Τ.Ε.Ι ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΘΕΜΑ: Η ΕΞΕΛΙΞΗ ΤΗΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

ΕΙΣΗΓΗΤΡΙΑ: ΒΑΣΙΟΥ ΓΕΩΡΓΙΑ

ΣΠΟΥΔΑΣΤΕΣ:

ΜΑΤΣΑΝΚΟΣ ΝΙΚΟΛΑΟΣ

ΚΟΝΤΟΒΑΣΙΛΗΣ ΕΥΑΓΓΕΛΟΣ

ΚΟΚΟΚΥΡΗΣ ΠΑΝΑΓΙΩΤΗΣ

ΠΑΤΡΑ 2015

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΛΗΨΗ 8

ΚΕΦΑΛΑΙΟ 1 9

ΕΙΣΑΓΩΓΗ 9

ΣΤΟΧΟΙ 9

ΟΡΟΛΟΓΙΑ 10

ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ 11

ΚΕΦΑΛΑΙΟ 2 13

2. Η ΙΣΤΟΡΙΑ ΤΗΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ 13

2.1 Η ΚΡΥΠΤΟΓΡΑΦΙΑ ΣΤΗΝ ΠΕΡΙΟΔΟ ΤΩΝ ΑΡΧΑΙΩΝ ΧΡΟΝΩΝ 13

2.1.1 Η ΣΠΑΡΤΙΑΤΙΚΗ ΣΚΥΤΑΛΗ 14

2.1.2 Ο ΔΙΣΚΟΣ ΤΗΣ ΦΑΙΣΤΟΥ 15

2.1.3 ΤΑ ΑΙΓΥΠΤΙΑΚΑ ΣΥΜΒΟΛΑ 15

2.1.4 Η ΓΡΑΜΜΙΚΗ ΓΡΑΦΗ 16

2.1.5. Ο ΜΥΣΤΙΚΟΣ ΚΩΔΙΚΑΣ ΣΤΑ ΚΕΙΜΕΝΑ ΤΟΥ ΠΛΑΤΩΝΑ 18

2.1.6Α ΤΟ ΤΕΤΡΑΓΩΝΟ ΤΟΥ ΠΟΛΥΒΙΟΥ 19

2.1.6Β Η ΚΡΥΠΤΟΓΡΑΦΙΑ ΣΤΟ ΤΕΤΡΑΓΩΝΟ ΤΟΥ ΠΟΛΥΒΙΟΥ 21

2.1.7 Η ΚΡΥΠΤΟΓΡΑΦΙΑ ΣΤΟ ΜΕΣΑΙΩΝΑ 21

2.1.8 ΠΑΡΟΥΣΙΑΣΗ ΤΟΥ ΚΡΥΠΤΟΓΡΑΜΜΑΤΟΣ VIGENERE 23

2.1.9Α ΜΗΧΑΝΗ VIGENERE ΣΕ ΛΕΙΤΟΥΡΓΙΑ 25

2.1.9Β Η ΙΣΤΟΡΙΑ ΜΙΑΣ ΑΣΠΑΣΤΗΣ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ 26

2.1.10 ΚΡΥΠΤΟΓΡΑΜΜΑ ΟΜΟΦΩΝΙΚΗΣ ΑΝΤΙΚΑΤΑΣΤΑΣΗΣ 27

2.1.11 ΤΟ «ΜΕΓΑΛΟ ΚΡΥΠΤΟΓΡΑΜΜΑ» ΤΟΥ ΛΟΥΔΟΒΙΚΟΥ ΙΔ' 30

2.1.12 Η ΔΙΑΦΟΡΙΚΗ ΜΗΧΑΝΗ ΤΟΥ ΜΠΑΜΠΑΤΖ 31

2.1.13 Η ΑΝΑΛΥΤΙΚΗ ΜΗΧΑΝΗ ΤΟΥ ΜΠΑΜΠΑΤΖ (1822) 31

2.2 ΔΕΥΤΕΡΗ ΠΕΡΙΟΔΟΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ (1900 μ.Χ-1950 μ.Χ) 32

2.2.1 ΚΩΔΙΚΑΣ ZIMMERMANN 33

2.2.2 ΛΟΓΟΙ ΑΠΟΡΡΙΩΗΣ ΤΗΣ ΓΕΡΜΑΝΙΚΗΣ ΠΡΟΤΑΣΗΣ 33

2.2.3 ΑΠΟΚΡΥΠΤΟΓΡΑΦΗΣΗ ΤΟΥ ΚΩΔΙΚΑ ZIMMERMANN 34

2.2.4 ΤΟ ΚΡΥΠΤΟΓΡΑΦΙΚΟ ΣΥΣΤΗΜΑ ENIGMA 35

2.2.5 ΠΕΡΙΓΡΑΦΗ ΛΕΙΤΟΥΡΓΙΑΣ ΤΗΣ ΜΗΧΑΝΗΣ ENIGMA 36

2.2.6 Η ΙΣΤΟΡΙΑ ΤΗΣ ΜΗΧΑΝΗΣ 40

2.2.6Α Η ΕΜΠΟΤΙΚΗ ΜΗΧΑΝΗ ENIGMA 40

2.2.6Β Η ΣΤΡΑΤΙΩΤΙΚΗ ΜΗΧΑΝΗ ENIGMA 41

2.2.7 ΚΩΔΙΚΑΣ NAVAXO 42

2.2.8 Η ΙΔΕΑ 42

2.2.9 ΤΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΗΣ ΓΛΩΣΣΑΣ NAVAXO 43

2.2.10 ΤΟ ΑΛΦΑΒΗΤΟ ΤΟΥ ΚΩΔΙΚΑ NAVAXO 44

2.3 ΤΡΙΤΗ ΠΕΡΙΟΔΟΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ (1950μ.Χ- ΣΗΜΕΡΑ) 46

2.3.1 Ο ΚΡΥΠΤΟΛΓΟΡΙΘΜΟΣ DES 46

2.3.2 ΠΕΡΙΓΡΑΦΗ ΤΟΥ DES 46

2.3.3 ΣΥΝΟΛΙΚΗ ΔΟΜΗ ΤΟΥ DES 47

2.3.4 Η ΣΥΝΑΡΤΗΣΗ ΦΑΙΣΤΕΛ (FEISTEL) 49

2.3.5. ΤΟ ΠΡΟΓΡΑΜΜΑ ΤΩΝ ΚΛΕΙΔΙΩΝ 50

2.4 Ο ΚΡΥΠΤΑΛΓΟΡΙΘΜΟΣ AES 52

2.4.1 ΠΕΡΙΓΡΑΦΗ ΑΛΓΟΡΙΘΜΟΥ AES 53

2.4.2 ΥΨΗΛΟΥ ΕΠΙΠΕΔΟΥ ΠΕΡΙΓΡΑΦΗ ΤΟΥ AES 54

2.4.3 ΤΟ ΣΤΑΔΙΟ SUBBYTES 55

2.4.4 ΤΟ ΣΤΑΔΙΟ SHIFTROW 55

2.4.5 ΤΟ ΣΤΑΔΙΟ MIXCOLUMNS 56

2.4.6 ΤΟ ΣΤΑΔΙΟ ADDROUNDKEY 57

2.4.7 ΒΕΛΤΙΣΤΟΠΟΙΗΣΗ ΤΗΣ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ 58

ΚΕΦΑΛΑΙΟ 3 59

3.ΣΥΓΧΡΟΝΕΣ ΜΟΡΦΕΣ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ 59

3.1 ΣΕ ΤΙ ΣΤΟΧΕΥΕΙ Η ΚΡΥΠΤΟΓΡΑΦΙΑ 59

3.1.1 ΕΙΔΗ ΣΥΣΤΗΜΑΤΩΝ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ 59

3.1.2 ΑΣΥΜΜΕΤΡΑ ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΑ 61

3.1.3 ΤΡΟΠΟΙ ΚΑΙ ΜΕΘΟΔΟΙ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ 62

3.1.4 ELECTRONIC CODEBOOK (ECB) 62

3.1.5 CIPHER BLOCK CHAINING (CBC) 62

3.1.6 CIPHER FEEDBACK (CFB) 63

3.1.7 OUTPUT FEEDBACK (OFB) 63

3.2 ΕΙΔΗ ΚΡΥΠΤΟΓΡΑΦΙΑΣ 64

3.3 ΕΦΑΡΜΟΓΕΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ 64

3.3.1 ΕΞΥΠΝΗ ΚΑΡΤΑ (SMART CARD) 65

3.3.2 ΙΔΙΩΤΙΚΑ ΔΙΚΤΥΑ (VPNS) 66

3.3.3 ΗΛΕΚΤΡΟΝΙΚΗ ΨΗΦΟΦΟΡΙΑ 66

3.3.4 ΗΛΕΚΤΡΟΝΙΚΗ ΔΗΜΟΠΡΑΣΙΑ 67

3.3.5 ΔΟΡΥΦΟΡΙΚΕΣ ΕΦΑΡΜΟΓΕΣ (ΔΟΡΥΦΟΡΙΚΗ ΤΗΛΕΟΡΑΣΗ) 68

3.3.6 ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ ……69

3.3.7 ΤΗΛΕΣΥΝΔΙΑΣΚΕΨΗ-ΤΗΛΕΦΩΝΑ ΜΕΣΩ ΔΙΑΔΙΚΤΥΟΥ (VOIP) ……..70

3.3.8 CLOBAL SYSTEM FOR MOBILE COMMUNICATIONS ……..71

3.3.9 ΗΛΕΚΤΡΟΝΙΚΟ ΓΡΑΜΜΑΤΟΚΙΒΩΤΙΟ ……72

3.3.10 ΣΥΣΤΗΜΑ ΙΑΤΡΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΑΛΛΩΝ ΒΑΣΕΩΝ ΔΕΔΟΜΕΝΩΝ ….72

3.3.11 ΣΥΣΤΗΜΑ ΒΙΟΜΕΤΡΙΚΗΣ ΑΝΑΓΝΩΡΙΣΗΣ ……..73

3.3.12 ΣΤΑΘΕΡΗ ΤΗΛΕΦΩΝΙΑ – CRYPTO PHONES ……..74

3.3.13 ΤΗΛΕΓΡΑΦΗΜΑ ……75

3.3.14 ΣΤΡΑΤΙΩΤΙΚΑ ΔΙΚΤΥΑ- ΤΑΚΤΙΚΑ ΣΥΣΤΗΜΑΤΑ ΕΠΙΚΟΙΝΩΝΙΩΝ ΜΑΧΗΣ ……..75

3.4 ΣΥΓΧΡΟΝΗ ΚΡΥΠΤΟΓΡΑΦΙΑ ……..75

3.5 ΙΟΙ ΥΠΟΛΟΓΙΣΤΩΝ ……..76

3.5.1 Η ΙΣΤΟΡΙΑ ΤΩΝ ΙΩΝ ……..77

3.5.2 ΤΥΠΟΙ ΙΩΝ ……..78

3.5.3 WORMS ……80

3.5.4 TROJAN ……80

3.6 ΔΗΜΟΣΙΟ ΚΛΕΙΔΙ ……..81

3.6.1 ΤΡΟΠΟΣ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ ……..84

3.7 ΚΡΥΠΤΟΓΡΑΦΙΑ ΚΑΙ ΠΡΟΣΤΑΣΙΑ ΔΙΚΤΥΟΥ ……86

3.7.1 ΣΥΝΑΡΤΗΣΕΙΣ ΑΝΑΣΚΟΠΗΣΗΣ ΜΗΝΥΜΑΤΟΣ ……..86

3.7.2 Η ΤΕΧΝΙΚΗ HMAC ……..87

3.7.3 Η ΣΕΙΡΑ MD ……88

3.7.4 Η SEIRA SHA ……88

3.7.5 ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ ……89

3.7.6 ΨΗΦΙΑΚΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ 89

3.7.7 ΠΡΟΤΥΠΟ X209. V3 89

3.8 ΚΡΥΠΤΟΓΡΑΦΙΚΑ ΣΥΣΤΗΜΑΤΑ 91

3.8.1 PGP 92

3.8.2 PCT 92

3.8.3 SHTTP 92

3.8.4 SET 92

3.8.5 DNSSEC 93

3.8.6 KERBEROS 93

3.8.7 ΑΝΤΑΛΛΑΓΗ ΚΛΕΙΔΙΩΝ 94

ΚΕΦΑΛΑΙΟ 4 95

4. ΟΙΚΟΝΟΜΟΛΟΓΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ 95

4.1 ΤΙ ΟΡΙΖΟΥΜΕ ΩΣ ΟΙΚΟΝΟΜΟΛΟΓΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ 95

4.2 ΟΙΚΟΝΟΜΟΛΟΓΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ ΤΩΝ 7 ΕΠΙΠΕΔΩΝ 96

4.2.1 ΕΙΣΑΓΩΓΗ ΣΤΟ ΜΟΝΤΕΛΟ ΤΩΝ 7 ΕΠΙΠΕΔΩΝ 96

4.2.2 ΤΟ ΜΟΝΤΕΛΟ ΤΩΝ 7 ΕΠΙΠΕΔΩΝ.....98

4.2.3 ΕΠΙΠΕΔΟ ΚΡΥΠΤΟΓΡΑΦΙΑ 99

4.2.4 ΕΠΙΠΕΔΟ ΤΕΧΝΟΛΟΓΙΑΣ ΛΟΓΙΣΜΙΚΟΥ 99

4.2.5 ΕΠΙΠΕΔΟ ΔΙΚΑΙΩΜΑΤΑ 100

4.2.6 ΕΠΙΠΕΔΟ ΛΟΓΙΣΤΙΚΗ 101

4.2.7 ΕΠΙΠΕΔΟ ΔΙΑΚΥΒΕΡΝΗΣΗ 102

4.2.8 ΑΠΙΠΕΔΟ ΑΞΙΑ 103

4.2.9 ΕΠΙΠΕΔΟ ΟΙΚΟΝΟΜΙΑ 104

4.2.10 ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΤΟΥ ΜΟΝΤΕΛΟΥ ……104

4.3 ΜΟΡΦΕΣ ΟΙΚΟΝΟΜΟΛΟΓΙΚΗΣ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ ΚΑΙ ΚΟΙΝΟΤΥΠΙΕΣ ……105

4.3.1 ALICE AND BOB ……105

4.3.2 SECURE SHELL ……105

4.3.3 DATA ENCRYPTION STANDARD (DES) ΚΑΙ TRIPLE DES ……106

4.3.4 GREEKLISH ……106

4.3.5 ΑΝΤΙΣΤΟΙΧΙΑ ΑΛΦΑΒΗΤΟΥ GREEKLISH ΜΕ ΤΟ ΕΛΛΗΝΙΚΟ ΑΛΦΑΒΗΤΟ ……107

ΚΕΦΑΛΑΙΟ 5 ……108

5. ΚΒΑΝΤΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ……108

5.1 ΕΙΣΑΓΩΓΗ……..108

5.2 ΚΒΑΝΤΙΚΗ ΠΛΗΡΟΦΟΡΙΑ:ΤΟ QBIT……109

5.3 ΜΕΘΟΔΟΙ ΚΒΑΝΤΙΚΗΣ ΚΡΥΠΤΟΓΡΑΦΙΣΗΣ……110

5.4 ΠΟΛΩΜΕΝΑ ΦΩΤΟΝΙΑ……111

5.5 ΔΙΑΠΛΕΓΜΕΝΑ ΣΩΜΑΤΙΑ……..113

5.6 ΟΑΛΓΟΡΙΘΜΟΣ ΤΟΥ SHOR……113

5.7 Ο ΑΛΓΟΡΙΘΜΟΣ OTP……114

5.8 ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΜΗΔΕΝΙΚΗΣ ΓΝΩΣΗΣ……116

5.9 NITROKEY: ΕΝΑ USB STICK ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ……117

ΣΥΜΠΕΡΑΣΜΑΤΑ ……119

ΒΙΒΛΙΟΓΡΑΦΙΑ- ΠΗΓΕΣ ……120

ΕΥΧΑΡΙΣΤΙΕΣ

Θα θέλαμε να ευχαριστήσουμε θερμά την επιβλέπων καθηγήτρια της πτυχιακής μας εργασίας κ. Βάσιου Γεωργία για την πολύτιμη βοήθεια και καθοδήγηση που μας παρείχε για την εκπόνηση αυτής. Επίσης και τις οικογένειες μας που μας στήριξαν και μας βοήθησαν καθόλη τη διάρκεια των σπουδών μας. Τέλος, θα θέλαμε να ευχαριστήσουμε όλους τους καθηγητές μας που μας μεταλαμπάδευσαν τις γνώσεις τους και μας έδωσαν εφόδια για την συνεχεία.

ΠΕΡΙΛΗΨΗ

Αντικείμενο της συγκεκριμένης πτυχιακής εργασίας είναι η Κρυπτογραφία και η εξέλιξη της.

Ειδικότερα, η εργασία ξεκινά με βασικές έννοιες της Κρυπτογραφίας, την ορολογία που χρησιμοποιεί ο συγκεκριμένος επιστημονικός κλάδος καθώς επίσης και σε τι ακριβώς στοχεύει.

Στην συνέχεια γίνεται 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.

Επίσης δίνονται βασικές έννοιες της κρυπτογραφίας όπως το κρυπτογράφημα ή το απλό κείμενο, καθώς και τα είδη της κρυπτογραφίας. Επιπλέον, γίνεται λεπτομερής παρουσίαση των εφαρμογών της κρυπτογραφίας σε αρκετούς τομείς όπως η οικονομία, η πληροφορική, η εκπαίδευση, ο στρατός κ.α., καθώς επίσης και ανάλυση των σύγχρονων κρυπτογραφικών συστημάτων και των εφαρμογών τους.

Τέλος, η εργασία παρουσιάζει την οικονομολογική κρυπτογραφία και την εξέλιξη της, καθώς επίσης και τις σύγχρονες μορφές κρυπτογραφίας που υπάρχουν μέχρι σήμερα.

ΚΕΦΑΛΑΙΟ 1

ΕΙΣΑΓΩΓΗ

Η **κρυπτογραφία** προέρχεται από τα συνθετικά «κρυπτός» και «γράφω» και είναι ο ένας από τους δύο κλάδους της κρυπτολογίας, ο άλλος είναι η κρυπτανάλυση , αντιστοίχως παρεμφερείς κλάδοι είναι η στεγανογραφία και η στεγανοανάλυση . Η κρυπτολογία είναι ένα πεδίο επιστημονικό με σκοπό την παροχή μηχανισμών για δύο ή περισσότερα μέλη και ως αποτέλεσμα αυτού να είναι η ασφαλής επικοινωνία. Η κρυπτογραφία ασχολείται με τη μελέτη, την ανάπτυξη και την χρήση τεχνικών κρυπτογράφησης και αποκρυπτογράφησης με σκοπό την απόκρυψη και την διαφύλαξη του περιεχομένου μηνυμάτων από το κοινό.

Η κρυπτογραφία χρησιμοποιείται για την μετατροπή πληροφοριών μέσω ενός μυστικού κώδικα από μια κανονική, κατανοητή μορφή σε έναν «γρίφο» όπου χωρίς την γνώση του συγκεκριμένου μυστικού κώδικα ο μετασχηματισμός στην αρχική πληροφορία θα παρέμενε ακατανόητος. Αξίζει να σημειωθεί πως παλαιότερα η επεξεργασία γινόταν πάνω στη γλωσσική δομή του μηνύματος ,ενώ τώρα πλέον εκείνος ο τρόπος έχει αντικατασταθεί με την χρήση του αριθμητικού ισοδύναμου. Με την μεγαλύτερη έμφαση να έχει δοθεί σε διάφορα πεδία των μαθηματικών όπως διακριτά μαθηματικά, θεωρία αριθμών, θεωρία πληροφορίας , υπολογιστική πολυπλοκότητα, στατιστική και συνδυαστική ανάλυση.

Στόχοι:

Η κρυπτογραφία παρέχει τέσσερις βασικές λειτουργίες («αντικειμενικοί σκοποί»)

- **Εμπιστευτικότητα**: Η πληροφορία κρυπτογραφείται με έναν αλγόριθμο σε μία ακατανόητη μορφή, έτσι ώστε να είναι προσβάσιμη μόνο στα εξουσιοδοτημένα μέλη και τους νόμιμους παραλήπτες όπου με την χρήση του αλγόριθμου θα επανέλθει στην κανονική της μορφή. (1)
- **Ακεραιότητα**: Οποιαδήποτε αλλοίωση που μπορεί να υποστεί η πληροφορία προέρχεται από τα εξουσιοδοτημένα μέλη ή από τους νόμιμους κατόχους , με την αλλοίωση που υπέστη η πληροφορία να είναι ανιχνεύσιμη. (1)

- **Μη απάρνηση**: Ο παραλήπτης ή ο αποστολέας της πληροφορίας δεν μπορεί να αρνηθεί την αυθεντικότητα της μετάδοσης ή της δημιουργίας της. (1)
- **Πιστοποίηση**: Οι αποστολέας και παραλήπτης μπορούν να εξακριβώνουν τις ταυτότητες τους καθώς και την πηγή και τον προορισμό της πληροφορίας με διαβεβαίωση ότι οι ταυτότητες τους δεν είναι πλαστές (1)

Ορολογία:

Κρυπτογράφηση (encryption) ονομάζεται η αρχική διαδικασία όπου το μήνυμα μετασχηματίζεται σε μία ακατανόητη μορφή, έτσι ώστε να μην μπορεί να διαβαστεί από κανέναν εκτός από τον νόμιμο παραλήπτη. Για να επιτευχτεί αυτό το αποτέλεσμα χρειαζόμαστε την χρήση κάποιου κρυπτογραφικού αλγόριθμου, τον οποίο γνωρίζουν μόνο οι δύο πλευρές. (1)

Αποκρυπτογράφηση (decryption) ονομάζεται η αντίστροφη διαδικασία ,δηλαδή είναι η διαδικασία όπου από το κρυπτογραφημένο κείμενο ξαναδημιουργείται το αρχικό μήνυμα (1)

Κρυπτογραφικός αλγόριθμος (cipher) είναι η μέθοδος η οποία μετασχηματίζει τα δεδομένα σε μια μορφή ακατανόητη, έτσι ώστε να μην επιτρέπεται η αποκάλυψη των περιεχομένων τους από μη εξουσιοδοτημένα μέρη. Κατά κανόνα ο κρυπτογραφικός αλγόριθμος είναι μία πολύπλοκη μαθηματική συνάρτηση. (1)

Αρχικό κείμενο (plaintext) είναι το μήνυμα το οποίο αποτελεί την εισαγωγή σε μία διεργασία κρυπτογράφησης. (1)

Κλειδί (key) είναι ένας αριθμός αρκετών bit που χρησιμοποιείται ως είσοδος στη συνάρτηση κρυπτογράφησης. (1)

Κρυπτογραφημένο κείμενο (cipher text) είναι το αποτέλεσμα της εφαρμογής ενός κρυπτογραφικού αλγόριθμου πάνω στο αρχικό κείμενο. (1)

Κρυπτανάλυση(cryptanalysis) είναι μια επιστήμη που ασχολείται με την αποκωδικοποίηση κάποιας κρυπτογραφικής τεχνικής ούτως ώστε χωρίς να είναι γνωστό το κλειδί της κρυπτογράφησης, να μπορούμε να φτάσουμε στο αρχικό κείμενο. (1)

Η κρυπτογράφηση και αποκρυπτογράφηση ενός μηνύματος γίνεται με τη βοήθεια ενός αλγορίθμου κρυπτογράφησης και ενός κλειδιού κρυπτογράφησης. Συνήθως ο αλγόριθμος κρυπτογράφησης είναι γνωστός, οπότε η εμπιστευτικότητα του κρυπτογραφημένου μηνύματος που μεταδίδεται βασίζεται ως επί το πλείστον στη μυστικότητα του κλειδιού κρυπτογράφησης. Το μέγεθος του κλειδιού κρυπτογράφησης μετριέται σε αριθμό bits. Γενικά ισχύει ο εξής κανόνας: όσο μεγαλύτερο είναι το κλειδί κρυπτογράφησης, τόσο δυσκολότερα μπορεί να αποκρυπτογραφηθεί το κρυπτογραφημένο μήνυμα από επίδοξους εισβολείς. Διαφορετικοί αλγόριθμοι κρυπτογράφησης απαιτούν διαφορετικά μήκη κλειδιών για να πετύχουν το ίδιο επίπεδο ανθεκτικότητας κρυπτογράφησης. (1)

Βασικές έννοιες:

Ο αντικειμενικός στόχος της κρυπτογραφίας είναι να δώσει τη δυνατότητα σε δύο πρόσωπα να επικοινωνήσουν μέσα από ένα μη ασφαλές κανάλι με τέτοιο τρόπο ώστε ένα τρίτο πρόσωπο μη εξουσιοδοτημένο να μην μπορεί να παρεμβληθεί στην επικοινωνία ή να κατανοήσει το περιεχόμενο των μηνυμάτων. Ένα κρυπτοσύστημα (σύνολο διαδικασιών κρυπτογράφησης – αποκρυπτογράφησης) αποτελείται από μια πεντάδα (P, C, k, E ,D): (1)

- Το P είναι ο χώρος όλων των δυνατών μηνυμάτων ή αλλιώς ανοικτών κειμένων .
- Το C είναι ο χώρος όλων των δυνατών κρυπτογραφημένων μηνυμάτων ή αλλιώς κρυπτοκειμένων .
- Το k είναι ο χώρος όλων των δυνατών κλειδιών ή αλλιώς κλειδοχώρος.
- Η E είναι ο κρυπτογραφικός μετασχηματισμός ή κρυπτογραφική συνάρτηση.
- Η D είναι η αντίστροφη συνάρτηση ή μετασχηματισμός αποκρυπτογράφησης

Η συνάρτηση κρυπτογράφησης E δέχεται δυο παραμέτρους, μέσα από τον χώρο P και τον χώρο k και παράγει μια ακολουθία που ανήκει στον χώρο C. Η συνάρτηση

αποκρυπτογράφησης D δέχεται δυο παραμέτρους, από τον χώρο k και παράγει μια ακολουθία που ανήκει στον χώρο P.

Το Σύστημα λειτουργεί με τον ακόλουθο τρόπο:

1. Ο αποστολέας επιλέγει ένα κλειδί μήκους n από το χώρο κλειδιών με τυχαίο τρόπο, όπου τα n στοιχειά του K είναι στοιχειά από ένα πεπερασμένο αλφάβητο.
2. Αποστέλλει το κλειδί στον παραλήπτη μέσα από ένα ασφαλές κανάλι.
3. Ο αποστολέας δημιουργεί ένα μήνυμα από το χώρο μηνυμάτων .
4. Η συνάρτηση κρυπτογράφησης παίρνει τις δύο εισόδους (κλειδί και μήνυμα) και παράγει μια κρυπτοακολουθία συμβόλων (έναν γρίφο) και η ακολουθία αυτή αποστέλλεται διάμεσου ενός μη ασφαλούς καναλιού.
5. Η συνάρτηση αποκρυπτογράφησης παίρνει ως όρισμα τις δύο τιμές (κλειδί και γρίφο) και παράγει την ισοδύναμη ακολουθία μηνύματος.

Ο αντίπαλος παρακολουθεί την επικοινωνία, ενημερώνεται για την κρυπτοακολουθία αλλά δεν έχει γνώση για την κλείδα που χρησιμοποιήθηκε και δεν μπορεί να αναδημιουργήσει το μήνυμα. Αν ο αντίπαλος επιλέξει να παρακολουθεί όλα τα μηνύματα θα προσανατολιστεί στην εξεύρεση του κλειδιού. Αν ο αντίπαλος ενδιαφέρεται μόνο για το υπάρχον μήνυμα θα παράγει μια εκτίμηση για την πληροφορία του μηνύματος. (1)

ΚΕΦΑΛΑΙΟ 2

2. Ιστορία της Κρυπτογραφίας

Η κρυπτογραφία, η επιστήμη των «μυστικών της πληροφορίας», μπορεί να χαρακτηριστεί ως η αρχαιότερη μέθοδος επικοινωνίας μεταξύ των πολιτισμών. Συγκεκριμένα, σε αυτό το κεφάλαιο θα αναφέρουμε και θα αναλύσουμε τις περιόδους εξέλιξης της Κρυπτογραφίας.

2.1 Η κρυπτογραφία στην περίοδο των αρχαίων χρόνων

Μερικές από τις παλαιότερες ιστορικές αναφορές στην κρυπτογραφία βρίσκουμε στον Ηρόδοτο, όπου αναφέρεται η αποστολή «κρυφών» μηνυμάτων είτε μέσω αντικειμένων είτε μέσω των αγγελιοφόρων τους.

Κατά το χτίσιμο της Περσέπολης, όλες οι πόλεις – κράτη της αυτοκρατορίας έστελναν δώρα στον Ξέρξη εκτός από την Αθήνα και την Σπάρτη. Θέλοντας λοιπόν να πάρει εκδίκηση γι' αυτή τους την συμπεριφορά, ξεκινά την συγκέντρωση στρατιωτικών δυνάμεων για να επιτεθεί στις ελληνικές πόλεις. Εν τω μεταξύ, κατά τη συγκρότηση αυτής της μεγάλης στρατιωτικής δύναμης, ο εξόριστος έλληνας και κάτοικος στα Σούσα της Περσίας Δημάρατος, αποφασίζει αν και εξόριστος να στείλει μήνυμα ώστε να προειδοποιήσει τους Σπαρτιάτες για το σχέδιο επίθεσης. Το πρόβλημα όμως που αντιμετώπιζε ο Δημάρατος ήταν με ποιόν τρόπο θα έστελνε το μήνυμα ώστε να μην μπορέσει να υποκλαπεί από τους Πέρσες. Συγκεκριμένα, αναφέρει ο Ηρόδοτος πως υπήρχε μόνο ένας τρόπος για να μην γίνει αντιληπτό το μήνυμα από τους Πέρσες και αυτός ήταν: να ξύσει το κερί από δύο πτυσσόμενες πινακίδες, να γράψει πάνω στο ξύλο που υπήρχε από κάτω και μετά να επικαλύψει το μήνυμα με κερί. Έτσι, οι πινακίδες θα φαινόντουσαν κενές και δεν θα προκαλούσαν την περιέργεια των φρουρών καθ' οδόν. Όταν το μήνυμα έφτασε στην Σπάρτη κανένας δεν κατάλαβε εκτός της Γοργούς, συζύγου του Λεωνίδα, η οποία πρότεινε να ξύσουν το κερί για να δουν κάτι γραμμένο στο

ξύλο. Αφού έξυσαν το κερί, το μήνυμα αποκαλύφθηκε και στην συνέχεια μεταδόθηκε στους υπόλοιπους Έλληνες. Αυτός ο μυστικός τρόπος επικοινωνίας ανήκει στην μέθοδο της στεγανογραφίας . (2)

Μια επιπλέον αναφορά για την αποστολή κρυφών μηνυμάτων μέσω αγγελιοφόρων μας παρουσιάζει ο Ηρόδοτος παρακάτω.

Σύμφωνα λοιπόν με τον Ηρόδοτο, ο Ιστιαίος, πρώην τύραννος της Μιλήτου και αιχμάλωτος του Δαρείου, θέλοντας να ειδοποιήσει τον διάδοχο του στην διοίκηση της Μιλήτου, Αρισταγόρα, να κηρύξει επανάσταση κατά των Περσών, κούρεψε έναν έμπιστο δούλο του και έγραψε στο δέρμα του κεφαλιού του το εξής μήνυμα: «Ἱστιαῖος Ἀρισταγόρᾳ· Ἰωνίαν ἀπόστησον», το οποίο μεταφράζεται ως: Ο Ιστιαίος προς τον Αρισταγόρα· ξεσήκωσε σε αποστασία την Ιωνία. Στην συνέχεια, αφού μεγάλωσαν τα μαλλιά του δούλου τον έστειλαν στον Αρισταγόρα, με την οδηγία να τον κουρέψει για να εμφανιστεί το μήνυμα. Βέβαια, το παραπάνω γεγονός δεν μπορεί να θεωρηθεί ως κρυπτογραφία, καθώς είχε γίνει απόκρυψη του ίδιου του μηνύματος και όχι του κλειδιού για την ανάγνωση του.

2.1.1 Η σπαρτιατική σκυτάλη

Μια ακόμα ιστορική μορφή κρυπτογραφίας συναντάμε στην σπαρτιατική σκυτάλη περίπου τον 5^{ο} αιώνα π.Χ. Η σκυτάλη ήταν μία ξύλινη ράβδος, συγκεκριμένου μεγέθους και διαμέτρου, η οποία ήταν τυλιγμένη ελικοειδώς από μία λωρίδα δέρματος ή περγαμηνής. Ο τρόπος με τον οποίο μπορούσε να γίνει επικοινωνία ήταν ο εξής: Ο αποστολέας γράφει ένα μήνυμα κατά μήκος της σκυτάλη δηλαδή το κείμενο ήταν γραμμένο σε στήλες όπου σε κάθε στήλη και ένα γράμμα. Όταν ξετύλιγαν την λωρίδα απλά υπήρχαν γραμμένα πάνω της κάποια γράμματα χωρίς νόημα καθώς, το μήνυμα είχε αναδιαταχτεί. Στην συνέχεια ο αγγελιοφόρος έπαιρνε την λωρίδα, τη τοποθετούσε στη ζώνη του με τα γράμματα να βρίσκονται στην μέσα πλευρά ώστε να μην γίνονται αντιληπτά. Τέλος, την έδινε στον παραλήπτη, ο οποίος με την σειρά του για να μπορέσει να διαβάσει το μήνυμα έπρεπε απλά να τυλίξει την λωρίδα, που του είχε αποσταλεί, σε μία σκυτάλη ίδιας διαμέτρου. Επομένως, το «κλειδί» για την ανάγνωση του μηνύματος ήταν η διάμετρος της σκυτάλης. Η συγκεκριμένη πολεμική συσκευή επικοινωνίας δηλώνει την χρήση

της, περίπου το 404 π.Χ. όταν ένας αγγελιαφόρος παραδίδει μια λωρίδα στον Σπαρτιάτη Λύσανδρο και αυτός αφού την διάβασε με την παραπάνω μέθοδο, έμαθε για την επίθεση που σχεδίαζε ο σατράπης Φαρνάβαζος και την απέκρουσε επιτυχώς

2.1.2 Δίσκος της Φαιστού

Ο δίσκος της Φαιστού είναι φτιαγμένος από πηλό με μέση διάμετρο 16 εκατοστά και πάχος περίπου τα 2,1 εκατοστά. Στις δύο όψεις του μπορούμε να διακρίνουμε 45 διαφορετικά σύμβολα, αρκετά από τα οποία είναι αναγνωρίσιμα αντικείμενα, όπως ανθρώπινες μορφές, ψάρια, πουλιά, έντομα, φυτά κ.α. Στο σύνολο τους είναι 241 σύμβολα, όπου 122 βρίσκονται στην πρώτη πλευρά και 119 στην δεύτερη. Όλα τα σύμβολα και στις δύο πλευρές είναι τοποθετημένα σπειροειδώς και χωρισμένα σε ομάδες με μικρές γραμμές που κατευθύνονται προς το κέντρο. (2)

Ο Δίσκος της Φαιστού χρονολογείται περίπου στο 1700 π.Χ., και έχει κεντρίσει το ενδιαφέρον πολλών αρχαιολόγων απ' όλο τον κόσμο για την αποκρυπτογράφηση του. Έχουν γίνει πάρα πολλές προσπάθειες και έχουν προταθεί ακόμα περισσότερες ερμηνείες του κειμένου του, ότι πρόκειται για προσευχή, για μια ιστορία, για ένα γεωμετρικό θεώρημα, για ημερολόγιο κ.α. Μέχρι σήμερα όμως, δεν έχει αποκρυπτογραφηθεί καθώς υπάρχουν ελάχιστες πληροφορίες για την αποκρυπτογράφηση του και γι' αυτό τον λόγο, οι έρευνες το καθιστούν ως το αρχαιότερο δείγμα στοιχειοθεσίας και ευρωπαϊκής γραφής. (2)

2.1.3 Τα αιγυπτιακά σύμβολα

Η πρώτη εμφάνιση ενός κρυπτογραφικού συστήματος επικοινωνίας εμφανίζεται το 3000 π.Χ. στην Αίγυπτο, με αρχαία εικονιστικά σύμβολα γνωστά και ως Ιερογλυφικά. Τα ιερογλυφικά ήταν μικροσκοπικά ανάγλυφα έργα τέχνης που συναντούμε σε ιερά θρησκευτικά κείμενα και μπορούν να αποδώσουν μια εσωτερική ιδέα μέσα από εικόνες. Λόγω όμως της υπερβολικής πολυπλοκότητας των συμβόλων για επικοινωνία, το 1900 π.Χ. αναπτύχθηκε μια απλουστευμένη μέθοδος επικοινωνίας, αλλά και γραφής των συμβόλων, η ιερατική γραφή.

Στα Αιγυπτιακά ιερογλυφικά σχεδόν όλα τα σύμβολα αντιπροσωπεύουν ένα έμψυχο ή άψυχο αντικείμενο, και στην πιο επεξεργασμένη τους μορφή ήταν μικροσκοπικά έργα τέχνης από μόνα τους, και επομένως ήταν ιδανικά για μνημεία και διακοσμητικούς σκοπούς. Τα ιερογλυφικά ήταν το σύστημα γραφής το οποίο αποτελούταν από ένα συνδυασμό συμβόλων, λογογραμμάτων και αλφαβητικών στοιχείων τα οποία αντιστοιχούσαν πάνω από 2000 σε αριθμό. Ασφαλώς, λόγω της πολυπλοκότητας των γραμμάτων των ιερογλυφικών, χρησιμοποιήθηκε ένα διαφορετικό είδος καλλιγραφικών γραμμάτων, τα οποία ήταν πιο εύκολα και γρήγορα στην γραφή τους. Οι πιο απλές μορφές ιερογλυφικής γραφής, όπως αναφέραμε ήταν η ιερατική και η δημοτική από τεχνικής άποψης, τις οποίες χρησιμοποιούσαν κυρίως σε θρησκευτικά κείμενα. Εξαιτίας του τεράστιου αριθμού αλλά και της πολυπλοκότητας των συμβόλων, ήταν απολύτως λογικό οι γραφείς να κάνουν αρκετά χρόνια για να μάθουν να γράφουν.

Την ίδια περίοδο, σε αντιστοιχία με την Αιγυπτιακή γραφή, εμφανίζεται η Κρητική εικονογραφική ή ιερογλυφική γραφή, η οποία μοιάζει αρκετά με την ιερογλυφική της Αιγύπτου, αλλά διαφέρει ως προς την ερμηνεία καθώς, οι εικόνες που χρησιμοποιεί παίρνουν φωνητική αξία. Η συγκεκριμένη γραφή συνυπήρχε μαζί με την γραμμική γραφή Α, κατά την Παλαιοανακτορική Περίοδο στην περιοχή της Κρήτης σύμφωνα με τις ανασκαφές που έγιναν στο ανάκτορο των Μαλίων. Εμφανίστηκε το 1908 στην νότια Κρήτη, όταν ανακαλύφτηκε ο πασίγνωστος Δίσκος της Φαιστού μαζί με άλλα αντικείμενα όπως σφραγίδες και πέλεκεις.

2.1.4. Η γραμμική γραφή

Η Κριτική εικονογραφική γραφή, δεν μας έχει αποκαλύψει τον κώδικα της ακόμα. Γνωρίζουμε, ωστόσο, ότι η συγκεκριμένη γραφή χρησιμοποιούσε τα σύμβολα ως φωνητική γραφή και όχι ως σημεία. Επίσης, όπως προαναφέραμε γνωρίζουμε ότι συνυπήρχε με την Γραμμική γραφή Α, τόσο χρονικά όσο και τοπικά, σύμφωνα με τις εργασίες ανασκαφής που έγιναν στα ανάκτορα των Μαλίων της Κρήτης.

Ο μεγάλος Άγγλος αρχαιολόγος Σερ Άρθουρ Έβανς (sir Arthur Evans) ανακάλυψε τις πρώτες επιγραφές που είχαν γραφεί με γραμμική γραφή, στις ανασκαφές που έκανε στα ανάκτορα της Κνωσού της Κρήτης το 1900. Η γραφή αυτή ονομάστηκε

γραμμική καθώς πήρε το όνομα της από τον ίδιο τον Έβανς, επειδή τα γράμματα της είναι γραμμές ή αλλιώς γραμμικά σχήματα εν αντιθέσει με άλλες γραφές όπου τα γράμματα ήταν σφήνες ή εικόνες όντων.. Η Γραμμική Γραφή Α πιθανότατα ήταν η γλώσσα των Μινωιτών της Αρχαίας Κρήτης, και ίσως ο πρόγονος του σημερινού ελληνικού αλφάβητου. (2)

Τα γραμμικά σχήματα της γραφής χαράζονταν μ' ένα είδος αιχμηρού αντικειμένου πάνω σε πλάκες, οι οποίες ήταν φτιαγμένες από πηλό, τις οποίες τις άφηναν να ξεραθούν σε φούρνους για να διατηρηθεί η γραφή. Οι περισσότερες επιγραφές με Γραμμική γραφή Α περιέχουν συντομογραφίες των εμπορεύσιμων προϊόντων καθώς και αριθμών για να υποδεικνύουν την ποσότητα ή την τιμή.

Τα σύμβολα τα οποία καταγράφηκαν από τον Έβανς είναι 135. Η γραμμική γραφή, βέβαια δεν χρησιμοποιήθηκε μόνο στην Κρήτη, καθώς ορισμένα ευρήματα καταδεικνύουν ότι αποτέλεσε μέσο γραφής και σε άλλες περιοχές, αφού σχετικές επιγραφές έχουν βρεθεί στην Μήλο αλλά και στη Θύρα. Παρά την εξέλιξη της τεχνολογίας, η Γραμμική γραφή Α δεν έχει αποκρυπτογραφηθεί ακόμη.

Ο μεγάλος αρχαιολόγος Έβανς, επιπλέον ανακάλυψε την συγγενική γραφή της Γραμμικής Α η οποία ήταν η Γραμμική Β, μία γραφή πιο πρόσφατη και πιο εξελιγμένη. Σύμφωνα με τις πληροφορίες που έχουμε, η Γραμμική Β χρησιμοποιήθηκε αποκλειστικά για λογιστικούς σκοπούς. Δείγματα γραφής με Γραμμική Β όπως πινακίδες κ.α. βρέθηκαν στην Κνωσό, τα Χανιά αλλά και στην Πύλο, τις Μυκήνες, τη Θήβα και την Τίρυνθα με τον αριθμό τους να φτάνει στο σύνολο, περίπου τα 10.000 τεμάχια. Τα σχήματα των πινακίδων είναι αρκετά και διαφορετικά μεταξύ τους, ως προς το μέγεθος ανάλογα πάντα με τις προτιμήσεις του γραφέα, με τα φυλλοειδή και τα «σελιδόσχημα» σχήματα να επικρατούν. Την συγκεκριμένη γραφή την έγραφαν πάνω σε επίπεδες, επιμήκης και συμπαγής πινακίδες, διαφοροποιημένες σε δύο επιφάνειες: μια επίπεδη λειασμένη, που επρόκειτο να αποτελέσει την κύρια γραφική επιφάνεια και μια κυρτή, που συνήθως έμενε άγραφη. Τις περισσότερες φορές, όταν τα κείμενα απαιτούσαν παραπάνω από μια πινακίδες, έχουμε τις επικαλούμενες «ομάδες» ή «πολύπτυχα» πινακίδων, τις οποίες εμφανίζουν κοινά ως προς τον τρόπο αποξήρανσης, το μίγμα του πηλού και φυσικά ως προς το γραφικό χαρακτήρα του κάθε συγγραφέα. Η φύλαξη τους γίνονταν σε αρχειοφυλάκια όπου ταξινομούνταν κατά θέματα σε ξύλινα κιβώτια.

Για να είναι γνωστό το περιεχόμενο των καλαθιών προς τους ενδιαφέροντες, χρησιμοποιούσαν ετικέτες: ένα σφαιρίδιο πηλού, εντυπωμένο στην πρόσθια πλευρά, στο οποίο καταγράφονταν συνοπτικές πληροφορίες.

Η συγκεκριμένη γραφή κίνησε το ενδιαφέρον του Άγγλου αρχιτέκτονα και ερασιτέχνη Μ. Βέντρις, ο οποίος ασχολήθηκε συστηματικά μαζί της. Ήταν ο πρώτος που υποστήριξε ότι επρόκειτο για κάποιο είδος ελληνικής γραφής, αλλά η άποψη του δεν έγινε αποδεκτή από τους ειδικούς. Στη συνέχεια, πολλοί από τους ειδικούς υποστήριξαν την άποψη του Άγγλου Μ. Βέντρις, και πιο συγκεκριμένα ο κρυπταναλυτής Τζον Τσάντγουκ, προσπάθησε να βοηθήσει στην κρυπτανάλυση της Γραμμικής Β, αλλά χωρίς κάποια ιδιαίτερη επιτυχία μέχρι τότε. Ωστόσο, η συνεργασία τους και ο συνδυασμός των γνώσεων τους έφεραν το αποτέλεσμα που ήθελαν, το οποίο καταγράφηκε το 1953 στο διάσημο σε όλους άρθρο για την κρυπτανάλυση «Μαρτυρίες για την ελληνική διάλεκτο στα μυκηναϊκά αρχεία». Η αποκρυπτογράφηση της Γραμμικής Β, αποδείχτηκε ένα σημαντικό επίτευγμα της εποχής, καθώς αποδείχτηκε ότι επρόκειτο για ελληνική γλώσσα, την οποία χρησιμοποιούσαν οι Μινωίτες της Κρήτης. (2)

2.1.5 Ο μυστικός κώδικας στα κείμενα του Πλάτωνα

Σύμφωνα με την έρευνα που έγινε στο Κέντρο Ιστορίας της Επιστήμης, Τεχνολογίας και Ιατρικής στο Πανεπιστήμιο του Μάντσεστερ, ο δρ Τζέι Κένεντυ υποστηρίζει ότι στα κείμενα του Πλάτωνα υπάρχει κάποιος μυστικός κώδικας γραφής. Βασίζοντας την ανακάλυψη του στον θαυμασμό του Πλάτων για την θεωρεία του Πυθαγόρα, ότι οι πλανήτες και τα αστέρια παράγουν μια μουσική, την γνωστή «αρμονία των σφαιρών», η οποία δεν είναι αντιληπτή από τους ανθρώπους αναφέρει πως «οι μυστικοί κώδικες του Πλάτωνα, τελικά υπάρχουν». (2)

Παρακολουθώντας τα βήματα του Πλάτωνα, αντιλήφθηκε πως υπήρχε μια μυστική διάταξη των συμβόλων, ένας «πλατωνικός κώδικας» ο οποίος χρησιμοποιήθηκε στα κείμενά του για να δώσει μια μουσική δομή. Αυτόν λοιπόν τον τρόπο κωδικοποίησης ισχυρίζεται ότι κατάφερε και «έσπασε» ο δρ. Κένεντυ αποκρυπτογραφώντας τα μηνύματα που υπήρχαν στα έργα του μεγάλου Έλληνα φιλοσόφου.

Στην αρχαιότητα, υπήρχαν πολλοί που πίστευαν ότι τα βιβλία του Πλάτωνα βρίσκονταν σ' ένα διαφορετικό επίπεδο, με πολύπλοκες έννοιες και αρκετούς κώδικες, όμως κανένας από τους σύγχρονους επιστήμονες δεν υποστήριξε αυτή την άποψη, εκτός από τον δρ. Κένεντυ ο οποίος αποκαλύπτει ότι τα βιβλία του μεγάλου φιλοσόφου έκρυβαν μια διαφορετική φιλοσοφία. Συγκεκριμένα, ο δρ Κένεντυ διαβάζοντας τα έργα του Πλάτωνα κατάφερε να ανακαλύψει την μουσικότητα που υπήρχε μέσα σε αυτά βρίσκοντας τις δώδεκα νότες της μουσικής.

Για ποιο λόγο όμως ο Πλάτωνας δημιούργησε έναν κώδικα στα έργα του; Η απάντηση στο ερώτημα είναι πως ο Πλάτωνας ήθελε να προστατευθεί μέσα από αυτόν τον κώδικα. Αυτό οφείλεται στο γεγονός ότι ο Πλάτωνας, 2.000 πριν υπάρξει η σύγχρονη επιστήμη, κατανόησε την ύπαρξη του σύμπαντος και ότι η δημιουργία του οφείλεται στα μαθηματικά και την λογική και όχι στους θεούς. Για εκείνη την εποχή αυτή η σκέψη ήταν βλασφημία και είχε ως τιμωρία την θανατική ποινή, γεγονός που ώθησε τον Πλάτωνα στην δημιουργία αυτού του μυστικού κώδικα, για να μπορέσει να κληροδοτήσει τις ιδέες του και τις απόψεις τους στις επόμενες γενεές.

2.1.6α Το Τετράγωνο του Πολύβιου

Το Τετράγωνο του Πολύβιου ή αλλιώς *Σκακιέρα του Πολύβιου* είναι συσκευή που εφευρέθηκε από τον Πολύβιο και χρησιμοποιήθηκε από τους Αρχαίους Έλληνες για την κωδικοποίηση των μηνυμάτων που αντάλλασσαν φυλάκια (σκοπιές) μεταξύ τους. Ο λόγος που ο Πολύβιος δημιούργησε αυτόν τον πίνακα δεν ήταν άλλος παρά να δημιουργήσει μια μέθοδο που θα μπορούσε απλό σχετικά τρόπο να μεταδώσει πληροφορίες μεταξύ απομακρυσμένων σημείων ιδιαίτερα αν τα σημεία αυτά είχαν οπτική επαφή (π.χ δύο πεντάδες από πυρσούς κλπ). Η μορφή που είχε ο πίνακας για την ελληνική γλώσσα είναι η εξής: (2)

	1	2	3	4	5
1	Α	Β	Γ	Δ	Ε
2	Ζ	Η	Θ	Ι	Κ
3	Λ	Μ	Ν	Ξ	Ο

4	Π	P	Σ	T	Y
5	Φ	X	Ψ	Ω	

Το αυθεντικό Τετράγωνο του Πολύβιου βασίστηκε στην ελληνική αλφάβητο (για αυτό το λόγο δεν είναι συμπληρωμένο το κελί 55), ωστόσο η ίδια μεθοδολογία μπορεί να εφαρμοσθεί με την ίδια επιτυχία για κάθε αλφάβητο (σχεδόν). Έτσι οι Ιάπωνες από το 1500 έως το 1910 έκαναν χρήση του Τετραγώνου του Πολύβιου, τροποποιημένο ώστε να καλύπτει τα 48 γράμματα της Ιαπωνικής (πίνακας 7x7). Αντίστοιχα το μέγεθος του πίνακα μπορεί να τροποποιηθεί σε 6 επί 6 δίνοντας τη δυνατότητα να κωδικοποιηθεί η Κυριλλική αλφάβητος (που περιλαμβάνει από 33 ως 37 γράμματα). (2)

Η εφαρμογή του τετραγώνου του Πολύβιου στην Αγγλική αλφάβητο, τυπικά έχει ως εξής:

	1	**2**	**3**	**4**	**5**
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Λόγω του ότι η Αγγλική έχει 26 γράμματα έναντι των 24 της Ελληνικής ένα από τα κελιά του πίνακα σε δύο γράμματα (συνήθως είναι το γράμμα I και J), ώστε να είναι εφικτή η τοποθέτηση όλων των γραμμάτων σε πίνακα 5 επί 5. Εναλλακτικά, κατά την Ιαπωνική μέθοδο, μπορεί να υιοθετηθεί ένας πίνακας με διαστάσεις 6 X 6, διατηρώντας άδεια τα κελιά που περισσεύουν. (2)

	1	**2**	**3**	**4**	**5**	**6**
1	A	B	C	D	E	F
2	G	H	I	J	K	L
3	M	N	O	P	Q	R
4	S	T	U	V	W	X

5	Y	Z
6		

Ο τρόπος λειτουργίας του πίνακα είναι απλός: κάθε γράμμα αναπαριστάται από τις συντεταγμένες του στο πίνακα. Έτσι ανάλογα με τη γλώσσα και το μέγεθος του πίνακα που έχουμε επιλέξει κωδικοποιούνται τα γράμματα και ακολούθως οι λέξεις. Έτσι για την αγγλική λέξη «BAT» με βάση το πρώτο πίνακα (διαστάσεων 5Χ5) η αντιστοίχηση είναι ‘’12 11 44’’ ενώ με τον δεύτερο πίνακα (διαστάσεων 6Χ6) γίνεται ‘’12 11 42’’. Η ελληνική λέξη «ΝΙΚΗ» μετασχηματίζεται στη σειρά ‘’33 24 25 22’’. (2)

2.1.6β Η κρυπτογραφία στο τετράγωνο του Πολύβιου

Η ασφάλεια του τετραγώνου του Πολύβιου είναι πολύ περιορισμένη ακόμα και συνδυαστεί με αλγορίθμους αντικατάστασης ή μεικτά αλφάβητα. Από την άλλη μεριά όμως, το Τετράγωνο του Πολύβιου για να βελτιωθεί ο βαθμός δυσκολίας του μπορεί α συνδυαστεί με αλγορίθμους κρυπτογράφησης ή ακόμα πιο αποτελεσματικά με πολύπλοκους αλγόριθμους όπως περιγράφει στο έργο τουCommunication Theory of Secrecy Systems ο Κλώντ Σάννον. Σύμφωνα με αυτή την θεωρεία, το Τετράγωνο του Πολύβιου αποτελεί σημαντικό τμήμα σε πολλούς αλγορίθμους κρυπτογράφησης καθώς επίσης, ένα χρήσιμο εργαλείο για την τηλεγραφία όπου επέτρεψε την εύκολη μετάδοση μηνυμάτων σε απόσταση μέσω μετασχηματισμού των γραμμάτων σε αριθμητικές απεικονίσεις.

2.1.7 Η κρυπτογραφία στο Μεσαίωνα

Κατά την διάρκεια του Μεσαίωνα, η κρυπτογραφία θεωρούταν και αποτελούσε για πολλούς μια μορφή αποκρυφισμού και μαύρης μαγείας, στοιχείο το οποίο λειτούργησε αρνητικά στην ανάπτυξή της.

Τα μυστικά της κρυπτογραφίας φυλάσσονταν στα μοναστήρια ή στα μυστικά αρχεία των βασιλιάδων της εποχής και λίγες μέθοδοι γίνονταν ευρέως γνωστοί. (2)

Οι αλχημιστές του μεσαίωνα συνήθιζαν να κρατούν ως επτασφράγιστα μυστικά τις λεπτομέρειες των τεχνικών τους και να κρατούν σημειώσεις με «κρυπτογραφικά» σύμβολα. Η συγκεκριμένη τεχνική για την φύλαξη των μυστικών τους, προήλθε από τον φόβο τους για την ποινή της Ιεράς εξέτασης, που δεν ήταν καμία άλλη παρά μόνο η θανατική, για τέτοιου είδους πρακτικές ή τελετουργίες. Αυτό είχε ως αποτέλεσμα να ταυτιστούν με μυστικιστικές ομάδες και συντεχνίες με «ύποπτους σκοπούς». Αλλά και οι ίδιοι οι αλχημιστές, τις περισσότερες φορές σκόπιμα επεδίωξαν να διαχωρίσουν την «τέχνη» τους από το υπερφυσικό, το μαγικό και την δεισιδαιμονία. (2)

Η εξέλιξη, τόσο της κρυπτογραφίας, όσο και των μαθηματικών, οφείλεται κυρίως στους Άραβες. Οι Άραβες είναι οι πρώτοι που επινόησαν αλλά και χρησιμοποίησαν μεθόδους κρυπτανάλυσης. Το κυριότερο εργαλείο στην κρυπτανάλυση, η χρησιμοποίηση των συχνοτήτων των γραμμάτων κειμένου, σε συνδυασμό με τις συχνότητες εμφάνισης στα κείμενα των γραμμάτων της γλώσσας, επινοήθηκε από αυτούς γύρω στο 14^{ο} αιώνα. Η κρυπτογραφία, λόγω των στρατιωτικών εξελίξεων, σημείωσε σημαντική ανάπτυξη στους επόμενους αιώνες.

Το έτος 1563 σημειώθηκε η έκδοση του βιβλίου «De furtivis literarum notis» από το Ιταλό Giovanni Batista Port, ο οποίος παρουσίασε για πρώτη φορά συστήματα με τη μέθοδο της πολυαλφαβητικής ανάλυσης κρυπτογράφησης. Παρόμοιο σύστημα κρυπτογράφησης παρουσιάστηκε και από τον Vigenere, το οποίο έχει τύχει τέτοιας αποδοχής από την επιστημονική κοινότητα που συνιστάται σε εφαρμογές κρυπτογράφησης και στη σημερινή εποχή. (2) (2)

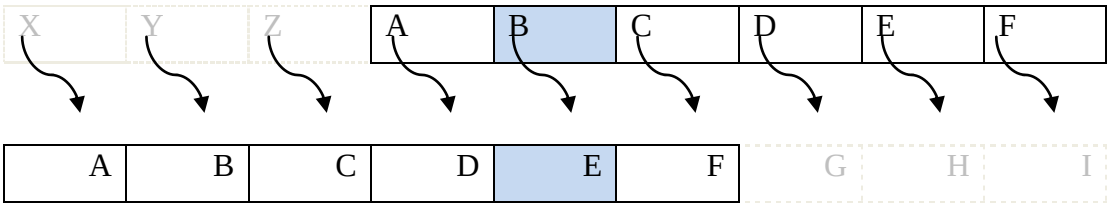
Μέσα από την αποκρυπτογράφηση της ακατάληπτης ερμητικής γλώσσας των αλχημιστών, οι ιστορικοί αρχίζουν να αντιλαμβάνονται όλο και περισσότερο την πνευματική σύνδεση που υπάρχει ανάμεσα στην αλχημική μέθοδο και σε άλλες όψεις της πολιτισμικής ιστορίας της Δύσης. Σημαντικό επίτευγμα για την συγκεκριμένη περίοδο, και βάση για την ανάπτυξη των κρυπτομηχανών, αποτέλεσε η κατασκευή της πρώτης κρυπτοσυσκευής από τον C. Wheatstone. Τον 17^{ο} αιώνα αναθερμάνθηκε το ενδιαφέρον για την αποκρυπτογράφηση των ιερογλυφικών, έπειτα από την σημαντική αποκρυπτογράφηση των αιγυπτιακών

ιερογλυφικών από τον Γάλλο Champolion, και έτσι το 1962 ο Γερμανός Ιησουΐτης Αθανάσιος Κίρχερ δημοσίευσε, χωρίς μεγάλη επιτυχία, ένα λεξικό για την ερμηνεία τους με τίτλο «Oedipus Aegyptiacus». Την λύση για την σωστή ερμηνεία των ιερογλυφικών την έδωσαν 2 μεγάλοι αποκρυπτογράφοι της εποχής ο Γιανγκ και ο Σαμπόλιον, χρησιμοποιώντας την περίφημη «Στήλη της Ροζέτας», η οποία βρέθηκε από τα Στρατεύματα του Ναπολέοντα στην Αίγυπτο. Αργότερα 1671 μ.Χ επινοήθηκε από τον Leibniz ένα σύστημα που χρησιμοποιούσε μια δυαδική κλίμακα που μέχρι τις μέρες μας αποτελεί το θεμέλιο του κώδικα ASCII. Έναν αιώνα περίπου αργότερα, ο Thomas Jefferson το έτος 1795 μ.Χ. θα εφεύρει μια πρώιμης μορφής κρυπτογραφική μηχανή που θα ονομαστεί τροχός κρυπτογράφησης ή “wheel cipher”.

Η εφεύρεση του τηλεγράφου και η ευκολία στην μετάδοση πληροφοριών έκανε περί τα μέσα του έτους 1844 μ .Χ. επιτακτική την ανάγκη για ανάπτυξη μεθόδων κρυπτογράφησης και ασφάλειας των μεταδιδόμενων μηνυμάτων. Λίγες δεκαετίες αργότερα, το έτος 1861 σημειώνεται η πρώτη παραβίαση του κώδικα κρυπτογράφησης του Vigenere από τον Kasiski, έναν απόστρατο αξιωματικό του πρωσικού στρατού. Σαν επιστέγασμα της επιτυχίας του ο Kasiski συνέγραψε το βιβλίο «Η μυστική γραφή και η τέχνη αποκρυπτογράφησης» όπου ανέλυε τις τεχνικές κρυπτογράφησης και αποκρυπτογράφησης.

2.1.8 Παρουσίαση του Κρυπτογράμματος Vigenere

Ο αλγόριθμος Κρυπτογράφησης Vigenere είναι μια μέθοδος κρυπτογράφησης σε αλφαβητικό κείμενο στο οποίο εφαρμόζονται διαφορετικοί τύποι αλγορίθμων κρυπτογράφησης Καίσαρα με βάση την θέση των γραμμάτων μιας λέξης ή φράσης κλειδί. Πιο συγκεκριμένα, η εφαρμογή του κώδικα Καίσαρα συνίσταται στην αντικατάσταση κάθε γράμματος του κειμένου με ένα άλλο το οποίο έχει σταθερή απόσταση από αυτό στο αλφάβητο. Όπως, φαίνεται και το παράδειγμα, χρησιμοποιείται μετατόπιση τριών θέσεων, έτσι ώστε το Β του κειμένου να γίνεται Ε στο κρυπτογραφημένο κείμενο. (2)



Σχήμα 1.: Απεικόνιση της αντικατάστασης των γραμμάτων.

Ο αλγόριθμος Vigenere πήρε το όνομα του από τον Blaise de Vigenere ο οποίος δεν ήταν αυτός που τον εφηύρε αλλά αυτός που τον ανέπτυξε και τον απέδωσε στην τελική του μορφή που γνωρίζουμε. Η Κρυπτογράφηση Vigenere, είναι μια μέθοδος κρυπτογράφησης που βασίζεται σε μια απλή μορφή πολυαλφαβητικής υποκατάστασης. Η Πολυπλοκότητα του προέρχεται από την χρήση όχι μόνο ενός, αλλά 24 κρυπτογραφικών αλφάβητων, όπου το καθένα από αυτά προκύπτει από την μετάθεση ενός γράμματος σε σχέση με το προηγούμενο. Έτσι η πρώτη σειρά παριστά το κανονικό μας αλφάβητο μετατοπισμένο κατά μια θέση δεξιά. Συνεχίζοντας με την ίδια λογική, η σειρά 2 το παριστά, μετατοπισμένο τώρα κατά 2 θέσεις δεξιά, κ.ο.κ. Η ξεχωριστή γραμμή πάνω από το τετράγωνο Vigenere, με μικρά γράμματα, παριστά τα γράμματα του κειμένου που θέλουμε να κρυπτογραφήσουμε.

Αλφάβητο	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω
1	β	γ	δ	ε	ζ	η	θ	ι	κ	λ	μ	ν	ξ	ο	π	ρ	σ	τ	υ	φ	χ	ψ	ω	α
2	γ	δ	ε	ζ	η	θ	ι	κ	λ	μ	ν	ξ	ο	π	ρ	σ	τ	υ	φ	χ	ψ	ω	α	β
3	δ	ε	ζ	η	θ	ι	κ	λ	μ	ν	ξ	ο	π	ρ	σ	τ	υ	φ	χ	ψ	ω	α	β	γ
4	ε	ζ	η	θ	ι	κ	λ	μ	ν	ξ	ο	π	ρ	σ	τ	υ	φ	χ	ψ	ω	α	β	γ	δ
5	ζ	η	θ	ι	κ	λ	μ	ν	ξ	ο	π	ρ	σ	τ	υ	φ	χ	ψ	ω	α	β	γ	δ	ε
6	η	θ	ι	κ	λ	μ	ν	ξ	ο	π	ρ	σ	τ	υ	φ	χ	ψ	ω	α	β	γ	δ	ε	ζ
7	θ	ι	κ	λ	μ	ν	ξ	ο	π	ρ	σ	τ	υ	φ	χ	ψ	ω	α	β	γ	δ	ε	ζ	η
8	ι	κ	λ	μ	ν	ξ	ο	π	ρ	σ	τ	υ	φ	χ	ψ	ω	α	β	γ	δ	ε	ζ	η	θ
9	κ	λ	μ	ν	ξ	ο	π	ρ	σ	τ	υ	φ	χ	ψ	ω	α	β	γ	δ	ε	ζ	η	θ	ι
10	λ	μ	ν	ξ	ο	π	ρ	σ	τ	υ	φ	χ	ψ	ω	α	β	γ	δ	ε	ζ	η	θ	ι	κ

11	μ	ν	ξ	ο	π	ρ	σ	τ	υ	φ	χ	ψ	ω	α	β	γ	δ	ε	ζ	η	θ	ι	κ	λ
12	ν	ξ	ο	π	ρ	σ	τ	υ	φ	χ	ψ	ω	α	β	γ	δ	ε	ζ	η	θ	ι	κ	λ	μ
13	ξ	ο	π	ρ	σ	τ	υ	φ	χ	ψ	ω	α	β	γ	δ	ε	ζ	η	θ	ι	κ	λ	μ	ν
14	ο	π	ρ	σ	τ	υ	φ	χ	ψ	ω	α	β	γ	δ	ε	ζ	η	θ	ι	κ	λ	μ	ν	ξ
15	π	ρ	σ	τ	υ	φ	χ	ψ	ω	α	β	γ	δ	ε	ζ	η	θ	ι	κ	λ	μ	ν	ξ	ο
16	ρ	σ	τ	υ	φ	χ	ψ	ω	α	β	γ	δ	ε	ζ	η	θ	ι	κ	λ	μ	ν	ξ	ο	π
17	σ	τ	υ	φ	χ	ψ	ω	α	β	γ	δ	ε	ζ	η	θ	ι	κ	λ	μ	ν	ξ	ο	π	ρ
18	τ	υ	φ	χ	ψ	ω	α	β	γ	δ	ε	ζ	η	θ	ι	κ	λ	μ	ν	ξ	ο	π	ρ	σ
19	υ	φ	χ	ψ	ω	α	β	γ	δ	ε	ζ	η	θ	ι	κ	λ	μ	ν	ξ	ο	π	ρ	σ	τ
20	φ	χ	ψ	ω	α	β	γ	δ	ε	ζ	η	θ	ι	κ	λ	μ	ν	ξ	ο	π	ρ	σ	τ	υ
21	χ	ψ	ω	α	β	γ	δ	ε	ζ	η	θ	ι	κ	λ	μ	ν	ξ	ο	π	ρ	σ	τ	υ	Φ
22	ψ	ω	α	β	γ	δ	ε	ζ	η	θ	ι	κ	λ	μ	ν	ξ	ο	π	ρ	σ	τ	υ	φ	Χ
23	ω	α	β	γ	δ	ε	ζ	η	θ	ι	κ	λ	μ	ν	ξ	ο	π	ρ	σ	τ	υ	φ	χ	ψ
24	α	β	γ	δ	ε	ζ	η	θ	ι	κ	λ	μ	ν	ξ	ο	π	ρ	σ	τ	υ	φ	χ	ψ	ω

Πίνακας 1.: Αλφάβητο για τον αλγόριθμο Vigenere

Για παράδειγμα, αν χρησιμοποιήσουμε, το αλφάβητο που βρίσκεται στην σειρά 7, τότε το γράμμα (α) του κανονικού αλφαβήτου εκπροσωπείται με (θ), ενώ αν χρησιμοποιήσουμε τη σειρά 21, το ίδιο γράμμα κρυπτογραφείται ως (Χ). Με αυτόν τον τρόπο, ο αποστολέας μπορεί να κρυπτογραφήσει οποιοδήποτε γράμμα του μηνύματός του με όποια σειρά του πίνακα θέλει. Η τεχνική όμως αυτή δημιουργεί αρκετά προβλήματα στον παραλήπτη του μηνύματος καθώς δεν γνωρίζει ποιες σειρές έχουν χρησιμοποιηθεί για την κρυπτογράφηση του μηνύματος. Την λύση έρχεται να δώσει μία λέξη κλειδί που βοηθάει στην αποκρυπτογράφηση του μηνύματος.

2.1.9α Μηχανή Vigenere σε λειτουργία

Για να μπορέσουμε να αντιληφθούμε τον τρόπο λειτουργίας της μηχανής, θα δώσουμε ένα παράδειγμα ενός κρυπτογραφημένου μηνύματος. Το μήνυμα που θα κρυπτογραφήσουμε είναι: α γ ά π η. Η λέξη κλειδί που θα μας βοηθήσει σε αυτό θα είναι Λ Ε Υ Κ Ο.

Πλατφόρμα Vigenere

Μήνυμα – Κείμενο : α γ ά π η

Λέξη κλειδί : Λ Ε Υ Κ Ο

Κρυπτογραφημένο : **μθφβχ**

Η διαδικασία ξεκινάει γράφοντας την λέξη κλειδί πάνω από το μήνυμα επαναλαμβάνοντας τόσες φορές τη λέξη κλειδί έως ότου καλυφθεί το μήνυμα που θα αποκρύψουμε. Για παράδειγμα, στην λέξη *ε υ τ υ χ ί α* με κλειδί ΛΕΥΚΟ θα έχουμε ΛΕΥΚΟΛΕ καθώς τα γράμματα της λέξης είναι 7 και του κλειδιού μας 5.

Στην συνέχεια ακολουθούμε με την σειρά τα παρακάτω βήματα:

1. Ξεκινάμε με το πρώτο γράμμα της λέξης μας, το (α).
2. Βρίσκουμε το γράμμα κλειδί που το έχει καλύψει από πάνω, το (Λ), το οποίο μας δείχνει σε ποια σειρά κρυπτογράφησης πρέπει να ψάξουμε.
3. Βρίσκουμε ότι η σειρά που θέλουμε είναι η 11, δηλαδή το αλφάβητο 11.
4. Πηγαίνουμε σε αυτή την σειρά (11), και ψάχνουμε να βρούμε σε ποιο γράμμα τέμνεται κάθετα με τη στήλη, που αρχίζει το γράμμα της λέξης μας, το (α).
5. Μετά κάνουμε αντικατάσταση το αρχικό γράμμα της λέξης μας με αυτό που βρήκαμε, δηλαδή το γράμμα (μ)

Η ίδια διαδικασία επαναλαμβάνεται μέχρι να κωδικοποιηθεί όλο το αρχικό μας μήνυμα. Το κρυπτογράφημα μας δουλεύει αναλογικά καθώς όσο μεγαλύτερη είναι η φράση ή το κείμενο για κρυπτογράφηση, τόσο μεγαλύτερο αριθμό σειρών θα χρησιμοποιήσουμε στην διαδικασία, με αποτέλεσμα να αυξηθεί η πολυπλοκότητα του κρυπτογραφήματος. Στον παραπάνω πίνακα έχουμε τονίσει, με διαφορετικό χρώμα, τις 5 σειρές – αλφάβητα που προσδιορίζονται από τα γράμματα της λέξης κλειδιού που χρησιμοποιήσαμε. (2)

2.1.9β Η ιστορία μιας άσπαστης κρυπτογράφησης

Πως όμως ξεκινάει η ιστορία της κρυπτογράφησης Vigenere; Η αλήθεια είναι ότι, η συγκεκριμένη μορφή κρυπτογράφησης έχει εφευρεθεί εκ νέου πολλές φορές. Η

μέθοδος αρχικά περιγράφεται από τον Giovan Battista Bellaso το 1553, στο βιβλίο του La cifra del. Sig. Giovan Battista Bellaso.

Η πρώτη τεκμηριωμένη πολυαλφαβιτική περιγραφή της κρυπτογράφησης, διατυπώθηκε από τον Leon Battista Alberti γύρω στο 1467, πάνω σε ένα δίσκο από μέταλλο. Αργότερα, ο Johannes Trithemius, το 1508, εφηύρε το tabula Recta, ένα πολύ σημαντικό συστατικό στην Κρυπτογράφηση Vigenere, το οποίο παρουσίασε στο έργο του Poligraphia. Η κρυπτογράφηση Vigenere, είχε αποκτήσει την φήμη ότι είναι εξαιρετικά αδύνατη η αποκρυπτογράφησή της, με το Scientific American, να την αναφέρει ως «αδύνατη της μετάφρασης» το 1917, γεγονός που δεν ίσχυε καθώς το 1854, ο Τσαρλς Μπάμπατζ είχε σπάσει μια παραλλαγή του αλγορίθμου.

Πριν όμως από το κρυπτόγραμμα Vigenere, οι μέθοδοι κρυπτογράφησης ήταν πιο απλές, καθώς χρησιμοποιούσαν μόνο ένα κρυπτογραφικό αλφάβητο για την υποκατάσταση του αρχικού μηνύματος. Σε αντίθεση με τα μονοαλφαβητικά κρυπτογράμματα, το Vigenere επέτρεπε την χρήση περισσότερων αλφάβητων στην υποκατάσταση του αρχικού μηνύματος, πράγμα που έκανε πιο δύσκολη την αποκρυπτογράφησή του. Παρ' όλα αυτά, η μεγάλη πολυπλοκότητα του συστήματος κάνει την διαδικασία αρκετά χρονοβόρα και την χρήση της αρκετά δύσκολη. (2)

Γι' αυτόν λοιπόν το λόγο, έπρεπε να βρεθεί ένα σύστημα το οποίο θα πρόσφερε τόσο ασφάλεια στα μηνύματα όσο και ταχύτητα στην κρυπτογράφηση.

2.1.10 Κρυπτόγραμμα ομοφωνικής αντικατάστασης

Ένα ιδιαίτερα αποτελεσματικό σύστημα ήταν το κρυπτόγραμμα ομοφωνικής υποκατάστασης. Σ' αυτό, κάθε γράμμα αντικαθίσταται από μια ποικιλία υποκατάστατων, των οποίων ο αριθμός είναι ανάλογος με τη συχνότητα εμφάνισης του συγκεκριμένου γράμματος στην γλώσσα που είναι γραμμένο το μήνυμα. (2)

Για παράδειγμα, στην ελληνική γλώσσα το πιο συχνά εμφανιζόμενο γράμμα είναι το Α, με μέση συχνότητα εμφάνισης το 12% περίπου. Έστω ότι ορίζουμε να το εκπροσωπούν 12 σύμβολα, και κάθε φορά που θα εμφανίζεται στο αρχικό μήνυμα θα αντικαθίσταται, με τυχαία σειρά, στο κρυπτογραφημένο κείμενο με 1 από τα 12 σύμβολα. Με την ίδια ακριβώς λογική, το γράμμα Γ το οποίο εμφανίζεται με μέσο ρυθμό 2%, θα έχει 2 σύμβολα να το αντιπροσωπεύουν. Έτσι κάθε φορά που θα

εμφανίζεται το γράμμα Γ στο αρχικό κείμενο θα αντικαθίσταται με 1 από τα 2 εναλλάξ σύμβολα στο κρυπτογραφημένο. Το ίδιο γίνεται για όλα τα γράμματα του αλφάβητου, πάντα χρησιμοποιώντας την ίδια διαδικασία. (2)

Στον πίνακα που ακολουθεί, φαίνεται ένα απλό παράδειγμα ομοφωνικής υποκατάστασης, στον οποίο τα κρυπτογραφικά σύμβολα είναι 99 διψήφιοι αριθμοί, κατανεμημένοι σύμφωνα με την συχνότητα εμφάνισης του κάθε γράμματος. (2)

Α	**Β**	**Γ**	**Δ**	**Ε**	**Ζ**	**Η**	**Θ**	**Ι**	**Κ**	**Λ**	**Μ**	**Ν**	**Ξ**	**Ο**	**Π**	**Ρ**	**Σ**	**Τ**	**Υ**	**Φ**	**Χ**	**Ψ**	**Ω**
94	22	13	68	23	28	11	49	76	55	04	90	61	15	12	20	91	83	75	51	08	38	97	64
53		29		70		19		60	48	98	47	52		77	81	01	84	43	86				
24				73		36		21	67	89	33	69		59	42	18	39	50	92				
16				88				05	07		58	17		27	74	31	45	52	79				
32				93				41				25		09	44	35	72	62					
87				71				57				34		14				64					
96				02				26				06		82				46					
51				30				99				10		80				78					
95														65				85					
03																							
40																							
56																							

Πίνακας 2.: Παρουσίαση ομοφωνικής αντικατάστασης στον πίνακα.

Σύμφωνα λοιπόν με τον παραπάνω πίνακα, παρατηρούμε πως όλοι οι διψήφιοι αριθμοί από κάθε στήλη αντιστοιχούν στο ίδιο γράμμα και εκπροσωπούν τον ίδιο ήχο στο κρυπτογραφημένο κείμενο. Γι’ αυτό το λόγο ονομάστηκε και «ομοφωνική». Με την ύπαρξη πολλών επιλογών για την υποκατάσταση των συχνά εμφανιζόμενων γραμμάτων σκοπεύει στην εξισορρόπηση των συχνοτήτων στο κρυπτογραφημένο κείμενο. Στην περίπτωση που θέλουμε να κρυπτογραφήσουμε ένα κείμενο με κάποιο απλό μονοαλφαβητικό κώδικα, θα ήταν αρκετά εύκολο για

κάποιον κρυπταναλυτή, λαμβάνοντας υπ' όψιν του την συχνότητα εμφάνισης των συμβόλων, να μαντέψει σε ποιο γράμμα αντιστοιχεί κάθε σύμβολο. Στην ομοφωνική κρυπτογράφηση όμως κανένα σύμβολο δεν εμφανίζεται συχνότερα από κάποιο άλλο με αισθητή διαφορά, δημιουργώντας δυσκολίες στην ανάλυση συχνοτήτων. (2)

Το συγκεκριμένο σύστημα θεωρείται αρκετά ισχυρό, αλλά δεν είναι «ανίκητο». Το κρυπτογραφημένο κείμενο εξακολουθεί να περιέχει στοιχεία, τα οποία μπορούν να βοηθήσουν τον κρυπταναλυτή στην λύση του συστήματος και στην επίλυση του κώδικα. Σε αρκετές γλώσσες παρατηρείται ότι κάποια γράμματα εμφανίζονται πιο συχνά όταν συνδυάζονται με άλλα. Για παράδειγμα, στην αγγλική γλώσσα και σε αρκετές ακόμα το γράμμα Q ακολουθείται σχεδόν πάντα από το γράμμα U. Κατά την διαδικασία της αποκρυπτογράφησης παρατηρούμε ότι το γράμμα Q είναι αρκετά «σπάνιο» και γι 'αυτό εκπροσωπείται από μόνο ένα σύμβολο. Αντίστοιχα το γράμμα U έχει συχνότητα εμφάνισης περίπου 3%, δηλαδή αν το σύνολο των συμβόλων είναι 100 τότε μπορούμε να υποθέσουμε ότι το συγκεκριμένο γράμμα το εκπροσωπούν 3 διαφορετικά σύμβολα. Επομένως, αν εντοπίσουμε ένα μοναδικό σύμβολο το οποίο ακολουθείται από 3 διαφορετικά σύμβολα, μπορούμε να υποθέσουμε ότι το αρχικό σύμβολο είναι το Q, ενώ τα άλλα 3 το γράμμα U. Η ίδια διαδικασία συμβαίνει και με τα υπόλοιπα γράμματα τα οποία γίνονται αντιληπτά από τις «σχέσεις» τους με τα άλλα γράμματα. (2)

Παρά το γεγονός ότι ένα ομοφωνικό σύστημα έχει αρκετές ομοιότητες με ένα πολυαλφαβητικό, καθώς κάθε γράμμα μπορεί να αντικατασταθεί με περισσότερους από έναν τρόπους, υπάρχει μία καίρια διαφορά που κάνει το ομοφωνικό κρυπτόγραμμα να θεωρείται ένας τύπος μονοαλφαβητικού συστήματος. Για παράδειγμα, σύμφωνα με τον παραπάνω πίνακα, το γράμμα Ε μπορεί να εκπροσωπείται από 8 αριθμούς, όμως κάθε αριθμός αντιστοιχεί μόνο σε αυτό το γράμμα. Γενικότερα, ένα γράμμα του αρχικού κειμένου μπορεί να εκπροσωπείται με περισσότερα από 1 σύμβολα, αλλά το κάθε σύμβολο αντιστοιχεί σε ένα μοναδικό γράμμα, σε αντίθεση με την πολυαλφαβητική μέθοδο στην οποία ένα σύμβολο μπορεί να αντιστοιχεί σε πολλά διαφορετικά γράμματα του αρχικού. Επιπλέον, η σταθερότητα είναι ένα χαρακτηριστικό που διαφαίνεται καθαρά στο κρυπτογραφικό αλφάβητο καθώς παραμένει ίδιο καθ' όλη την διάδικασία της κρυπτογράφησης, σε αντίθεση με πολυαλφαβητική όπου ο κρυπτογράφος πρέπει

συνεχώς να χρησιμοποιεί διαρκώς διαφορετικά αλφάβητα, σύμφωνα πάντα με μία λέξη- κλειδί. (2)

2.1.11 Το «Μεγάλο Κρυπτόγραμμα» του Λουδοβίκου ΙΔ'

Η μονοαλφαβητική κρυπτογράφηση είχε αρκετές παραλλαγμένες μορφές με χαρακτηριστικό παράδειγμα εκείνης της εποχής το «Μεγάλο Κρυπτόγραμμα» του Λουδοβίκου ΙΔ'. Η συγκεκριμένη μορφή κρυπτογράφηση είχε ως σκοπό να διατηρήσει ασφαλή και απόρρητα τα μηνύματα του βασιλιά, τα οποία είχαν στοιχεία για τα σχέδια του, τις δολοπλοκίες του και τις πολιτικές του κινήσεις.

Δημιουργοί του Μεγάλου Κρυπτογραφήματος ήταν οι Αντουάν και Μποναβεντίρ Ροσινιόλ. Ο Αντουάν, πατέρας του Μποναβεντίρ, διακρίθηκε για πρώτη φορά το 1626 καθώς κατάφερε να αποκρυπτογραφήσει μια επιστολή, οδηγώντας τη Γαλλία σε μια άκοπη νίκη απέναντι στους Ουγενότους. Το κατόρθωμα του αυτό αναγνωρίστηκε και οι Ροσινιόλ διορίστηκαν σε υψηλά αξιώματα, παίζοντας κεντρικό ρόλο στην διαμόρφωση της διπλωματικής πολιτικής της Γαλλίας. Οι επιτυχίες τους στην αποκρυπτογράφηση τους ώθησε ώστε να δημιουργήσουν το δικό τους κρυπτογραφικό σύστημα. Έτσι εμπνεύστηκαν το Μεγάλο Κρυπτόγραμμα, το οποίο αποτέλεσε πρόκληση για' τους εχθρούς της εποχής, αλλά και για τους ιστορικούς. (2)

Οι ιστορικοί γνώριζαν την τεράστια ιστορική αξία των κρυπτογραφημένων μηνυμάτων, καθώς, αν τα αποκρυπτογραφούσαν θα αποκάλυπταν όλα τα σημαντικά γεγονότα εκείνης της εποχής. Πέρασε αρκετός καιρός μέχρι το κρυπτόγραμμα να αποκαλύψει τα μυστικά του στα τέλη του 19^{ου} αιώνα, όταν ο Ετιέν Μπαζερί κατάφερε να σπάσει τον μέχρι τότε ανίκητο κώδικα. Η πρώτη ανάλυση έδειξε πως το κρυπτογράφημα περιείχε χιλιάδες αριθμούς, αλλά μόνο οι 587 ήταν διαφορετικοί. Η πρώτη σκέψη του Μπάζερι ήταν πως είχε να αντιμετωπίσει έναν ομοφωνικό κώδικα, όμως η υπόθεση και οι προσπάθειές του ήταν λάθος. Στην συνέχεια υπέθεσε πως σε κάθε αριθμό αντιστοιχεί ένα ζευγάρι γραμμάτων, σύμφωνα με τις συχνότητες εμφάνισης των αριθμών στο κκρυπτόγραμμα. Και πάλι όμως οι προσπάθειες του δεν απέδωσαν. Στο τέλος, λίγο πριν παρατήσει αυτήν την προσπάθεια σκέφτηκε να εφαρμόσει κάτι άλλο. Υπέθεσε πως κάθε αριθμός αντιστοιχεί σε μία ολόκληρη συλλαβή. Μετά από κάποιες προσπάθειες, επιχείρησε να ταιριάξει έναν πολύ συχνό συνδυασμό με τις

συλλαβές “les-en-nemi-s” το οποίο σημαίνει «εχθροί». Αυτή η προσπάθεια απέδωσε αμέσως, και έτσι αντικαθιστώντας κάθε συλλαβή, το κείμενο άρχισε να αποκαλύπτεται. Η αποκρυπτογράφηση του Μεγάλου Κρυπτογράμματος ήταν τεράστιας σημασίας για τους ιστορικούς, καθώς αποκαλύφθηκε ένα τεράστιο κομμάτι της ιστορίας το οποίο είχε παραμείνει σκοτεινό για αρκετούς αιώνες. (2)

2.1.12 Η Διαφορική μηχανή του Μπάμπατζ

Στις αρχές της δεκαετίας του 1820, ο Μπάμπατζ δούλευε πάνω σ’ ένα πρωτότυπο της πρώτης διαφορικής μηχανής του. Η διαφορική μηχανή ήταν μια αυτόματη μηχανική αριθμομιχανή η οποία ήταν σχεδιασμένη να συνοψίζει πολυωνυμικές συναρτήσεις. Τόσο οι λογαριθμικές όσο και οι τριγωνομετρικές συναρτήσεις μπορούν να προσεγγισθούν με πολυώνυμα, έτσι και η αναλυτική μηχανή μπορεί να υπολογίσει πολλά χρήσιμα σύνολα αριθμών. Η δια φορική μηχανή ήταν σχεδιασμένη να κάνει πρόσθεση, αφαίρεση πολλαπλασιασμό και διαίρεση με ακρίβεια 6 δεκαδικών ψηφίων. Η μηχανή παρέμεινε ατελής, και το μέρος που συμπληρώθηκε βρίσκεται στο Μουσείο Επιστημών στο Λονδίνο. Η πρώτη διαφορική μηχανή αποτελούταν από περίπου από 25.000 κομμάτια, τα οποία ζύγιζαν 13.600 κιλά και είχαν 2.4 μέτρα ύψος περίπου. Παρότι υπήρξε χρηματοδότηση για την κατασκευή της μηχανής, εκείνη δεν ολοκληρώθηκε ποτέ.

2.1.13 Η Αναλυτική Μηχανή του Μπάμπατζ (1822)

Ο 19^{ος} αιώνας μπορεί να χαρακτηριστεί ως ο αιώνας του ατμού, καθώς οι περισσότερες μηχανές που είχαν εφευρεθεί λειτουργούσαν αυτόματα με ατμό. Μετά την ματαίωση της προσπάθειας για την κατασκευή της διαφορικής μηχανής, ο Μπάμπατζ άρχισε να σχεδιάζει μια διαφορετική και ακόμα πιο πολύπλοκη μηχανή, η οποία θα χρησιμοποιούταν για την εκτέλεση υπολογισμών και θα λειτουργούσε αυτόματα με ατμό. Η κατασκευή αυτή ονομάστηκε Αναλυτική μηχανή και αποτέλεσε μια διαδοχή από σχέδια, τα οποία συνέχισε να τροποποιεί μέχρι τον θάνατό του ο Μπάμπατζ, το 1871. Μεταξύ των δυο μηχανών του Μπάμπατζ υπήρχε μια βασική διαφορά, η οποία ήταν πως η «νέα» μηχανή (αναλυτική), μπορούσε να προγραμματιστεί χρησιμοποιώντας Διατρητές κάρτες, τεχνική η οποία χρησιμοποιείται ακόμα και σήμερα. Με αυτόν τον τρόπο

λειτουργίας, ο Μπάμπατζ μπορούσε να αποθηκεύει προγράμματα σε αυτές τις κάρτες έτσι ώστε ο χρήστης να μπορούσε να δημιουργήσει το πρόγραμμα μόνο μια φορά και με την βοήθεια της κάρτας να το «τρέχει» ξανά και ξανά. Αυτή η μηχανή προοριζόταν να έχει αρκετά από τα χαρακτηριστικά ενός σύγχρονου υπολογιστή, όπως ο έλεγχος κατά ακολουθίες (sequential control), η διακλάδωση (branching) και οι βρόχοι (looping). Οι ιδέες όμως ήταν πολύ πρωτοποριακές, καθώς η τεχνολογία της εποχής υστερούσε κατά πολύ. Γι αυτό λοιπόν, η αναλυτική μηχανή δεν κατασκευάστηκε ποτέ, και έμεινε στην θεωρία παρά τις φιλόδοξες προσπάθειες του δημιουργού της.

2.2 Δεύτερη Περίοδος Κρυπτογραφίας (1900 μ.Χ - 1950 μ.Χ)

Στις αρχές του 20^{ου} αιώνα ξεκινά η δεύτερη περίοδος της Κρυπτογραφίας και ολοκληρώνεται το 1950 μ.Χ. Τοποθετείται στο διάστημα μεταξύ των δύο παγκοσμίων πολέμων και εξαιτίας αυτών (για μεγαλύτερη ασφάλεια πληροφοριών και μετάδοσης μηνυμάτων μεταξύ των στρατευμάτων), έγινε επιτακτική ανάγκη η ανάπτυξη της κρυπτογραφίας πιο πολύ από κάθε άλλη περίοδο στην ιστορία. Την ίδια περίοδο η εισαγωγή των μηχανικών και των ηλεκτρομηχανικών κατασκευών σε συνδυασμό με την πολυπλοκότητα των συστημάτων δημιουργούν ένα νέο τομέα στα κρυπτοσυστήματα, τις λεγόμενες «κρυπτομηχανές». Η διαδικασία της κρυπτανάλυσής τους ήταν ένα κομμάτι δύσκολο και χρονοβόρο, καθώς χρειάζονταν μεγάλο αριθμό προσωπικού και μεγάλη υπολογιστική δύναμη. Κατά τη διάρκεια της συγκεκριμένης περιόδου, η κρυπτανάλυση των συστημάτων ήταν επιτυχημένη, παρά τον μεγάλο βαθμό πολυπλοκότητας που είχε αναπτυχθεί. Παράλληλα λοιπόν με την ανάπτυξη των συστημάτων κρυπτογράφησης είχαμε την άνθηση των τεχνικών αποκρυπτογράφησης και κρυπτανάλυσης ώστε καμία συσκευή ή αλγόριθμος να μην μπορεί να θεωρηθεί απολύτως ασφαλής. Κατά την περίοδο των παγκοσμίων πολέμων παρουσιάστηκε και χρησιμοποιήθηκαν αρκετά κρυπτογραφικά συστήματα αλλά και κώδικες. (1)

2.2.1 Κώδικας Zimmermann

Το 1917 η Γερμανία απέστειλε μία διπλωματική πρόταση, σχετικά με τον κώδικα Zimmermann, προς το Μεξικό προκειμένου να κηρύξει τον πόλεμο κατά των Ηνωμένων Πολιτειών της Αμερικής. Το κωδικοποιημένο τηλεγράφημα, το οποίο στάλθηκε από τον ίδιο τον Arthur Zimmermann, είχε ως σκοπό τον αποπροσανατολισμό των Αμερικάνων από τον πόλεμο στην Γηραιά Ήπειρο και την συμμαχία μεταξύ Γερμανίας και Ιαπωνίας. Για να μπορέσουν να επιτύχουν την συμμαχία με τους Μεξικάνους, τους υποσχέθηκαν τις πολιτείες του Τέξας, του Νέο Μέξικο και της Αριζόνα. Από την άλλη πλευρά όμως, η Κυβέρνηση του Μεξικό, ξέροντας τις δυσκολίες σύγκρουσης με τις πανίσχυρες Η.Π.Α. αγνόησε την γερμανική πρόταση και τελικά την απέρριψε όταν αυτές εισήλθαν στον πόλεμο. (2)

2.2.2. Λόγοι απόρριψης της γερμανικής πρότασης

Μετά το τέλος της μελέτης για ανακατάληψη των πρώην εδαφών του Μεξικό, έπειτα από εντολή του τότε πρωθυπουργού της χώρας Venustiano Carranza, αποφασίστηκε ότι κάτι τέτοιο δεν ήταν εφικτό για τους εξής λόγους:

- Η ανακατάληψη των περιοχών συνδέονταν άμεσα σε πόλεμο με τις πολύ ισχυρές για την εποχή στρατιωτικές δυνάμεις των Η.Π.Α.
- Επιπλέον, η πιθανή γερμανική βοήθεια προς το Μεξικό ήταν αβέβαιη καθώς οι προμήθειες όπλων της χώρας γίνονταν από τις Η.Π.Α, ενώ οποιοσδήποτε άλλος «δρόμος» για προμήθειες ήταν κλειστός από συμμάχους των Η.Π.Α..
- Ένας ακόμα λόγος, σε περίπτωση νίκης των Μεξικανών, ήταν ο δύσκολος τρόπος διακυβέρνησης των περιοχών καθώς απαρτίζονταν από πολλούς αγγλόφωνους πολίτες και είχαν διαφορετική κουλτούρα, γλώσσα και πολιτισμό. Αυτό σε συνδυασμό με τον οπλισμό των περισσότερων πολιτών έκανε ακόμα πιο εύκολη την απόρριψη της πρότασης.
- Τέλος, αν το Μεξικό επιτίθονταν στις Η.Π.Α. θα ερχόταν σε σύγκρουση και με άλλες δυνάμεις της περιοχής όπως η Βραζιλία, η Αργεντινή και η Χιλή καθώς είχε συνάψει συνθήκη για την αποκατάσταση της ηρεμία στην περιοχή.

2.2.3 Αποκρυπτογράφηση του κώδικα Zimmermann

Σύμφωνα με την επικρατέστερη άποψη το τηλεγράφημα δεν μπορούσε να μεταφερθεί αμέσως στο Μεξικό, επειδή οι Βρετανοί είχαν κόψει τις γερμανικές υπερατλαντικές γραμμές. Παρόλα αυτά όμως, οι γερμανοί κατείχαν κάποιες από τις γραμμές για διπλωματικούς και μόνο σκοπούς, τις οποίες τις είχαν παραχωρήσει οι αμερικάνοι, δεδομένου ότι δεν θα δέχονταν κρυπτογραφημένα - κωδικοποιημένα μηνύματα. Η κίνηση αυτή όμως των αμερικάνων, ήθελαν να διατηρήσουν καλές σχέσεις με του γερμανούς προσπαθώντας παράλληλα να τους πείσουν να σταματήσει αυτός ο καταστροφικός πόλεμος. (2)

Επειδή όμως, ο κώδικας δεν μπορούσε να αποσταλεί χωρίς κρυπτογράφηση, οι γερμανοί ζήτησαν μια εξαίρεση για την μεταφορά του μέσω των υπερατλαντικών γραμμών, οι οποίες περνούσαν από βρετανικό έδαφος, και συγκεκριμένα από το κέντρο της βρετανικής αποκρυπτογράφησης, το γνωστό «Δωμάτιο 40». Ο χώρος αυτός, αποτέλεσε σημαντικό στοιχείο και έπαιξε καθοριστικό ρόλο στη έκβαση του πολέμου καθώς οι ικανοί γλωσσολόγοι και αναλυτές μπορούσαν να αποκρυπτογραφήσουν αρκετά μηνύματα. Αξίζει να σημειωθεί ότι, ο Nigel de Grey και ο Μοντγκόμερι κατάφεραν μια μέρα μετά την μεταβίβαση του τηλεγραφήματος να αποκρυπτογραφήσουν μερικώς τον κώδικα.

Ο αρχηγός του «Δωματίου 40», Στρατηγός Hall, θέλοντας να αποκαλύψει το κωδικοποιημένο μήνυμα του τηλεγραφήματος περίμενε για τρεις βδομάδες μέχρι την πλήρη κρυπτογράφηση του για να σταματήσει η φιλική στάση των αμερικάνων προς τους γερμανούς.

Μετά την αποκρυπτογράφηση του κώδικα, το τηλεγράφημα δόθηκε στην δημοσιότητα παραλλαγμένο ως προς τις οδηγίες και την διεύθυνση παραλήπτη, έτσι ώστε να μην γίνει αντιληπτή η παρακολούθηση των αμερικανικών γραμμών από τους Βρετανούς και οι γερμανοί να θεωρήσουν ότι κλάπηκε από την Πρεσβεία στο Μεξικό και όχι ότι το αποκρυπτογράφησαν οι Βρετανοί. Με αυτό λοιπόν τον τρόπο, ο τηλεγράφημα διαδόθηκε παντού μέσω του Τύπου και έγινε ευρέως γνωτές οι προθέσεις των Γερμανών. (2)

2.2.4 Το Κρυπτογραφικό σύστημα Enigma

Η μηχανή Enigma (Αίνιγμα) ανακαλύφθηκε από τον Γερμανό μηχανικό Arthur Scherbius κατά το τέλος του Πρώτου Παγκοσμίου Πολέμου. Πρόκειται για μια οικογένεια ηλεκτρομηχανολογικών μηχανών, που χρησιμοποιούνται για την κρυπτογράφηση και αποκρυπτογράφηση μηνυμάτων. Τα πρώτα μοντέλα χρησιμοποιήθηκαν κυρίως για εμπορικούς σκοπούς, όμως μετά την έγκρισή τους, στις αρχές του 1920, χρησιμοποιήθηκαν για στρατιωτικούς σκοπούς από την Ναζιστική Γερμανία, πριν και κατά την διάρκεια του 2^{ου} Παγκοσμίου Πολέμου. Όπως προαναφέρθηκε, καμία συσκευή κρυπτογράφησης δεν ήταν άτρωτη σε επιθέσεις κρυπτανάλυσης κι έτσι το Δεκέμβριο του 1932, η μυστική υπηρεσία της Πολωνίας, και συγκεκριμένα ο Πολωνός Marian Rojewski, κατάφερε να σπάσει τους αλγορίθμους κρυπτογράφησης της Γερμανίας, αποτελώντας το μεγαλύτερο επίτευγμα της εποχής, αναφορικά με το πεδίο της κρυπτανάλυσης. Οι Πολωνοί συνέχισαν να αποκρυπτογραφούν τα μηνύματα του συστήματος Enigma μέχρι και το 1939. (3)

Γι' αυτό ακριβώς τον λόγο, ο γερμανικός στρατός προχώρησε σε σημαντικές αλλαγές του συστήματος enigma, και έτσι διέκοψαν την παρακολούθηση των μηνυμάτων τους από τους Πολωνούς, καθώς δεν διέθεταν τους απαραίτητους πόρους για την αποκρυπτογράφησή τους. Για να μπορέσουν να παρακολουθήσουν τις αλλαγές στο σύστημα αίνιγμα, οι Πολωνοί συνεργάστηκαν με τους Γάλλους και τους Βρετανούς, μεταβιβάζοντας τις γνώσεις τους και τον εξοπλισμό τους. Σημαντικές συνεργασίες έγιναν αυτήν την περίοδο μεταξύ κορυφαίων μαθηματικών και κρυπτογράφων, όπως οι Rejewski, Biuro Szyfrow, Άλαν Τούρινγκ (Alan Turing), Γκόρντον Ουέλτσμαν (Gordon Welchman) και άλλοι, οι οποίοι κατάφεραν να αποκρυπτογραφήσουν διάφορες παραλλαγές του συστήματος enigma, με την βοήθεια ενός Βρετανικού υπολογιστή, ο οποίος ονομαζόταν Colossus. Οι κρυπτογράφοι του αμερικανικού ναυτικού (σε συνεργασία με Βρετανούς και Ολλανδούς κρυπτογράφους μετά από το 1940) κατάφεραν και «έσπασαν» αρκετά κρυπτοσυστήματα του Ιαπωνικού ναυτικού. Η αποκρυπτογράφηση ενός κρυπτογραφικού συστήματος, του JN-25 οδήγησε στην αμερικανική νίκη στη Ναυμαχία της Μιντγουέι καθώς και στην εξόντωση του Αρχηγού του Ιαπωνικού Στόλου, Ιζορόκου Γιαμαμότο. (2)

Το Ιαπωνικό Υπουργείο Εξωτερικών χρησιμοποίησε ένα τοπικά αναπτυγμένο κρυπτογραφικό σύστημα, με όνομα Purple, καθώς επίσης και διάφορες μηχανές που βοήθησαν στις συνδέσεις μεταξύ των ιαπωνικών πρεσβειών. Όμως το ασφαλέστερο ιαπωνικό διπλωματικό κρυπτοσύστημα Purple, κατάφερε να αποκρυπτογραφηθεί από μια αμερικανική στρατιωτική ομάδα , αποκαλούμενη SIS πριν ακόμα αρχίσει ο $2^{ος}$ Παγκόσμιος Πόλεμος. Το αποτέλεσμα της κρυπτανάλυσης του συστήματος Purple, ονομάστηκε από του Αμερικάνους ως Magic, δηλαδή μαγεία.

Κατά την διάρκεια του δεύτερου Παγκοσμίου πολέμου, τα ηλεκτρομηχανικά σχέδια που χρησιμοποιήθηκαν στις συμμαχικές κρυπτομηχανές ήταν το βρετανικό TypeX και το Αμερικανικό SIGABA. Και τα δύο σχέδια ήταν παρόμοια στο πνεύμα με το Enigma, με σημαντικές βελτιώσεις, οι οποίες βοήθησαν στην διατήρηση των μυστικών πληροφοριών τους. (3) (4)

2.2.5 Περιγραφή λειτουργίας της μηχανής Enigma

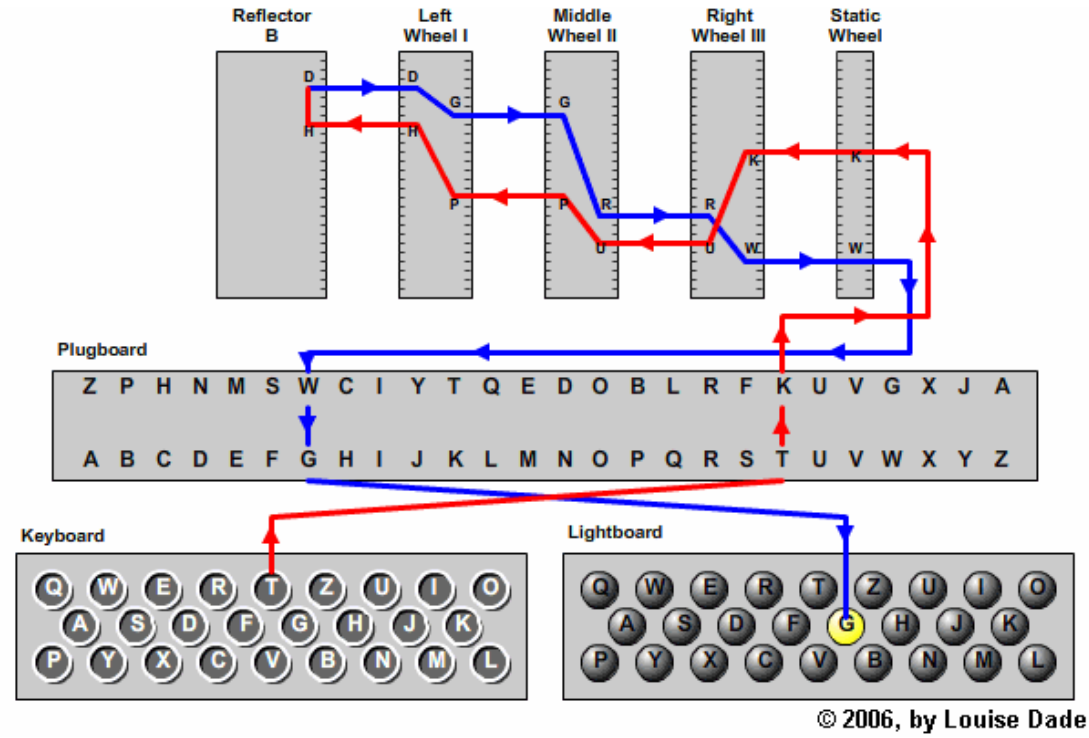
Ηλεκτρικές διαδρομές

Η μηχανή λειτουργούσε από ένα μεταβαλλόμενο ηλεκτρικό κύκλωμα το οποία σχηματιζόταν από την κίνηση των μηχανικών μερών της. Συγκεκριμένα, όταν πατηθεί ένα πλήκτρο τότε ένα κύκλωμα θα ολοκληρώνονταν με ρεύμα το οποίο θα έρρεε μέσω τον διάφορων συστατικών τα οποία ήταν σε σταθερή διάταξη και θα είχε ως αποτέλεσμα να ανάψει μια λάμπα, το οποίο θα υποδείκνυε την επιστολή εξόδου. Για παράδειγμα, ένας αποστολέας προσπαθεί να κρυπτογραφήσει ένα μήνυμα εκκίνησης τύπου ANX. Ο χειριστής θα πατήσει πρώτα το γράμμα A στην μηχανή, αλλά ο λαμπτήρας που θα ανάψει θα είναι το Z, έτσι ώστε το Z να είναι το πρώτο γράμμα του κειμένου αποκρυπτογράφησης. Ακολουθώντας ακριβώς την ίδια διαδικασία και για τα άλλα γράμματα (N,X) θα δημιουργήσουν πολλαπλές ηλεκτρικές διαδρομές μέσα από την μηχανή, ονομάζοντας αυτήν την διαδικασία ως πολυαλφαβητική κρυπτογράφηση αντικατάστασης ή αλλιώς scrambler enigma. Αξίζει να σημειωθεί ότι αυτή η τεχνική παρείχε υψηλή ασφάλεια στην μηχανή και στα μηνύματα. (4)

Στροφείς

Όπως οι περισσότερες μηχανές της εποχής, έτσι και η Αίνιγμα χρησιμοποιούσε ρότορες, δηλαδή τροχούς που αποτελούσαν την καρδιά του συστήματος. Κάθε δίσκος του συστήματος είχε διάμετρο 10 εκατοστών και ήταν κατασκευασμένα είτε από σκληρό πλαστικό είτε από επένδυση υψηλής πίεσης - βακελίτη με ελατήριο ορειχάλκινων πείρων στην μία όψη με διάταξη κύκλου. Ομοίως και στην άλλη πλευρά της μηχανής υπάρχουν ισάριθμες ηλεκτρικές επαφές. Οι ακίδες και οι επαφές αντιπροσωπεύουν το αλφάβητο, δηλαδή τα 26 γράμματα από A-Z. Όταν οι δρομείς τοποθετήθηκαν δίπλα-δίπλα επί της ατράκτου, οι πείροι του ενός υδραυλικού κυλίνδρου περιστροφής-ανάπαυσης κατά τις επαφές του με το γειτονικό υδραυλικό κύλινδρο δημιουργούν μία ηλεκτρική σύνδεση. Μέσα στον υδραυλικό κύλινδρο, τα 26 σύρματα που συνδέουν κάθε ακίδα με μία ξεχωριστή επαφή, δημιουργώντας έτσι ένα πολύπλοκο μοτίβο. Το πιο σύνηθες μοτίβο που βρέθηκε ήταν σε ρωμαϊκό ρυθμό. (4)

Είναι αρκετά απλό να δημιουργήσουμε έναν απλό τύπο κρυπτογράφησης με μία κρυπτογράφηση αντικατάστασης. Για παράδειγμα, ας δούμε την πορεία όταν πληκτρολογούμε το γράμμα **T** και ανάβει η λυχνία του γράμματος **G** έτσι ώστε να δούμε τις επιμέρους λειτουργίες των επι μέρους εξαρτημάτων της μηχανής. (4)



Σχήμα 2.: Τρόπος λειτουργίας εσωτερικών εξαρτημάτων της μηχανής Enigma

Όταν ο χρήστης πατήσει το γράμμα Τ δημιουργείται ένα ηλεκτρικό σήμα το οποίο δείχνει την διαδρομή που ακολούθησε όταν ανάψει κάποια λυχνία μέσα στον πίνακα όπου είναι και το τέλος της διαδρομής του.

Όπως φαίνεται και από την εικόνα, η πρώτη στάση έπειτα από την πληκτρολόγησή του γράμματος **T** είναι στο plugboard ή αλλιώς πίνακα βυσμάτων. Η διαδικασία που εκτελείται σε αυτό το σημείο είναι πολύ απλή. Ουσιαστικά ο πίνακας εκτρέπει το σήμα από το γράμμα **T** σε μία διαφορετική διαδρομή προς ένα άλλο γράμμα. Θα μπορούσαμε να παρομοιάσουμε την διαδικασία αυτήν με την λειτουργία ενός αναλογικού τηλεφωνικού κέντρου όπου συνδέουμε διαφορετικά βύσματα για να δημιουργήσουμε επικοινωνία. Πλέον μετά την αντιστοίχιση το γράμμα μας είναι το **K.** (4)

Υπάρχουν πέντε δίσκοι που μπορούν να χρησιμοποιηθούν με οποιαδήποτε σειρά στους τρείς αναδιατάκτες που φαίνονται στο σχήμα: δεξιός (**Right Wheel III**) μεσαίος (**Middle Wheel II**) και αριστερός (**Left Wheel I**).

Ο κάθε αναδιατάκτης φέρει έναν περιστρεφόμενο δίσκο στην δεξιά πλευρά του στροφείου (εξωτερικός) και έναν σταθερό στην αριστερή πλευρά του στροφείου (εσωτερικός) με σκοπό την αλλαγή διαδρομής του σήματος.

Οι επαφές του εξωτερικού δίσκου, όποια και να είναι η ρύθμισή του, ενώνουν τους αναδιατάκτες μεταξύ τους καθώς επίσης με τον σταθερό δίσκο (staticrotor) με τον ανακλαστήρα (Reflector) και με τον εσωτερικό δίσκο του ιδίου αναδιατάκτη. (4)

Ο εσωτερικός δίσκος μπορεί να περιστρεφέται σε σχέση με τον εξωτερικό, κάτι το οποίο έχει ως αποτέλεσμα επιπλέον εφικτές συνδέσεις και κατά συνέπεια περισσότερες αντικαταστάσεις γραμμάτων. (4)

Οι δύο δίσκοι (εσωτερικός και εξωτερικός) αποτελούν ένα στροφείο ή αναδιατάκτη ο οποίος μπορεί να περιστρέφεται σε σχέση με τον στατικό δίσκο ώστε η έξοδος Α του στατικού δίσκου να μην αντιστοιχεί στην είσοδο Α του περιστρεφόμενου δακτυλίου. (4)

Επιπλέον, για κάθε εισερχόμενο γράμμα οι δίσκοι περιστρέφονται κατά μία θέση (1/26, καθώς φέρουν 26 δυνατές ρυθμίσεις, μία για κάθε γράμμα) έτσι ώστε τα ίδια γράμματα να μη συνδέονται με τα ίδια κρυπτογράμματα στο ίδιο μήνυμα. Ο κάθε

δίσκος φέρει εγκοπές (βλ. τον αριθμό 8 στο παρακάτω σχεδιάγραμμα) σε διαφορετικά σημεία από τους άλλους, στις οποίες όταν φτάσει με τις περιστροφικές αλλαγές θέσεων για κάθε εισερχόμενο γράμμα, συμπαρασύρει σε κίνηση τον επόμενο δίσκο στα αριστερά του. Ο μεσαίος δίσκος προκαλεί την κίνηση σε αυτόν που βρίσκεται αριστερά του ενώ παράλληλα η δική του συνεχίζεται. (4)

Τα στροφεία μπορούσαν να τοποθετηθούν όλα ή μεμονωμένα και με οποιαδήποτε σειρά : 123, 132, 213, 231, 312, 321

Αν η μηχανή είχε έναν στροφέα τότε το 27ο γράμμα που θα εισερχόταν θα είχε το ίδιο αποτέλεσμα με το 1ο αφού ο στροφέας θα είχε επιστρέψει στην αρχική του θέση μετά από μία πλήρη περιστροφή. Οι 26 αναδιατάξεις θα ήταν μεγάλη αδυναμία της μηχανής και για τον λόγο αυτόν τοποθετήθηκε δεύτερος στροφέας ανεβάζοντας τις δυνατότητες σε 676 (26Χ26) και στην συνέχεια μέχρι να φθάσουμε στο αρχικό μοντέλο, προστέθηκε τρίτος, ανεβάζοντας τον πήχη στα 17.576 (26χ26χ26) κρυπτογραφημένα αλφάβητα. Αργότερα έγιναν περαιτέρω προσθήκες στροφείων με τις πιθανότητες να εκτινάσσονται σε αστρονομικά ύψη.

Ανακλαστήρας – Reflector

Ο ανακλαστήρας λαμβάνει το σήμα στην είσοδό του και το στέλνει πίσω στους αναδιατάκτες. Υπάρχουν δύο πιθανοί ανακλαστήρες, ο καθένας από τους οποίους είναι διαφορετικά καλωδιωμένος ώστε το γράμμα εισόδου να μετατρέπεται σε διαφορετικό γράμμα όταν ανακλάται. Στο δικό μας παράδειγμα χρησιμοποιούμε τον ανακλαστήρα B (reflector B) ο οποίος το γράμμα εισόδου **H** το μετατρέπει σε **D**. (4)

Είναι πολύ σημαντικό το σήμα να εκτρέπεται όταν ανακλάται και επιστρέφει καθώς η μηχανή είναι αμφίδρομα σχεδιασμένη έτσι ώστε όταν εισάγεις κρυπτογράφημα να παίρνεις το κείμενο προς κρυπτογράφηση. Αν ο ανακλαστήρας δεν άλλαζε το γράμμα τότε αυτό θα επέστρεφε στην μορφή που εισήχθη. (4)

Το ταξίδι της επιστροφής

Το σήμα καθώς ανακλάται περνά από τους αναδιατάκτες οι οποίοι εργάζονται με τον ίδιο τρόπο αλλά με αντίθετη φορά. Έτσι το γράμμα μας **D** περνά από τον αριστερό δίσκο και γίνεται **G** το οποίο περνά από τον μεσαίο δίσκο και γίνεται **R** το οποίο περνά από τον δεξί δίσκο και γίνεται **W**. Το σήμα παραμένει ίδιο καθώς περνά από τον στατικό δίσκο ξανά για να φθάσει στον πίνακα βυσμάτων όπου και πάλι δεν θα αλλάξει αν δεν έχουμε επιλέξει κάτι τέτοιο που θα αντιστοιχούσε το γράμμα **W** με κάποιο άλλο. Το δικό μας **W** έχει αντιστοιχηθεί με το **G** οπότε και στον πίνακα βυσμάτων η έξοδος είναι **G**. (4)

Πίνακας λυχνιών – Lampboard

Η τελευταία στάση είναι ο πίνακας λυχνιών όπου ο πίνακας βυσμάτων είναι συνδεδεμένος με την λυχνία που αντιστοιχεί σε αυτό το γράμμα. Στο παράδειγμά μας ανάβει το γράμμα **G**, που σημαίνει ότι το προς κρυπτογράφηση **T** έγινε **G**.

Ο κρυπτογράφος έπρεπε να σημειώνει το κάθε γράμμα που άναβε στον πίνακα λυχνιών έως ότου ολοκληρωθεί το μήνυμα προς αποστολή. Στη συνέχεια, έστελνε το σύνολο των ακατανόητων γραμμάτων με κώδικα Μόρς.

Ο κρυπταναλυτής που θα λάμβανε το μήνυμα έπρεπε να έχει την αντίστοιχη μηχανή με τις ίδιες εσωτερικές καλωδιώσεις στα στροφεία. Στην συνέχεια όφειλε να γνωρίζει πόσα στροφεία θα τοποθετήσει, με ποια σειρά και ποια θα είναι η αρχική τους ρύθμιση. (4)

Αυτές οι ρυθμίσεις της εγκατάστασης ήταν αρχειοθετημένες στην διάθεση αμφότερων των εμπλεκομένων.

2.2.6 Η ιστορία της μηχανής

2.2.6.α.Η Εμπορική μηχανή Enigma

Στην οικογένεια Αίνιγμα (Enigma) ανήκουν αρκετές μηχανές, διαφορετικές μεταξύ τους σχεδιαστικά αλλά και τεχνικά. Οι πρώτες μηχανές ήταν εμπορικά μοντέλα που ξεκίνησαν στις αρχές τις δεκαετίας του 1920. Στα μέσα της ίδιας δεκαετίας οι

Γερμανοί προσπάθησαν να "στρατολογήσουν" την μηχανή, δημιουργώντας διάφορες παραλλαγές της με σκοπό την βελτίωση σε θέματα ασφάλειας.

Στις 23 Φεβρουαρίου 1918, ο Γερμανός μηχανικός Arthur Scherbius σε συνεργασία με τον RIchard E. Ritter ιδρύουν την δική τους εταιρεία μηχανών με ονομασία Scherdius & Ritter. Την ίδια εποχή, πλησίασαν το γερμανικό ναυτικό και το Υπουργείο Εξωτερικών για να τους παρουσιάσουν την δική τους πρόταση, αλλά κανένας από τους δύο δεν έδειξε ιδιαίτερο ενδιαφέρον με αποτέλεσμα να αναθέσουν τα δικαιώματα ευρεσιτεχνίας στον Gewerkschaft Securitas, ο οποίος μετέπειτα, στις 9 Ιουλίου του 1923,ίδρυσε την δική του εταιρεία με ονομασία Chiffriermaschinen Aktien-Gesellschaft. Η Chiffriermaschinen AG, έχοντας στο διοικητικό της συμβούλιο τους Scherdius και Ritter, άρχισε να διαφημίζει την μηχανή Enigma A, η οποία παρουσιάστηκε στο συνέδριο της Διεθνούς Ταχυδρομικής Ένωσης το 1923 -1924. Τα τεχνικά χαρακτηριστικά του μοντέλου σε αριθμητικά δεδομένα ήταν 65 x 45 x 35 εκατοστά και ζύγιζε περίπου 50 κιλά (110 λίβρες) με ενσωματωμένη γραφομηχανή.

Το 1925 στην οικογένεια Αίνιγμα προστέθηκε το Enigma B, η οποία δεν απείχε πολύ από το προηγούμενο μοντέλο καθώς ήταν παρόμοια σε μέγεθος και κατασκευή. Και τα Δύο μοντέλα A και B παρουσιάζουν αρκετές διαφορές με τις νεότερες εκδόσεις που εισήχθησαν από την εταιρία με κυρίαρχη την εισαγωγή του ανακλαστήρα στο μοντέλο C. Ο ανακλαστήρας εισήχθη για πρώτη φορά το 1926 στην Enigma C και από τότε παρέμεινε βασικό χαρακτηριστικό των μηχανών Enigma. (4)

Το μοντέλο C είχε διαφορετική κατασκευή και σχεδίαση καθώς η αφαίρεση της γραφομηχανής την έκανε πιο μικρή και φορητή και ευκολότερη στην χρήση της.

2.2.6.β. Η Στρατιωτική μηχανή Enigma

Το 1926 ο γερμανικός στρατός και συγκεκριμένα το πολεμικό ναυτικό, υιοθέτησε την μηχανή enigma και συγκεκριμένα την έκδοση Funkschlussel C, η οποία είχε τεθεί σε παραγωγή από το 1925. Το πληκτρολόγιο και ο πίνακας είχε 29 γράμματα τα οποία ήταν σε αλφαβητική σειρά. Οι ρότορες είχαν 28 επαφές, με το γράμμα X ενσύρματο έτσι ώστε να έχει την δυνατότητα να παρακάμψει τα στροφεία. Στις 15 Ιουλίου 1928 ο γερμανικός στρατός είχε την δική του πρόταση καθιερώνοντας την

δική του εκδοχή της μηχανής αίνιγμα από το μοντέλο Enigma G στο Enigma I μέχρι και τον Ιούνιο του 1930. Η συγκεκριμένη εκδοχή της Enigma είναι αρκετά γνωστή καθώς χρησιμοποιήθηκε αρκετά από τις γερμανικές στρατιωτικές υπηρεσίες όπως και άλλους κυβερνητικούς οργανισμούς.

Το 1930 είχε προταθεί στο Πολεμικό Ναυτικό η υιοθέτηση της στρατιωτικής μηχανής καθώς τα οφέλη που παρείχε η μηχανή σε θέματα ασφάλειας και ευκολότερης επικοινωνίας την έκαναν ιδανική. Τελικά, έπειτα από αρκετές συζητήσεις, το Ναυτικό συμφώνησε και το 1934 θα τείθονταν σε λειτουργία η έκδοση του ναυτικού Enigma, το οποίο ονομαζόταν M3.

Τον Δεκέμβριο του 1938, το Πολεμικό Ναυτικό πρόσθεσε επιπλέον δύο ρότορες φτάνοντας τους πέντε, παρέχοντας έτσι μεγαλύτερη ασφάλεια απ' ότι προηγουμένως με την επιλογή των τριών. Αξίζει να σημειωθεί ότι τον Αύγουστο του 1935 η Πολεμική Αεροπορία εισήγαγε επίσης την Βέρμαχτ Αίνιγμα για ευκολότερες επικοινωνίες.

2.2.7 Κώδικας Ναβάχο

2.2.8 Η ιδέα

Ο Philip Johnston κατά την διάρκεια του Δευτέρου Παγκοσμίου Πολέμου είχε μια αρκετά πρωτότυπη ιδέα σχετικά με την επικοινωνία μεταξύ των στρατιωτικών δυνάμεων των ΗΠΑ. Ο Philip Johnston πρότεινε να χρησιμοποιηθεί η γλώσσα της φυλής Ναβάχο έτσι ώστε να δημιουργηθεί ένας άσπαστος νέος κώδικας επικοινωνίας, ο οποίος θα βρισκόταν αρκετά κοντά στις προσδοκίες των στρατιωτικών δυνάμεων, καθώς η γλώσσα δεν ήταν γραπτή και είχε μεγάλο βαθμό πολυπλοκότητας. Η Πολυπλοκότητα στην σύνταξή της αλλά και στον τονισμό της, την καθιστούσαν ακατανόητη σε οποιονδήποτε δεν ήξερε την φιλοσοφία και τον τρόπο ζωής των Ναβάχο. (2)

Στις αρχές του 1942, ο Johnston ξεκίνησε τις απαραίτητες ενέργειες έτσι ώστε να η γλώσσα των Ναβάχο να γίνει ο νέος τρόπος επικοινωνίας των στρατιωτικών δυνάμεων των ΗΠΑ. Αρχικά πραγματοποίησε μία σημαντική συνάντηση με τον επικεφαλή στρατηγό του Αμφίβιου σώματος του Ειρηνικού Στόλου, Clayton B.

Vogel όπου μέσα από μία παρουσίαση σε συνθήκες πολεμικών επιχειρήσεων ο κώδικας Ναβάχο μπορούσε να κωδικοποιήσει και να μεταδώσει ένα αγγλόφωνο μήνυμα σε είκοσι δευτερόλεπτα, την στιγμή που οι κρυπτογραφικές μηχανές της εποχής ήθελαν τριάντα δεύτερα για την ίδια ακριβώς διαδικασία. Πεπεισμένος από την παρουσίαση και την ισχύ του κώδικα, και πιεζόμενοι από τον χρόνο οι Ναβάχο επιλέχθηκαν σαν αποκρυπτογραφιστές από τον αντισυνταγματάρχη James Jones.

Τον Μάιο του ίδιου έτους, 29 Ναβάχο αποτέλεσαν την πρώτη ομάδα που παρακολούθησε μαθήματα σε κέντρο εκπαίδευσης νεοσυλλέκτων και δημιούργησαν τον κώδικα. Ανέπτυξαν λεξικό και διάφορες λέξεις για στρατιωτικούς όρους. Για παράδειγμα, το τεθωρακισμένο όχημα το ονόμαζαν "χελώνα" στην κοινή γλώσσα. Το λεξιλόγιο και όλες οι κωδικοποιημένες λέξεις έπρεπε να μαθευτούν από την νεοσύλλεκτη ομάδα. Μόλις τελείωνε η διαδικασία της εκμάθησης και ολοκληρωνόταν η προετοιμασία τους, κάθε Ναβάχο στέλνονταν στο ναυτικό τάγμα του Ειρηνικού. Ο κύριος σκοπός των "Code Talker" όπως τους ονόμαζαν ήταν να επικοινωνούν μεταδίδοντας πληροφορίες περί τακτικών και της κίνησης των στρατευμάτων και μέσω άλλων ζωτικών μορφών επικοινωνίας του πεδίου μάχης όπως τα τηλέφωνα και το ραδιόφωνο. Επιπροσθέτως, δρούσαν κυρίως σαν αγγελιοφόροι και υπηρετούσαν την γενική θητεία τους σαν ναυτικοί. (2)

2.2.9 Τα χαρακτηριστικά της γλώσσας Ναβάχο

Κατά την διάρκεια του πολέμου οι Ναβάχο αντιμετώπισαν αρκετά προβλήματα όπως ήταν αναμενόμενο, καθώς λόγω των φυλετικών διακρίσεων αντιμετωπίστηκαν ως παρείσακτοι και έτσι αναγκάστηκαν να ζουν σε άθλιες συνθήκες και κατηγορήθηκαν πως αλλοιώνουν την ομοιομορφία και τον εθνικό χαρακτήρα του Αμερικανικού στρατού. (2)

Οι Ναβάχο, ως αμιγώς ιθαγενής φυλή, δεν διέθεταν στο λεξιλόγιο τους στρατιωτική ορολογία και έπρεπε να αφιερωθεί αρκετός χρόνος ώστε να επινοηθούν νέες λέξεις που θα περιέγραφαν ακριβώς κάθε στρατιωτικό όρο. Έτσι λοιπόν, το σώμα πεζοναυτών φρόντισε να καταρτίσει ένα καινούργιο λεξικό όρων των Ναβάχο όπου θα αντικαθιστούσαν τις αγγλικές λέξεις έτσι ώστε να αρθεί κάθε αμφισημία. Οι Ναβάχο ως Ινδιάνοι και καθαρά επηρεασμένοι από την κουλτούρα τους κατάφεραν να συσχετίσουν λέξεις που ανήκαν στην εννοιολογική έννοια

‘’φύση’’ με λέξεις που αναφερόταν στον πόλεμο. Αντίστοιχα η αεροπορία πήρε όρους που χαρακτήριζαν τα ιπτάμενα ζώα και τα θαλάσσια ζώα έδωσαν ονόματα στα πλοία .Οι κλασσικές ινδιάνικες περιφραστικές εκφράσεις που γνωρίζουμε από διάφορες ταινίες χαρακτήριζαν τώρα ποια στρατηγούς η τάγματα.

Τα ονόματα πολυπλοκότερων εννοιών και χωρών κωδικοποιούνταν ως εξής: έπαιρναν τα γράμματα της λέξης και για κάθε γράμμα αντιστοιχούσαν μια λέξη των Ναβάχο που δίνονταν από το κωδικό αλφάβητο. Αυτή η τακτική είχε ένα μεγάλο μειονέκτημα καθώς σπάζονταν εύκολα με την χρήση συχνοτήτων δηλαδή η λέξη ‘’dzeh’’ που αντιστοιχούσε στο γράμμα e θα εμφανιζόταν συνέχεια και έτσι θα μπορούσαν να ορίσουν και τελικά να αποκρυπτογραφήσουν τον κώδικα. Έτσι χρησιμοποίησαν υποκατάστατες λέξεις που θα χρησιμοποιούσαν εναλλάξ για κάθε φωνήεν και για τα πιο κοινά σύμφωνα. Η γλώσσα τους δεν παρουσίαζε καμία ομοιότητα με τις γλώσσες που προέρχονταν από την Ασία ή την Ευρώπη. Η μορφή του ρήματος επηρεάζονταν και από το υποκείμενο και το αντικείμενο συγχρόνως αλλά και την μορφή του αντικειμένου που περιγράφεται (μακρύ, κοντό, υδατικό). Μια τελείως άγνωστη πτυχή της γλώσσας και συγχρόνως πρωτοφανής για της άλλες γλώσσες ήταν ότι τα ρήματα δήλωναν αν ο ομιλητής έχει εμπειρία για αυτό που μιλάει, αν το γνωρίζει εξ’ ακοής ή οπτικά και πολλές φορές ένα ρήμα αντιστοιχούσε σε μία σύνθετη πρόταση που ήταν αδύνατο να αποκρυπτογραφηθεί. (2)

2.2.10 Το Αλφάβητο του Κώδικα Ναβάχο

Στον Παρακάτω Πίνακα παρουσιάζετε το αλφάβητο του κώδικα Ναβάχο και η αντιστοιχία με τα γράμματα του Λατινικού αλφαβήτου.

Λατινικό Γράμμα	Μετάφραση (Ελληνικά)	Γλώσσα Ναβάχο
A	Ant= μυρμήγκι	wol la chee
B	Bear = αρκούδα	shush
C	Cat = γάτα	moasi

D	Deer = ελάφι	be
E	Elk = τάρανδος	dzeh
F	Fox = αλεπού	ma e
G	Goat = κατσίκα	kliziie
H	Horse = άλογο	lin
I	Ice = πάγος	tkin
J	Jackass = γάιδαρος	Tkele cho gi
K	Kid = παιδί	Klizzie yazzi
L	Lamb = αρνί	Dibeh yazzi
M	Mouse = ποντίκι	Na as tso si
N	Nut = καρύδι	Nesh chee
O	Owl = κουκουβάγια	Ne ah jsh
P	Pig = χοίρος	Bi sodih
Q	Quiver = φαρέτρα	Ca yeilith
R	Rabbit = λαγός	gah
S	Sheep = πρόβατο	Dibeh
T	Turkey = γαλοπούλα	Than zie
U	Ute = φορτηγό	No dah ih
V	Victor = νικητής	A keh di glini
W	Weasel = νυφίτσα	Gloe ih
X	Cross = σταυρός	Al na as dzoh
Y	Yucca = γιούκα	Tsah as zih

Πίνακας 3.:Παρουσίαση αλφαβήτου και κώδικα Ναβάχο σε αντιστοιχία με το λατινικό αλφάβητο. (2)

2.3 Τρίτη Περίοδος Κρυπτογραφίας (1950 μ.Χ – Σήμερα)

Η ανάπτυξη των επιστημονικών κλάδων και η εισαγωγή νέων τεχνολογικών εννοιών και μέσων είναι τα κύρια χαρακτηριστικά αυτής της περιόδου. Η αρχή της σύγχρονης κρυπτογραφίας ξεκινά με τον Claude Shannon, και το έργο του «Θεωρεία επικοινωνίας των συστημάτων μυστικότητας» το οποίο δημοσιεύθηκε το 1949 στο τεχνικό περιοδικό Bell System. Μέσα από τις προσωπικές του εργασίες, αλλά και σε συνεργασία με άλλους ειδικούς του χώρου, όπως ο Waren Weaver καθιέρωσε μια στερεά θεωρητική βάση για την κρυπτογραφία και την κρυπτανάλυση. Εκείνη την εποχή, η κρυπτογραφία αρχίζει να εξαφανίζεται και να φυλάσσεται από τις μυστικές υπηρεσίες των κυβερνητικών υπηρεσιών. Πολύ λίγες εξελίξεις δημοσιεύθηκαν, μέχρι και τα μέσα της δεκαετίας του ’70 όπου και υπήρξαν σημαντικές αλλαγές.

2.3.1 Ο κρυπταλγόριθμος DES

Στις αρχές της δεκαετίας του 1970 ο κρυπταλγόριθμος DES (Data Enchyption Standard) έκανε την εμφάνιση του, έχοντας επιλεγεί ως επίσημο Ομοσπονδιακό Πρότυπο Πληροφοριών (Federal Information Processing Standard - FIPS) για τις Ηνωμένες Πολιτείες της Αμερικής. Σκοπός του αλγορίθμου φυσικά ήταν η κρυπτογράφηση ευαίσθητων πληροφοριών με ασφάλεια. Έτσι το 1972, έπειτα από μελέτες για την ασφάλεια των υπολογιστών της κυβέρνησης των Η.Π.Α , το σωματείο NBS (National Bureau of Standards) – γνωστό πλέον ως NIST (National Institute of Standards and Technology), διαπραγματεύθηκε με την NSA και ενέκρινε την δημιουργία ενός αλγορίθμου κρυπτογράφησης, ο οποίος θα ανταποκρινόταν σε κριτήρια αυστηρού σχεδιασμού. (5)

2.3.2 Περιγραφή του DES

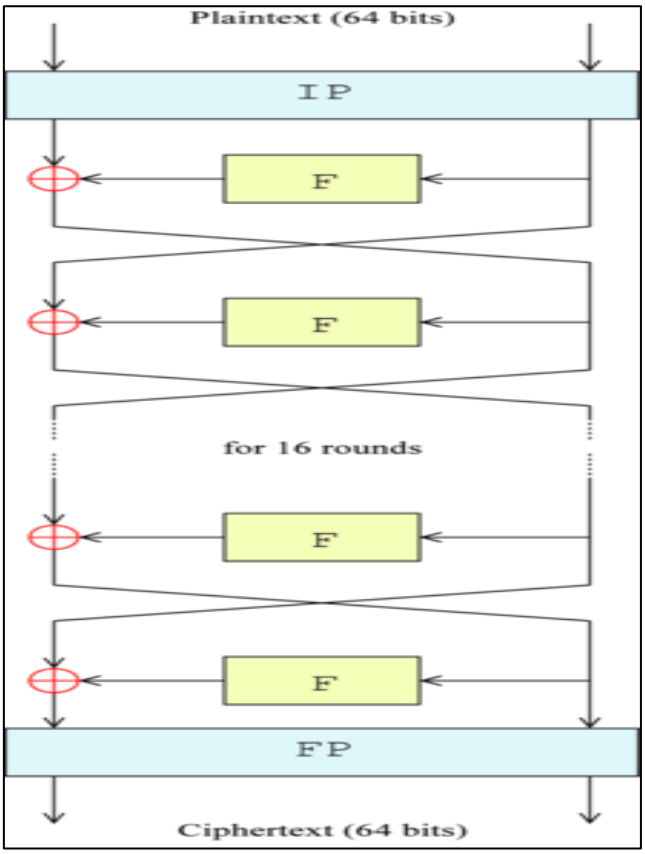
Για να μπορέσει να δημιουργηθεί ο καινούργιος αλγόριθμος καθοριστικό ρόλο έπαιξε η IBM, η οποία ήταν υπεύθυνη για την ανάπτυξή του βασισμένη σε έναν προηγούμενο αλγόριθμο, τον Lucifer.

Ο DES είναι αρχετυπικός block chipper, δηλαδή ένας πρωτότυπος κρυπταλγόριθμος συμμετρικού κλειδιού, ο οποίος δέχεται - λαμβάνει μια σειρά από bits απλού κειμένου, τα οποία έχουν σταθερό μήκος, και τα μετατρέπει μέσω πολύπλοκων διαδικασιών και ενεργειών σε μια νέα σειρά από bits, η οποία έχει το ίδιο μήκος και αποτελεί το κρυπτοκείμενο (chiphertext). Όταν ο αλγόριθμος χρησιμοποιείται για την επικοινωνία, τόσο ο αποστολέας όσο και ο παραλήπτης πρέπει να γνωρίζουν το ίδιο μυστικό κλειδί το οποίο θα χρησιμοποιηθεί για την κρυπτογράφηση ή την αποκρυπτογράφηση του μηνύματος ή για την επαλήθευση ενός κώδικα ταυτότητας μηνυμάτων (MAC). Η σταθερή σειρά μπλοκ που χρησιμοποιεί ο DES είναι 64 bits. Όπως όλοι οι αλγόριθμοι, έτσι και ο DES χρησιμοποιεί ένα κλειδί ασφαλείας για να μπορέσει να προσαρμόσει την μετατροπή των κειμένων – μηνυμάτων ώστε στην συνέχεια να μπορούν να αποκρυπτογραφηθούν μόνο από εκείνους που γνωρίζουν το συγκεκριμένο κλειδί κατά την κρυπτογράφηση. Το κλειδί αποτελείται από 64 bits αλλά μόνο τα 56 από αυτά χρησιμοποιούνται από τον αλγόριθμο, καθώς τα υπόλοιπα 8 bits χρησιμοποιούνται αποκλειστικά για τον έλεγχο της ισοτιμίας και στην συνέχεια απορρίπτονται. Όπως πολλοί άλλοι αλγόριθμοι κρυπτογράφησης, έτσι και ο DES δεν παρέχει από μόνος του έναν ασφαλή τρόπο κρυπτογράφησης, αλλά πρέπει να χρησιμοποιηθεί με ειδικό τρόπο λειτουργίας (mode of operation). Ο DES μπορεί επίσης να χρησιμοποιηθεί για μεμονωμένους χρήστες κρυπτογράφησης, όπως για την αποθήκευση αρχείων σε έναν σκληρό δίσκο σε κρυπτογραφημένη μορφή. (5)

2.3.3 Συνολική Δομή του DES

Όπως παρουσιάζεται και στο παρακάτω σχήμα, φαίνεται η συνολική δομή του αλγορίθμου. Συγκεκριμένα υπάρχουν 16 στάδια επεξεργασίας τα οποία είναι όμοια μεταξύ τους και ονομάζονται rounds. Υπάρχει επίσης μια αρχική και τελική μετάθεση, η οποία ονομάζεται IP και FP, οι οποίες έχουν αντίστροφες ιδιότητες. Δηλαδή η IP «αναιρεί» την δράση της FP, και το αντίστροφο. Οι IP και FP δεν

συμμετέχουν σε καμία κρυπτογραφική επεξεργασία, απλά συμπεριλήφθηκαν προκειμένου να διευκολυνθεί η λειτουργία του αλγορίθμου. (5)



Σχήμα 3.:Συνολική δομή του αλγορίθμου.

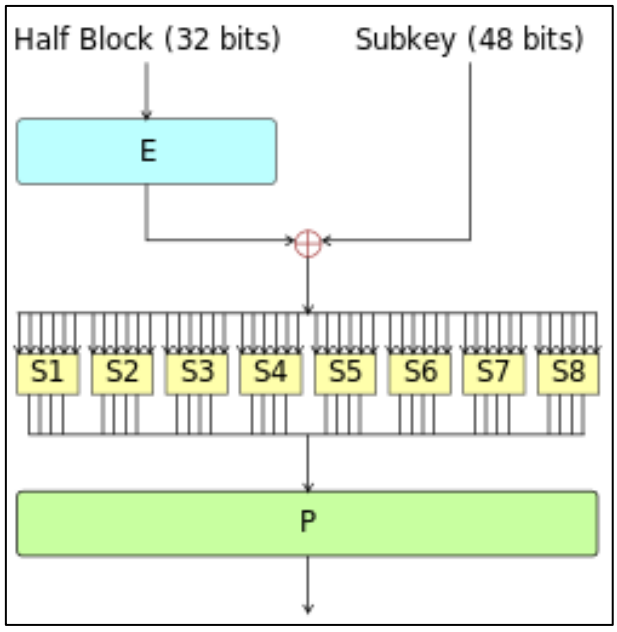
Πριν από την κύρια λειτουργία των rounds, το συγκρότημα χωρίζεται σε δύο ίσα μέρη των 32-bit όπου γίνεται η επεξεργασία εναλλάξ. Αυτή η συγκεκριμένη διασταυρούμενη διαδικασία είναι γνώστη ως συνάρτηση Φάιστελ (Feistel). Η δομή της συνάρτησης εξασφαλίζει ότι η κρυπτογράφηση και η αποκρυπτογράφηση είναι αρκετά παρόμοιες διαδικασίες – με μόνη διαφορά ότι τα δευτερεύοντα κλειδιά εφαρμόζονται με αντίστροφη σειρά κατά την αποκρυπτογράφηση. Το υπόλοιπο του αλγορίθμου είναι πανομοιότυπο. Αυτό απλοποιεί σε μεγάλο βαθμό την εφαρμογή, ιδιαίτερα στο σύνολο του υπολογιστικού υλικού (hardware), καθώς δεν υπάρχει ανάγκη για ξεχωριστή κρυπτογράφηση και αποκρυπτογράφηση των αλγορίθμων. (5)

Το σύμβολο ⊕ δηλώνει την αποκλειστική διαδικασία διάζευξης (XOR). Η συνάρτηση F ανακατεύει το μισό τετράγωνο μαζί με μερικά από τα δευτερεύοντα κλειδιά. Η έξοδος από την συνάρτηση F συνδυάζεται κατόπιν με το υπόλοιπο

ήμισυ του μπλοκ, με αποτέλεσμα τα δύο ήμισυ να ανταλλάσσονται πριν από το επόμενο round.Έτσι λοιπόν, έπειτα από το δέκατο-έκτο round τα δύο μισά έχουν ανταλλάξει μεταξύ τους. Αυτό είναι ένα χαρακτηριστικό γνώρισμα της δομής Φάιστελ (Feistel) που καθιστά την κρυπτογράφηση και την αποκρυπτογράφηση ως παρόμοιες διαδικασίες. (5)

2.3.4 Η συνάρτηση Φάιστελ (Feistel)

Όπως φαίνεται και στο σχήμα 4, η συνάρτηση F λειτουργεί στο μισό μπλοκ, δηλαδή με τα 32-bits κάθε φορά, όπως αναφέραμε και προηγουμένως, και αποτελείται από τέσσερα βασικά στάδια.



Σχήμα 4.: Περιγραφή λειτουργία της συνάρτησης Feistel στο μισό μπλοκ.

Τα τέσσερα στάδια της συνάρτηση Feistel παρουσιάζονται ως εξής:

Επέκταση: Είναι το στάδιο όπου το μισό μπλοκ των 32- bit επεκτείνεται σε 48-bits χρησιμοποιώντας την διαδικασία της επεκτατικής μεταλλαγής ή διαφορετικά expansion permutation, η οποία αντιγράφει ορισμένα bits. Στο σχήμα 4 απεικονίζεται ως το γαλάζιο ορθογώνιο με το γράμμα **E** στο κέντρο.

Ανάμειξη κλειδιών: Είναι το στάδιο όπου το αποτέλεσμα μέσω μιας πράξης αποκλειστικής διάζευξης (XOR) συνδυάζεται με ένα δευτερεύον κλειδί. Δεκαέξι κλειδιά των 48-bit προέρχονται από το κύριο κλειδί μέσω της χρήσης του Χρονοδιαγράμματος ή του προγράμματος των κλειδιών. Αξίζει να αναφερθεί ότι τα κλειδιά είναι δεκαέξι διότι και οι κύκλοι (rounds) είναι δεκαέξι όπως προαναφέραμε.

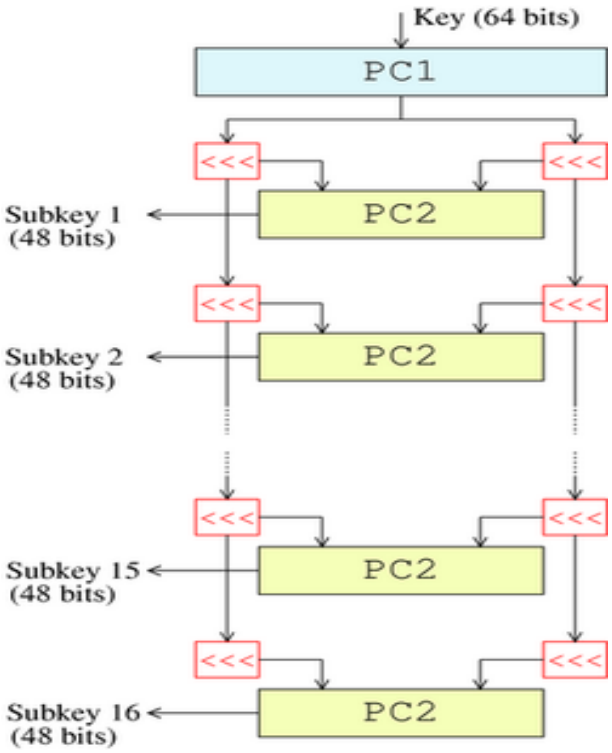
Αντικατάσταση: Στο συγκεκριμένο στάδιο, το μπλοκ διαιρείται σε οκτώ ίσα τμήματα των έξι μπιτ πριν ξεκινήσει η διαδικασία της επεξεργασίας από τα κουτιά αντικατάστασης, τα οποία απεικονίζονται ως μικρά κίτρινα S-boxes. Τα συγκεκριμένα κουτιά είναι βασικό χαρακτηριστικό της ασφάλειας του αλγορίθμου DES, καθώς περιέχουν τον «πυρήνα» ασφαλείας του. Όπως παρατηρούμε από το σχήμα 4, τα οκτώ κουτιά αντικαθιστά τις εισόδους των έξι μπιτ με εξόδους των τεσσάρων μπιτ σύμφωνα με ένα μη γραμμικό μετασχηματισμό, που παρέχεται με την μορφή ενός πίνακα αναζήτησης ή αλλιώς από έναν lookup table. Αξίζει να σημειωθεί ότι χωρίς την χρήση των S-boxes το κρυπτό-αλγόριθμος θα ήταν γραμμικός και έτσι κοινότυπα εύθραυστος.

Μεταλλαγή: Το τελικό στάδιο της συνάρτησης F είναι η σταθερή μεταλλαγή, η οποία απεικονίζεται στο σχήμα 4 ως ορθογώνιο κουτί P. Οι 32 έξοδοι από τα κουτιά αντικατάστασης S-boxes καταλήγουν στο P-box.

Η εναλλαγή της αντικατάστασης από τα κουτιά αντικατάστασης καθώς και η μεταλλαγή από το P-box και την E-επέκταση, παρέχει την λεγόμενη «σύγχυση και διάχυση» αντίστοιχα, μια έννοια η οποία προσδιορίστηκε από τον Αμερικάνο Μαθηματικό και Ηλεκτρολόγο μηχανικό Κλοντ Σάνον (Claude Shannon), γνωστό και ως «ο πατέρας της θεωρίας της πληροφορίας» και της σύγχρονης κρυπτολογίας. Αυτή η έννοια αποτέλεσε απαραίτητη προϋπόθεση για την ασφαλή αλλά και πρακτική κρυπτογράφηση. (5)

2.3.5 Το πρόγραμμα των κλειδιών

Στο παρακάτω σχήμα παρουσιάζεται η διαδικασία της κρυπτογράφησης και η δημιουργία των υποκλειδιών από τον αλγόριθμο.



Σχήμα 5.: Παρουσίαση της διαδικασίας δημιουργίας των υποκλειδιών από τον αλγόριθμο.

Αρχικά η διαδικασία ξεκινά επιλέγοντας 56 bits του κλειδιού από τα 64 bits από την μεταλλαγμένη επιλογή 1 (Permuted Choice 1: PC1). Τα υπόλοιπα 8 bits όπως αναφέραμε και πριν, αν δεν απορριφθούν χρησιμοποιούνται ως bits ελέγχου ισοτιμίας (parity bits). Στη συνέχεια τα 56 bits χωρίζονται σε δύο ίσα τμήματα των 28 bits από τα οποία το καθένα εξετάζεται χωριστά. Στους διαδοχικούς γύρους , τα δύο ίσα τμήματα των 28 bits περιστρέφονται προς τα αριστερά κατά ένα ή δύο bits και έπειτα, τα 48 bits του υποκλειδιού επιλέγονται από την μεταλλαγμένη επιλογή 2 (Permuted Choice 2: PC2) – 28 από το αριστερό μισό και 28 από το δεξί μισό. Οι περιστροφές, οι οποίες συμβολίζονται στην εικόνα με το εικονίδιο (<<<) στο διάγραμμα σημαίνει ότι ένα διαφορετικό σύνολο των bits χρησιμοποιείται σε κάθε δευτερεύον κλειδί. Κάθε μπιτ χρησιμοποιείται περίπου σε 14 από τα 16 υποκλειδιά. Αξίζει να αναφερθεί ότι για την διαδικασία της αποκρυπτογράφησης χρησιμοποιείται το ίδιο πρόγραμμα κλειδιών με κύρια αλλαγή την αντίστροφη διάταξη των υποκλειδιών έναντι της κρυπτογράφησης. (5)

Για παράδειγμα, έστω ότι κατά την διαδικασία της κρυπτογράφησης το πρόγραμμα χρησιμοποιεί τα δευτερεύον κλειδιά (s1, sb2, sb3,… sb16) ξεκινώντας από το sb1.

Τότε για την διαδικασία της αποκρυπτογράφησης το πρόγραμμα θα είναι (sb16, sb15, sb14,… sb1), ξεκινώντας αυτήν την φορά από το sb16. Εκτός από αυτήν την αλλαγή η διαδικασία είναι ακριβώς η ίδια. Τα ίδια 28 bits θα περάσουν απ' όλες τις θέσεις της περιστροφής. (5)

2.4. Ο κρυπταλγόριθμος AES

Ο κρυπταλγόριθμος AES (Advanced Encryption Standard) γνωστός και ως Rijndael αποτελεί μια βασική προδιαγραφή για την κρυπτογράφηση των ηλεκτρονικών στοιχείων που καθορίζονται από το αμερικανικό Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας το 2001. (6)

Ο AES βασίζεται στην αρχική κρυπτογράφηση Rijndael που αναπτύχθηκε από δύο Βέλγους κρυπτογράφους, τους Joan Daemen και Vincent Rijmen, οι οποίοι υπέβαλαν πρόταση στο Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) κατά τη διάρκεια της διαδικασίας επιλογής του AES. Το όνομα Rijndael είναι ένα λογοπαίγνιο με τα ονόματα των δύο εφευρετών Joan Daemen και Vincent Rijmen. Ο Rijndael είναι μία «οικογένεια» από αλγόριθμους κρυπτογράφησης η οποία έχει ως χαρακτηριστικό διαφορετικά κλειδιά και μέγεθος στα μπλοκ τους. Για τον AES, το NIST επέλεξε τρία από τα μέλη της οικογένειας κρυπταλγορίθμων Rijndael, το καθένα με μέγεθος 128 bits, αλλά με τρία διαφορετικά μεγέθη κλειδιών: 128 bits, 192 bits και 256 bits αντίστοιχα. (6)

Ο AES έχει εγκριθεί από την κυβέρνηση των ΗΠΑ και τώρα χρησιμοποιείται σε όλον τον κόσμο. Ο AES αντικατέστησε επίσημα τον DES το 2001 όταν ανήγγειλε ο NIST το FIPS 197. Ο αλγόριθμος που περιγράφεται από τον AES είναι συμμετρικός με κοινό κλειδί το οποίο χρησιμοποιείται τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση των δεδομένων. Στις Ηνωμένες Πολιτείες, ο AES ανακοινώθηκε από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας των ΗΠΑ με τίτλο FIPS RUB 197 στις 26 Νοεμβρίου του 2001. Η ανακοίνωση αυτή ακολούθησε μια διαδικασία τυποποίησης πέντε ετών κατά την οποία δεκαπέντε ανταγωνιστικά σχέδια παρουσιάστηκαν και αξιολογήθηκαν, πριν ακόμα επιλεχτεί ο αλγόριθμος κρυπτογράφησης Rijndael ως το πλέον κατάλληλο. (6)

Ο AES τέθηκε σε ισχύ ως ομοσπονδιακό πρότυπο της κυβέρνησης στις 26 Μάη του 2002 μετά την έγκριση από τον Υπουργό Εμπορίου. Ο AES είναι διαθέσιμο σε πολλά διαφορετικά πακέτα κρυπτογράφησης και είναι ο πρώτος δημόσια προσβάσιμος και ανοιχτός αλγόριθμος κρυπτογράφησης, ο οποίος έχει εγκριθεί από την Εθνική Υπηρεσία Ασφαλείας (NSA) για τις κορυφαίες μυστικές πληροφορίες όταν χρησιμοποιείται από εγκεκριμένη μονάδα της NSA. (6)

2.4.1 Περιγραφή αλγορίθμου AES

Ο AES βασίζεται στην αρχή του σχεδιασμού, που είναι γνωστή ως δίκτυο υποκατάστασης μεταθέσεων, το οποίο είναι ένας συνδυασμός υποκατάστασης και μετάθεσης το οποίο λειτουργεί γρήγορα τόσο σε software όσο και σε hardware. Σε αντίθεση με τον προκάτοχο του τον DES, ο AES δεν χρησιμοποιεί την συνάρτηση Feistel, αλλά μια παραλλαγή του αλγόριθμου Rijndael η οποία έχει σταθερό μέγεθος μπλοκ των 128 bits αλλά τα μεγέθη των κλειδιών του κυμαίνεται σε 128, 192 και 256 bits. Αντίθετα, το Rijndael καθορίζεται από μεγέθη μπλοκ και κλειδιών που μπορεί να είναι οποιοδήποτε πολλαπλάσιο των 32 bits, με μία ελάχιστη απαίτηση των 128 και ανώτατο όριο των 256 bits. (6)

Ο AES λειτουργεί σε μια κατάσταση πίνακα γραμμών – στηλών από bytes μεγέθους 4 επί 4 (4x4), η οποία δεν είναι συνηθισμένη καθώς στον αλγόριθμο Rijndael χρησιμοποιούνται μεγαλύτερο μέγεθος στηλών. Οι περισσότεροι υπολογισμοί του AES έχουν γίνει σε ένα ειδικά πεπερασμένο πεδίο. (6)

Το μέγεθος του κλειδιού που χρησιμοποιείται για την κρυπτογράφηση AES καθορίζει τον αριθμό των επαναλήψεων των γύρων σχηματισμού που μετατρέπουν την είσοδο, το οποίο ονομάζεται απλό κείμενο (plaintext) σε τελικό αποτέλεσμα, που ονομάζεται κρυπτογράφημα (ciphertext).

Ο αριθμός των κύκλων των επαναλήψεων είναι ως εξής:

- 10 κύκλους επανάληψης για κλειδιά 128-bits
- 12 κύκλους επανάληψης για κλειδιά 192-bits
- 14 κύκλους επανάληψης για κλειδιά 256-bits

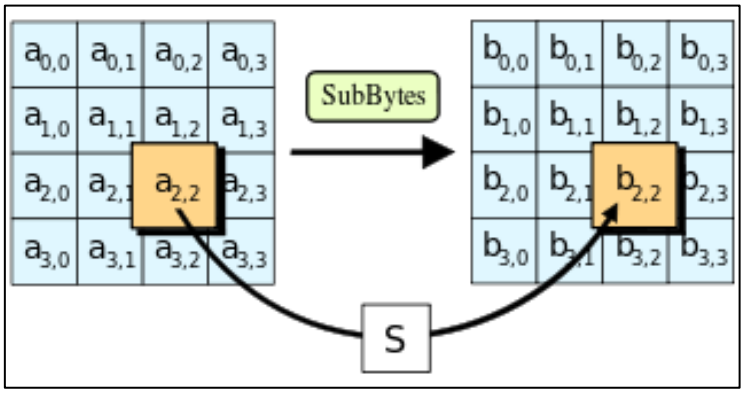
Κάθε γύρος αποτελείται από διάφορα στάδια επεξεργασίας, που το καθένα περιέχει τέσσερα παρόμοια αλλά ταυτοχρόνως διαφορετικά στάδια, συμπεριλαμβανομένου ενός που εξαρτάται από το ίδιο το κλειδί κρυπτογράφησης. Ένα σύνολο αντίστροφων επαναλήψεων εφαρμόζεται για να μετατρέψει το κρυπτογράφημα (ciphertext) πίσω στην αρχική του κατάσταση του απλού κειμένου, χρησιμοποιώντας το ίδιο το κλειδί κρυπτογράφησης. (6)

2.4.2. Υψηλού επιπέδου περιγραφή του AES

1) Key Expansions: Τα κλειδιά από τους γύρους προέρχονταν κυρίως από το κλειδί κρυπτογράφησης χρησιμοποιώντας το κλειδί Rijndael από το χρονοδιάγραμμα. Ο AES απαιτεί για κάθε γύρο ένα ξεχωριστό κλειδί των 28-bits συν ένα ακόμα.
2) Initial Round – Αρχικός Γύρος
    - Add Round Key: Κάθε byte της κατάστασης συνδυάζεται με ένα μπλοκ από το κλειδί του κάθε γύρου χρησιμοποιώντας την λογική πράξη XOR.
3) Rounds – Γύροι
    - Sub Bytes: Μία μη –γραμμική βαθμίδα υποκατάστασης όπου κάθε byte αντικαθίσταται με ένα άλλο σύμφωνα με ένα άλλο πίνακα αναζήτησης.
    - Shift Rows: Ένα στάδιο μεταφοράς, όπου οι τρεις τελευταίες σειρές της κατάστασης μετατοπίζονται κυκλικά σε ένα συγκεκριμένο αριθμό βημάτων.
    - Mix Columns: Μία λειτουργία ανάμειξης, η οποία χειρίζεται τις στήλες της κατάστασης, συνδυάζοντας τα τέσσερα bytes σε κάθε στήλη.
    - Add Round Key: Όπως προηγουμένως.
4) Final Round – Τελικός Γύρος
    - Sub Bytes
    - Shift Rows
    - Add Round Key

2.4.3. Το στάδιο SubBytes

Στο στάδιο αυτό, κάθε byte A_{i , j} που βρίσκεται στην κατάσταση του πίνακα αντικαθίσταται με ένα υπό – byte S (A_{i , j}) χρησιμοποιώντας ένα κουτί υποκατάστασης (s-box) των 8-bit. Αυτή η λειτουργία παρέχει την μη – γραμμικότητα στον αλγόριθμο. (6)

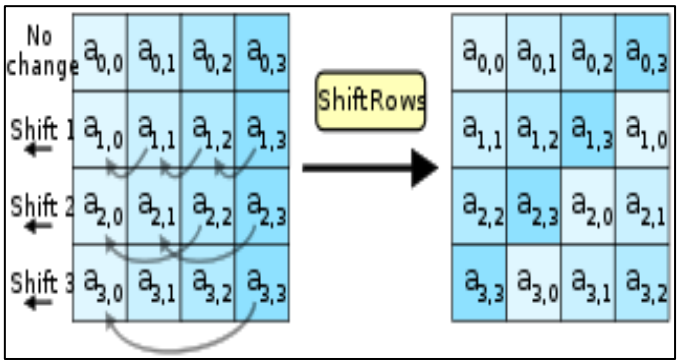


Σχήμα 6.: Στο στάδιο SubBytes, κάθε byte στην κατάσταση αντικαθίσταται στην είσοδο του με ένα σταθερό πίνακα αναζήτησης των 8-bit.

Το κουτί υποκατάστασης (S-box) για να αποφύγει επιθέσεις που βασίζονται σε απλές αλγεβρικές ιδιότητες, συνδυάζει την αντίστροφη λειτουργία με έναν αναστρέψιμο συσχετισμένο μετασχηματισμό. (6)

2.4.4. Το στάδιο ShiftRow

Το στάδιο αυτό δραστηριοποιείται κυρίως στις γραμμές της κατάστασης του πίνακα, καθώς μετατοπίζει τα bytes κυκλικά σε κάθε σειρά με ένα συγκεκριμένο αντισταθμιστή (offset). Για τον AES, η πρώτη γραμμή παραμένει σταθερή και επομένως και αμετάβλητη. (6)

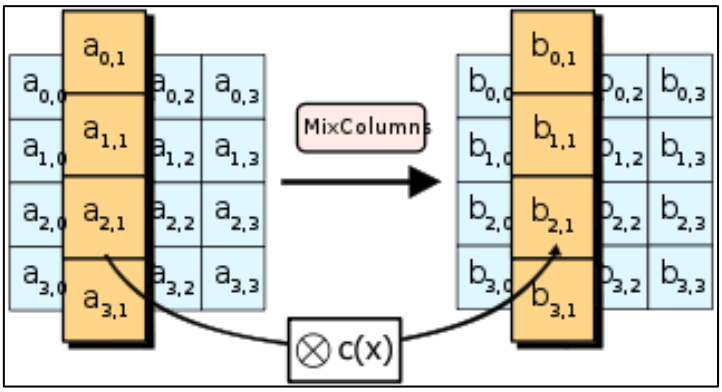


Σχήμα 7.: Τα byte κάθε σειράς από την κατάσταση του πίνακα μετατοίζονται κυκλικά προς τα αριστερά. Ο αριθμός των θέσεων των bytes που μετατοπίζονται διαφέρει για κάθε γραμμή.

Όπως φαίνεται και στο σχήμα 7, κάθε byte της δεύτερης σειράς μετατοπίζεται μία θέση προς τα αριστερά. Ομοίως, και για την Τρίτη και τέταρτη σειρά η οποίες μετατοπίζονται με μεταθέσεις των δύο και τριών θέσεων αντίστοιχα. Για τα μπλοκ των 128-bits και 192- bits το μοτίβο των μετατοπίσεων παραμένει ίδιο. Αν θέλαμε να το παρουσιάσουμε με μια μαθηματική περιγραφή θα λέγαμε ότι, η γραμμή n μετατοπίζεται κυκλικά προς τα αριστερά με n-1 bytes. Με αυτόν τον τρόπο κάθε στήλη της κατάστασης εξόδου του σταδίου ShiftRow αποτελείται από bytes από κάθε στήλη της κατάστασης εισόδου. (6)

2.4.5 Το στάδιο MixColumns

Σε αυτό το στάδιο, τα τέσσερα bytes της κάθε στήλης της κατάστασης του πίνακα συνδυάζονται χρησιμοποιώντας ένα αντιστρέψιμο γραμμικό μετασχηματισμό. Η λειτουργία MixColumns δέχεται τέσσερα bytes ως είσοδο και παράγει τέσσερα bytes ως έξοδο, όπου το κάθε byte εισόδου επηρεάζει όλα τα τέσσερα εξόδου. Το στάδιο ShiftRow μαζί με το MixColunms παρέχει διάχυση μέσα στην διαδικασία της κρυπτογράφησης. (6)

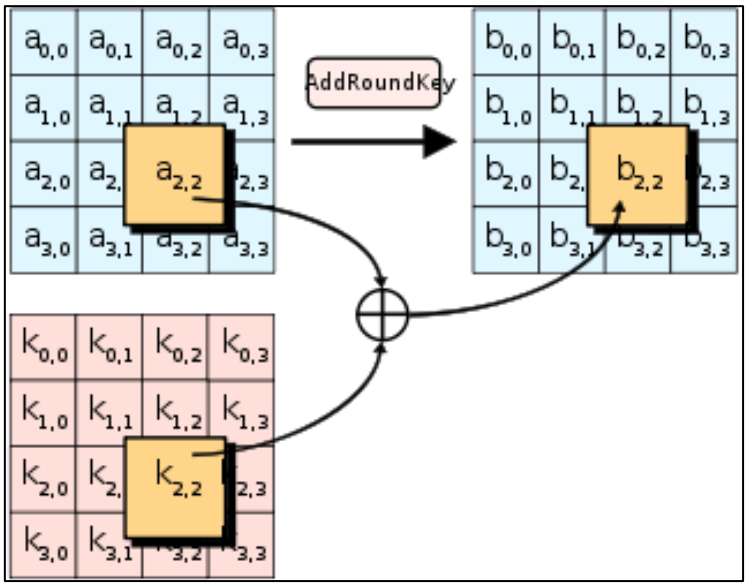


Σχήμα 8.: Στο στάδιο MixColumns, κάθε στήλη της κατάστασης πολλαπλασιάζεται με ένα πολυώνυμο σταθερό c (x).

Κατά την διάρκεια αυτής της λειτουργίας που παρουσιάζεται στο σχήμα 8, κάθε στήλη μετασχηματίζεται χρησιμοποιώντας έναν σταθερό πίνακα (ο πίνακας πολλαπλασιάζεται κάθε φορά με μία στήλη και δίνει μια νέα τιμή στην στήλη της κατάστασης). (6)

2.4.6 Το στάδιο AddRoundKey

Σε αυτό το στάδιο, το δευτερεύον κλειδί συνδυάζεται με την κατάσταση του πίνακα. Για κάθε γύρο, το δευτερεύον κλειδί που προέρχεται από το κύριο κλειδί του αλγορίθμου Rijndael. Κάθε byte της κατάστασης συνδυάζεται με ένα μπλοκ από το κλειδί του κάθε γύρου χρησιμοποιώντας την λογική πράξη XOR. (6)



Σχήμα 9.: Στο στάδιο AddRoundKey, κάθε byte της κατάστασης συνδυάζεται με ένα byte του γύρου δευτερεύον κλειδί, χρησιμοποιώντας τη λειτουργία XOR (⊕).

2.4.7 Βελτιστοποίηση της Κρυπτογράφησης

Σε συστήματα με 32-bit ή μεγαλύτερα, είναι πιθανή η επιτάχυνση της εφαρμογής στην κρυπτογράφηση με των συνδυασμό των SubBytes και ShiftRows με το στάδιο MixColunms μετατρέποντας τα σε μία αλληλουχία πινάκων αναζήτησης. Για να γίνει αυτό, απαιτούνται τέσσερα 256 – εισαγωγικούς πίνακες των 32 –bit και χρησιμοποιεί ένα σύνολο τεσσάρων kilobytes μνήμης (4096 Bytes), ένα για κάθε πίνακα. Ένας γύρος μπορεί στην συνέχεια να ολοκληρωθεί με 16 πίνακες αναζήτησης ακολουθούμενο από τέσσερα 32-bit από το στάδιο AddRoundKey. (6)

Εάν το αποτέλεσμα των τεσσάρων kilobyte έχει δημιουργήσει ένα μεγάλο σε μέγεθος πίνακα, η λειτουργία του πίνακα αναζήτησης μπορεί να πραγματοποιηθεί με ένα μόνο 256 εισαγωγικό 32 – bit πίνακα (δηλαδή ένα kilobyte) μέσω της χρήσης της κυκλικής περιστροφής. (6)

Χρησιμοποιώντας ένα byte προσανατολισμένο κατά προσέγγιση, είναι δυνατον να συνδυαστούν και τα τρία στάδια (SubBytes, ShiftRows, MixColunms) σε ένα μόνο γύρο. (6)

ΚΕΦΑΛΑΙΟ 3: ΣΥΓΧΡΟΝΕΣ ΜΟΡΦΕΣ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ

3.1 Σε τι στοχεύει η Κρυπτογραφία;

Στόχοι της Κρυπτογραφίας είναι αρχικά η παράδοση των κρυπτογραφημένων πληροφοριών με επιτυχία που είναι ισάξια σε σημασία με την αποκλειστική ανάγνωση των πληροφοριών μόνο από τους επιλεγμένους παραλήπτες. Ακόμη, σκοπός είναι η πιστοποίηση της ταυτότητας του προσώπου που στέλνει τις πληροφορίες, δηλαδή του αποστολέα. Εξίσου σημαντική είναι η διατήρηση των πληροφοριών και η , κατά συνέπεια, φραγή κάθε τυχαίας παρεμβολής από τρίτα πρόσωπα. Τέλος, μεγάλη σημασία έχει η απαγόρευση απάρνησης κάθε είδους πιστοποίησης αυθεντικότητας. Αν, δηλαδή σταλεί ένα μήνυμα από έναν αποστολέα ‘χ’ προς έναν παραλήπτη ‘ψ’ τότε επιβάλλεται η διασφάλιση της απόδειξης ότι ο ‘χ’ αποστολέας όντως έστειλε το μήνυμα στον παραλήπτη ‘ψ’, πράξη που πρέπει να είναι μη αναστρέψιμη και μη επεξεργάσιμη. (2)

3.1.1 Είδη Συστημάτων Κρυπτογράφησης

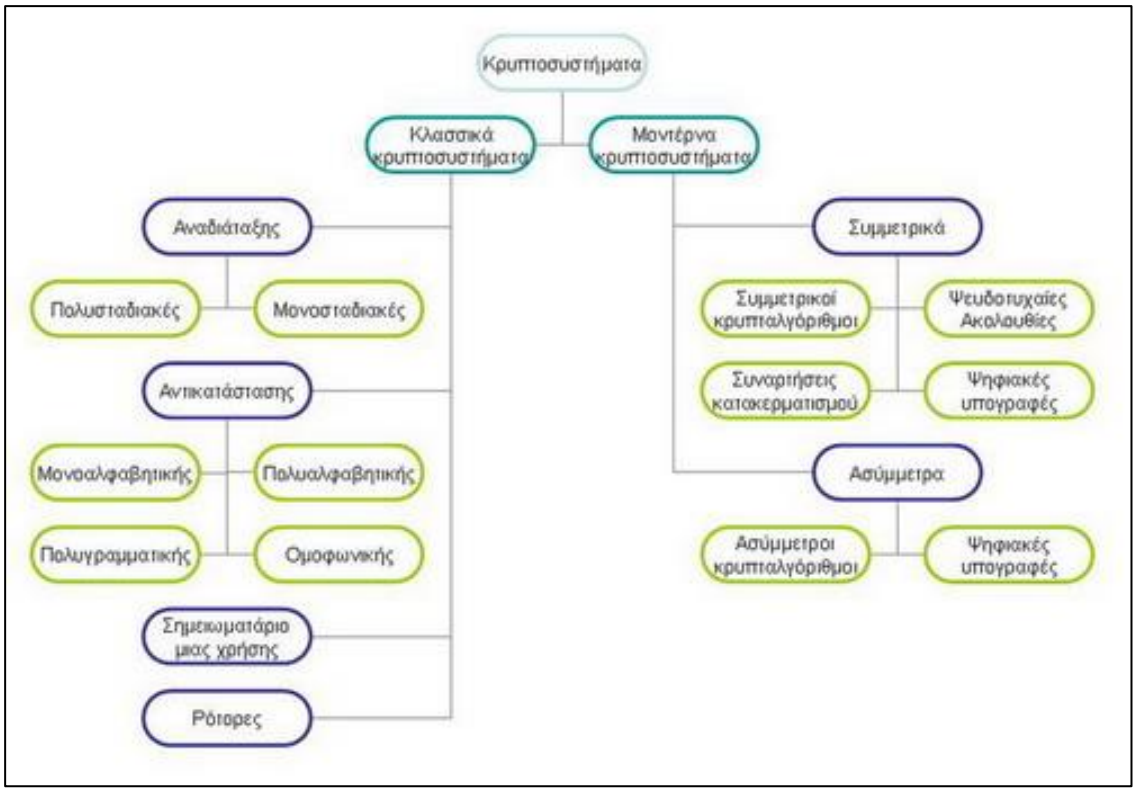
Τα κρυπτοσυστήματα χωρίζονται σε δύο μεγάλες κατηγορίες τα Κλασσικά Κρυπτοσυστήματα και τα Μοντέρνα Κρυπτοσυστήματα. Επιπροσθέτως, οι κρυπτογραφικοί αλγόριθμοι μπορούν να χωριστούν σε δύο διαφορετικές κατηγορίες με βάση τον τρόπο κρυπτογράφησης των μηνυμάτων:

1. Δέσμης (Block Ciphers), οι οποίοι χωρίζουν το μήνυμα σε κομμάτια και κρυπτογραφούν κάθε ένα από τα κομμάτια αυτά χωριστά.
2. Ροής (Stream Ciphers), οι οποίοι κρυπτογραφούν μία ροή μηνύματος (stream) χωρίς να την διαχωρίζουν σε τμήματα.

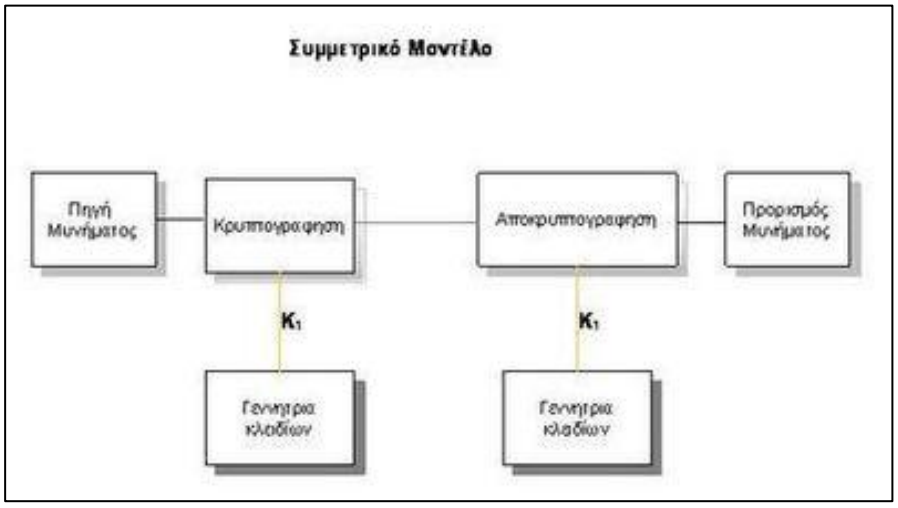
-Κλασσικά Κρυπτοσυστήματα

-Μοντέρνα Κρυπτοσυστήματα

-Συμμετρικά Κρυπτοσυστήματα



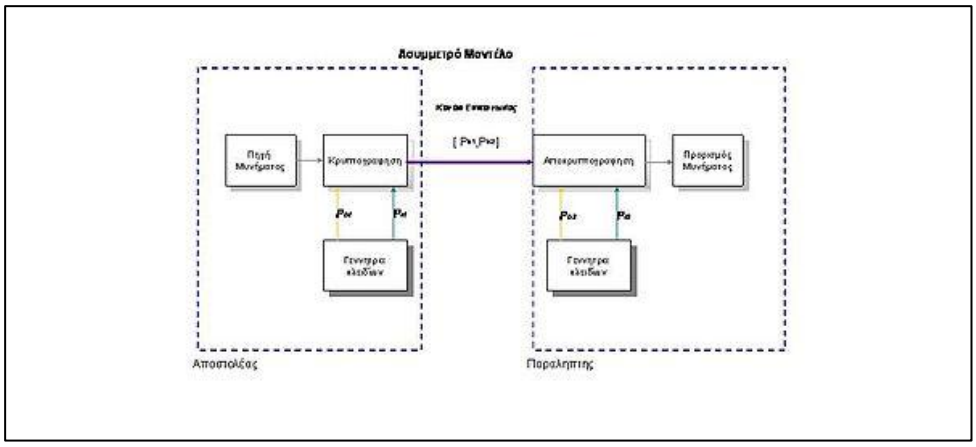
Συμμετρικό κρυπτοσύστημα είναι το σύστημα το οποίο χρησιμοποιεί κατά την διαδικασία της κρυπτογράφησης και της αποκρυπτογράφησης ένα κοινό κλειδί. Η ασφάλεια αυτών των αλγορίθμων βασίζεται στην μυστικότητα του κλειδιού. Τα συμμετρικά συστήματα κρυπτογραφίας προϋποθέτουν την ανταλλαγή του κλειδιού μέσα από ένα ασφαλές κανάλι επικοινωνίας ή μέσα από την φυσική παρουσία των προσώπων. Αυτό το χαρακτηριστικό καθιστά δύσκολη την επικοινωνία μεταξύ απομακρυσμένων ατόμων. (1)



Για παράδειγμα, έστω ότι έχουμε το αρχικό μήνυμα (ένα σύνολο δυαδικών ψηφίων) {μi, όπου i = 1,2,..n} και το κλειδί είναι γνωστό στον αποστολέα και στον παραλήπτη {κi, όπου i = 1,2,..n}. Αν δημιουργήσουμε τον γρίφο που θα αποσταλεί, (ένα σύνολο δυαδικών ψηφίων γi, που να ικανοποιούν την σχέση {γi = μi⊕κi, όπου = 1,2,.. n} τότε θα ισχύει επίσης ότι {μi = γi i⊕κi, όπου το i=1,2,..n} και ο παραλήπτης του γρίφου με χρήση του κλειδιού θα αναδημιουργήσει το μήνυμα. Μηνύματα μεγάλου μήκους μπορούν να κρυπτογραφούνται σε ομάδες των nδυαδικών αριθμών.

3.1.2 Ασύμμετρα κρυπτοσυστήματα

Το ασύμμετρο κρυπτοσύστημα ή κρυπτοσύστημα δημοσίου κλειδιού δημιουργήθηκε για να καλύψει την αδυναμία μεταφοράς κλειδιών που παρουσίαζαν τα συμμετρικά συστήματα. Χαρακτηριστικό του είναι ότι έχει δύο είδη κλειδιών, ένα δημόσιο και ένα ιδιωτικό. Το δημόσιο είναι διαθέσιμο σε όλους ενώ το ιδιωτικό μυστικό. Η βασική σχέση μεταξύ τους είναι μόνο αυτά που μπορεί να κρυπτογραφήσει το ένα μπορεί να κρυπτογραφήσει και το άλλο.



Οι δυνατότητες της ασύμμετρης κρυπτογραφίας οδήγησαν στην δημιουργία ψηφιακών υπογραφών και ακολούθως στην ανάπτυξη της Υποδομής Δημοσίου Κλειδιού και στα Ψηφιακά Πιστοποιητικά. (1)

3.1.3 Τρόποι και μέθοδοι Κρυπτογράφησης

Οι τρόποι κρυπτογράφησης μυστικού κλειδιού τυπικά χωρίζονται σε 2 κατηγορίες. Η πρώτη περιλαμβάνει διαδικασίες κρυπτογράφησης που εφαρμόζονται πάνω σε ένα μοναδικό bit (ή byte ή word) και υλοποιούν κάποιο μηχανισμό ανατροφοδότησης έτσι ώστε το κλειδί να αλλάζει συνεχώς. Για αυτό και ονομάζονται κρυπτογράφοι ροής (stream ciphers). Η δεύτερη κατηγορία (κρυπτογράφοι μπλοκ - block ciphers) αποτελείται από αλγορίθμους κρυπτογράφησης που λειτουργούν πάνω σε ομάδες δεδομένων κάθε χρονική στιγμή χρησιμοποιώντας το ίδιο κλειδί για κάθε ομάδα. Έτσι στην γενική περίπτωση, όταν το ίδιο μυστικό κλειδί χρησιμοποιείται, η ίδια ομάδα δεδομένων ενός plaintext θα κρυπτογραφηθεί στο ίδιο ciphertext όταν η κρυπτογράφηση γίνεται με έναν αλγόριθμο κρυπτογράφησης μπλοκ αλλά σε διαφορετικό ciphertext όταν χρησιμοποιηθεί ένας κρυπτογράφος ροής. Για τους κρυπτογράφους μπλοκ, έχουν επινοηθεί αρκετοί τρόποι λειτουργίας (modes) ώστε να βελτιωθούν κάποια χαρακτηριστικά τους όπως η ασφάλεια που προσφέρουν ή να γίνουν πιο κατάλληλοι για διάφορες εφαρμογές. Τέσσερις είναι οι κυριότεροι τρόποι λειτουργίας :

3.1.4 Electronic Codebook (ECB)

Αυτός ο τρόπος λειτουργίας είναι ο απλούστερος και ο πλέον προφανής. Το μυστικό κλειδί χρησιμοποιείται για την κρυπτογράφηση κάθε μπλοκ δεδομένων του plaintext. Κατά συνέπεια με την χρήση του ίδιου κλειδιού, το ίδιο plaintext μπλοκ θα μετατρέπεται πάντα στο ίδιο ciphertext μπλοκ. Είναι ο πλέον κοινός τρόπος λειτουργίας των κρυπτογράφων μπλοκ γιατί είναι ο απλούστερος και άρα ο πιο εύκολα υλοποιήσιμος και συνάμα ο πιο γρήγορος καθώς δεν χρησιμοποιείται κάποιου είδους ανατροφοδότηση. Μειονέκτημα του είναι ότι είναι ο πιο ευάλωτος τρόπος κρυπτογράφησης σε επιθέσεις τύπου brute-force (ως επίθεση brute-force θεωρείται η προσπάθεια εύρεσης του μυστικού κλειδιού με την εξαντλητική δοκιμή πιθανών κλειδιών).

3.1.5 Cipher Block Chaining (CBC)

Χρησιμοποιώντας την CBC λειτουργία, προστίθεται σε έναν κρυπτογράφο μπλοκ ένας μηχανισμός ανατροφοδότησης. Ο τρόπος αυτός λειτουργίας ορίζει ότι προτού

να γίνει η κρυπτογράφηση ενός νέου μπλοκ plaintext, γίνεται XOR (αποκλειστικό-Ή) του μπλοκ αυτού και του ciphertext μπλοκ που μόλις πριν έχει παραχθεί. Με τον τρόπο αυτό, 2 ταυτόσημα μπλοκ plaintext δεν κρυπτογραφούνται ποτέ στο ίδιο ciphertext. Σε σχέση με τον ECB προσφέρεται μεγαλύτερη ασφάλεια, με κόστος όμως κυρίως στην ταχύτητα κρυπτογράφησης καθώς για να ξεκινήσει η επεξεργασία ενός μπλοκ plaintext είναι απαραίτητο να έχει ολοκληρωθεί πλήρως η κρυπτογράφηση του προηγούμενου μπλοκ. Αποτρέπεται έτσι η χρήση τεχνικών pipelining (software ή hardware) που μπορούν να επιταχύνουν την διαδικασία.

3.1.6 Cipher Feedback (CFB)

Ο τρόπος αυτός λειτουργίας επιτρέπει σε έναν κρυπτογράφο μπλοκ να συμπεριφερθεί σαν ένας κρυπτογράφος ροής. Αυτό είναι θεμιτό όταν πρέπει να κρυπτογραφούνται δεδομένα που μπορεί να έχουν μέγεθος μικρότερο από ένα μπλοκ. Παράδειγμα τέτοιας εφαρμογής μπορεί να είναι η διαδικασία κρυπτογράφησης ενός terminal session. Περιληπτικά, κατά την CFB λειτουργία χρησιμοποιείται ένας shift καταχωρητής στο μέγεθος του block μέσα στον οποίο τοποθετούνται τα δεδομένα προς κρυπτογράφηση. Όλος ο καταχωρητής κρυπτογραφείται και αυτό που προκύπτει είναι το ciphertext. Η ποσότητα των δεδομένων που μπαίνουν μέσα στον shift καταχωρητή καθορίζεται από την εφαρμογή.

3.1.7 Output Feedback (OFB)

Στόχος και αυτού του τρόπου λειτουργίας των μπλοκ κρυπτογράφων είναι να εξασφαλίσει ότι το ίδιο plaintext μπλοκ δεν μπορεί να παράγει το ίδιο ciphertext μπλοκ. Σε σχέση με το CBC, χρησιμοποιείται και εδώ ένας μηχανισμός ανατροφοδότησης παρόλα αυτά είναι εσωτερικός και ανεξάρτητος από τα plaintext και ciphertext δεδομένα. Σημαντικοί αλγόριθμοι αυτής της κατηγορίας είναι οι DES (Data Encryption Standard), 3DES, DESX, ο AES (Advanced Encryption Standard), οι RC2, RC4, RC5 και IDEA (International Data Encryption Algorithm). Οι αλγόριθμοι της σειράς DES είναι οι πλέον χρησιμοποιούμενοι σήμερα αλγόριθμοι, αν και πλέον αντικαθιστούνται από τον AES. Επινοήθηκαν από την IBM την δεκαετία του '70 και υιοθετήθηκαν από το National Bureau of

Standards (νυν NIST) των ΗΠΑ. Οι DES αλγόριθμοι χρησιμοποιούν κλειδιά μήκους 56 bits (ο 3DES και ο DESX επεκτείνουν κατάλληλα αυτόν τον αριθμό χρησιμοποιώντας περισσότερα κλειδιά) και επεξεργάζονται μπλοκ των 64 bits. Ο AES αλγόριθμος είναι το πρότυπο που καθιερώθηκε από το NIST ως διάδοχος του DES και πλέον αποτελεί τον προτεινόμενο αλγόριθμο κρυπτογράφησης για εφαρμογές υψηλής ασφάλειας. Οι αλγόριθμοι RC είναι αλγόριθμοι μεταβλητού κλειδιού από την RSA Security ενώ ο IDEA χρησιμοποιείται στο πρότυπο PGP (Pretty Good Privacy).

3.2 Είδη κρυπτογραφίας

Τα κρυπτοσυστήματα χωρίζονται σε δύο μεγάλες κατηγορίες, τα κλασσικά και τα μοντέρνα κρυπτοσυστήματα. Κάθε μία από αυτές τις κατηγορίες χωρίζεται σε υποκατηγορίες. Τα κλασσικά κρυπτοσυστήματα χωρίζονται σε αναδιάταξης, αντικατάστασης, σημειωματάριο μιας χρήσης και ρότορες. Τα κρυπτογραφήματα αναδιάταξης χωρίζονται σε πολυσταδιακές και μονοσταδιακές αναδιατάξεις. Τα κρυπτογραφήματα αντικατάστασης χωρίζονται σε μονοαλφαβιτικής, πολυαλφαβητικής, πολυγραμματικής και ομοφωνικής αντικατάστασης. Τα μοντέρνα κρυπτογραφήματα χωρίζονται σε συμμετρικά, τα οποία με τη σειρά τους χωρίζονται σε συμμετρικούς κρυπταλγορίθμους, ψευδοτυχαίες ακολουθίες, συναρτήσεις κατακερματισμού και ψηφιακές υπογραφές, και τα ασύμετρα, τα οποία χωρίζονται σε ασύμετρους κρυπταλγορίθμους και ψηφιακές υπογραφές. (1)

3.3 Εφαρμογές κρυπτογραφίας

- Ασφάλεια συναλλαγών σε τράπεζες δίκτυα – ATM
- Κινητή τηλεφωνία (ΤΕΤΡΑ-ΤΕΤΡΑΠΟΛ-GSM)
- Σταθερή τηλεφωνία (cryptophones)
- Διασφάλιση Εταιρικών πληροφοριών
- Στρατιωτικά δίκτυα (Τακτικά συστήματα επικοινωνιών μάχης)
- Διπλωματικά δίκτυα (Τηλεγραφήματα)

- Ηλεκτρονικές επιχειρήσεις (πιστωτικές κάρτες, πληρωμές)
- Ηλεκτρονική ψηφοφορία
- Ηλεκτρονική δημοπρασία
- Ηλεκτρονικό γραμματοκιβώτιο
- Συστήματα συναγερμών
- Συστήματα βιομετρικής αναγνώρισης
- Έξυπνες κάρτες
- Ιδιωτικά δίκτυα (VPN)
- Word Wide Web 65
- Δορυφορικές εφαρμογές (δορυφορική τηλεόραση)
- Ασύρματα δίκτυα (Hipperlan, 65luetooth, 802.11x)
- Συστήματα ιατρικών δεδομένων και άλλων βάσεων δεδομένων
- Τηλεσυνδιάσκεψη – Τηλεφωνία μέσω διαδικτύου (VOIP)

Η εξέλιξη της χρησιμοποίησης της κρυπτογραφίας ολοένα αυξάνεται καθιστώντας πλέον αξιόπιστη την μεταφορά της πληροφορίας για διαφόρους λειτουργικούς σκοπούς:

3.3.1 Έξυπνη κάρτα (smart card):

Είναι μια κάρτα της οποίας η εξωτερική εμφάνιση μοιάζει με μια πιστωτική κάρτα. Υπάρχουν όμως κάποιες διαφορές γιατί η ομοιότητα είναι μόνο στην εξωτερική τους εμφάνιση, εσωτερικά η έξυπνη κάρτα έχει ενσωματωμένο έναν μικροεπεξεργαστή, ο οποίος βρίσκεται κάτω από μια επαφή από χρυσό προσαρμοσμένο στη μια πλευρά της. Ενώ αντίθετα η πιστωτική κάρτα είναι πλαστική και έχει μια μαγνητική ταινία ενσωματωμένη, στην οποία είναι εγγεγραμμένα κάποια στοιχειά του ιδιοκτήτη/χρήστη Η βασικότερη διαφορά μεταξύ των δυο καρτών όμως είναι ότι στη μαγνητική ταινία της πιστωτικής κάρτας μπορούν εύκολα να διαφοροποιηθούν τα δεδομένα της η ακόμα και να καταστραφούν κάτι που είναι αδύνατο στην έξυπνη κάρτα, γιατί ο μικροεπεξεργαστής δεν περιέχει δεδομένα για τον χρήστη. Ο μικροεπεξεργαστής

της κάρτας και ο υπολογιστής με τον οποίο συνδέεται επικοινωνούν πριν ο μικροεπεξεργαστής επιτρέψει την πρόσβαση στα δεδομένα που περιέχονται στη μνήμη της κάρτας. Με τον τρόπο αυτό δεν επιτρέπεται σε κανέναν παρεμβολέα να παραχαράξει τα δεδομένα της και έτσι ο χρήστης διασφαλίζεται στην περίπτωση που η κάρτα του βρεθεί σε διαφορετική ιδιοκτησία. Οι έξυπνες κάρτες όπως και οι πιστωτικές κάρτες χρησιμοποιούνται για συναλλαγές μέσω Internet και ATM.

3.3.2 Ιδιωτικά Δίκτυα(VPNs):

Οι δρομολογητές (routers) και τα τείχη προστασίας (firewalls) χρησιμοποιούν κρυπτογραφία για την ασφαλή σύνδεση ενός υπολογιστή με ένα εταιρικό δίκτυο. Η αποδοχή της Αρχής Πιστοποίησης συνεπάγεται την προσθήκη ψηφιακών πιστοποιητικών στον browser του χρήστη του Internet. Με βάση τα ιδιαίτερα χαρακτηριστικέ του πιστοποιητικού αυτού, ο χρήστης έχει τη δυνατότητα να επισκεφτεί ασφαλείς δικτυακούς τόπους και να προσπελάσει δεδομένα, χωρίς αυτά να είναι δημοσιευμένα σε κοινή θέα.

3.3.3 Ηλεκτρονική ψηφοφορία:

Με τον όρο ηλεκτρονική ψηφοφορία εννοούμε την άσκηση του εκλογικού δικαιώματος, με την χρήση ηλεκτρονικών μεθόδων. Η διαδικασία της ηλεκτρονικής ψηφοφορίας πραγματοποιείται σε τέσσερα στάδια.

a. *Εγγραφή*: η εκλογική αρχή δημιουργεί την εκλογική λίστα και την δημοσιεύει στο δίκτυο. Ακολουθεί μια περίοδος όπου οι ψηφοφόροι μπορούν να εκθέσουν τις αντιρρήσεις τους.
b. *Ψηφοφορία*: όπου χωρίζεται σε 2 φάσεις :
    i. Επιβεβαίωση: περιλαμβάνει τον έλεγχο της εγκυρότητας αυτών που επιχειρούν να ψηφίσουν και επιτρέπει μόνο στους νόμιμους ψηφοφόρους που δεν έχουν ψηφίσει ακόμη να προχωρήσουν στη διαδικασία.
    ii. Συλλογή : Διαδικασία συλλογής των έγκυρων ψήφων.

c. *Καταμέτρηση*: Η αρχή συλλογής ψήφων σταματά να δέχεται ψήφους και αρχίζει την καταμέτρηση. Τα τελικά αποτελέσματα δίνονται στη δημοσιότητα.

Θεμελιώδες Απαιτήσεις Ασφάλειας

Η ψηφοφορία δεσμευτικού χαρακτήρα διέπεται από συνταγματικού κατοχυρωμένες καταστατικές αρχές.

- Καθολική ψηφοφορία
- Ισότητα της ψήφου
- Ελευθερία της ψήφου και της ψηφοφορίας
- Μυστικότητα της ψήφου
- Αμεσότητα της ψήφου και της ψηφοφορίας

Σε ένα σύστημα ηλεκτρονικής ψηφοφορίας, η εφαρμογή των πέντε καταστατικών αρχών προσδιορίζει ένα σύνολο θεμελιωδών απαιτήσεων ασφάλειας που πρέπει να ικανοποιούνται. Οι απαιτήσεις αυτές είναι οι εξής :

- Δημοκρατικότητα
- Ορθότητα – Ακρίβεια
- Μυστικότητα
- Μη αναγκαιότητα έκδοσης απόδειξης
- Προστασία από εξαναγκασμό
- Δικαιοσύνη
- Επαληθευσιμότητα
- Επαληθεύσιμη συμμετοχή
- Ανθεκτικότητα

3.3.4 Ηλεκτρονική Δημοπρασία :

Μια πλατφόρμα δημοπρασιών (ή ηλεκτρονική πλατφόρμα αγοραπωλησιών, ηλεκτρονική πλατφόρμα διεξαγωγής δημοπρασιών) είναι μια ιστοσελίδα που προσφέρει υπηρεσίες δημοπρασίας και πωλήσεων. Για να συμμετέχει κάποιος πρέπει να γραφτεί μέλος. Συνήθως η συμμετοχή είναι δωρεάν, ενώ πολλές φορές ο

πολίτης έχει να πληρώσει προμήθεια στην εταιρία που προσφέρει την υπηρεσία. Ορισμένες πλατφόρμες προσφέρουν και ηλεκτρονικά καταστήματα για εμπόρους που είναι συνδεδεμένα με την πλατφόρμα. Σε πολλές χώρες η πιο ισχυρή είναι το eBay, σε κάποιες Ευρωπαϊκές είναι το Ricardo σημαντικό και στην Κινά το TaoBao.

3.3.5 Δορυφορικές εφαρμογές (δορυφορική τηλεόραση):

Τηλεπικοινωνιακός δορυφόρος ονομάζεται ο μη επανδρωμένος τεχνητός δορυφόρος, μέσω του οποίου παρέχονται υπηρεσίες μεγάλων αποστάσεων, όπως τηλεοπτικής και ραδιοφωνικής μετάδοσης, τηλεφωνικών επικοινωνιών και συνδέσεων ηλεκτρονικών υπολογιστών. Για την επίτευξη της επικοινωνίας μέσω δορυφόρου είναι απαραίτητο να χρησιμοποιηθούν κάποια πρότυπα και πρωτόκολλα. Οι επίγειοι σταθμοί εκπέμπουν πλαίσια δεδομένων τα οποία μετατρέπονται σε σήματα συγκεκριμένης συχνότητας , από εκεί ο δορυφόρος τα εκπέμπει στη γη σε άλλη συχνότητα και στον επίγειο σταθμό μετατρέπονται σε πλαίσια δεδομένων.

Για το δορυφορικό διαδίκτυο υπάρχουν δυο τρόποι χρήσης του:

- Ο πρώτος τρόπος είναι η μονόδρομη δορυφορική σύνδεση, που επιτρέπει μόνο downloading. Πρόκειται δηλαδή για έναν συνδυασμό επίγειας και δορυφορικής σύνδεσης. Ο χρήστης ανεξάρτητα του τι επίγεια σύνδεση διαθέτει, πρέπει να εφοδιαστεί με το ειδικό δορυφορικό “ πιάτο” και την ειδική κάρτα σύνδεσης του δεκτή με τον υπολογιστή.
- Ο δεύτερος τρόπος δορυφορικής σύνδεσης που ανεξαρτητοποιεί εντελώς τον χρήστη από τα επίγεια καλώδια και τους τηλεφωνικούς –Διαδικτυακούς παρόδους είναι η αμφίδρομη δορυφορική σύνδεση, που προσφέρεται ειδικά για τις επιχειρήσεις σε χαμηλή τιμή.

3.3.6 Ασύρματα δίκτυα:

Ως ασύρματο δίκτυο χαρακτηρίζεται το τηλεπικοινωνιακό δίκτυο, συνήθως τηλεφωνικό ή δίκτυο υπολογιστών, το οποίο χρησιμοποιεί ραδιοκύματα ως φορείς πληροφορίας.

- Bluetooth:

  Στη μικρότερη τάξη μεγέθους ασύρματων δικτύων συναντάμε τα Bluetooth (WPAN), τοπικά δίκτυα πολύ μικρής εμβέλειας με σκοπό την ασύρματη δικτύωση ετερογενών φορητών συσκευών. Έχουν δημιουργηθεί διαφορετικά πρωτόκολλα για διαφορετικές εφαρμογές τα οποία ονομάζονται προφίλ και καθένα από αυτά περιλαμβάνει πρότυπα για όλα τα επίπεδα και προσφέρει λύσεις για τη διασύνδεση με διαφορετικά δίκτυα μεγαλύτερης κλίμακας.
- Ασύρματα τοπικά και προσωπικά δίκτυα:

Τα ασύρματα προσωπικά δίκτυα παρέχουν εύκολη διασύνδεση ετερογενών, φορητών συσκευών τοποθετημένων σε μικρή απόσταση μεταξύ τους. Παρόλο που είναι δίκτυα υπολογιστών δεν έχουν σχεδιαστεί για ενσωμάτωση σε μεγαλύτερα δίκτυα καθώς έχουν ως στόχο τις καταναλωτικές φορητές συσκευές περιορισμένων πόρων(κινητά τηλέφωνα, συσκευές αναπαραγωγής πολυμέσων). Αντίθετα, τα ασύρματα τοπικά δίκτυα συνήθως αποτελούν δίκτυα υπολογιστών με δυνατότητα ενσωμάτωσης σε ευρύτερα ενσύρματα ή ασύρματα δίκτυα. Τα ενσύρματα σικτυα παρέχουν ευελιξία, κινητικότητα και υπό προϋποθέσεις χαμηλότερο κόστος. Μπορούν να χρησιμοποιηθούν:

- Για ασύρματη επέκταση ενός προϋπάρχοντος ενσύρματου δικτύου, με έναν κόμβο να συνδέεται μέσω LAN και να επικοινωνεί με άλλους σταθμούς ασύρματα.
- Για διασύνδεση LAN σε διαφορετικά κτίρια, συνήθως με συνδέσεις από σημείο σε σημείο μεταξύ γεφυρών η δρομολογητών των επιμέρους LAN.
- Για παροδική ασύρματη ζεύξη μεταξύ LAN και κινητού τερματικού (νομαδική πρόσβαση)
- Για δικτύωση αδόμητη – ασύρματα δίκτυα ομότιμων κόμβων και αυθαίρετα μεταβαλλόμενης τοπολογίας τα οποία δεν απαιτούν καμία

προϋπάρχουσα υποδομή και δημιουργούνται δυναμικά, με κόμβους να προστίθενται αυτομάτως στο δίκτυο όταν βρίσκονται εντός της εμβέλειας του.

Τα WLAN λειτουργούν με ένα από τα τρία ακόλουθα φυσικά μέσα:

- υπέρυθρες ακτίνες
- μικροκύματα με διασπορά φάσματος
- μικροκύματα με στενή ζώνη

3.3.7 Τηλεσυνδιάσκεψη – Τηλεφωνία μέσω διαδικτύου (VoIP)

Το πρωτόκολλο επικοινωνίας SIP είναι ένα πρωτόκολλο επικοινωνίας μέσω δικτύων υπολογιστών που επιτρέπει την μεταφορά πολυμεσικών πληροφοριών είτε μέσω του διαδικτύου, είτε μέσω ενός τοπικού δικτύου. Για να εφαρμοστεί είναι απαραίτητη η χρήση ενός υπολογιστή που να έχει τον ρόλο του εξυπηρετητή SIP. Το SIP κατέχει πολύ σημαντική θέση στη διαδικτυακή τηλεφωνία, γιατί δεν δεσμεύει τον χρήστη σε κάποιο συγκεκριμένο πάροχο , εφόσον εάν έχει τις γνώσεις μπορεί να το αξιοποιήσει ατομικά , είτε μέσω των εκατοντάδων παρόχων VoIP με υποστήριξη SIP.

Η τηλεφωνία μέσω διαδικτύου ή Voice over IP ή VoIP χαρακτηρίζει μια ομάδα πρωτοκόλλων – τεχνολογιών, η οποία προσφέρει φωνητική συνομιλία σε πραγματικό χρόνο σε πολύ καλή ποιότητα και στην ουσία χωρίς κόστος. Παλιότερα οι συνομιλίες αυτές γίνονταν αποκλειστικά μέσω ηλεκτρονικού υπολογιστή που ήταν συνδεδεμένο στο διαδίκτυο. Πλέον υπάρχουν εφαρμογές σε κινητά τηλέφωνα που η μόνη προϋπόθεση είναι το smart phone να είναι συνδεδεμένο σε κάποιο δίκτυο. Η κλήση καταλήγει σε κάποιον άλλο χρήστη χωρίς να υπάρχει κάποια επιπλέον χρέωση πέραν αυτής για πρόσβαση στο διαδίκτυο, από την στιγμή που δεν μεσολαβεί κάποιος παραδοσιακός φορέας τηλεπικοινωνιών.

3.3.8 Global System for Mobile Communications

Το Παγκόσμιο Σύστημα Κινητών Επικοινωνιών είναι ένα κοινό Ευρωπαϊκό ψηφιακό σύστημα κινητής τηλεφωνίας. Είναι ένα κυψελοειδές ψηφιακό σύστημα κινητής τηλεφωνίας δεύτερης γενιάς, το οποίο χρησιμοποιεί ηλεκτρομαγνητικά σήματα και την τεχνική πολλαπλής πρόσβασης με διαχωρισμό του διαθέσιμου φάσματος συχνοτήτων σε ένα αριθμό καναλιών και την διαίρεση αυτών σε χρονοθυρίδες για την μετάδοση σημάτων.

Ένας χρήστης για να μπορέσει να χρησιμοποιήσει το δίκτυο τότε το δίκτυο θα πρέπει πρώτα να τον πιστοποιήσει. Για την επίτευξη αυτού κάθε κινητό πρέπει να διαθέτει ένα κρυμμένο κλειδί το οποίο βρίσκεται συγκεκριμένα στην κάρτα SIM του και στο Κέντρο Πιστοποίησης. Όταν ενεργοποιείται το κινητό, το κέντρο πιστοποίησης στέλνει ένα τυχαίο αριθμό στο κινητό και αυτόν τον αριθμό τον χρησιμοποιούν μαζί με το κρυμμένο κλειδί και με έναν κρυπτογραφημένο αλγόριθμο για την δημιουργία ενός νέου αριθμού. Το κινητό στέλνει πίσω στο κέντρο πιστοποίησης τον αριθμό αυτό και το κέντρο πιστοποίησης με την σειρά του ελέγχει αν είναι ίδιος με αυτόν που έφτιαξε. Αν ο αριθμός είναι ίδιος τότε ο χρήστης πιστοποιήθηκε ειδάλλως τον ειδοποιεί ότι η διαδικασία εγγραφής στο δίκτυο ήταν ανεπιτυχής. Κάθε κινητό τηλέφωνο έχει την δικιά του ταυτότητα IMEI των συνδρομητών της. Πρώτη λίστα είναι η λεύκη λίστα που υπάρχουν όλα τα IMEI των κινητών που λειτουργούν φυσιολογικά και μπορούν να συνδεθούν στο δίκτυο με ασφάλεια. Δεύτερη λίστα είναι η γκρι λίστα που υπάρχουν τα IMEI των κινητών που είναι υπό-παρακολούθηση λόγω πιθανών προβλημάτων που δημιουργούν. Τρίτη λίστα είναι η μαύρη λίστα που υπάρχουν τα IMEI των κινητών που έχουν δηλωθεί από του κατόχους τους σαν κλεμμένους ή απολεσθέν τους και ανάλογα την περίπτωση διενεργείται παρακολούθηση των κινητών αυτών αν χρησιμοποιούν ή την άρνηση εγγραφής τους με το δίκτυο, λειτουργιές αυτές ανήκουν στο MSC.

3.3.9 Ηλεκτρονικό γραμματοκιβώτιο

Το ηλεκτρονικό γραμματοκιβώτιο είναι ένα είδος ηλεκτρονικής θυρίδας στην οποία καταχωρούνται κάθε τύπου δεδομένα που στέλνονται από άλλες επιχειρήσεις. Η φυσική θέση του ηλεκτρονικού γραμματοκιβώτιου βρίσκεται στους δίσκους του φορέα. Ο χρήστης της ηλεκτρονικής θυρίδας μπορεί να διαβάσει τα δεδομένα ή τα μηνύματα. Παρέχοντας αυτές τις υπηρεσίες ο φορέας προσθέτει αξία στη μετάδοση των δεδομένων και γι αυτό το λέγεται ότι εκτελείται ένα δίκτυο προστιθεμένης αξίας. Είναι προφανές ότι μια ομάδα επιχειρήσεων θα πρέπει να συμφωνεί πλήρως προς τα πρότυπα της επικοινωνίας και τις παραστάσεις ώστε να λειτούργει επιτυχώς.

Αυτή η διαδικασία διασφαλίζει πολλά οφέλη :

- Τη διεκπεραίωση μια επιχειρησιακής συναλλαγής στον ελάχιστο χρόνο
- Τον περιορισμό της γραφειοκρατίας κατά τη διεκπεραίωση των συναλλαγών.
- Τη μείωση του κόστους της επεξεργασίας των συναλλαγών και της ανάγκης για ανθρώπινες επεμβάσεις.
- Ελαχιστοποίηση των ανθρώπινων λαθών, λόγω της μειωμένης ανθρώπινης εμπλοκής στις διαδικασίες.
- Το μόνο μειονέκτημα είναι το κόστος αγοράς και εγκατάστασης του απαραίτητου εξοπλισμού.

3.3.10 Συστήματα Ιατρικών δεδομένων και άλλων βάσεων δεδομένων

Η ιατρική μπορεί να καλύψει περιστατικά παγκοσμίως εκμεταλλευομένη το παγκόσμιο δίκτυο και τις δορυφορικές εφαρμογές. Κάνοντας χρήση του παγκόσμιου δικτύου κάποιος ιατρός μπορεί να κάνει:

- Τηλεδιάγνωση, που καλύπτει την από απόσταση μελέτη από ειδικούς των αποτελεσμάτων των ιατρικών εξετάσεων και τη σύνταξη σχετικών αναφορών.
- Τηλεθεραπεία, που καλύπτει την από απόσταση παρακολούθηση ασθενών, όπου ο ασθενής επισκεπτόμενος την πλησιέστερη προς τον τόπο διαμονής

του ιατρική μονάδα μπορεί να τυγχάνει ιατρικής φροντίδας από απομακρυσμένο ιατρικό κέντρο ως προς την πάθηση του.

- Τηλεκπαίδευση, που καλύπτει τις ανάγκες του ενεργού ιατρικού και παραϊατρικού προσωπικού για συνεχή ενημέρωση σε διάφορους τομείς της ιατρικής. Επιπλέον εξασφαλίζεται εκπαίδευση του υγιούς πληθυσμού για πρόληψη των νοσημάτων αλλά και προστασία και προαγωγή της υγείας.
- Τηλεσυμβουλευτική, που καλύπτει την ανάγκη ανταλλαγής απόψεων καθώς και την οργάνωση συμβουλίων ειδικών ιατρών για την αντιμετώπιση συγκεκριμένων σύνθετων καταστάσεων που απαιτείται η ταυτόχρονη μελέτη της κατάστασης του ασθενούς από ειδικούς διαφορετικών ειδικοτήτων.

Το αποτέλεσμα της εξέλιξης της ιατρικής μέσω του παγκόσμιου ιστού ήταν να δημιουργηθούν online βάσεις δεδομένων και βιβλιοθήκες. Οι πολίτες μπορούν να ενημερωθούν άμεσα και να θέσουν τις ερωτήσεις, απορίες ή ακόμη και να ζητήσουν βοήθεια για περιστατικά που τους απασχολούν. Οι ιατροί από την άλλη μπορούν να κρατήσουν τις διαγνώσεις τους στη βάση για μετέπειτα παρόμοια περιστατικά, να συλλέξουν πορίσματα από συναδέλφους τους από απόσταση, και να συγκεντρώσουν στατιστικά στοιχειά για περιστατικά και διαγνώσεις.

3.3.11 Συστήματα βιομετρικής αναγνώρισης

Ένα σύστημα βιομετρικής αναγνώρισης είναι μια εφαρμογή που χρησιμοποιείται για αυτοματοποιημένη αναγνώριση ή επιβεβαίωση της ταυτότητας ενός ατόμου από κάποια χαρακτηριστικά του όπως πρόσωπο ή δακτυλικά αποτυπώματα.

- Τα Συστήματα αναγνώρισης προτύπων ακολουθούν μια τυπική αρχιτεκτονική που περιλαμβάνει τέσσερα βασικά στάδια επεξεργασίας:
- Λήψη μετρήσεων για κάποιες από τις ιδιότητες του αντικειμένου που μας αφορούν
- Προεπεξεργασία των μετρήσεων για τη μείωση θορύβου και κανονικοποίηση των μετρήσεων
- Εξαγωγή χαρακτηριστικών με τα οποία γίνεται η διάκριση των προτύπων

- Ταξινόμηση, που περιλαμβάνει τη σύγκριση των χαρακτηριστικών του αντικειμένου με κάποια χαρακτηριστικά που το σύστημα ήδη γνωρίζει που ανήκουν, ώστε να το αντιστοιχήσει σε κάποια κλάση.

Για την επίτευξη ακόμα καλύτερων αποτελεσμάτων, με μεγαλύτερη εγκυρότητα, χρησιμοποιείται μια επιπλέον διαδικασία, γίνεται χρήση αλγορίθμων για τη μετατροπή ενός τμήματος της επιφάνειας σε μαθηματικές ακολουθίες, μετρήσιμες στο χώρο.

3.3.12 Σταθερή τηλεφωνία – Crypto phones

Τα Crypto phones είναι τηλέφωνα που παρέχουν ασφάλεια έναντι υποκλοπών και ηλεκτρονικής παρακολούθησης.

Η παρακολούθηση των τηλεπικοινωνιών έχει γίνει μια μεγάλη βιομηχανία και μάστιγα των τελευταίων ετών. Οι περισσότερες από τις μυστικές υπηρεσίες του κόσμου και πολλοί ιδιωτικοί οργανισμοί έχουν υποκλέψει τηλεφωνικές επικοινωνίες για να ληφθεί η στρατιωτική, οικονομική και πολιτική ενημέρωση. Η τιμή των απλών τηλεφωνικών κινητών συσκευών είναι πολύ χαμηλή που ο κάθε άνθρωπος μπορεί να την αντέξει οικονομικά και να τις χρησιμοποιήσει για δικό του συμφέρον. Οι πρόοδοι στην τεχνολογία έχουν καταστήσει δύσκολο να προσδιοριστεί ποιος παρεμβαίνει και καταγραφή ιδιωτικές επικοινωνίες.

Τα Crypto phones μπορούν να προστατεύουν τις κλήσεις από υποκλοπές με τη χρήση αλγορίθμων για την κρυπτογράφηση σημάτων. Τα τηλέφωνα αυτά έχουν ένα κρυπτογραφικό τσιπ που χειρίζεται την κρυπτογράφηση και αποκρυπτογράφηση. Δυο αλγόριθμοι είναι προγραμματισμένοι στο τσιπ:

- Ένας αλγόριθμος για ανταλλαγή κλειδιών για το πρωτόκολλο συμφωνίας κλειδιού
- Δεύτερος είναι ο αλγόριθμος συμμετρικού κλειδιού για την κρυπτογράφηση φωνής.

3.3.13 Τηλεγράφημα

Η τηλεγραφία είναι η μεγάλης απόστασης μετάδοση γραπτών μηνυμάτων, (τηλε – (μακριά) γραφή), χωρίς φυσική μεταφορά των επιστολών, αρχικά με την αλλαγή αντικειμένων που μπορούσαν να γίνουν ορατά από απόσταση (οπτική τηλεγραφία). Η ραδιοτηλεγραφία ή ασύρματη τηλεγραφία μεταδίδει μηνύματα με τη χρήση ραδιοκυμάτων.

Μηνύματα τηλεγραφίας τα οποία αποστέλλονται από χειριστές τηλεγράφων με χρήση σημάτων Μορς λέγονται τηλεγραφήματα. Τα τηλεγραφήματα θεωρούνται δεσμευτικά νομικά έγγραφα για την ολοκλήρωση εμπορικών συναλλαγών.

Τα σήματα Μορς ή κώδικας Μορς είναι μια μέθοδος για μετάδοση πληροφορίας με παλμούς μικρής και μεγάλης διάρκειας ή σημάδια (τελείες και παύλες). Επινοήθηκε για τη μετάδοση μηνυμάτων μέσω τηλεγράφου.

3.3.14 Στρατιωτικά δίκτυα – Τακτικά συστήματα επικοινωνιών μάχης

Το σύστημα επικοινωνιών ζώνης μάχης είναι ένα ψηφιακό τακτικό σύστημα επικοινωνιών που παρέχει επικοινωνίες υψηλής ασφάλειας, ποιότητας και αξιοπιστίας, ικανό να υποστηρίξει με μεγάλη ευκαμψία τα τακτικά σχέδια επιχειρήσεων στη ζώνη μάχης. Στους χρηστές του συστήματος παρέχονται δυνατότητες επικοινωνίας σε τηλεφωνία, τηλετυπία, τηλεομοιοτυπία και μετάδοση δεδομένων.

Τα τακτικά συστήματα επικοινωνιών στηρίζονται στην ανάπτυξη ενός πυκνού πλέγματος υπεραστικών κόμβων οι οποίοι αποτελούν τον κορμό του δικτύου στο γεωγραφικό χώρο που πρόκειται να εξυπηρετήσουν επικοινωνιακά.

3.4 Σύγχρονη Κρυπτογραφία

Η κρυπτογραφία χρησιμοποιείται μέχρι και σήμερα ως ένα χρήσιμο εργαλείο στην ασφάλεια πληροφοριών, δηλαδή την προστασία των δεδομένων ως τους την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητά τους. Τους εξετάσουμε τους σχετιζόμενους με την κρυπτογραφία βασικούς όρους: Κρυπτογραφικός

αλγόριθμος (cipher): αποτελείται από έναν αλγόριθμο κρυπτογράφησης και αποκρυπτογράφησης. Αλγόριθμος Κρυπτογράφησης: τους αλγόριθμος κρυπτογράφησης (Encryption) μετατρέπει τα δεδομένα σε μη αναγνώσιμη μορφή, με σκοπό την διασφάλιση τους εμπιστευτικότητας των δεδομένων (confidentiality). Η κρυπτογράφηση προσφέρει το ψηφιακό ισοδύναμο τους σφραγισμένου φακέλου. Αλγόριθμος Αποκρυπτογράφησης: τους αλγόριθμος αποκρυπτογράφησης (Decryption) αντιστρέφει την διαδικασία τους κρυπτογράφησης, μετατρέπει τα κρυπτογραφημένα δεδομένα στην αρχική τους μορφή. Κρυπτογραφικό κλειδί: η σύγχρονη κρυπτογραφία, χρησιμοποιεί ένα κλειδί (key), δηλαδή μία συμβολοσειρά η οποία μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση ή αποκρυπτογράφηση, καθώς και για τη δημιουργία ή επαλήθευση ψηφιακής υπογραφής. Τα κρυπτογραφικά κλειδιά μπορεί να χρησιμοποιούνται από συμμετρικούς ή μη συμμετρικούς (δημόσιου κλειδιού) κρυπτογραφικούς αλγόριθμους. (2)

3.5 Ιοί Υπολογιστών

Ο ιός είναι ένα πρόγραμμά το οποίο εισέρχεται στον υπολογιστή χωρίς την άδεια του χρήστη και προκαλεί προβλήματα, μικρά ή μεγάλα. Μπορεί να είναι απλά ενοχλητικός και να σου βγάζει μηνύματα ανά τυχαία χρονικά διαστήματα ή να πηγαίνει το ποντίκι όπου θέλει για λίγο. Μπορεί όμως να είναι και επικίνδυνος αποκτώντας πρόσβαση σε οποιοδήποτε αρχείο του υπολογιστή, χωρίς ο χρήστης να το καταλάβει. Κατ' επέκταση μπορεί να διαγράψει από προσωπικά αρχεία του χρήστη, ανεκτίμητης αξίας για αυτόν, μέχρι και ζωτικά για την ομαλή λειτουργία του υπολογιστή αρχεία. Φυσικά δεν στοχεύουν μόνο σε άτομα, αλλά και σε επιχειρήσεις. Ο προγραμματιστής του ιού μπορεί να αποκτήσει πρόσβαση σε οποιοδήποτε υπολογιστή “μολυσμένο” με τον ιό του. Μπορεί να υποκλέψει μέχρι και κρατικές πληροφορίες, όχι μόνο έγγραφα εταιριών. Αυτοί οι ιοί μπορεί να είναι κρυμμένοι μέσα σε ένα αρχείο και να ανοίξουν παράλληλα με την εκτέλεση του αρχείου, αλλά μπορούν να μεταδοθούν και μέσω μέσων μεταφοράς αρχείων, κάρτες μνήμης, δισκέτες, USB Sticks κ.α. Ένα νεότερο είδος ιού απλά σου κλέβει τα προσωπικά δεδομένα, και τα χρησιμοποιεί για δικούς του σκοπούς. Αυτοί είναι αρκετά δύσκολοι στον εντοπισμό τους και ακόμα και αν σου έχουν κλέψει τα

δεδομένα αυτά, ακόμα δεν το καταλαβαίνεις παρά όταν δεις κάποια "ύποπτη" κίνηση στους προσωπικούς σου λογαριασμούς Το είδος αυτό δεν χρειάζεται κάποιον συγκεκριμένο ξενιστή. Μπορεί απλά να διαδοθεί μέσω ηλεκτρονικού ταχυδρομείου Οι τελευταίοι είναι αρκετά επικίνδυνοι γιατί διαδίδονται κατά εκατομμύρια παγκοσμίως και σε ημερήσια βάση. Αυτοί, η πλειοψηφία τουλάχιστον, είναι οι – γνωστοί πια – δούρειοι ίπποι, κοινώς trojan. Με αυτούς θα ασχοληθούμε περισσότερο, επειδή είναι οι πιο διαδεδομένοι και λειτουργούν κρυφά, δεν τους καταλαβαίνει ούτε το αντιϊκό αρκετές φορές. Αμέσως μετά τη γέννηση των ιών βγήκε και το πρώτο αντιϊκό πρόγραμμα, που εντόπιζε τον ιό και τον διέγραφε. Αργότερα οι υπολογιστές απέκτησαν ένα, τουλάχιστον, στοιχειώδες τείχος προστασίας προς τους ιούς, ιδιαίτερα με την ραγδαία ανάπτυξη του διαδικτύου, αλλά εξακολουθούν να είναι αρκετά αδύναμα σε σχέση με τα προγράμματα τρίτων. Παρόλα αυτά όμως οι ιοί συνεχίζουν να εισβάλουν στους υπολογιστές μας και να προκαλούν προβλήματα. Θα έχετε την – εύλογη- απορία πως καταφέρνουν να περνάνε απαρατήρητοι "κάτω από τη μύτη" των προγραμμάτων αυτών, και εκεί έρχομαι να σας απαντήσω εγώ. Ας κάνουμε μια εισαγωγή στην φύση του ιού. Ο ιός είναι ουσιαστικά ένα πρόγραμμα, σαν όλα τα άλλα, με τη διαφορά ότι έχει την ικανότητα να αναπαράγεται και με αυτόν τον τρόπο να μεταφέρεται από υπολογιστή σε υπολογιστή. Ουσιαστικά ένας ιός εκτελεί διάφορες λειτουργίες, επιβλαβείς και μη, χωρίς την άδεια του χρήστη. Μπορεί να αντιγράφει/ διαγράφει αρχεία ή απλά να αναπαράγει τον εαυτό του, δεν έχει την άδεια όμως για να εκτελέσει κανένα από αυτά τα δύο. (2)

3.5.1 Η Ιστορία Των Ιών

Ο πρώτος ηλεκτρονικός υπολογιστής, δηλαδή που λειτουργούσε με ρεύμα και εκτελούσε μαθηματικές πράξεις ανά δευτερόλεπτο, κατασκευάστηκε το 1945. Ο πρώτος ιός κατασκευάστηκε αρκετά αργότερα, το 1971, και δεν είχε κάποιο σκοπό,απλά εμφάνιζε ένα μήνυμα στην οθόνη. Είχε επίσης την ικανότητα να αναπαράγεται, όποιον υπολογιστή έβρισκε στο δίκτυο τον μόλυνε. Άμεσα το πρώτο αντιϊκό δημιουργήθηκε για την καταπολέμηση του. Μετά από μια δεκαετία

περίπου δημιουργήθηκε και ο πρώτος ιός για προσωπικούς ηλεκτρονικούς υπολογιστές. Ούτε αυτός ήταν κακόβουλος, σαν το πρώτο απλά εμφάνιζε ένα ποιηματάκι στην οθόνη. Ήταν όμως ο πρώτος ιός "εκτός εργαστηρίου", που διαδόθηκε σε πολλά συστήματα, πέραν αυτού που δημιουργήθηκε. Μεταφερόταν μέσω μίας δισκέτας, η οποία περιείχε ένα παιχνίδι, και δεν ενεργοποιούνταν αμέσως. Μετά το 50ό άνοιγμα του παιχνιδιού άνοιγε και μόλυνε τον υπολογιστή. 67 Ήταν λοιπόν ο πρώτος ιός που χρησιμοποιούσε κάποια συνθήκη για την ενεργοποίηση του. Από εκείνη τη δεκαετία και μετά άρχισαν να εξαπλώνονται οι ιοί. Στην αρχή μέσω δισκετών, που ήταν το κύριο μέσο μεταφοράς αρχείων εκείνη την εποχή, και ύστερα μέσω δικτύων. Προσπαθούσαν να μολύνουν κοινόχρηστους φακέλους, ώστε να εξασφαλίσουν την ευκολότερη εξάπλωση τους σε όσο περισσότερους υπολογιστές γίνεται. Τη δεκαετία του '90 εμφανίστηκαν οι ιοί στις μακροεντολές του Microsoft Office. Με την εκτέλεση της μακροεντολής ο ιός ενεργοποιούνταν. Δεν είχε τη δυνατότητα όμως να αποστείλει μολυσμένα e-mail, παρά μόνο να κατάφερνε να μολύνει το Outlook. Ένας ιός έχει επίσης τη δυνατότητα να αποστείλει ένα άμεσο μύνημα με μία διεύθυνση, ώστε ο λήπτης του μηνύματος, πιστεύοντας πως προέρχεται από αξιόπιστη πηγή, να ανοίξει το σύνδεσμο και να μολυνθεί και ο δικός του υπολογιστής. (2)

3.5.2 Τύποι Ιών

Οι ιοί και τα worms είναι χωρισμένα σε πολλές κατηγορίες, με βάση το ποιό μέρος του υπολογιστή μολύνουν και πως ενεργοποιούνται,μερικές από τις πίο βασικές κατηγορίες είναι:

- Ιοί Τομέα Εκκίνησης (Boot Sector Viruses): Οι ιοί αυτοί μολύνουν το μέσο αποθήκευσης από το οποίο εκκινεί το λειτουργικό σύστημα. Πιο συγκεκριμένα μολύνει μία συγκεκριμένη εγγραφή, της οποίας ο ρόλος αναφέρθηκε πιο πάνω, φορτώνει το λειτουργικό σύστημα, και στη συνέχεια μολύνεται όλο το μέσο αποθήκευσης. Ακόμα και αν ένα μολυσμένο δευτερεύον μέσο αποθήκευσης μείνει στον υπολογιστή και γίνει επανεκκίνηση με αυτό συνδεδεμένο, τότε μολύνεται το πρωτεύον μέσο αποθήκευσης και, στη συνέχεια, όποιο άλλο δευτερεύον αποκτήσει πρόσβαση στον υπολογιστή. (2)

- Ιοί Προγραμμάτων: Αυτοί οι ιοί ενεργοποιούνται μέσω εκτελέσιμων προγραμμάτων. Όταν το πρόγραμμα αυτό εκτελείται τότε αποκτούν και αυτή πρόσβαση σε όσα αρχεία έχει πρόσβαση και το πρόγραμμα αυτό. Στη συνέχεια αντιγράφουν τον εαυτό τους, μολύνοντας όλο και περισσότερα αρχεία. (2)

- Πολυμερείς Ιοί: Οι πολυμερείς ιοί είναι ένας υβριδικός τύπος ιού, που συνδυάζει στοιχεία και από τους δύο προηγούμενους τύπους. Ξεκινούν μολύνοντας ένα αρχείο, και στην πορεία αποκτούν πρόσβαση στον τομέα εκκίνησης του μέσου αποθήκευσης. Είναι δύσκολοι ιοί, καθώς για να τους ξεφορτωθείς πρέπει να «απολυμάνεις» τόσο τα μολυσμένα αρχεία, όσο και τον μολυσμένο τομέα, αλλιώς τα αποτελέσματα είναι απλά προσωρινά. (2)

- "Κρυφοί" Ιοί: Αυτοί είναι οι "νιντζα" των ιών. Μπορούν να "ξεφύγουν" από τη σάρωση του αντιϊκού με μερικές, πονηρές, τακτικές. Μπορεί να αποκρύπτει κάποιο μολυσμένο αρχείο ή να στέλνει την σάρωση σε καθαρό τομέα κάθε φορά, κάνοντας την "σύλληψη" του αρκετά δύσκολη. Παρόλο που μπορεί να φαίνεται δύσκολος ιός, προγραμματιστικά, ο πρώτος ιός ήταν τέτοιου τύπου και μπορούσε να δημιουργήσει πολύ μεγάλα προβλήματα στους ανυποψίαστους χρήστες. (2)

- Πολυμορφικοί Ιοί: Οι πολυμορφικοί ιοί από την άλλη είναι οι "χαμαιλέοντες" της υπόθεσης. Κάθε φορά που μολύνουν ένα καινούργιο αρχείο αλλάζουν το σήμα τους, κάνοντας την εύρεση τους πραγματικό άθλο, ακόμα και για αυτά τα αντιϊκά. Κρυπτογραφούν τον εαυτό τους με μεταβλητό κλειδί, κάνοντας ακόμα και τους προγραμματιστές "ανίκανους" στην αρχή να τους βρουν. Οι τελευταίοι χρησιμοποιούν διάφορα σχήματα κρυπτογράφησης, από τα οποία μόνο ένα θα είναι ορατό σε όλα τα στάδια της μόλυνσης. (2)

- Ιοί Μακροεντολής: Αυτοί οι ιοί είναι προγραμματισμένοι σε μακροεντολές, οι οποίες εκτελούνται με το άνοιγμα της αντίστοιχης εφαρμογής. Αφού ενεργοποιηθεί μια φορά, στη συνέχει μολύνει κάθε αρχείο που

επεξεργάζεται με τη συγκεκριμένη εφαρμογή, αντιγράφοντας έτσι τον εαυτό του. Μπορούν ακόμα και να αποκτήσουν περαιτέρω πρόσβαση σε άλλα σημεία του υπολογιστή, όπως οι επαφές σου και να τις στέλνουν με e-mail. (2)

3.5.3 Worms

Για να εξαπλωθεί ένα worm δεν χρειάζεται κάποια ειδική παρέμβαση από το χρήστη. Το μόνο που χρειάζεται είναι να βρει μία έξοδο προς έναν άλλο υπολογιστή, και τότε μολύνει και εκείνον. Αυτό το είδος είναι κοινό σε δίκτυα υπολογιστών, και σχεδόν πάντα προκαλεί κάποια ζημιά στο δίκτυο. Ανάλογα τον προγραμματισμό τους μπορούν να βλάψουν το δίκτυο με πολλούς τρόπους, όπως να διαγράψουν αρχεία, να στείλουν αρχεία με e-mail, ακόμα και να επιτρέψουν την πρόσβαση τρίτων στον υπολογιστή, δίνοντας του πλήρη έλεγχο. Μπορούν όμως απλά να χρησιμοποιούν το δίκτυο καθυστερώντας έτσι την μεταφορά των δεδομένων. Είχαν γίνει κάποιες προσπάθειες για να φτιάξουν καλοπροαίρετα worms, αλλά βρήκαν αδιέξοδο στην πράξη από την θεωρία. (2)

3.5.4 Trojan

Οι Trojan ή δούρειοι ίπποι είναι ένα "ύπουλο" είδος ιού, θα μπορούσε κανείς να πει. Είναι malware, το οποίο είναι αρχικά για "κακόβουλο λογισμικό" (malicious software), και μεταμφιέζεται ώστε να μη γίνεται εύκολα αντιληπτός. Συνήθως παρουσιάζεται ως ένα αρχείο νόμιμο, που δεν παραβιάζει τους όρους χρήσης του λειτουργικού συστήματος και δεν γίνεται αντιληπτό ως απειλή από το αντιϊκό πρόγραμμα, ή ως ένα βοηθητικό πρόγραμμα. Τις περισσότερες φορές επισυνάπτονται σε εκτελέσιμα αρχεία, ώστε με το άνοιγμα του αρχείου αυτού να αποκτούν άμεση πρόσβαση στον κώδικα του υπολογιστή, στην μνήμη του και γενικά στα περισσότερα αρχεία. Ο πραγματικός τους σκοπός όμως είναι να βλάψουν τον υπολογιστή, να κλέψουν πληροφορίες ή ακόμα να επιτρέψουν την, απομακρυσμένη, πρόσβαση στο μηχάνημα από τρίτους. Τώρα πια είναι μακράν οι πιο διαδεδομένοι ιοί στο διαδίκτυο. Αυτό δεν το οφείλουν μόνο στην ικανότητα

τους να καμουφλάρονται, αλλά και στο ότι εκμεταλλεύονται τα worms με τρόπο τέτοιο ώστε να μπορούν να "ταξιδέψουν" στο διαδίκτυο γρήγορα και να χρησιμοποιούν τα κενά ασφαλείας των υπολογιστών για να εισέρχονται κατευθείαν στο πιο βολικό σημείο. Οι δούρειο ίπποι μπορεί να είναι "κρυμμένοι" μέσα στον κώδικα ενός προγράμματος, ξεγελώντας 68 τους χρήστες πως πρόκειται για το γνήσιο πρόγραμμα. Αν ένα άτομο επικοινωνεί με ένα άλλο μέσο κρυπτογραφημένων μηνυμάτων και ένας τρίτος θέλει να μάθει τι λένε, ακόμα και αν υποκλέψει τα μηνύματα, εφόσον είναι σε κρυπτογραφημένη μορφή θα του είναι άχρηστα. Εκεί παίρνει θέση ο δούρειος ίππος. Καμουφλαρισμένος σαν ένα καθημερινό πρόγραμμα, ίσως το πρόγραμμα ανταλλαγής μηνυμάτων ή το πρόγραμμα που κρυπτογραφεί- αποκρυπτογραφεί τα μηνύματα, καταφέρνει να υποκλέψει το κλειδί, χωρίς να το υποψιαστούν οι δύο συνομιλητές. Τότε το τρίτο άτομο μπορεί να υποκλέψει τα μηνύματα και να τα αποκρυπτογράφηση ή ακόμα, εφόσον έχει ήδη παρεμβληθεί στο δίκτυο ανταλλαγής μηνυμάτων, να εμποδίσει τα μηνύματα του ενός από το να φτάσουν στον παραλήπτη τους και στη θέση τους να στείλει δικά του μηνύματα, τα οποία θα εξυπηρετούν τους δικούς του σκοπούς. Βέβαια αυτή η τακτική έχει και μερικά αδύνατα σημεία, στα οποία όμως δεν θα αναφερθώ. Το πρόγραμμα μπορεί να στέλνει στοιχεία στον προγραμματιστή του χωρίς να χρειάζεται ο τελευταίος να μεσολαβήσει στο κανάλι ανταλλαγής μηνυμάτων, αρκεί ο τελευταίος να έχει προγραμματίσει και μία "πίσω πόρτα" στο πρόγραμμα αυτό. Σε ένα πρόγραμμα κρυπτογράφησης, όπως το προαναφερθέν, αυτό μπορεί να έχει τρομερές συνέπειες και για τις δύο πλευρές. Η μία πλευρά μαθαίνει όλες τις πληροφορίες που θέλει χωρίς ιδιαίτερο κόπο, ενώ η άλλη παθαίνει τρομερή ζημιά καθώς τα, προφανώς, απόρρητα μηνύματα της αποκαλύπτονται. Βέβαια μέχρι να το καταλάβει η δεύτερη πλευρά το ποιο πιθανό είναι να είναι αργά. (2)

3.6 Δημόσιο Κλειδί

Έχουμε δύο άτομα τα οποία θέλουν να ανταλλάξουν ένα κρυφό μήνυμα από το τηλέφωνο. Ο αποστολέας θα πρέπει πρώτα να το κρυπτογραφήσει. Για την κρυπτογράφηση του μηνύματος θα πρέπει να χρησιμοποιήσει ένα κλειδί το οποίο είναι κι εκείνο μυστικό. Έτσι θα υπάρχει πρόβλημα παράδοσης του κλειδιού στον δέκτη έτσι ώστε να μεταφερθεί το μήνυμα. Έτσι λοιπόν αν δύο άτομα

αποφασίσουν να ανταλλάξουν ένα μυστικό (κωδικοποιημένο μήνυμα) θα πρέπει πρώτα να ξέρουν και οι δύο ένα μυστικό (κλειδί). Ας υποθέσουμε πως έχουμε τρία άτομα ,την Μαρία τον Γιώργο και την Ελένη. Αρχικά η Μαρία θέλει να στείλει ένα μήνυμα στον Γιώργο, ίσως και το αντίστροφο και η Ελένη προσπαθεί να το κλέψει. Αν η Μαρία αποφασίσει να στείλει ιδιωτικά μηνύματα στον Γιώργο, κάθε φορά θα τα κρυπτογραφεί προηγουμένως χρησιμοποιώντας ξεχωριστό κλειδί. Αντιμετωπίζει όμως το πρόβλημα της παράδοσης των κλειδιών στον Γιώργο επειδή ο τρόπος μετάδοσης τους πρέπει να είναι ασφαλής. Ένας τρόπος για να μεταδοθεί με ασφαλή τρόπο το κλειδί είναι: να συναντιούνται μία φορά την εβδομάδα ο Γιώργος με την Μαρία για να ανταλλάσσουν τα κλειδιά που χρειάζονται για την αποκρυπτογράφηση των μηνυμάτων. Ο τρόπος είναι ασφαλής, αλλά και άβολος γιατί αν τύχει κάτι στον έναν από τους δύο, το σύστημα δεν μπορεί να λειτουργήσει. Κάποια στιγμή ένα πείραμα ήρθε να αναιρέσει τη λογική αυτή. Ας πούμε πως η Μαρία βάζει σε ένα σιδερένιο κουτί το μήνυμα που θέλει να στείλει στον Γιώργο και το κλειδώνει με λουκέτο και κλειδί. Το δίνει στο ταχυδρόμο και κρατάει το κλειδί. Ο Γιώργος παραλαμβάνει το κουτί με το μήνυμα αλλά δεν μπορεί να το ανοίξει διότι δεν έχει το κλειδί του λουκέτου. Για να αντιμετωπιστεί αυτό το πρόβλημα είναι να βγάλει η Μαρία αντίγραφο του κλειδιού της και να το δώσει στον Γιώργο όταν συναντηθούν. Συμπεραίνουμε λοιπόν πως δεν μπορούμε να αποφύγουμε την μετάδοση των κλειδιών. Αν μεταφράσουμε αυτή την ιστορία με κρυπτογραφικούς όρους, αν η Μαρία θέλει να κρυπτογραφήσει ένα μήνυμα έτσι ώστε να είναι δυνατό μόνο για τον Γιώργο να το αποκρυπτογραφήσει θα πρέπει να του δώσει ένα αντίγραφο του κλειδιού. Αν φανταστούμε το ίδιο σενάριο, η Μαρία θέλει να στείλει ένα ιδιαίτερα ιδιωτικό μήνυμα στον Γιώργο. Βάζει το μήνυμα της στο κουτί και το κλειδώνει με το λουκέτο, όταν το κουτί φτάσει στον Γιώργο εκείνος βάζει το δικό του λουκέτο στο κουτί και το κλειδώνει με το δικό του κλειδί και το επιστρέφει πάλι πίσω στη Μαρία. Όταν εκείνη παραλαμβάνει το κουτί αφαιρεί με το κλειδί της το λουκέτο της και το στέλνει πάλι πίσω στον Γιώργο. Παρατηρούμε τώρα πως το κουτί έχει μόνο ένα λουκέτο πάνω, το κλειδί του Γιώργου. Τώρα ο Γιώργος μπορεί να ανοίξει το λουκέτο γιατί το λουκέτο ανοίγει με το δικό του κλειδί. Αυτή η ιστορία μας αποκαλύπτει ένα μυστικό μήνυμα, ότι δηλαδή δύο άτομα μπορούν να επικοινωνήσουν κρυπτογραφημένα χωρίς να είναι απαραίτητη η ανταλλαγή κλειδιών. Με κρυπτογραφική ορολογία: Η Μαρία χρησιμοποιεί το κλειδί της για να

κρυπτογραφήσει ένα μήνυμα προς τον Γιώργο, εκείνος το κρυπτογραφεί με το δικό του κλειδί και το επιστρέφει στη Μαρία. ΗΜαρία λαμβάνει ένα διπλά κρυπτογραφημένο μήνυμα. Αποκρυπτογραφεί τη δική της κρυπτογράφηση και το στέλνει πίσω στον Γιώργο ο οποίος τώρα μπορεί να το αποκρυπτογραφήσει και να δει το μήνυμα. Το σύστημα αυτό δεν είναι και τόσο εύκολο για το λόγο ότι υπάρχει ένα πρόβλημα. Το πρόβλημα υπάρχει στη σειρά με την οποία γίνονται οι κρυπτογραφήσεις και οι αποκρυπτογραφήσεις. Η σειρά πρέπει να συμβαδίζει με τον κανόνα: 'τελευταίο προστιθέμενο, πρώτο αφαιρούμενο'. Διαφορετικά, το τελευταίο στάδιο της κρυπτογράφησης θα πρέπει να είναι το πρώτο το οποίο θα αποκρυπτογραφηθεί. Ας δούμε τι θα γινόταν εάν η σειρά κρυπτογράφησης δεν υπάκουε στον κανόνα. (2)

Κλειδί Μαρίας : 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

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

Κλειδί Γιώργου : 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

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

Μήνυμα : meet me at noon

Κρυπτογραφημένο με κλειδί Μαρίας : YYGC YG HC JBBJ

Κρυπτογραφημένο με κλειδί Γιώργου : LNNM LN OM EPPE

Αποκρυπτογραφημένο με κλ. Μαρίας : ZQQX ZQ LX KPPK

Αποκρυπτογραφημένο με κλ. Γιώργου : wnnt wn yt xbbx

Το μήνυμα δεν βγάζει νόημα επειδή αποκρυπτογραφήθηκε με λανθασμένη σειρά. Αυτό έκανε δύο κρυπτογράφους, τους Ντίφι και Χέλμαν να κάνουν μια έρευνα σχετικά με την προσπέραση του βήματος ανταλλαγής κλειδιών. Εξέτασαν έτσι

διάφορες μαθηματικές συναρτήσεις. Οι περισσότερες συναρτήσεις λέγονται αμφιμονοσήμαντες διότι εκτελούνται και αναστρέφονται εύκολα. Ας τις παρομοιάσουμε με μία καθημερινή μας συνήθεια. Ανάβουμε το φως με τον διακόπτη, η πράξη αυτή είναι μια συνάρτηση επειδή μετατρέπει έναν λαμπτήρα σε αναμμένο λαμπτήρα. Αυτή είναι μια αμφιμονοσήμαντη συνάρτηση γιατί είναι απόλυτα εύκολο όπως άναψα το φως να το σβήσω και να το επαναφέρω στην αρχική του κατάσταση. Οι δύο αυτοί κρυπτογράφοι, έστρεψαν την προσοχή τους στις μονοσήμαντες συναρτήσεις, τις συναρτήσεις δηλαδή που εύκολα εκτελούνται αλλά δύσκολα ακυρώνονται. Π.χ η ανάμειξη δύο χρωμάτων είναι μονοσήμαντη συνάρτηση γιατί είναι δύσκολο να επαναφέρω τα δύο χρώματα στην αρχική τους κατάσταση. (2)

3.6.1 Τρόπος Κρυπτογράφησης

Ο τρόπος που κρυπτογραφείται ένα μήνυμα είναι μαθηματικός. Η κρυπτογράφηση γίνεται με βάση την μοδιακή συνάρτηση. Η ιδέα ήταν του κρυπτογράφου Ουίτφιλντ Ντίφι. Εξετάζουμε μια κυκλική διάταξη των αριθμών.

Για παράδειγμα, έχουμε ένα ρολόι με 7 αριθμούς, από το 0 έως το 6. Το ρολόι αυτό αναπαριστά το μοδιακό 7 (modulo 7). Για να βρούμε το άθροισμα 2+3 ξεκινάμε από το 2 και προχωράμε 3 θέσεις και βρίσκουμε το 5. Για να βρούμε όμως το άθροισμα 2+6 ξεκινάμε ξανά από το 2 και προχωράμε 6 θέσεις. Αυτή τη φορά περνάμε από την αρχή του κύκλου και φτάνουμε στο 1 και έτσι βλέπουμε πως το αποτέλεσμα είναι διαφορετικό από αυτό που θα είχαμε στα κανονικά μαθηματικά.

Δηλαδή: 2+3=5 (modulo 7) 2+6=1 (modulo 7) Αντί οι μαθηματικοί να φαντάζονται ρολόγια κάνουν το εξής για τους υπολογισμούς:

- Κάνουν την πράξη στα κανονικά μαθηματικά.

- Για να βρουν την απάντηση στη (modulo x) διαιρούμε την κανονική απάντηση δια του x και σημειώνουμε το υπόλοιπο. Το υπόλοιπο που θα βρούμε είναι η απάντηση στη (modulo x). 72 Π.χ 11 Χ 9 (modulo 13) = $11 \cdot 9 \rightarrow 99/13 = 7$, υπόλοιπο $8 \rightarrow 11 \cdot 9 = 8$ (modulo 13)

x	1	2	3	5	6
3^x	3	9	27	243	729
3^x(modulo 7)	3	2	6	5	1

Τώρα ας δούμε πως ο Γιώργος και η Μαρία κατάφεραν να ανταλλάξουν ιδιωτικά πληροφορίες μέσω μια κοινής γραμμής τηλεφώνου με την Εύα , χωρίς να καταφέρει να υποκλέψει το μήνυμα. Αρχικά ο Γιώργος και η Μαρία συμφωνούν στις τιμές που θα πάρουν τα Υ κ Ρ, πρέπει όμως Υ < Ρ . Οι τιμές αυτές είναι δημόσιες. Άρα:

Στάδιο 1:

Μαρία: Η Μαρία επιλέγει έναν αριθμό π.χ το 3 και τον κρατά κρυφό. Τον ονομάζουμε Α.

Γιώργος: Ο Γιώργος επιλέγει έναν αριθμό π.χ το 6 και τον κρατά κρυφό. Τον ονομάζουμε Β.

Στάδιο 2:

Μαρία: Η Μαρία εισάγει το 3 στην μονοσήμαντη συνάρτηση και βρίσκει το αποτέλεσμα της πράξης 7^A (modulo 11) → 7^3 (mod 11) = 343(mod 11) = 2.

Γιώργος: Ο Γιώργος εισάγει το 3 στην μονοσήμαντη συνάρτηση και βρίσκει το αποτέλεσμα της πράξης $7^{\mathbf{B}}$ (modulo 11) → 7^6 (mod 11) = 117.649 (mod11) = 4.

Στάδιο 3:

Σε αυτό το στάδιο, η Μαρία και ο Γιώργος ανταλλάσσουν πληροφορίες και η Εύα έχει τη δυνατότητα να κρυφακούσει τις λεπτομέρειες της ανταλλαγής. Τελικά η Εύα μπορεί να κρυφακούσει και το σύστημα να παραμείνει ασφαλές. Ο Γιώργος και η Μαρία ανταλλάσσουν τις αξίες των Υ και Ρ δημόσια και η Εύα κλέβει τους

αριθμούς 2 και 4. Αυτοί οι αριθμοί δεν είναι το κλειδί και έτσι είναι άχρηστοι στην Εύα.

Στάδιο 4:

Η Μαρία παίρνει το αποτέλεσμα του Γιώργου και βρίσκει το αποτέλεσμα της πράξης $\beta^A \pmod{11} \rightarrow 4^3 \pmod{11} = 4^3 \pmod{11} = 64 \pmod{11} = 9$

Ο Γιώργος παίρνει το αποτέλεσμα της Μαρίας και βρίσκει το αποτέλεσμα της πράξης $\alpha^B \pmod{11} \rightarrow 4^3 \pmod{11} = 2^6 \pmod{11} = 64 \pmod{11} = 9$

Το Κλειδί:

Η Μαρία και Ο Γιώργος κατέληξαν στον ίδιο αριθμό , το 9. Αυτό είναι το κλειδί.

3.7. Κρυπτογραφία και προστασία Δικτύου.

Σε αυτή την ενότητα θα ασχοληθούμε με τις δυνατότητες της κρυπτογραφίας στην διασφάλιση προστασίας ενός συνδεδεμένου στο δίκτυο συστήματος από εισβολείς.

3.7.1 Συναρτήσεις ανασκόπησης μηνύματος

Είναι μαθηματικές συναρτήσεις που όταν εφαρμοστούν σε ένα αρχείο επιστρέφουν έναν αριθμό γνωστό ως ανασκόπηση (digest) που παρέχει ένα σχεδόν μοναδικό χαρακτηρισμό του αρχείου . Ένα παράδειγμα μιας ιδιαίτερα αναποτελεσματικής συνάρτησης ανασκόπησης μηνύματος θα ήταν αν για κάθε χαρακτήρα του αρχείου με τη σειρά προσθέταμε τους κωδικούς bit τους και παίρναμε στο τέλος το υπόλοιπο του αθροίσματος αυτού με ένα πολύ μεγάλο αριθμό. Μια συνάρτηση ανασκόπησης μηνύματος θα πρέπει να έχει τα εξής χαρακτηριστικά:

Κάθε κομμάτι της εισόδου στη συνάρτηση θα πρέπει να επηρεάζει το αποτέλεσμα. Αν κάποιος κωδικός bit χαρακτήρα στην είσοδο της συνάρτησης ανασκόπησης μηνύματος μεταβληθεί, τότε το κάθε bit στο αποτέλεσμα της συνάρτησης θα έχει

πιθανότητα να αλλάξει. Θα πρέπει να είναι υπολογιστικά ανέφικτο να βρεθούν δυο αρχεία που να δίνουν ίδια τιμή συνάρτησης ανασκόπηση μηνύματος. Υπάρχουν διάφορες χρήσεις αυτών των συναρτήσεων. Μια χρήση είναι να ανακαλύψουμε αν κάποιο αρχείο στο σύστημα έχει μεταβληθεί είτε από εισβολέα είτε από ιό. Στα πρώτα χρόνια εμφάνισης των ιών ήταν εύκολο να τους διακρίνει και να τους εντοπίσει κανείς απλά κοιτώντας το μέγεθος σε bytes του κώδικα. Ωστόσο αυτό το πρόβλημα οι κατασκευαστές ιών κατάφεραν να το επιλύσουν και να παρακάμψουν αυτό το εμπόδιο είτε φτιάχνοντας ιούς οι οποίοι κόβουν χρήσιμο κώδικα από υπάρχοντα προγράμματα και ενσωματώνουν τον εαυτό τους έτσι ώστε το μέγεθος του αρχείου να φαίνεται ακριβώς ίδιο, είτε παραπλανώντας το ίδιο το λειτουργικό σύστημα και το σύστημα αρχείων σχετικά με το πραγματικό μέγεθος του αρχείου. Γι αυτό ένας τρόπος να εντοπιστούν αλλαγές σε αρχεία είναι να συγκριθεί το αποτέλεσμα της συνάρτησης ανασκόπησης του αρχείου με την προηγούμενη τιμή. Αν είναι ίδια τότε υπάρχει πολύ μεγάλη πιθανότητα το αρχείο να μην έχει τροποποιηθεί, αλλά αν δεν είναι ίδια τότε το αρχείο σίγουρα έχει υποστεί τροποποίηση. (7)

Υπάρχει μια σειρά συναρτήσεων ανασκόπησης μηνύματος και σχετικών τεχνολογιών που έχουν αναπτυχθεί.

3.7.2 Η τεχνική HMAC:

Είναι μια τεχνική που χρησιμοποιείται ια να ελέγχεται αν κάποιο αρχείο έχει τροποποιηθεί. Χρησιμοποιεί μια συνάρτηση μηνύματος και ένα ιδιωτικό κλειδί. Μια συνάρτηση ανασκόπησης μηνύματος στο κείμενο, κρυπτογραφείται και αποστέλλεται με το κείμενο. Ο παραλήπτης αποκρυπτογραφεί την ανασκόπηση μηνύματος, χρησιμοποιεί τη συνάρτηση ανασκόπησης πάνω στο κείμενο και συγκρίνει τα δυο αποτελέσματα. Αν τα αποτελέσματα συμφωνούν τότε το μήνυμα δεν έχει τροποποιηθεί. (7)

3.7.3 Η σειρά MD:

Είναι μια σειρά συναρτήσεων ανασκόπησης μηνύματος. Όλες παράγουν ως αποτέλεσμα μια ανασκόπηση των εκατό είκοσι οκτώ (128) bit. Διαφέρουν μεταξύ τους όσον αφορά την ταχύτητα με την όποια μπορούν να υπολογιστούν και την αντοχή της συνάρτησης : το πόσο εύκολο είναι να ανακαλύψει κανείς ένα αρχείο που δίνει το ίδιο αποτέλεσμα με ένα άλλο. (7)

3.7.4 Η σειρά SHA

Αυτές οι συναρτήσεις ανασκόπησης μηνύματος αναπτύχτηκαν από την αμερικανική εθνική υπηρεσία ασφάλειας. Παράγουν ανασκοπήσεις μεγέθους εκατό εξήντα (160) bit. Υπάρχουν και άλλες χρήσεις των συναρτήσεων ανασκόπησης μηνύματος εκτός από τον έλεγχο αρχείων για παραποίηση. Χρησιμοποιούνται και για κώδικες πιστοποίησης μηνύματος. Σε αυτή την χρήση υπολογίζεται το αποτέλεσμα της συνάρτησης για ένα μήνυμα το οποίο στέλνεται από κάποιον αποστολέα σε κάποιον παραλήπτη και στη συνέχεια επισυνάπτεται στο τέλος του μηνύματος. Και οι δυο πλευρές πρέπει να χρησιμοποιούν την ίδια συνάρτηση ανασκόπησης μηνύματος. Ο αποστολέας θα τη χρησιμοποιήσει για να υπολογίσει τον αριθμό που πρέπει να επισυνάψει στο μήνυμα και ο παραλήπτης θα την χρησιμοποιήσει για να υπολογίσει και επαληθεύσει τον αριθμό ανασκόπησης του μηνύματος που παρέλαβε. Αν η τιμή που υπολόγισε ο παραλήπτης είναι ίδια με αυτή που υπήρχε στο τέλος του μηνύματος, τότε είναι πιθανό πως δεν υπήρξε παραποίηση του μηνύματος κατά τη μεταφορά του από το τηλεπικοινωνιακό δίκτυο. (7)

Άλλη μια χρήση των συναρτήσεων ανασκόπησης μηνύματος είναι η παραγωγή ενός συνθηματικού από μια σειρά λέξεων γνωστή ως συνθηματική φράση (passphrase). Τέτοιες φράσεις χρησιμοποιούνται για να θυμάται κάποιος ένα δύσκολο συνθηματικό. Οι συναρτήσεις ανασκόπησης μηνύματος χρησιμοποιούνται και σε ψηφιακές υπογραφές.

3.7.5 Ψηφιακές υπογραφές

Μια ψηφιακή υπογραφή είναι κάποια δεδομένα τα οποία με μοναδικό τρόπο προσδιορίζουν κάποιο άτομο ή οργανισμό. Οι ψηφιακές υπογραφές βασίζονται σε συναρτήσεις ανασκόπησης μηνύματος και στη κρυπτογραφία δημόσιου κλειδιού. Η λειτουργία του είναι όταν ο αποστολέας έχει δημοσιοποιήσει το δημόσιο κλειδί του, και οι δυο πλευρές γνωρίζουν τη συνάρτηση ανασκόπησης μηνύματος που χρησιμοποιείται, τότε πραγματοποιούνται τα βήματα : ο αποστολέας υπολογίζει την ανασκόπηση του μηνύματος που θέλει να στείλει. Η ανασκόπηση κρυπτογραφείται χρησιμοποιώντας το ιδιωτικό κλειδί. Αυτή είναι η ψηφιακή υπογραφή. Το μήνυμα μαζί με την ψηφιακή υπογραφή στέλνεται στον παραλήπτη. Ο παραλήπτης αποκρυπτογραφεί την ψηφιακή υπογραφή χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα για να πάρει την ανασκόπηση. Ο παραλήπτης στη συνέχεια υπολογίζει την ανασκόπηση χρησιμοποιώντας την ίδια συνάρτηση ανασκόπησης μηνύματος και τη συγκρίνει με την αποκρυπτογραφημένη τιμή. Αν ταιριάζουν το μήνυμα έχει σταλεί πράγματι από τον κάτοχο του κλειδιού που χρησιμοποιήθηκε. Είναι σημαντικό να σημειώσουμε ότι οι ψηφιακές υπογραφές αποδεικνύουν αδιάψευστα αν το μήνυμα έχει παραποιηθεί κατά τη μεταφορά του. Στοιχειοθετούν την ακεραιότητα του μηνύματος αλλά όχι και την ιδιωτικότητα δηλαδή δεν μπορούμε να γνωρίζουμε αν έχει διαβαστεί από κάποιον τρίτο. (7)

3.7.6 Ψηφιακά πιστοποιητικά

Το πρόβλημα που αντιμετωπίζεται με τα συστήματα δημοσίου κλειδιού είναι ότι ενώ παρέχουν τη δυνατότητα ασφαλούς επικοινωνίας μεταξύ ατόμων δεν επιτρέπουν εύκολα πιο δημόσιες μορφές επικοινωνίας. Δεν υπάρχει τρόπος πιστοποίησης και ταυτοποίησης κάποιου ατόμου που δημοσιεύει ένα συγκεκριμένο κλειδί ότι είναι πράγματι αυτός που ισχυρίζεται πως είναι.

3.7.7 Πρότυπο x209. v3

Το πρότυπο x209. v3 είναι πιθανότατα το πιο διαδεδομένο πρότυπο για ψηφιακά πιστοποιητικά. Περιέχει όλα τα στοιχεία σχετικά με τις ψηφιακές υπογραφές και

επιπλέον περιγράφει την δυνατότητα των ψηφιακών πιστοποιητικών να περιλαμβάνουν ζευγάρια ονόματος – τιμής που βοηθούν την πιστοποίηση. Για παράδειγμα ένα πιστοποιητικό που ορίζεται μπορεί να περιλαμβάνει πληροφορίες σχετικά με το ποια συνάρτηση ανασκόπησης μηνύματος χρησιμοποιήθηκε για να δημιουργήσει την ψηφιακή υπογραφή του πιστοποιητικού.

Για την επίλυση του προβλήματος αυτού έχουν αναπτυχθεί τα ψηφιακά πιστοποιητικά. Ένα ψηφιακό πιστοποιητικό είναι ένα έγγραφο που εκδίδεται από έναν έμπιστο τρίτο οργανισμό και δίνει στοιχειά για έναν χρήστη. Το πιστοποιητικό θα περιέχει στοιχειά όπως το όνομα του χρήστη, ένα μοναδικό σειριακό αριθμό και το δημόσιο κλειδί του. Το πιστοποιητικό θα έχει μια ψηφιακή υπογραφή του οργανισμού που το εξέδωσε. Για να πιστοποιήσει την αυθεντικότητα ενός ψηφιακού πιστοποιητικού , ο παραλήπτης ενός μηνύματος θα πρέπει να έχει το δημόσιο κλειδί του έμπιστου οργανισμού που το εξέδωσε. Συχνά, πολλά από τα κλειδιά μεγάλων δημοσίων οργανισμών περιλαμβάνονται σε λογισμικό όπως οι φυλλομετρητές.

Ο πελάτης για να πειστεί ότι διαλέγεται με μια συγκεκριμένη οντότητα όπως μια εταιρία, πρέπει να εκτελέσει τις ακόλουθες διαδικασίες αφού έχει εκδοθεί το πιστοποιητικό.

Να αποκτήσει το δημόσιο κλειδί. Να ελέγξει ότι η υπογραφή που παρέχεται από την υπηρεσία πιστοποίησης είναι έγκυρη χρησιμοποιώντας το δημόσιο κλειδί της. Είναι πιθανόν αυτό να υπάρχει στο φυλλομετρητή. Να χρησιμοποιήσει το δημόσιο κλειδί που υπάρχει στο ψηφιακό πιστοποιητικό για να κρυπτογραφήσει τα δεδομένα που θέλει να στείλει στον κάτοχο του πιστοποιητικού. Κάποιες φορές τα δεδομένα μπορεί απλά να είναι ένα κλειδί το οποίο θα χρησιμοποιηθεί στη συνέχεια μεταξύ των δυο πλευρών για επικοινωνία μέσω κάποιας απλούστερης μεθόδου συμμετρικού κλειδιού. Ένα πρακτικό παράδειγμα αποτελούν τα ψηφιακά πιστοποιητικά που σχετίζονται με την τεχνολογία Επίπεδο Ασφαλών Συναρμογών (Secure Sockets Layer (SSL) . Το SSL συνήθως χρησιμοποιείται για την αποστολή κρυπτογραφημένων μηνυμάτων μεταξύ ενός περιηγητή και ενός διακομιστή.

Όταν ένας περιηγητής συνδέεται με ένα διακομιστή διαδικτύου που χρησιμοποιεί SSL, το πρώτο πράγμα που πραγματοποιείται είναι ο διακομιστής να στείλει στον περιηγητή ένα ψηφιακό πιστοποιητικό τύπου x209. v3 το οποίο περιέχει το

δημόσιο κλειδί του διακομιστή. Ο φυλλομετρητής τότε ελέγχει την εγκυρότητα του πιστοποιητικού εξετάζοντας την ψηφιακή του υπογραφή . Αν ο έλεγχος είναι επιτυχής , τότε το ενσωματωμένο στο πιστοποιητικό δημόσιο κλειδί χρησιμοποιείται από τον πελάτη για την αποκωδικοποίηση των αρχικών πληροφοριών που στέλνει ο διακομιστής. Η αρχική εγκατάσταση της σύνδεσης περιλαμβάνει και κάποια συμφωνία για το πώς θα γίνει στη συνέχεια η επικοινωνία μεταξύ των δυο πλευρών.

Υπάρχουν τέσσερα είδη ψηφιακών υπογραφών που χρησιμοποιούνται στο διαδίκτυο. Όλα ακλουθούν το πρότυπο x209. v3 **.**

1. Πιστοποιητικά αρχών πιστοποίησης. Αυτά χρησιμοποιούνται για την πιστοποίηση της ταυτότητας μιας αρχής που εκδίδει ψηφιακά πιστοποιητικά.
2. Πιστοποιητικά διακομιστή. Αυτά πιστοποιούν ένα διακομιστή αποδεικνύοντας ότι είναι αυτός που ισχυρίζεται πως είναι. Τέτοια πιστοποιητικά χρησιμοποιούνται σε συνδυασμό με κάποια άλλη τεχνολογία όπως το SSL.
3. Προσωπικά πιστοποιητικά. Αυτά πιστοποιούν μεμονωμένα άτομα.
4. Πιστοποιητικά εταιριών λογισμικού. Αυτά χρησιμοποιούνται για να πιστοποιούν προγράμματα τα οποία πωλούνται και διανέμονται.

3.8 Κρυπτογραφικά συστήματα

Ο στόχος αυτής της ενότητας είναι να περιγράψει τις λεπτομέρειες κάποιων εμπορικών προϊόντων που χρησιμοποιούν τεχνικές κρυπτογραφίας. Μερικά από αυτά τα προϊόντα είναι πακέτα λογισμικού ενώ αλλά παρέχουν υπηρεσίες αποστολής δεδομένων και είναι οντότητες που βρίσκονται βαθιά κρυμμένες μέσα στο λογισμικό συστήματος.

3.8.1 PGP

Αυτό είναι ένα δημόσια διαθέσιμο σύστημα για κρυπτογράφηση αρχείων και μηνυμάτων e-ταχυδρομείου. Ήταν ένα από τα πρώτα εμπορικά προϊόντα που χρησιμοποιούσαν κρυπτογραφία δημόσιου κλειδιού. Χρησιμοποιεί τη μέθοδο RSA για την ανταλλαγή συμμετρικών κλειδιών, τον αλγόριθμο IDEA για την αποστολή δεδομένων χρησιμοποιώντας το συμμετρικό κλειδί που ανταλλάχτηκε με τη μέθοδο RSA και τη μέθοδο MD5 για την διασφάλιση της ακεραιότητας των μηνυμάτων.

Το PGP είναι διαθέσιμο είτε σαν ένα ξεχωριστό σύστημα για e-ταχυδρομείο είτε σαν ένα πακέτο για κρυπτογράφηση αρχείων. Η βασική αδυναμία του συστήματος είναι η διαχείριση των ιδιωτικών κλειδιών . Αν η μυστικότητα ενός ιδιωτικού κλειδιού τεθεί σε κίνδυνο, τότε θα πρέπει να σταλεί ένα πιστοποιητικό ανάκλησης σε οποιονδήποτε επικοινωνεί με το άτομο ή οργανισμό που κατέχει το κλειδί.

Στο PGP ένα δημόσιο κλειδί είτε διαφημίζεται σε ειδικούς διακομιστείς δημοσίων κλειδιών είτε αναπαράγεται σε κάποια ιστοσελίδα.

3.8.2 PCT

Αυτό είναι ένα προϊόν της Microsoft το οποίο είναι παρόμοιο με το SSL. Καθώς το SSL γίνεται όλο και πιο δημοφιλές, αναμένεται ότι αυτή η τεχνολογία θα πέψη να χρησιμοποιείται.

3.8.3 SHTTP

Αυτή είναι μια έκδοση του πρωτοκόλλου HTTP που επιτρέπει ασφαλείς συναλλαγές μέσω του ιστού. Ωστόσο, καθώς οι κατασκευαστές περιηγητών δεν έδειξαν μεγάλο ενδιαφέρων γι αυτό , δεν χρησιμοποιείται σχεδόν καθόλου.

3.8.4 SET

Αυτό είναι ένα πρωτόκολλο το οποίο χρησιμοποιείται για αποστολή στοιχείων πιστωτικών καρτών μέσω του διαδικτύου. Έχει τρία συστατικά στοιχειά : ένα e-πορτοφόλι που βρίσκεται στον υπολογιστή του πελάτη, ένα διακομιστή SET, για

τον οποίο είναι υπεύθυνος κάποιος πωλητής ή έμπορος και ένα διακομιστή πληρωμών που βρίσκεται σε μια τράπεζα ή σε μια εταιρία πιστωτικών καρτών.

Το πρώτο πράγμα που πρέπει να κάνει ο χρήστης όταν χρησιμοποιεί το SET είναι να εισάγει τα στοιχειά της πιστωτικής του κάρτας στο e-πορτοφόλι του. Αυτά θα αποθηκευτούν σε ένα κρυπτογραφημένο αρχείο στον υπολογιστή του χρηστή. Παράλληλα, το πρόγραμμα που διαχειρίζεται το Set στον υπολογιστή του χρηστή θα παράγει ένα δημόσιο και ένα ιδιωτικό κλειδί.

Όταν πραγματοποιείται μια αγορά από έναν χρηστή του SET, τα στοιχειά της πιστωτικής κάρτας κρυπτογραφούνται με το δημόσιο κλειδί και στέλνονται στον έμπορο του προϊόντος το οποίο θα πληρωθεί με την πιστωτική κάρτα. Ο διακομιστής του εμπόρου επισυνάπτει μια ψηφιακή υπογραφή στις λεπτομέρειες της πιστωτικής κάρτας για να προσδιορίσει την ταυτότητα του εμπόρου. Κατόπιν όλα μαζί στέλνονται στον υπολογιστή της τράπεζας ή της εταιρίας πιστωτικών καρτών. Αυτός ο υπολογιστής επιβεβαιώνει την κάρτα και στέλνει μια απόδειξη στον έμπορο και στον πελάτη. Ένα πλεονέκτημα αυτής της τεχνολογίας είναι ότι ο έμπορος δεν μπορεί να δει τις λεπτομέρειες της πιστωτικής κάρτας και η τράπεζα δε γνωρίζει τι αγόρασε ο πελάτης, κάτι που ελαχιστοποιεί τον κίνδυνο άπατης.

3.8.5 DNSSEC

Αυτά είναι τα αρχικά για το Πρότυπο Ασφάλειας Συστήματος Ονομάτων Πεδίων (Domain Name System Security Standard). Σχεδιάστηκε για να αποτρέψει επιθέσεις όπως τη παραποίηση DNS. Και αυτό χρησιμοποίει κρυπτογραφία δημόσιου κλειδιού, όπου κάθε διακομιστής ονομάτων σχετίζεται με ένα ζευγάρι δημόσιου- ιδιωτικού κλειδιού. Σε κάθε όνομα διεύθυνσης στο διαδίκτυο ανατίθεται ένα δημόσιο κλειδί το οποίο χρησιμοποιείται από τους συνδεδεμένους στο διαδίκτυο υπολογιστές για να το πιστοποιήσουν.

3.8.6 Kerberos

Αυτό είναι ένα δικτυακό σύστημα ασφαλείας το οποίο αναπτύχτηκε στο MIT. Χρησιμοποιεί κρυπτογραφία συμμετρικού κλειδιού για τη μετάδοση μηνυμάτων από και προς υπολογιστές συνδεδεμένους σε ένα δίκτυο και χρησιμοποιείται για πιστοποίηση χρηστών. Κάθε χρήστης του Kerberos έχει ένα συνθηματικό το οποίο χρησιμοποιεί για την αποστολή και τη λήψη δεδομένων. Υπάρχουν εκδόσεις του

Kerberos για δημοφιλή διαδικτυακά πρωτόκολλα όπως το POP3, το Telnet και το FTP.

3.8.7 Ανταλλαγή κλειδιών

Μια χρήση της κρυπτογραφίας δημοσίου κλειδιού είναι για τη μεταφορά μιας μυστικής πληροφορίας όπως ένα κλειδί που χρησιμοποιείται σε ένα συμμετρικό σύστημα. Ένα παράδειγμα είναι το σύστημα ανταλλαγής κλειδιών των Diffie-Hellman. Αυτή είναι μια τεχνική που χρησιμοποιείται για να προστατέψει ένα κλειδί που χρησιμοποιείται σε συμμετρικά συστήματα. Με αυτό, οι δυο πλευρές που πρόκειται να επικοινωνήσουν πρώτα ανταλλάσσουν πληροφορίες για το συμμετρικό κλειδί χρησιμοποιώντας κρυπτογραφία δημόσιου κλειδιού.

ΚΕΦΑΛΑΙΟ 4: ΟΙΚΟΝΟΜΟΛΟΓΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ

4.1 Τι ορίζουμε ως Οικονομολογική Κρυπτογραφία

Οικονομολογική Κρυπτογραφία είναι η χρήση της κρυπτογραφίας σε εφαρμογές στις οποίες οι οικονομικές απώλειες θα μπορούσαν να προκύψουν από την ανατροπή το συστήματος μηνυμάτων. Οι «κρυπτογράφοι» σκέφτονται τον οικονομικό τομέα ως μια περιοχή παραγωγής βασισμένο στο έργο του Δρ. Ντέιβιντ Τσαμ που εφηύρε την κρυφή υπογραφή. Αυτή η ειδική μορφή κρυπτογραφημένης υπογραφής επιτρέπει σε ένα εικονικό νόμισμα να υπογραφεί, χωρίς να χρειάζεται η παρουσία του υπογράφοντα για να δει το πραγματικό νόμισμα. Η συγκεκριμένη διαδικασία καθιστά δυνατή μια μορφή ψηφιακών συμβολικών χρημάτων που προσφέρονται ανώνυμα. Αυτή η μορφή είναι διαδεδομένη ως ψηφιακό νόμισμα. (8)

Ένας ευρέως χρησιμοποιούμενος και ανεπτυγμένος κατά το παρελθόν κρυπτογραφικός μηχανισμός είναι τα Πρότυπα Κρυπτογράφησης Δεδομένων, τα οποία χρησιμοποιούνται κυρίως για την προστασία των ηλεκτρονικών εμβασμάτων και μεταφορών. Ωστόσο, ήταν έργο του Ντέιβιντ Τσαμ, που ενθουσίασε την «κρυπτογραφική κοινότητα» σχετικά με τις δυνατότητες των κρυπτογραφημένων μηνυμάτων ως πραγματικά χρηματοοικονομικά και χρηματοδοτικά μέσα. (8)

Η οικονομολογική Κρυπτογραφία περιλαμβάνει μηχανισμούς και αλγορίθμους οι οποίοι είναι αναγκαίοι για την προστασία των οικονομικών μεταβιβάσεων, εκτός από την δημιουργία νέων μορφών χρήματος. Απόδειξη των εργασιών αυτών και των διαφόρων πρωτοκόλλων δημοπρασίας τα οποία εμπίπτουν κάτω από την ομπρέλα της οικονομολογικής κρυπτογραφίας, είναι ο μετρητής κατακερματισμού χρησιμοποιείται για τον περιορισμό των ενοχλητικών μηνυμάτων τύπου spam. Η οικονομολογική κρυπτογραφία διακρίνεται από την παραδοσιακή μορφή και έννοια της κρυπτογραφίας καθώς στο μεγαλύτερο μέρος της ιστορίας έχει καταγραφεί πως χρησιμοποιείται σχεδόν εξ ολοκλήρου για στρατιωτικά και διπλωματικά θέματα. (8)

Ως μέρος ενός επιχειρηματικού μοντέλου, η οικονομολογική κρυπτογραφία ακολούθησε τον οδηγό της κρυπτογραφίας και μόνο οι πιο απλές ιδέες έγιναν αποδεκτές και εγκρίθηκαν. Συστήματα χρηματικών λογαριασμών προστατεύονται από το SSL, όπως Pay-Pal και το e-Gold τα οποία γνώρισαν μια σχετική επιτυχία, αλλά και πιο καινοτόμους μηχανισμούς ασφαλείας όπως τα κρυφά συμβολικά χρήματα κλπ.

Αξίζει να σημειωθεί ότι η οικονομολογική κρυπτογραφία θεωρείται, αρκετά συχνά πως μπορεί και καλύπτει ένα ευρύ πεδίο εφαρμογής. Σύμφωνα με τον Ian Grigg, η οικονομολογική κρυπτογραφία μπορεί να διαιρεθεί σε επτά διαφορετικά επίπεδα, τα οποία θα αναλύσουμε παρακάτω. Αυτά τα επτά επίπεδα είναι ένας συνδυασμός μεταξύ διαφορετικών ειδικοτήτων όπως η κρυπτογραφία, η τεχνολογία λογισμικού, τα δικαιώματα, τη λογιστική, τη διακυβέρνηση, την αξία, και αρκετές οικονομικές εφαρμογές. Σύμφωνα λοιπόν με αυτές τις ειδικότητες, οι επιχειρηματικές αποτυχίες μπορούν να οφείλονται στην απουσία ενός ή περισσότερων από αυτούς τους κλάδους, ή ακόμα και στην κακή εφαρμογή τους. Για αυτό το λόγω η οικονομολογική Κρυπτογραφία θεωρείται ως ένα διεπιστημονικό θέμα, δεδομένου ότι η οικονομία και η κρυπτογραφία είναι το καθένα ξεχωριστά βασισμένο πάνω σε πολλαπλές ειδικότητες. (8)

4.2. Οικονομολογική Κρυπτογραφία των 7 επιπέδων.

4.2.1 Εισαγωγή στο μοντέλο των 7 επιπέδων.

Η οικονομολογική κρυπτογράφηση σύμφωνα με τον Ian Grigg, είναι αρκετά περίπλοκη διότι απαιτεί ικανότητες που προέρχονται από ποικίλους και ασυμβίβαστους μεταξύ τους επιστημονικούς κλάδους. Η συγκεκριμένη επιστήμη βρίσκεται μεταξύ των Κεντρικών Τραπεζών και της Κρυπτογραφίας ή ακόμα καλύτερα μεταξύ των λογιστών και των προγραμματιστών, οι οποίοι κάνουν προσπάθειες για την κατασκευή ενός οικονομολογικού συστήματος κρυπτογράφησης, το οποίο θα απλοποιήσει ή καλύτερα θα παραλείψει τους κρίσιμους επιστημονικούς κλάδους. (9)

Η Οικονομολογική Κρυπτογραφία φαίνεται να είναι μια επιστήμη ή αλλιώς μια τέχνη, που βρίσκεται σε ένα ειδικό σημείο συνάντησης μεταξύ πολλών διαφορετικών κλάδων και ειδικοτήτων όπως:

- Λογιστική και Έλεγχος
- Προγραμματισμός
- Αρχιτεκτονική Συστημάτων
- Κρυπτογραφία
- Οικονομικά
- Διαδίκτυο
- Ασφάλεια
- Χρηματοδότηση και τραπεζικές συναλλαγές
- Κίνδυνος
- Εμπορία και Διανομή
- Δραστηριότητες Κεντρικών Τραπεζικών

Με τόσες πολλές και διαφορετικές ειδικότητες τα προβλήματα είναι σίγουρο πως θα προκύψουν και αυτό είναι αναπόφευκτο αλλά όχι λανθασμένο. Δεν είναι μόνο η αναπόφευκτη σπατάλη και σύγχυση των πόρων, αλλά και η δυσκολία στην απόκτηση τεχνικών, την διαχείριση και το ταλέντο στο μάρκετινγκ που μπορούν άνετα να εργαστούν στον τομέα. (9)

Ως πρώτο βήμα για να γίνουν καλύτερα κατανοητά τα έργα της Οικονομολογικής Κρυπτογραφίας, χρησιμοποιείται αρκετά συχνά μια διαφορετική διάρθρωση των κλάδων σε μοντέλα τα οποία βοηθούν το διάλογο, τις συγκρίσεις αλλά και την ορθή λήψη αποφάσεων.

Στο συγκεκριμένο μοντέλο των επτά επιπέδων παρουσιάζεται μια μέθοδος η οποία επιχειρεί να περιγράψει έναν εισαγωγικό τρόπο για την ενίσχυση κατά την εκμάθηση. Σε αυτό το μοντέλο οι όροι Κρυπτογραφία και Οικονομία είναι «απλωμένοι» με σκοπό να αποκαλύψουν τους κλάδους που βρίσκονται κρυμμένοι χωρίς να το γνωρίζουμε.

Φυσικά, κανένα μοντέλο δεν μπορεί να καλύψει σε βάθος αλλά και σε εύρος τόσο πειστικά ένα τόσο περίπλοκο ζήτημα. Σκοπός του συγκεκριμένου μοντέλου, είναι να γίνει αντιληπτός και κατανοητός ο τομέας μέσα από τον προσδιορισμό των

σχέσεων μεταξύ των κλάδων, χωρίς να χρειαστεί να ξοδευτεί πολύς χρόνος για την λεπτομερή φύση του κάθε στοιχείου. Συνεπώς, το βάθος «θυσιάζεται» για το εύρος. (9)

4.2.2 Το μοντέλο των 7 επιπέδων

Στον παρακάτω πίνακα παρουσιάζεται το μοντέλο των επτά επιπέδων σύμφωνα με το Ανοιχτό Σύστημα Διασύνδεσης Μοντέλων Αναφοράς.

7. Οικονομία	Εφαρμογές για χρηματοδοτικούς χρήστες, εκδότες ψηφιακής αξίας και αγορά και εμπορία των επιχειρήσεων.
6. Αξία	Μέσα τα οποία ασκού ή φέρουν κάποια χρηματική ή άλλη αξία.
5. Διακυβέρνηση	Προστασία του συστήματος από μη-τεχνικής φύσεως απειλές.
4. Λογιστική	Πλαίσιο το οποίο εμπεριέχει την αξία μέσα σε ελεγχόμενες και καθορισμένες θέσεις.
3. Δικαιώματα	Μια ιδέα ελέγχου ταυτότητας, με την ιδιοκτησία που διατίθεται για μονάδες αξίας, και μεθόδους για μετακίνηση των τιμών μονάδας μεταξύ στοιχείων ταυτότητας και μονάδας.
2. Τεχνολογία Λογισμικού	Τα εργαλεία για μετακίνηση των πληροφοριών μέσα από το διαδίκτυο, και να παραμείνουν οι πληροφορίες και τα νούμερα σταθερά και αξιόπιστα στους κόμβους.

1. Κρυπτογραφία	Μαθηματικές τεχνικές για να δηλώσουν ορισμένες αλήθειες που μπορεί να μοιραστούν μεταξύ των μερών της αξίας.

Ένα πλεονέκτημα αυτού του μοντέλου είναι η διάσχιση από το τεχνικό κομμάτι στην εφαρμογή, δίνοντας έτσι βασικά και εύκολα σημεία εισόδου. Ο πιο συνηθισμένος τρόπος εφαρμογής είναι να ξεκινήσουμε, όπως φαίνεται και στο σχήμα, από την οικονομία και να συνεχίσουμε προς τα κάτω. Από την άλλη πλευρά όμως, μπορούμε να αρχίσουμε την εφαρμογή μας από το στρώμα της Κρυπτογράφησης και σύμφωνα με κάποια ειδικά πακέτα εργαλείων να προσφέρουμε στα υψηλότερα στρώματα. Υπάρχει δηλαδή μια αναλογία μεταξύ των πιο εξελιγμένων χαμηλών επιπέδων του μοντέλου και των υψηλότερων, καθώς όσο πιο εξελιγμένα είναι τόσο καλύτερες επιλογές για το επίπεδο της οικονομίας μπορούμε να έχουμε. (9)

4.2.3 Επίπεδο Κρυπτογραφία

Στο τελευταίο επίπεδο του μοντέλου βρίσκεται η Κρυπτογραφία. Σε κάποιο βαθμό, η καθαρή περιοχή της επιστήμης της κρυπτογραφίας λύνει τα προβλήματα μόνο από μαθηματική πλευρά, αλλά παρέχει χρήσιμες ιδιότητες συμπεριλαμβανομένων:

- Εμπιστευτικότητα – Αλγορίθμους κρυπτογράφησης
- Ακεραιότητα
- Έλεγχο ταυτότητας – ψηφιακές υπογραφές

Η Κρυπτογραφία, επίσης, μπορεί να λύσει ειδικά προβλήματα, όταν φυσικά αυτά είναι διαμορφωμένα σωστά. Για παράδειγμα, πως μπορεί η Αλίκη να υπογράψει μία δήλωση του Μπομπ, χωρίς να λάβει γνώση του περιεχομένου της δήλωσης.

4.2.4 Επίπεδο Τεχνολογίας Λογισμικού

Η Τεχνολογία Λογισμικού ή αλλιώς Software Engineering χρειάζεται να βρίσκεται στο ακριβώς επόμενο επίπεδο από την κρυπτογραφία για να μπορέσει να αντλήσει όλες τις ιδιότητες του προηγούμενου επιπέδου. Έτσι μπορούν να συνδυαστούν

άψογα η θεωρεία βάσεων δεδομένων (ατομικότητα, συναλλαγή, ακεραιότητα και ανάκτηση) μαζί με την θεωρεία δικτύων (ανατροφοδότηση) για να προσθέσουμε και άλλα στοιχεία όπως η αξιοπιστία και η ευρωστία.

Η Τεχνολογία Λογισμικού μας παρέχει ένα πρακτικό δίκτυο. Μας δίνει την δυνατότητα να στείλουμε ένα μήνυμα σε ένα ανοικτό δίκτυο, όπου γνωρίζουμε πως τελικά θα σταλεί στον παραλήπτη. Με τις τεχνικές ακεραιότητας του προηγούμενου επιπέδου, μπορούμε να γνωρίζουμε ότι οι πληροφορίες που έλαβε ο παραλήπτης ήταν ακριβώς όπως εστάλησαν. Με την χρήση των εξειδικευμένων ακολουθιών της θεωρίας της βάσης δεδομένων, μπορούμε να διατηρήσουμε την ακεραιότητα των μηνυμάτων με την πάροδο του χρόνου, για την αντιμετώπιση τυχόν προβλημάτων λογισμικού ή τεχνολογίας υλικών. (9)

4.2.5 Επίπεδο Δικαιώματα

Με την βοήθεια τόσο της Κρυπτογραφίας όσο και της Τεχνολογίας Λογισμικού μπορούμε να έχουμε δίκτυο πάνω στο οποίο μπορούμε να βασιστούμε, και να σκεφτούμε την διανομή μηνυμάτων που έχουν σχεδιαστεί για τους σκοπούς της Οικονομολογικής Κρυπτογραφίας. Σε αυτό το επίπεδο των Δικαιωμάτων, προσπαθούμε να δημιουργήσουμε ένα πρωτόκολλο το οποίο θα παρέχει στον χρήστη των έλεγχο των περιουσιακών στοιχείων σύμφωνα με έναν καθορισμένο τρόπο. Τεχνικές που αποσκοπούν στην επίτευξη του στόχου αυτού περιλαμβάνουν:

- Συστήματα ελέγχου ταυτότητας που βασίζονται σε αυτά των τραπεζικών συστημάτων. Σε γενικές γραμμές, τα συστήματα αυτά βασίζονται στην παροχή (σε έναν ήδη υπάρχοντα κάτοχο λογαριασμού) ενός αριθμού λογαριασμού και τον κωδικό πρόσβασης τα οπαία δίνουν την δυνατότητα πρόσβασης στον λογαριασμό του χρήση μέσω μιας κρυπτογραφημένης SSL ιστοσελίδας.
- Ειδικά Χρήματα τα οποία εξομοιώνουν τα ανώνυμα χρηματικά μέσα με τα οποία οι καταναλωτές είναι εξοικειωμένοι.
- Μηχανισμοί Μεταφοράς για άλλα συστήματα πληρωμών, όπως η χρήση των συστημάτων που βασίζονται σε SSL για να μεταφέρουν στοιχεία της πιστωτικής κάρτας.

- Υβριδικά Συστήματα, τα οποία αποφεύγουν απορρίπτουν την εφαρμογή των λύσεων του μοντέλου από κάτω προς τα πάνω, καθώς θα ανταποκρίνονται περισσότερο στην δύναμη και τους περιορισμούς του δικτύου. Για παράδειγμα, ο SOX είναι ένα τέτοιο σύστημα το οποίο παρουσιάζεται στο επόμενο τμήμα. Μια παραλλαγή αυτού του θέματος της περιβαλλοντικής εμπάθειας, είναι η γλώσσα E η οποία είναι κατασκευασμένη από ισχυρές δυνατότητες και έννοιες, και έτσι μπορεί εύκολα να μετατραπεί σε μια μορφή οικονομολογικής κρυπτογραφησης.
- Λύσεις βασισμένες στην τεχνολογία υλικών (Hardware) όπως είναι οι έξυπνες κάρτες.

4.2.6 Επίπεδο Λογιστική

Στα προηγούμενα επίπεδα αναλύσαμε μεθόδους που είναι επαρκώς αξιόπιστες και μπορούν να χρησιμοποιηθούν για κάτι αξιόλογο, πάνω σε ένα ακατάλληλο δίκτυο, το οποίο το ονομάζουμε δικαιώματα. Τώρα σε αυτό το επίπεδο χρειαζόμαστε τις τεχνικές της λογιστικής, προκειμένου να αποθηκεύουν και να διαχειρίζονται τα δικαιώματα με την πάροδο του χρόνου. Οι κρυπτογράφοι που ασχολούνται με τα οικονομικά θέματα θεωρούν ότι η λογιστική είναι ένας κοινότυπος τομέας, και αυτό ίσως την κάνει πιο ελκυστική για να μπορέσει να την αγνοήσει, αλλά η εμπειρία δείχνει ότι τα συστήματα δίχως συμβατικά λογιστικά χαρακτηριστικά τείνουν να χάνουν την αξία που τους έχει ανατεθεί. (9)

Οι τεχνικές της «λογιστικής πειθαρχίας» περιλαμβάνουν διπλογραφική λογιστική, ισολογισμούς, και την λογιστική παρακολούθηση. Οι λογιστικές έννοιες επιτρέπουν στους κατασκευαστές των οικονομολογικών κρυπτογραφικών συστημάτων να κατασκευάσουν πολύπλοκα συστήματα τα οποία εγγυάται ότι δεν θα χαθεί καμία αξία εφόσον όλοι οι χρήστες ακολουθούν τους κανόνες και θα μπορεί να εντοπίζει όσους δεν τους ακολουθούν.

Το παραπάνω επίπεδο ορίζει ουσιαστικά τι πρέπει ακριβώς να λαμβάνεται υπόψη. Ως παράδειγμα θα μπορούσε να αποτελέσει η πιο βασική μέθοδος τα ειδικά ή αλλιώς συμβολικά χρήματα. Ένα λογιστικό μοντέλο που βασίζεται σε μάρκες ή σε κέρματα θα χρειαζόταν ένα απλό κατάστημα κερμάτων για έναν πελάτη. Ο

διακομιστής θα είναι πιο περίπλοκος, καθώς απαιτεί έναν λογαριασμό ανέκδοτης αξίας, έναν απλό λογαριασμό και μία διπλή δαπάνης βάση δεδομένων η οποία θα ταιριάζει κάθε φορά το ποσό του απλού λογαριασμού.

4.2.7 Επίπεδο Διακυβέρνηση

Καθώς δεν υπάρχει εγγύηση ότι τα ψηφιακά ποσά – οι λογιστικοί αριθμοί – υπό διαχείριση μπορούν να περάσουν με ασφάλεια μέσα από το Διαδίκτυο, και στους ασφαλείς κόμβους, θα πρέπει να τεθεί υπό συζήτηση η ασφάλεια για ευρύτερες απειλές έξω από τον τεχνικό τομέα. (9)

Σε κάθε τεχνολογική εργασία, είτε πρόκειται για διαπραγμάτευση ή για αγορά της μετρητοίς, η απειλή της κλοπής ή της κατάχρησης υπάρχει από την πλευρά που εμπιστεύτηκε τη διαχείριση του συστήματος. Το πρόβλημα αυτό, γνωστό ως πρόβλημα οργανισμού, μπορεί να ξεπεραστεί με μια ευρεία ποικιλία από τεχνικές που θα έχουν ως κύρια ετικέτα τους την διαχείριση – διοίκηση – διακυβέρνηση.

Η Διακυβέρνηση περιλαμβάνει αυτές τις τεχνικές:

- Παρακαταθήκη αξίας σε αξιόπιστους τρίτους. Για παράδειγμα, τα κεφάλαια που αποτελούν εγγενή όρο για το δολάριο θα πρέπει να τοποθετηθούν σε έναν τραπεζικό λογαριασμό.
- Διαχωρισμός των αρμοδιοτήτων: διαχείριση της ρουτίνας από την δημιουργία αξίας, έλεγχος ταυτότητας από την λογιστική, συστήματα από το μάρκετινγκ.
- Διαφορές διαδικασιών επίλυσης, όπως η διαμεσολάβηση, διαιτησία, διαμεσολαβητές και το δικαστικό σώμα.
- Χρήση των τρίτων για κάποιο σημείο του πρωτοκόλλου, όπως είναι η δημιουργία αξίας εντός ενός κλειστού συστήματος.
- Τεχνικές ελέγχου που επιτρέπουν την εξωτερική παρακολούθηση των επιδόσεων και των περιουσιακών στοιχείων.
- Δημιουργία αναφορών για την διατήρηση των πληροφοριών που ρέουν προς τους ενδιαφερόμενους. Για παράδειγμα, ο χρήστης καθοδηγείται με γνώμονα την απεικόνιση των αποκλειστικών κεφαλαίων κατά την οποία ένα νόμισμα υποστηρίζεται.

4.2.8 Επίπεδο Αξία

Με ένα σύστημα που παρέχει εσωτερική και εξωτερική σταθερότητα και ασφάλεια, μπορούμε να αναθέσουμε την αξία στην κυρίως δομή. Χρησιμοποιώντας την αξία, εννοούμε την ενιαία λογιστική μονάδα, την έννοια της εν λόγω μονάδας, καθώς και το εύρος των αριθμών που μπορούν να εφαρμοστούν. (9)

Για παράδειγμα, ένα επίπεδο αξιών μπορεί να αποδώσει τους παρακάτω αριθμούς στα κατώτερα επίπεδα:

- Δολάρια, σε ένα εύρος συναλλαγών των 25 σεντ έως και τα 500 δολάρια.
- Ομόλογα και μετοχές, που αντιπροσωπεύουν την διαπραγμάτευση των περιουσιακών στοιχείων με σκοπό την άντληση κεφαλαίων.
- Μάρκες καζίνου, οι οποίες μπορεί να χορηγηθούν για την αγορά αγαθών.
- Δημόσια Αγαθά όπως τόνοι ιχθύων σε αντίθεση με δημόσια κακά όπως τόνοι ρύπανσης.
- Μετοχές σε εικονικά έργα.
- Funny money ή αλλιώς «αστεία χρήματα», τα οποία είναι εσωτερικά χρήματα για τις εταιρικές ομάδες.

Καθώς το λογισμικό είναι αδιάφορο σε αυτή την απόφαση, θα μπορούσαμε να χρησιμοποιήσουμε το εξίσου εύκολα το λογισμικό για οποιαδήποτε άλλη αξία, αλλά στις επιχειρήσεις χρειάζεται να εναρμονίζεις τις συνέπειες της ασφάλειας με το κόστος.

Επομένως θα μπορούσαμε να χαρακτηρίσουμε αυτό το επίπεδο ως το επίπεδο σύμβασης ως μία ηλεκτρονική μορφή σύμβασης μεταξύ του κατόχου και του ιδιοκτήτη. Σε αυτό ακριβώς το επίπεδο σχεδιάζεται το συμβόλαιο που επισημοποιεί την συμφωνία μεταξύ του εκδότη και του χρήστη.

4.2.9 Επίπεδο Οικονομία

Τέλος στην κορυφή του μοντέλου μας, το επίπεδο της Οικονομίας, η οποία παρέχει μια δομή για τις οικονομικές συναλλαγές οι οποίες μπορούν να βοηθήσουν στην οικοδόμηση της εφαρμογής του μοντέλου.

Σε αυτό το επίπεδο θα χρησιμοποιήσουμε οποιαδήποτε εφαρμογή θα μπορούσε να βοηθήσουν εύκολα τους χρήστες. Για παράδειγμα:

- Ο κλάδος της λιανικής πώλησης που περιλαμβάνει την αγορά αγαθών.
- Επενδυτική διαπραγμάτευση κινητών αξιών.
- Συστήματα εμπιστοσύνης και συστήματα επιβράβευσης για την ενθάρρυνση των επιχειρήσεων, όχι όμως κατ' ανάγκη να αντικαταστήσει τις υπάρχουσες μεθόδους πληρωμής.
- Αγορές για την δίκαιη κατανομή των περιορισμένων δημοσίων αγαθών όπως είναι οι ανεξάντλητες αλιευτικές ζώνες ή η ρύπανση.
- Διαμεσολάβηση των αγορών εργασίας.
- Κλειστά ή περιορισμένης χρήσης συστήματα όπως είναι οι πωλήσεις δοκιμαστικής χρήσης λογισμικού ή λογιστικά συστήματα ομίλου.

4.2.10 Πλεονεκτήματα του μοντέλου

Το μοντέλο των 7 επιπέδων λειτουργεί καλά για την αντιμετώπιση και την μείωση της πολυπλοκότητας της Οικονομολογικής Κρυπτογραφίας. Αυτό επιτυγχάνεται με την διαίρεση του πεδίου σε 7 επίπεδα καθώς μας παρέχει μία μέθοδο διασύνδεσης μεταξύ τους. (9)

Υπάρχει μια ξεχωριστή συνδεσιμότητα μεταξύ των επιπέδων και των στρωμάτων τους καθώς εμπλέκονται πολλές και διάφορες ειδικότητες σχετικές και μη μεταξύ τους. Αυτή όμως η πολυπλοκότητα δίνει περισσότερες επιλογές στην υλοποίηση των διαδικασιών και των εργασιών που πρέπει να γίνει για να εφαρμοστεί το μοντέλο.

Συγκεκριμένα, ο υπεύθυνος του έργου, έχει την βασική ευθύνη υλοποίησης του έργου, επομένως μέσα από το μοντέλο προσφέρεται ένας φυσικός πίνακας ελέγχου

των διαδικασιών μέσα από μια σταθερή ορολογία λέξεων για τον συντονισμό όλων των δραστηριοτήτων.

4.3 Μορφές Οικονομολογικής Κρυπτογράφησης και κοινοτυπίες

4.3.1 Alice and Bob

Τα ονόματα αυτά αποτελούν μια συνήθη επιλογή ψευδωνύμων στον χώρο της κρυπτογραφίας τόσο όσο και της Φυσικής. Η χρήση τους βοήθα στην απλοποίηση κατανόησης δυσνόητων και πολύπλοκων σεναρίων σε προβλήματα κρυπτογραφίας. Ωστόσο αυτά δεν είναι τα μοναδικά ψευδώνυμα που χρησιμοποιούνται για την διευκόλυνση μας, υπάρχουν και άλλα που αντιπροσωπεύουν χαρακτήρες μιας υπόθεσης σε ένα πρόβλημα και όλα ακολουθούν το αγγλικό αλφάβητο. Μερικά από αυτά είναι τα παρακάτω : Carol/Carlos/Charlie, Dave, Eve ,Isaac, Ivan, Justin, Mallory, Walter, Zoe. Πολλά από αυτά συμβολίζουν κάτι λεξικά συνδεδεμένο με την συνήθη επιλογή της φύσης τους ως χαρακτήρες σε μια υπόθεση, όπως Zoe ή Walter, στο πρώτο όνομα το πρώτο γράμμα αποτελεί το εικοστό έκτο και τελευταίο γράμμα του αγγλικού αλφαβήτου και ως αποτέλεσμα συμβολίζει και το τελικό πρόσωπο σε μια υπόθεση. Walter είναι αγγλικό λογοπαίγνιο με την ηχητικά παρεμφερή αγγλική λέξη warden που σημαίνει δεσμοφύλακας / αρχιφύλακας / επίτροπος. (2)

4.3.2 Secure Shell

Το Secure Shell ή αλλιώς SSH αποτελεί ένα ασφαλές πρωτόκολλο δικτύου, μέσω του οποίου επιταχύνεται η μεταφορά πληροφοριών ανάμεσα σε δυο υπολογιστές. Δεν αποτελεί μόνο έναν κρυπτογράφο αλλά παράλληλα διασφαλίζει διαφορές μεταφορές αρχείων και είναι ένα σύστημα αναγνώρισης με ασφάλεια. Δημιουργήθηκε με σκοπό την αντικατάσταση ανασφαλών ομοιότυπων πρωτοκόλλων. (2)

4.3.3 Data Encryption Standard (DES) και Triple DES.

Αν και για την εποχή που κατασκευάστηκε εθεωρείτο ένα μεγάλο βήμα για την κρυπτογραφία που ξέρουμε σήμερα και αμφιλεγόμενος ως προς το λόγο δημιουργίας του, ο DES είναι ένα κλειδί το οποίο είχε κάποτε προταθεί από την Αμερικανική Κυβέρνηση. Ο DES 'σπάστικε' για πρώτη φορά μετά από είκοσι τρία χρόνια χρήσης του από μια μηχανή της Electronic Frontier Foundation και έκτατε έχει 'σπαστεί' πολλές φορές και ακόμη έχει αντικατασταθεί για τις περισσότερες χρήσης του από τον AES.

Ο Triple DES είναι με συνοπτική περιγραφή τρεις DES στην σειρά. Ουσιαστικά το πέρας του ενός αποτελεί την αρχή του επόμενου στην σειρά(είσοδος – έξοδος). Είναι σαφώς πιο δύσκολο να αποκτηθεί πρόσβαση σε αυτόν τον τύπο του DES αφού χρειαζόμαστε τρία κλειδιά για να το αποκρυπτογραφήσουμε.

4.3.4 Greeklish

Είναι μια σύγχρονη κρυπτογράφηση και καλείται η γραφή ελληνικών λέξεων, εκφράσεων και του συνόλου της ελληνικής γλώσσας σε ένα γενικότερο επίπεδο με χρήση λατινικών χαρακτήρων. Χρησιμοποιείται κυρίως από τη νεολαία για την αποφύγει σπατάλης χρόνου αλλά και για ένα είδος ημικρυπτογράφησης πληροφοριών ανάμεσα σε δυο ή παραπάνω άτομα. Αρχικά χρησιμοποιήθηκαν με την χρήση του προγράμματος άμεσης συνομιλίας / διαδικτυακής επικοινωνίας. Η αποκρυπτογράφηση της είναι εύκολη γιατί η μοναδικές προϋποθέσεις είναι να φαίνονται οπτικά όμοιοι, να προφέρονται περίπου το ίδιο, ή να είναι ομόηχοι. Μερικά παραδείγματα αντιστοιχίας μεταξύ του ελληνικού αλφαβήτου με τα Greeklish είναι Γ=G, Ξ= Ks ή 3 (τρία, λόγω παρεμφερούς σχήματος) , Ψ= Ps, Θ= Th ή 8 (οκτώ, λόγω παρεμφερούς σχήματος).Όσο εύχρηστα και αν είναι τα Greeklish για τον οποιοδήποτε ελληνόφωνο με γνώσεις αγγλικών, εάν υπάρχει συχνή εκτενής χρήση, τότε προκαλούν αλλοίωση των ορθογραφικών μας γνώσεων. (2)

4.3.5 Αντιστοιχία αλφαβήτου Greeklish με το Ελληνικό Αλφάβητο:

Α=A Β=V ή πιο περιστασιακά	Β
Γ=G	Δ=D
Ε=E	Ζ=Z
Η=H	Θ=Th η 8 (οκτώ, λόγω του παρεμφερούς σχήματος)
Ι=I	Κ=K
Λ=L	Μ=M
Ν=N	Ξ=Ks ή 3 (τρία λέγω του παρεμφερούς σχήματος) ή Χ (ως ομόηχο, αγγλικό αντίστοιχο γράμμα)
Ο=O	Π=P
Σ=S ή C (περιστασιακή χρήση) ή 5 (πέντε λέγω του παρεμφερούς σχήματος)	Τ=Τα
Υ=Y ή U	Φ=F ή Ph Χ=X Ψ=Ps ή 4 (περιστασιακή χρήση)
Ω=W	Δίφθογγοι: Αι=Ai Οι=Oi Γκ/ΓΓ= G/Gk/Gg Σπ=Sp Στ=St Ει=Ei Υι=Yi ή Ui Μπ= Β ή Mp

ΚΕΦΑΛΑΙΟ 5: ΚΒΑΝΤΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ

5.1. Εισαγωγή

Η κβαντική κρυπτογραφία συνίσταται συνίσταται στην εκμετάλλευση κάποιων ιδιοτήτων ενός φυσικού συστήματος, οι οποίες προβλέπονται από την κβαντομηχανική, έτσι ώστε να δημιουργηθεί ένα κλειδί κρυπτογράφησης το οποίο θα εξασφαλίζει ένα ασφαλές κανάλι επικοινωνίας μεταξύ των κατόχων του.

Το κύριο χαρακτηριστικό της κβαντικής κρυπτογραφίας, που την διαφοροποιεί από τις κλασσικές μεθόδους κρυπτογράφησης είναι ότι οι μετέχοντες στο ασφαλές κανάλι έχουν την δυνατότητα να καταλάβουν πότε και αν κάποιος υποκλέπτει την επικοινωνία τους. Αυτό συμβαίνει γιατί η διαδικασία της μέτρησης, όπως έχουμε ήδη εξηγήσει, διαταράσσει το κβαντικό σύστημα – το κλειδί στην προκειμένη περίπτωση – και έτσι αυτό υφίσταται αλλοιώσεις. Τις αλλοιώσεις αυτές μπορούν να τις αναγνωρίσουν οι μετέχοντες, με την βοήθεια κάποιων αλγοριθμικών διαδικασιών, να τις διορθώσουν και εξασφαλίσουν έτσι μία απολύτως ασφαλή επικοινωνία. Σε αντίθεση με την κλασσική κρυπτογραφία, που βασίζεται πάνω σε ιδιότητες υπολογιστικής πολυπλοκότητας κάποιων συγκεκριμένων μαθηματικών συναρτήσεων, οι οποίες δεν προσφέρουν καμία εγγύηση καθώς εξαρτώνται μεταξύ άλλων και από την υπάρχουσα τεχνολογία, η κβαντική κρυπτογραφία βασίζεται πάνω στα καλά ελεγμένα θεμέλια της κβαντικής μηχανικής.

Ας σημειωθεί ότι οι υπάρχουσες μέθοδοι κβαντικής κρυπτογραφίας χρησιμοποιούν τις φυσικές ιδιότητες του συστήματος μόνο για την παραγωγή του κλειδιού· η ίδια η μεταφορά της πληροφορίας γίνεται με τον κλασσικό τρόπο και για την κρυπτογράφηση μπορεί να χρησιμοποιηθεί οποιοσδήποτε από τους γνωστούς αλγορίθμους. Συνήθως, όμως, ο αλγόριθμος που χρησιμοποιείται στην πλειοψηφία των περιπτώσεων είναι ο OTP (one-time pad), μίας και έχει αποδειχθεί ότι είναι απαραβίαστος σε συνδυασμό με την χρήση ενός τυχαίου κλειδιού.

5.2 Κβαντική Πληροφορία: το Qbit

Μια σημαντική έννοια στην μελέτη της κβαντικής κρυπτογραφίας είναι αυτή της κβαντικής πληροφορίας στην κλασσική ψηφιακή θεωρία πληροφορίας, η βασική μονάδα είναι το bit, μια μονάδα «Z» που μπορεί να πάρει μόνο μία εκ των δύο τιμών «0» και «1». Στην προκειμένη περίπτωση, η αντίστοιχη μονάδα πληροφορίας είναι το επονομαζόμενο qbit γνωστό και ως "quantum bit". Το qbit αποτελεί ένα καταστατικό διάνυσμα ενός κβαντικού συστήματος δύο καταστάσεων. Κάθε τέτοιο σύστημα, μπορεί να παρασταθεί σαν ένα σημείο σε έναν διανυσματικό χώρο δύο διαστάσεων στο σώμα των μιγαδικών. Αν συμβολίσουμε τις δύο βασικές καταστάσεις του συστήματος με |0> και |1>, (σύμφωνα με τον συμβολισμό του Dirac) σε αντιστοιχία με το κλασσικό bit, τότε κάθε δυνατή κατάσταση – που εκφράζεται από μία κυματοσυνάρτηση ψ – μπορεί να εκφραστεί ως γραμμικός συνδυασμός αυτών.

$$|\psi\rangle=\alpha|0\rangle+\beta|1\rangle.\ \{\alpha,\beta\}\subset\mathbb{C}$$

Λέμε τότε ότι το σύστημα βρίσκεται σε μια κατάσταση (κβαντικής) «υπέρθεσης» και τα |0> και |1> αποτελούν μία βάση του χώρου. Σύμφωνα με την ερμηνεία που έχουμε δώσει για την κυματοσυνάρτηση, οι τιμές $|\alpha|^2$ και $|\beta|^2$ είναι η πιθανότητα εμφάνισης της κατάστασης |α> ή |β> αντίστοιχα κατά την ανάγνωση (μέτρηση) ενός qbit και θα πρέπει να ικανοποιούν την σχέση κανονικοποίησης.

$$\alpha|^2 + |\beta|^2 = 1$$

Με άλλα λόγια, όπως και το bit, έτσι και το qbit μπορεί να πάρει μόνο μία εκ των δύο τιμών «0» και «1», που αντιστοιχούν στα αντίστοιχα ket· η διαφορά έγκειται στο γεγονός ότι η τιμή του bit είναι ντετερμινιστική και προκαθορισμένη, ενώ του qbit είναι μη ντετερμινιστική και καθορίζεται πιθανοκρατικά κατά την ανάγνωσή του, βάσει της κυματοσυνάρτησης που εκφράζει το σύστημα που χρησιμοποιούμε για να κωδικοποιήσουμε την πληροφορία στον φυσικό κόσμο. Γίνεται πλέον φανερό ότι με qbyte μπορούμε να κωδικοποιήσουμε μια πληθώρα διαφορετικών συμβολοσειρών, σε αντίθεση με το byte, συμπιέζοντας έτσι κατά κάποιον τρόπο την πληροφορία. Αυτή η «πλεονάζουσα» πληροφορία όμως καταστρέφεται κατά την ανάγνωση του qbyte και αφήνει στην θέση της μόνο μία εκ των εναλλακτικών.

Αυτή η ιδιότητα του είναι που κάνει την κβαντική πληροφορία τόσο δύσκολη στην χειραγώγησή της, καθώς για να εκμεταλλευτεί κανείς την πλεονάζουσα πληροφορία για κάθε παράλληλους υπολογισμούς, θα πρέπει να βρει ένα πρακτικό και πιο κατανοητό τρόπο έτσι ώστε να μην την καταστρέφει.

Αξίζει να σημειωθεί ότι το qbit παρουσιάζει καταστάσεις και περιπτώσεις ζευγών τα οποία είναι διαπλεγμένα μεταξύ τους. Για παράδειγμα, έστω ότι έχουμε την κατάσταση

$$|\psi>=\frac{1}{\sqrt{2}}(|00>+|11>)$$

Τότε έχουμε ένα σύστημα όπου τα δύο qbit μπορούν να πάρουν με την ίδια πιθανότητα είτε με την τιμή «0» είτε με την τιμή «1». Αν με κάποιο τρόπο καταφέρουμε να μοιράσουμε τα δύο qbit σε δύο διαφορετικούς παρατηρητές, έστω αυτοί η Alice και ο Bob, τότε αν η Alice μετρήσει «0» για το δικό της qbit, τότε και ο Bob θα πάρει με πιθανότητα 1 την ίδια τιμή, λόγω της κβαντικής διαπλοκής. Η μέθοδος αυτή χρησιμοποιείται στους κβαντικούς υπολογιστές, όπου η πληροφορία κρατείται σε πολλά «αντίγραφα» χάριν της διαπλοκής και έτσι δεν καταστρέφεται με μία μόνο μέτρηση.

Παραδείγματα φυσικών κβαντικών συστημάτων δύο καταστάσεων που μπορούν να χρησιμοποιηθούν για την κωδικοποίηση ενός qbit αποτελούν ένα μόνο φωτόνιο, βάσει της πόλωσής του, ένα ηλεκτρόνιο, βάσει του spin του, ή ακόμα και ένας κατάλληλος πυρήνας, βάσει πάλι του spin του, με την χρήση Πυρηνικού Μαγνητικού Συντονισμού (NMR).

5.3 Μέθοδοι Κβαντικής κρυπτογράφησης

Οι διάφορες μέθοδοι κβαντικής κρυπτογράφησης στην ουσία αποτελούν παραλλαγές δύο βασικών διαφορετικών μεθόδων που αξιοποιούν είτε το φαινόμενο της κβαντικής διαπλοκής που μελετήσαμε κατά την ανάλυση του παραδόξου EPR, είτε την αρχή της απροσδιοριστίας του Heisenberg, την οποία απλώς αναφέραμε έως τώρα.

Η αρχή της απροσδιοριστίας, δίνει το κάτω όριο του γινομένου των τυπικών αποκλίσεων της ορμής και της θέσης ενός κβαντικού συστήματος, υποδηλώνοντας έτσι ότι είναι αδύνατον να γνωρίζει κανείς με απόλυτη ακρίβεια την θέση και την ορμή του αυτού συστήματος κατά την ίδια χρονική στιγμή. Το γεγονός αυτό δεν είναι συνέπεια κάποιας ατέλειας της διαδικασίας της μέτρησης, είναι μια μαθηματική συνέπεια των βασικών αρχών της κβαντικής μηχανικής. Οποιεσδήποτε άλλες ατέλειες της ίδιας της μέτρησης απλώς συνεισφέρουν στην ελάχιστη αυτή απροσδιοριστία.

Στην αρχική της μορφή, που εμπλέκει την ορμή και την θέση, η μαθηματική της έκφραση είναι

$$\Delta\chi * \Delta\rho \geq \hbar/2$$

Η γενικότερη έκφραση είναι:

$$\Delta A * \Delta B = \frac{1}{2}| < [A, B] > |$$

Όπου Α και Β οι τελεστές δύο φυσικών μεγεθών ,[A,B] είναι ο μεταθέτης των τελεστών αυτών και <X> είναι η μέση τιμή του μεγέθους Χ. Από την γενικευμένη αυτή σχέση προκύπτει πλήθος ειδικών σχέσεων, όπως μεταξύ των τριών συνιστωσών της στροφορμής, αλλά και της σχέσης χρόνου και ενέργειας.

$$\Delta E * \Delta t \geq \hbar/2$$

Παρακάτω ακολουθεί μία περιγραφεί των πρωτοκόλλων που έχουν αφαιρεθεί για την ανταλλαγή κβαντικών κλειδιών. Και στις δύο περιπτώσεις θεωρούμε δύο μετέχοντες που θέλουν να επικοινωνήσουν, την Alice (A) και τον Bob (B) και έναν υποκλοπέα που θέλει να μάθει το κλειδί την Eve (E).

5.4 Πολωμένα φωτόνια

Η μέθοδος αυτή προτάθηκε για πρώτη φορά το 1984 από τους Charles H.Bennett και Gilles Brassard και είναι γνωστή με την επονομασία BB84. Σε αυτή την μέθοδο χρησιμοποιείται ένα κβαντικό κανάλι για την μεταφορά του κλειδιού και ένα κανονικό κλασσικό κανάλι για την ανταλλαγή της πραγματικής πληροφορίας.

Υποθέτουμε ότι η Eve μπορεί να παρατηρήσει την πληροφορία που αποστέλλεται και στα δύο κανάλια.

Αρχικά η Alice μέσω ενός κβαντικού καναλιού αποστέλλει στον Bob μια αλληλουχία από qbit, τα οποία είναι κωδικοποιημένα με τυχαία επιλογή βάσης κάθε φορά.

Κάθε φωτόνιο που λαμβάνει ο Bob, το μετράει βάσει τυχαίας επιλογής και κρατάει τα αποτελέσματα των μετρήσεων κρυφά. Μετά το πέρας των μετρήσεων, επικοινωνεί στην Alice μέσω του κλασσικού καναλιού. Από το ίδιο κανάλι, η Alice του απαντά ποιες από τις βάσεις που χρησιμοποίησε ήταν επιλεγμένες σωστά και έτσι κρατούν τα qbit που σχηματίζουν το κλειδί. Έτσι και οι δύο έχουν μια αλληλουχία από ισάριθμα qbit που συμφωνούν ένα προς ένα στις τιμές τους. Βάσει πιθανοτήτων, περίπου τα μισά qbit θα είναι ίσα, δηλαδή οι μισές μετρήσεις θα έχουν γίνει με σωστή βάση.

Από την άλλη, αν υποθέσουμε ότι η Eve παρεμβαίνει στο κβαντικό κανάλι, τότε το πλήθος των σωστών qbit που θα βρει ο Bob είναι μικρότερο. Για την ακρίβεια, όπως και με τον Bob, κάθε μέτρηση που κάνει η Eve έχει 50/50 πιθανότητα να είναι λάθος. Από τον πολλαπλασιαστικό νόμο των πιθανοτήτων, αυτό σημαίνει ότι ο Bob έχει 25% πιθανότητα να κάνει σωστή την μέτρηση για κάθε Qbit που υπέκλεψε η Eve. Έτσι από την κατανομή των σωστών τιμών, η Alice και Bob μπορούν να καταλάβουν αν κάποιος τους παρακολουθούσε, αλλά ακόμη και το ποσοστό της πληροφορίας που υπέκλεψε.

Στην πράξη, βέβαια, θα υπάρχουν και λάθη που θα οφείλονται στην αλληλεπίδραση του συστήματος κωδικοποίησης με το περιβάλλων. Για παράδειγμα, στην περίπτωση των φωτονίων, αν αυτά μεταφέρονται με οπτικές ίνες, τότε κάποιο ποσοστό των λαθών θα οφείλεται στην αλληλεπίδραση των φωτονίων με ατέλειες στην επίστρωση των ινών και με τον ίδιο τον αέρα. Επειδή είναι αδύνατον να διαχωριστεί αυτός ο «θόρυβος» από την πραγματική υποκλοπή, η μόνη ασφαλής λύση είναι να υποτεθεί ότι όλα τα λάθη οφείλονται στην Eve. Τότε, ο Bob και η Alice μπορούν να εφαρμόσουν μια μέθοδος ενίσχυσης ιδιωτικότητας, η οποία παράγει μικρότερα πανομοιότυπα κλειδιά από μεγαλύτερα παρόμοια. Η μέθοδος αυτή είναι μια μορφή κρυπτογραφικής διόρθωσης λαθών και αν και οι κλασσικές μέθοδοι ενίσχυσης μπορούν να εφαρμοσθούν με επιτυχία και

στα δύο πρωτόκολλα που μελετάμε, είναι σαφώς αποδοτικότερη στην περίπτωση των διαπλεγμένων σωματίων, καθώς τότε μπορεί να γίνει αυτόματα σε κβαντικό επίπεδο.

5.5 Διαπλεγμένα σωμάτια

Το πρωτόκολλο αυτό εφευρέθηκε μερικά χρόνια αργότερα, το 1991, από τον Artur Ekert. Όπως και προηγουμένως, χρησιμοποιείται ένα κβαντικό κανάλι για την καθιέρωση του κλειδιού και ένα κλασσικό κανάλι για την μεταφορά της πληροφορίας. Στην περίπτωση αυτή όμως, το φυσικό σύστημα που κωδικοποιεί τα qbit αποτελείται από ζεύγη διαπλεγμένων σωματίων – συνήθως φωτόνια – και έκαστοι οι Alice και Bob λαμβάνουν ένα σωμάτιο από κάθε ζεύγος. Μετά το πέρας των εκπομπών οι Alice και Bob έχουν από μία ακολουθία από bit που είναι συμπληρωματική η μία της άλλης· αν η Alice έχει π.χ. την ακολουθία 00101, τότε ο Bob θα έχει την NOT 00101 = 11010, οπότε και μπορούν να συμφωνήσουν μέσω του κλασσικού καναλιού στην επιλογή μιας εκ των δύο ως κλειδί, χωρίς να την ανακοινώσουν άμεσα. Πάλι, όπως και στο πρωτόκολλο BB84, θόρυβος και υποκλοπές θα αλλοιώνουν τις μετρήσεις και η σχέση μεταξύ των δύο ακολουθιών δεν θα είναι μια ακριβής σχέση NOT. Όμως χάρη στην κβαντική διαπλοκή, η Alice θα έχει πιθανότητα μεγαλύτερη του 50% να συνάγει σωστά την ακολουθία του Bob, και αντιστρόφως, πιθανότητα που είναι σημαντικά μεγαλύτερη από οποιαδήποτε άλλη κλασσική μέθοδος ή απόπειρα μαντείας μπορεί να προσφέρει. Τεχνικές μηδενικής γνώσεις μπορούν να επιστρατευθούν για την επαλήθευση των ακολουθιών μεταξύ της Alice και του Bob, χωρίς να χρειαστεί να τις ανακοινώσουν αυτές καθ' εαυτές από το κλασσικό κανάλι.

5.6 Ο αλγόριθμος του Shor

Έως τώρα, πρέπει να έχει γίνει σαφές ότι οι διάφορες μέθοδοι κβαντικής κρυπτογραφίας περιορίζονται απλώς στην εύρεση ενός πρωτοκόλλου ανταλλαγής κλειδιού μέσω ενός κβαντικού καναλιού. Από κει και πέρα, η διαδικασία

επικοινωνίας δεν διαφέρει σε τίποτα από τις κλασσικές μεθόδους· βάσει του κλειδιού, επιλέγεται ένας αλγόριθμος κρυπτογράφησης και η επικοινωνία γίνεται από ένα κλασσικό κανάλι. Οι περισσότεροι αλγόριθμοι κρυπτογράφησης, όμως, όπως ο κατά πολύ διαδεδομένος RSA, βασίζονται στην δυσκολία που παρουσιάζει η παραγοντοποίηση μεγάλων πρώτων αριθμών. Η συνεχής έρευνα, όμως, πάνω στους κβαντικούς υπολογιστές έχει δείξει ότι είναι δυνατόν να παραγοντοποιήσει κανείς μεγάλους πρώτους αριθμούς σε πολυωνυμικό χρόνο με την χρήση κβαντικών αλγορίθμων πιθανοτήτων. Ένας τέτοιος αλγόριθμος είναι και αυτός του Shor.

Αν και η αναγκαία τεχνολογία για την υλοποίηση κβαντικών υπολογιστών είναι ακόμα στα σπάργανά της, και απ΄ό,τι δείχνουν τα πράγματα, κάθε κβαντικός υπολογιστής θα είναι φτιαγμένος για μια συγκεκριμένη δουλειά, σε αντίθεση με τους κλασσικούς επεξεργαστές γενικής χρήσης, γίνεται πρόοδος με μεγάλη ταχύτητα τα τελευταία χρόνια, και ήδη υπάρχουν κάποιο πρότυποι τέτοιοι υπολογιστές. Το 2001, η IBM έκανε μια επίδειξη όπου παραγωντοποίησε τον αριθμό 15 στο γινόμενο 3 επί 5 με την χρήση 7 qbit. Επιπλέον με κάποιες μεταποιήσεις στον αλγόριθμο του Shor, έχει δειχθεί ότι το κβαντικό μέρος του αλγόριθμου μπορεί να τερματίσει σε τέσσερις με οκτώ επαναλήψεις μόνο. Οπωσδήποτε, τέτοια αποτελέσματα είναι ενδείξεις του ότι θα πρέπει σύντομα να ευρεθούν νέες μέθοδοι κρυπτογράφησης, οι οποίες να είναι «άτρωτες» σε τέτοιους υπολογιστές.

5.7 Ο Αλγόριθμος OTP

Η μέθοδος αυτή εφευρέθηκε το 1917 και συνίσταται στην modulus πρόσθεση ενός τυχαίου, ισομήκους με το μήνυμα, κλειδιού με το μήνυμα προς αποστολή. Στην περίπτωση μιας γλώσσας με μοναδικά ψηφία το “0” και το “1”, αυτό ισοδυναμεί με την πράξη XOR. Αν και πολύ απλή σαν μέθοδος, χρειάστηκαν 25 χρόνια από την εφεύρεσή της για να αναγνωριστεί η ιδιάζουσα αξία της· ο Claude Shannon απέδειξε τότε ότι αν η μέθοδος αυτή εφαρμοσθεί με ένα πραγματικά τυχαίο – και όχι ψευδοτυχαίο – κλειδί, το οποίο θα κρατηθεί απόλυτα μυστικό και δεν θα χρησιμοποιηθεί πάνω από μία φορά, τότε επιτυγχάνεται η πλήρης εχεμύθεια. *Ακόμα απέδειξε ότι οποιαδήποτε άλλη μέθοδος σκοπεύει στην πλήρη εχεμύθεια,

τότε αυτή θα πρέπει να πληροί τις παραπάνω προϋποθέσεις, δηλαδή ο αλγόριθμος OTP είναι «πλήρης» όσον αφορά την εχεμύθεια. Η μη χρήση του ιδίου κλειδιού πάνω από μία φορά είναι σημαντική για την επιτυχία της μεθόδου· ακόμα και αν χρησιμοποιηθεί μόνο δύο φορές το ίδιο κλειδί, τότε είναι εύκολο να ανακτηθεί με την χρήση κρυπτοαναλυτικών μεθόδων. Λόγω, των αυστηρών περιορισμών στην υλοποίησή της, η μέθοδος αυτή αν και πολύ παλαιά δεν έτυχε ιδιαίτερης χρήσης και αναγνώρισης. Αυτό, όμως, έμελλε να αλλάξει με την εισαγωγή της κβαντικής κρυπτογραφίας. Η απαίτηση χρήσης ενός πραγματικά τυχαίου κλειδιού ταιριάζει όμορφα με τις ίδιες της αρχές της κβαντομηχανικής· η τυχαία διάταξη που πρεσβεύει η θεωρία για την υπόσταση του φυσικού κόσμου μπορεί να αξιοποιηθεί προς την επίτευξη της ασφάλειας Shannon. Η τυχαία διάταξη κάποιων δεδομένων ως γνωστόν μετριέται με βάση την εντροπία. Η μέθοδος που έχει προταθεί από τον Von Neumann, ονόματι «λεύκανση Von Neumann» έχει ως εξής:

Είσοδος	**Έξοδος**
00	Τίποτα
01	1
10	0
11	Τίποτα

Η διαδικασία αυτή παράγει μια ομοιογενώς τυχαία ακολουθία από bit, το καθένα με εντροπία ίση με την μονάδα, υπό την προϋπόθεση ότι η ακολουθία εισόδου είναι πραγματικά τυχαία. Βλέπουμε λοιπόν ότι αν και οι κβαντικοί υπολογιστές απειλούν με κατάρρευση τους πιο διαδεδομένους αλγόριθμους κρυπτογράφησης, αυτοί οι ίδιοι είναι που προσφέρουν την λύση προς μια πιο ασφαλής κρυπτογραφία, με μια ιδιαιτέρως απλή εφαρμογή.

5.8 Κρυπτογράφηση μηδενικής γνώσης

Ένα μεγάλο κομμάτι της προστασίας που παρέχεται στις ψηφιακές πληροφορίες, προκειμένου να διασφαλιστούν εναντίον παραβιάσεων δεδομένων και κυβερνο-επιθέσεων, οι οποίες μάλιστα τον τελευταίο καιρό έχουν γίνει συχνό φαινόμενο, χτυπώντας ακόμη και κολοσσιαίους οργανισμούς, έχει σχέση με τη χρήση πολύπλοκων μαθηματικών τύπων, την κρυπτογράφηση όπως είναι γνωστή. Με την μέθοδο αυτή τα δεδομένα μετατρέπονται σε ασυνάρτητη και ακατανόητη πληροφορία που δεν μπορούν να την εκμεταλλευτούν οι επιτιθέμενοι ή όσοι θέλουν να την υποκλέψουν.

Η κρυπτογράφηση μηδενικής γνώσης αποτελεί μια παραλλαγή της συνηθισμένης ρουτίνας, με την οποία επιτρέπεται στους χρήστες να κρυπτογραφήσουν τοπικά τα δεδομένα τους (δηλαδή στην προσωπική τους ηλεκτρονική συσκευή, το PC, το Mac ή το tablet τους), προτού αυτά διαβιβαστούν μέσω του διαδικτύου στις εταιρίες που παρέχουν τις υπηρεσίες στον ιστό. Το κλειδί για την συγκεκριμένη διαδικασία κρυπτογράφησης, είναι πως δεν λαμβάνει χώρα ποτέ εκτός των φυσικών ορίων του μηχανήματος του χρήστη και με τον τρόπο αυτό κάνει αδύνατο να αποκαλυφθούν είτε από ατύχημα, είτε από δόλο, είτε εξαιτίας κάποιας κυβερνοεπίθεσης με θύμα την εταιρία, τα προσωπικά δεδομένα των χρηστών που χρησιμοποιούν την υπηρεσία.

Είναι σημαντικό να σημειωθεί πως η κρυπτογράφηση μηδενικής γνώσης, δεν προσφέρει μεγαλύτερη, ούτε αποτελεσματικότερη κρυπτογράφηση στα δεδομένα μας. Αυτό που κάνει είναι πως διασφαλίζει πως η Apple ή το Dropbox για παράδειγμα, δεν θα έχουν πλέον τη «δυνατότητα» να χάσουν αποκρυπτογραφημένα δεδομένα των πελατών τους κατά τη διάρκεια μιας κυβερνοεπίθεσης. Για τους χρήστες αυτό συνεπάγεται πως δεν θα αναγκάζονται πλέον να εμπιστεύονται τις εταιρίες που τους παρέχουν διαδικτυακές υπηρεσίες, σε σχέση με την κρυπτογράφηση και τη συνολική ασφάλεια των δεδομένων τους.

Μία ακόμα καινοτομία που έχει αρχίσει να δείχνει σημάδια εμπορικής προοπτικής είναι η ομομορφική κρυπτογράφηση, η οποία επιτρέπει να γίνονται υπολογισμοί και επεξεργασία πάνω σε δεδομένα που είναι κρυπτογραφημένα, χωρίς να

απαιτείται προηγουμένως η αποκρυπτογράφησή τους. Η συγκεκριμένη προσέγγιση μπορεί να παρέχει την υπόσχεση της πραγματικής εμπιστευτικότητας, αφού η πληροφορία χρησιμοποιείται και αποθηκεύεται κάθε φορά σε κρυπτογραφημένη μορφή. Για την ώρα δεν υπάρχουν τέτοια συστήματα που να λειτουργούν πλήρως σε εμπορική χρήση, όμως σε ακαδημαϊκό επίπεδο υπάρχουν ενδείξεις πως η ολοκλήρωση τέτοιων συστημάτων κρυπτογράφησης είναι πολύ κοντά.

5.9 NITROKEY: Ένα usb stick για κρυπτογράφηση

Το Nitrokey πρόκειται για ένα usb – stick ανοιχτού σχεδιασμού (σε hardware και software) που αναπτύχθηκε από το German Privacy Foundation, για κρυπτογράφηση ηλεκτρονικού ταχυδρομείου, με χρήση One Time Passwords, κρυπτογράφηση αρχείων που υπάρχουν στους δίσκους και ενεργούν ως ένα διπλό διακριτικό ταυτότητας, και για την διαχείριση ψηφιακών πιστοποιητικών σε ιστοσελίδες που έχουν υιοθετήσει το πρότυπο Universal 2nd Factor U2F, το οποίο υποστηρίζεται από τις υπηρεσίες της Google, OpenSSH και Wordpress.

Ο σχεδιασμός του εξοπλισμού και του λογισμικού κώδικα αυτής της thumbdrive κρυπτογράφησης, είναι ανοιχτού κώδικα για να καταστεί δυνατή η επανεξέταση της ασφάλειάς του, καθώς και για τους προγραμματιστές να είναι σε θέση να ενσωματώσουν δικές τους εφαρμογές.

Το thumbdrive, με χωρητικότητα 32 GB κρατά τρία κλειδιά κρυπτογράφησης RSA έως 4096 bits, που συνδέονται όλα με την ίδια ταυτότητα, αλλά χρησιμοποιούνται για διαφορετικούς σκοπούς (authentication, signing, encryption). Τα κλειδιά είναι ενσωματωμένα στην συσκευή, γεγονός που καθιστά αδύνατο την εξαγωγή και μετάδοση ιών. Τα One – Time Passwords είναι συμβατά με το Google Authenticator και hardware κρυπτογράφηση, χρησιμοποιώντας τον αλγόριθμο AES256bits με αληθοφανή δυνατότητα άρνησης μέσω hidden volumes. Το dongle έρχεται με ένα προεπιλεγμένο PIN διαχειριστή, το 12345678 που πρέπει φυσικά να αλλάξει. Διαθέτει και άλλη μία έκδοση, το NitroKey Storage που επιτρέπει την αποθήκευση έως και 64 GB κρυπτογραφημένων δεδομένων στην συσκευή, ενώ σε κάθε περίπτωση είναι όλα ασφαλισμένα με την χρήση κρυπτογράφησης υλικού AES256bit.

Το usb thumbdrive θα λειτουργεί σε όλα τα λειτουργικά συστήματα, συμπεριλαμβανομένου και του Linux, μπορώντας να χρησιμοποιηθεί για έλεγχο ταυτότητας (authentication), καθώς και για κρυπτογράφηση. Επίσης σε περίπτωση που ο υπολογιστής έχει κάποιους δούρειους ίππους (Trojan horses), τα οποία επιχειρούν να υποκλέψουν τα κλειδιά κρυπτογράφησης, το NitroKey έχει την δυνατότητα να σταματήσει οποιαδήποτε τέτοια ενέργεια. Τα πάντα θα βρίσκονται σε αυτό το «έξυπνο» στικάκι αντί για τον σκληρό δίσκο του Υπολογιστή, ενώ φυσικά η open source κατασκευή του NitroKey επιτρέπει τον έλεγχο της ακεραιότητας του firmware του και οι προγραμματιστές του το διαφημίζουν ως έναν τρόπο που μπορεί να ανατρέψει την πρακτική NSA, με υποκλοπές υλικού «σπέρνοντας» ή αλλιώς δημιουργώντας κερκόπορτες.

Δεν μπορούμε να θεωρήσουμε ότι είναι ένα ακόμα φθηνό dongle, καθώς υπάρχουν πολύ φθηνότερα, αλλά κανένα δεν έχει ουσιαστικές δυνατότητες κρυπτογράφησης, εκτός από τον έλεγχο ταυτότητας U2F. Σε αντίθεση με το NitroKey το οποίο προσφέρει κρυπτογράφηση e-mail και δεδομένων, με βασικό του πλεονέκτημα ότι είναι ένα «στικάκι» ανοικτού κώδικα και υποστηρίζει όλα τα πρότυπα προγράμματα ασφαλείας. Οι προγραμματιστές του αναφέρουν επίσης ότι το κλειδί έχει ένα tamper – proof design κάτι που το κάνει απαραβίαστο, μπορώντας να δημιουργηθεί ένα hidden encrypted container, για να αποφευχθεί υποχρεωτική καταβολή κωδικών πρόσβασης σε περίπτωση που θα ζητηθεί για την επιβολή του νόμου ή και σε χώρες όπου γίνεται έλεγχος.

Εκτός από τα θετικά του NitroKey, πρέπει να αναφέρουμε και τα μειονεκτήματα που έχει καθώς το βασικό μειονέκτημα των συσκευών σε αυτήν την κατηγορία είναι ότι ο κωδικός ασφαλείας που χρησιμοποιείς κάθε φορά, τον πληκτρολογείς μέσω του πληκτρολογίου. Επομένως, αν κάποιος πάρει τα keystrokes θα έχει και τον κωδικό που χρησιμοποίησες. Έτσι προκύπτει και άλλο ένα μειονέκτημα το οποίο το κάνει δύσκολο στην χρήση του, καθώς πρέπει να υπάρχει αλλαγή των κωδικών ασφαλείας και πρόσβασης σε τέτοια συχνότητα ώστε να υπάρχει ασφάλεια.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Η Κρυπτογραφία είναι ίσως από τις πιο εξελίξιμες αρχαίες επιστήμες παγκοσμίως, και αυτό δεν είναι ένα τυχαίο, αν αναλογιστεί κανείς την χρήση της και την συμβολή της στην καθημερινότητα μας όπως και στην εξέλιξη της ιστορίας γενικότερα. Ασφαλώς, ο κόσμος μας θα ήταν διαφορετικός χωρίς την συμβολή της κρυπτογραφίας και αυτό μπορεί να γίνει αντιληπτό κυρίως στους πιο πρόσφατους πολέμους. Γι' αυτό τον λόγο στα συμπεράσματα μας θέτουμε την παρακάτω ερώτηση αλλά και την απάντηση της:

Γιατί δεν μπορεί να απαγορευτεί η κρυπτογραφία;

Το μόνο που μπορούν να κάνουν βραχυχρόνια οι κυβερνήσεις είναι να ελέγξουν την παράγωγη ή εμπορία ισχυρών κρυπτογραφικών μηχανών. Η μετάδοση και η λήψη μηνυμάτων είναι αδύνατον να απαγορευτεί. Ένα κρυπτογραφημένο μήνυμα προστατεύεται από την αρχή της ελευθερίας του λόγου. Όλοι οι άνθρωποι έχουν δικαίωμα να γράψουν μια λέξη με όποιον τρόπο θέλουν. Αν ποινικοποιηθεί η μετάδοση κρυπτογραφημένων μηνυμάτων, τότε ποινικοποιούνται ευρύτερες μορφές έκφρασης όπως μια κίνηση τον χεριών ή των ματιών γιατί ουσιαστικά κρυπτογραφούμε το μήνυμα που εκστομίζουμε. Είναι αδύνατον να ξεχωρίσει κάποιος τρίτος ένα κρυπτογραφημένο μήνυμα από το θόρυβο του καναλιού στο οποίο μεταδίδεται το κρυπτογραφημένο μήνυμα, γιατί αν προσπαθήσει να παρακολουθήσει το ψηφιακό τηλέφωνο που μεταδίδει το μήνυμα αυτό το μόνο που θα ακούσει είναι ένα διαρκές «φύσημα». Τέλος η σύγχρονη κρυπτογραφία μπορεί και εκμεταλλεύεται τα κενά στην μετάδοση των ψηφιακών μηνυμάτων, στα κενά δηλαδή μιας ψηφιακής κασέτας μπορούν να χωρέσουν πάρα πολλές κρυπτογραφημένες πληροφορίες.

Στην εποχή μας, η κρυπτογραφία μαζί με την εξέλιξη των πληροφοριών γνωρίζει μια παράλληλη εξελικτική άνθηση. Είναι ένα χρήσιμο εργαλείο το οποίο όταν χρησιμοποιείται σωστά μας εξασφαλίζει μια καλύτερη ζωή.

Στην εργασία αυτή προσπαθήσαμε να δώσουμε στον αναγνώστη μια γενική εικόνα για την επιστήμη της Κρυπτογραφίας, την ιστορία της αλλά και τις εφαρμογές της, μέσα από κάποια παραδείγματα, έτσι ώστε ο αναγνώστης να καταλάβει τις βασικές αρχές της και την εξέλιξή της.

ΒΙΒΛΙΟΓΡΑΦΙΑ – ΠΗΓΕΣ

A. U.S DEPARTMENT OF COMMERCE/National Institute of Standards and Technology. **FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION.**

B. Καρατζάς Ε., Κασσιός Α., Χριστοδούλου Δ. (2001). **Τεχνικές Κρυπτογραφίας και η εφαρμογή τους στον χώρο του Διαδικτύου.** Μεταπτυχιακή Εργασία στα πλαίσια του μαθήματος «Αλγοριθμικά θέματα Δικτύων και Τηλεματικής». Τμήμα Μηχανικών Η/Υ και Πληροφορικής Πανεπιστημίου Πατρών.

C. Singh S. (1999). **Κώδικες και Μυστικά.**

Διαδικτυακές Διευθύνσεις

1. https://el.wikipedia.org/wiki/Κρυπτογραφία
2. http://1lyk-vyron.att.sch.gr/EEBa4_2012_2013_text.pdf
3. http://www.ww2.gr/index.php?option=articles&search=Enigma
4. http://chilonas.com/2014/05/03/enigma-%CF%84%CE%BF-%CE%BC%CF%85%CF%83%CF%84%CE%B9%CE%BA%CF%8C-%CF%8C%CF%80%CE%BB%CE%BF-%CF%84%CE%B7%CF%82-%CE%B2%CE%AD%CF%81%CE%BC%CE%B1%CF%87%CF%84/
5. https://el.wikipedia.org/wiki/Data_Encryption_Standard
6. https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
7. http://users.uom.gr/~kaklaman/book/Chapters/C11/Technologies%20based%20on%20encryption%205.htm
8. https://en.wikipedia.org/wiki/Financial_cryptography
9. http://iang.org/papers/fc7.html
10. http://www.philzimmermann.com/EL/bibliography/
11. https://el.wikipedia.org/wiki/Κρυπτογραφικοί_Αλγόριθμοι_Ροής
12. http://www.ww2.gr/index.php?option=articles&search=Enigma
13. http://digilib.lib.unipi.gr/dspace/bitstream/unipi/4214/1/Verikios.pdf