηση Φ(n) και η παράμετρος N. Ταυτόχρονα μα ζητείται να εισάγουμε το μήνυμα το οποίο θα κρυπτογραφηθεί και αποκρυπτογραφηθεί :



Οι τιμές που παρήχθησαν είναι :

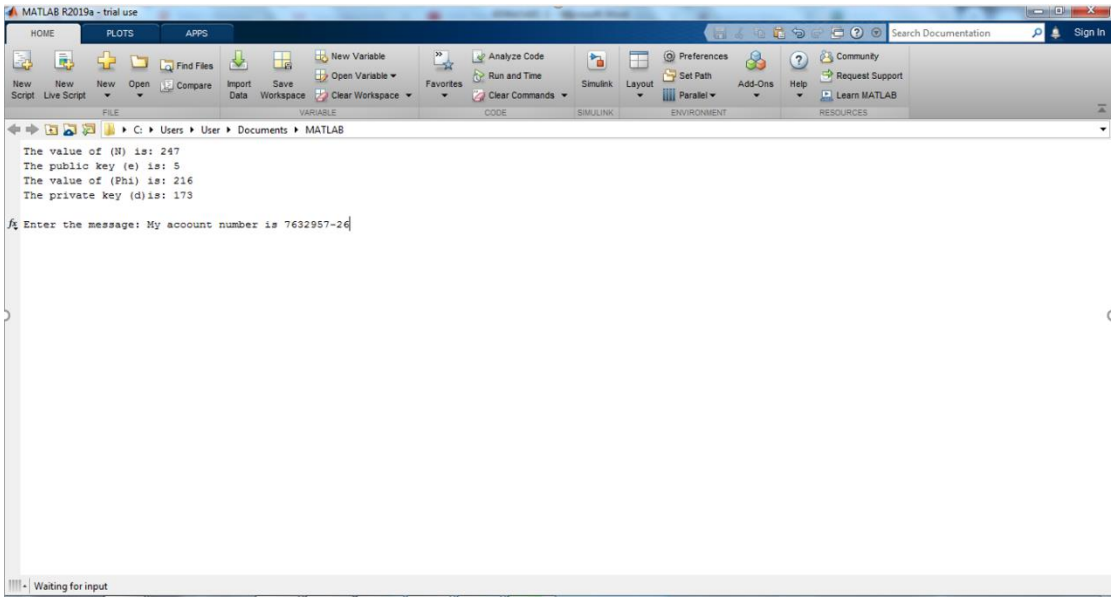
The value of (N) is: 247

The public key (e) is: 5

The value of (Phi) is: 216

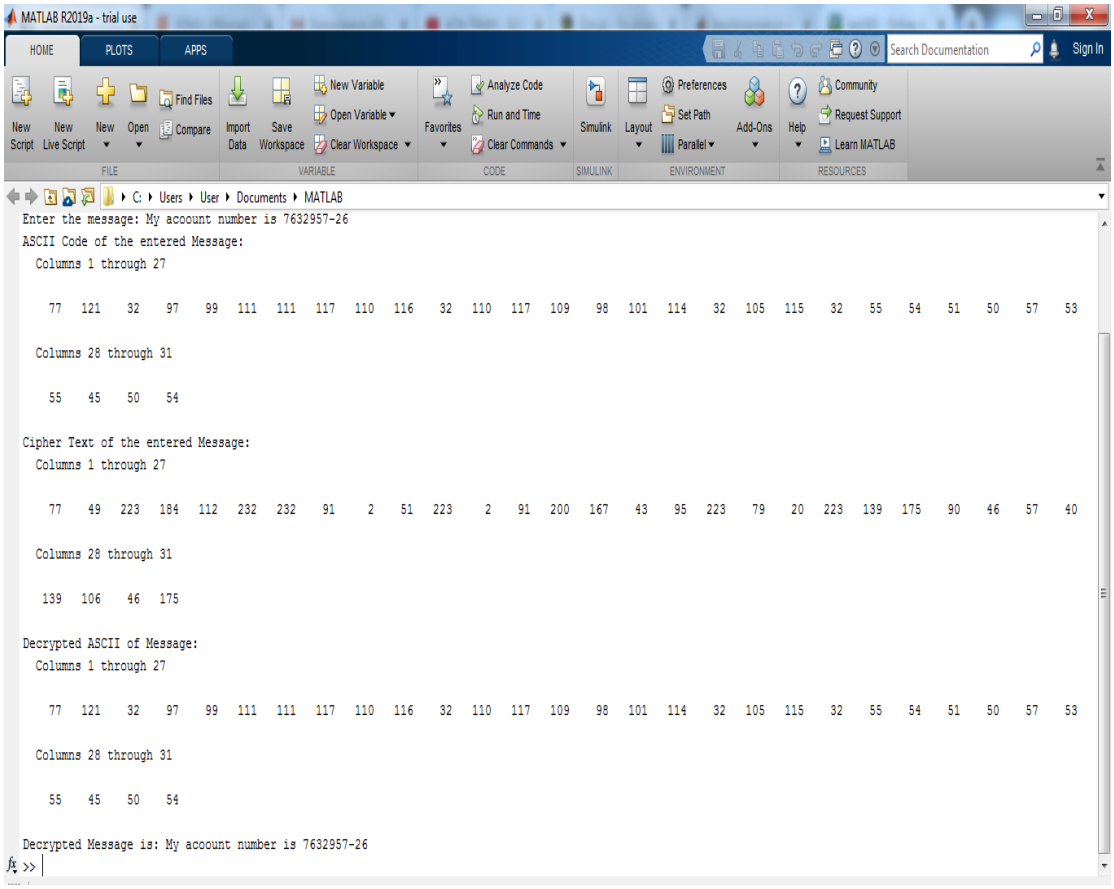
The private key (d) is: 173

Ταυτόχρονα μας ζητείται να εισάγουμε το μήνυμα που ο αλγόριθμος θα κρυπτογραφήσει /α-ποκρυπτογραφήσει



Τοποθετήσαμε το μήνυμα : My account number is 7632957-26

Με την είσοδο του μηνύματος και πατώντας «enter» παίρνουμε το αποτέλεσμα :



Enter the message: My account number is 7632957-26

ASCII Code of the entered Message:

Columns 1 through 27

77 121 32 97 99 111 111 117 110 116 32 110 117 109 98 101 114 32 105 115 32 55 54 51 50 57 53

Columns 28 through 31

55 45 50 54

Cipher Text of the entered Message:

Columns 1 through 27

77 49 223 184 112 232 232 91 2 51 223 2 91 200 167 43 95 223 79 20 223 139 175 90 46 57 40

Columns 28 through 31

139 106 46 175

Decrypted ASCII of Message:

```
Columns 1 through 27

   77   121    32    97    99   111   111   117   110   116    32   110   117   109    98   101   114
32   105   115    32    55    54    51    50    57    53

Columns 28 through 31

   55    45    50    54

Decrypted Message is: My account number is 7632957-26
```

Στα αποτελέσματα παρουσιάζονται ο κώδικας ASCII του αρχικού μηνύματος , και του κρυπτογραφημένου μηνύματος καθώς και του αποκρυπτογραφημένου μηνύματος όπου όπως ήταν αναμενόμενο ο πρώτος και ο τρίτος ταυτίζονται. Και τέλος προκύπτει το αρχικό μήνυμα σε μορφή αλφαριθμητικού που φυσικά είναι το αρχικό μας μήνυμα όπως θα το διαβάσει ο παραλήπτης.

ΠΑΡΑΡΤΗΜΑ Α

“RSA.m” Function

```
clc;
disp('Implementation of RSA Algorithm');
clear all; close all;
p = input('\nEnter the value of p: ');
q = input('\nEnter the value of q: ');
[Pk,Phi,d,e] = intialize(p,q);
M = input('\nEnter the message: ','s');
x=length(M);
c=0;
for j= 1:x
   for i=0:122
      if strcmp(M(j),char(i))
         c(j)=i;
      end
   end
end
disp('ASCII Code of the entered Message:');
disp(c);
% % %Encryption
for j= 1:x
  cipher(j)= crypt(c(j),Pk,e);
end
disp('Cipher Text of the entered Message:');
disp(cipher);
% % %Decryption
for j= 1:x
  message(j)= crypt(cipher(j),Pk,d);
end
disp('Decrypted ASCII of Message:');
disp(message);
disp(['Decrypted Message is: ' message]);
```

“Crypt.m” Function

```
function mc = crypt(M,N,e)
e=dec2bin(e);
k = 65535;
c  = M;
cf = 1;
cf=mod(c*cf,N);
for i=k-1:-1:1
   c = mod(c*c,N);
   j=k-i+1;
    if e(j)==1
       cf=mod(c*cf,N);
    end
end
mc=cf;
```

ΠΑΡΑΡΤΗΜΑ Β

Intialize.m" Function

```
function [Pk,Phi,d,e] = intialize(p,q)
clc;
disp('Intaializing:');
Pk=p*q;
Phi=(p-1)*(q-1);
%Calculate the value of e
x=2;e=1;
while x > 1
   e=e+1;
   x=gcd(Phi,e);
end
%Calculate the value of d
i=1;
r=1;
while r > 0
   k=(Phi*i)+1;
   r=rem(k,e);
   i=i+1;
end
d=k/e;
clc;
disp(['The value of (N) is: ' num2str(Pk)]);
disp(['The public key (e) is: ' num2str(e)]);
disp(['The value of (Phi) is: ' num2str(Phi)]);
disp(['The private key (d)is: ' num2str(d)]);
```

"dec2bin.m" Function

```
function a = dec2bin(d)
i=1;
a=zeros(1,65535);
while d >= 2
   r=rem(d,2);
   if r==1
      a(i)=1;
   else
      a(i)=0;
   end
   i=i+1;
   d=floor(d/2);
end
if d == 2
   a(i) = 0;
else
   a(i) = 1;
end
x=[a(16) a(15) a(14) a(13) a(12) a(11) a(10) a(9) a(8) a(7) a(6) a(5) a(4) a(3) a(2) a(1)];
```

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] I van Damgard. A ‘proof-reading’ of some issues in cryptography. In Automata, Languages and Programming, pages 2–11. Springer, 2007.

[2] W. Diffie and M. Hellman. New directions in cryptography. IEEE Trans. Inf. Theor., 22(6):644–654, November 1976.

[3] Shafi Goldwasser and Silvio Micali. Probabilistic encryption & how to play mental poker keeping secret all partial information. In STOC ’82: Proceedings of the fourteenth annual ACM symposium on Theory of computing, pages 365–377, New York, NY, USA, 1982. ACM Press.

[4] Neal Koblitz and Alfred J Menezes. Another look at “provable security”. Journal of Cryptology, 20(1):3–37, 2007.

[5] Tom M. Apostol. Introduction to Analytic Number Theory. Springer-Verlag, 1976.

[6] Jonathan Katz and Yehuda Lindell. Introduction to Modern Cryptography (Chapman & Hall/Crc Cryptography and Network Security Series). Chapman & Hall/CRC, 2007.

[7] Χρήστος Καπούτσης. Κρυπτοσυστήματα πακέτου: από το des στο aes. Master’s thesis, University Of Athens, Greece, 2000. Διαθέσιμο στο : http://www.math.uoa.gr/~mpla/thesis/cak.ps.

[8] E. R. Berlekamp. Algebraic coding theory. McGraw-Hill, New York, 1968.

[9] Eli Biham and Adi Shamir. Differential cryptanalysis of des-like cryptosystems. Journal of CRYPTOLOGY, 4(1):3–72, 1991.

[10] Ε. Ζάχος, Α. Παγουρτζής , Π.Γρόντας. Υπολογιστική Κρυπτογραφία , ΣΥΝΔΕΣΜΟΣ ΕΛΛΗΝΙΚΩΝ ΑΚΑΔΗΜΑΪΚΩΝ ΒΙΒΛΙΟΘΗΚΩΝ ,Εθνικό Μετσόβιο Πολυτεχνείο ,2015

[11] C.Adams, S.Loyd. (1999). Understanding Public-Key Infrastructure, Macmillan Technical Publishing.

[12] Menezes, P. van Oorschot, and S.A. Vanstone. (1997). “Handbook of Applied Cryptography” CRC Press.

[13] Schneier B. (1996). Applied Cryptography, John Wiley and Sons Inc.

[14] L.G.Pierson, (2000). Comparing Cryptographic Modes of Operation using Flow Diagrams, Sandia National Laboratories. Available at http://csrc.nist.gov/CryptoToolkit/modes/workshop1/presentations/slides-pierson.pdf.