Π Α Ν Ε Π Ι Σ Τ Η Μ Ι Ο Π ΑΤ Ρ Ω Ν

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

& ΠΛΗΡΟΦΟΡΙΚΗΣ

Ε Ρ ΓΑ Σ Ι Α Ε Ξ Α Μ Η Ν Ο Υ

ΓΙΑ ΤΟ ΜΑΘΗΜΑ

ΔΙΚΤΥΑ ΔΗΜΟΣΙΑΣ ΧΡΗΣΗΣ ΚΑΙ ΔΙΑΣΥΝΔΕΣΗΣ ΔΙΚΤΥΩΝ

ΚΡΥΠΤΟΓΡΑΦΙΑ

ΤΣΟΤΣΟΥ ΑΙΚΑΤΕΡΙΝΗ

Α.Μ. 6248

ΔΙΔΑΣΚΩΝ: ΧΡΗΣΤΟΣ ΜΠΟΥΡΑΣ

ΠΑΤΡΑ 2018

ΠΕΡΙΕΧΟΜΕΝΑ

Κεφάλαιο 1: Εισαγωγή

1.1 Ιστορική Αναδρομή

Ανέκαθεν οι άνθρωποι είχαν τα μυστικά τους, άλλα πιο σημαντικά και άλλα πιο ασήμαντα. Υπήρχε δηλαδή από πάντα η ανάγκη για μετάδοση πληροφοριών χωρίς αυτές να μπορούν να διαβαστούν και να γίνουν κατανοητές από τρίτους. Αυτή η ανάγκη ήταν που οδήγησε τους ανθρώπους να επινοήσουν διάφορα συστήματα και μεθόδους κρυπτογραφίας, φτάνοντας στο σήμερα όπου έχει δημιουργηθεί ολόκληρος επιστημονικός κλάδος που ασχολείται με αυτή. Ας δούμε όμως ποια ήταν τα πρώτα δείγματα της κρυπτογραφίας στην καταγεγραμμένη ανθρώπινη ιστορία.

Πρώτη Περίοδος κρυπτογραφίας (5ος αι. π.Χ. – 20ος αι. μ.Χ.)

Όπως προκύπτει από μία μικρή σφηνοειδή επιγραφή, που ανακαλύφθηκε στις όχθες του ποταμού Τίγρη, οι πολιτισμοί που αναπτύχθηκαν στη Μεσοποταμία ασχολήθηκαν με την κρυπτογραφία ήδη από το 1500 π.Χ. Η επιγραφή αυτή περιγράφει μία μέθοδο κατασκευής σμάλτων για αγγειοπλαστική και θεωρείται ως το αρχαιότερο κρυπτογραφημένο κείμενο σύμφωνα με τον αρχαιολόγο Kahn. Επίσης, ως το αρχαιότερο βιβλίο κρυπτοκωδικών στον κόσμο, θεωρείται μία σφηνοειδής επιγραφή στα Σούσα της Περσίας. η οποία περιλαμβάνει τους αριθμούς 1 έως 8 και από το 32 έως το 35, τοποθετημένους τον ένα κάτω από τον άλλο, ενώ απέναντι τους βρίσκονται τα αντίστοιχα για τον καθένα σφηνοειδή σύμβολα.

Φυσικά μια τέτοια μέθοδος επικοινωνίας δεν θα μπορούσε να μην εξυπηρετήσει και στρατιωτικούς σκοπούς. Ήδη από τον 5ο αιώνα π.Χ. οι Σπαρτιάτες εφηύραν τη «σκυτάλη», την πρώτη κρυπτογραφική συσκευή, στην οποία χρησιμοποίησαν για την κρυπτογράφηση τη μέθοδο της μετάθεσης. Όπως αναφέρει ο Πλούταρχος, η «Σπαρτιατική Σκυτάλη», ήταν μια ξύλινη ράβδος, ορισμένης διαμέτρου, γύρω από την οποία ήταν τυλιγμένη ελικοειδώς μια λωρίδα περγαμηνής. Το κείμενο ήταν γραμμένο σε στήλες, ένα γράμμα σε κάθε έλικα, όταν δε ξετύλιγαν τη λωρίδα, το κείμενο ήταν ακατάληπτο εξαιτίας της αναδιάταξης των γραμμάτων. Το «κλειδί» ήταν η διάμετρος της σκυτάλης.

Τον 3ο και 2ο αιώνα π.Χ. εμφανίζεται η Κρητική εικονογραφική ή ιερογλυφική γραφή, η οποία δεν αποκρυπτογραφηθεί ακόμα. Εικάζεται ότι πρόκειται για μια φωνητική γραφή, της οποίας χαρακτηριστικό εύρημα αποτελεί ο δίσκος της Φαιστού (εικόνα 1.1.1), που ανακαλύφθηκε το 1908 στη νότια Κρήτη. Μέχρι σήμερα δεν έχει αποκρυπτογραφηθεί και παραμένει η πιο μυστηριώδης αρχαία ευρωπαϊκή γραφή.

Την ίδια περίπου περίοδο, τον 2ο π.Χ. αιώνα εμφανίστηκαν ακόμα δύο γραφές, η Γραμμική Α και η Γραμμική Β, οι οποίες ανακαλύφθηκαν στις αρχές του 1900 από τον Άγγλο αρχαιολόγο Άρθουρ Έβανς. Η Γραμμική Α, η οποία θεωρείται και πρόγονος της Γραμμικής Β, δεν έχει αποκρυπτογραφηθεί ακόμα και αποτελεί ένα από τα μεγαλύτερα μυστήρια της σύγχρονης αρχαιολογίας. Αντίθετα, η Γραμμική Β αποκρυπτογραφήθηκε από τον νεαρό γλωσσολόγο-αρχιτέκτονα Michael Ventris το 1952 με τη βοήθεια του κλασσικού φιλόλογου John Chadwick.

εικόνα 1.2.1 Πηγή: http://www.metafysiko.gr/?p=4742

Συνεχίζοντας την ιστορική αναδρομή φτάνουμε στον Μεσαίωνα όπου η κρυπτολογία, επομένως και η κρυπτογραφία, ήταν κάτι απαγορευμένο αφού αποτελούσε μια μορφή αποκρυφισμού και μαύρης μαγείας. Ως αποτέλεσμα η ανάπτυξή της αυτή τη περίοδο ήταν πολύ περιορισμένη.

Τον 17ο αιώνα ο Γερμανός Ιησουΐτης Athanasius Kircher συντέλεσε σημαντικά στη σωστή ερμηνεία των ιερογλυφικών χάρη στην ανακάλυψη της «Στήλης της Ροζέτας». Η στήλη αυτή είναι μια πέτρινη στήλη που βρέθηκε στην Αίγυπτο από τα στρατεύματα του Ναπολέοντα. Πάνω της ήταν χαραγμένο το ένα κείμενο σε τρείς διαφορετικές γλώσσες-διαλέκτους, στα ιερογλυφικά, στα ελληνικά και σε μια ιερατική γραφή. Την αποκρυπτογράφησή της ανέλαβαν δύο μεγάλοι αποκρυπτογράφοι της εποχής, ο Γιάνγκ και ο Σαμπολιόν.

Τον 19ο αιώνα ο C.Wheatstone, γνωστός από τις μελέτες του στον ηλεκτρισμό, παρουσίασε την πρώτη μηχανική κρυπτοσυσκευή, η οποία απετέλεσε τη βάση για την ανάπτυξη των κρυπτομηχανών της δεύτερης ιστορικής περιόδου της κρυπτογραφίας. Η μεγαλύτερη αποκρυπτογράφηση ήταν αυτή των αιγυπτιακών ιερογλυφικών τα οποία, επί αιώνες, παρέμεναν μυστήριο και οι αρχαιολόγοι μόνο εικασίες μπορούσαν να διατυπώσουν για τη σημασία τους. Ωστόσο, χάρη σε μία κρυπταναλυτική εργασία, τα ιερογλυφικά εν τέλει αναλύθηκαν και έκτοτε οι αρχαιολόγοι είναι σε θέση να διαβάζουν ιστορικές επιγραφές.

Δεύτερη Περίοδος κρυπτογραφίας (1900 μ.Χ. – 1950 μ.Χ.)

Η δεύτερη περίοδος τοποθετείται το πρώτο μισό του 20ου αιώνα. Περιλαμβάνει δηλαδή, τους δύο παγκόσμιους πολέμους, εξαιτίας των οποίων αναπτύχθηκε ραγδαία, τόσο όσο δεν είχε αναπτυχθεί τα προηγούμενα 3000 χρόνια. Αυτό συνέβη λόγω της εξαιρετικά μεγάλης ανάγκης που υπήρχε για την ασφάλεια και τη μετάδοση ζωτικών πληροφοριών μεταξύ των αντίπαλων στρατευμάτων, αλλά και την ανάγκη για αναγνώριση των στρατηγικών κινήσεων των αντιπάλων. Τα κρυπτοσυστήματα αυτής της περιόδου αρχίζουν να γίνονται πολύπλοκα, και να αποτελούνται από μηχανικές και ηλεκτρομηχανικές κατασκευές, οι οποίες ονομάζονται «κρυπτομηχανές». Η κρυπτανάλυση τους, απαιτεί μεγάλο αριθμό προσωπικού, το οποίο εργαζόταν επί μεγάλο χρονικό διάστημα ενώ ταυτόχρονα γίνεται εξαιρετικά αισθητή η ανάγκη για μεγάλη υπολογιστική ισχύ. Παρά την πολυπλοκότητα που αποκτούν τα συστήματα κρυπτογράφησης κατά τη διάρκεια αυτής της περιόδου η κρυπτανάλυση τους είναι συνήθως επιτυχημένη. Εκείνη τη περίοδο επινοήθηκε, από τους Γερμανούς, η γνωστή σε όλους συσκευή κρυπτογράφησης Enigma(εικόνα 1.2.2).

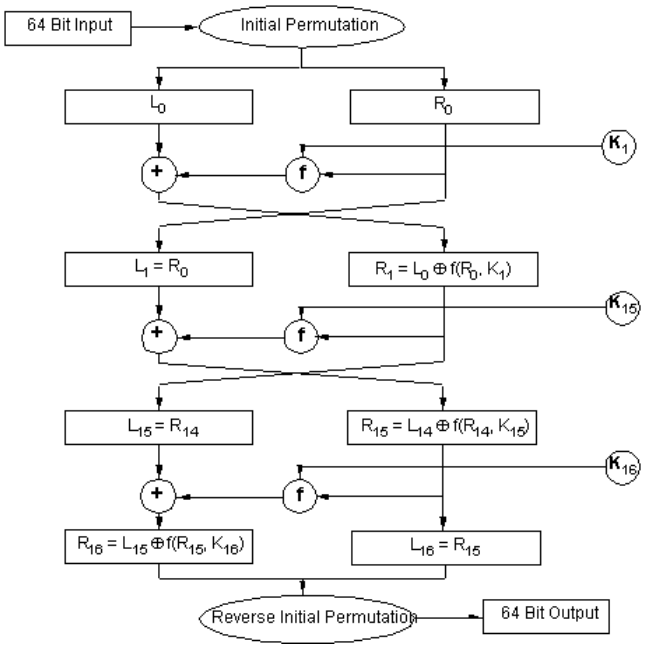
εικόνα 1.2.2 Πηγή: http://ethw.org/Cryptography

Ο Marian Rejewski, στην Πολωνία, προσπάθησε και, τελικά, παραβίασε την πρώτη μορφή του γερμανικού στρατιωτικού συστήματος Enigma (που χρησιμοποιούσε μια ηλεκτρομηχανική κρυπτογραφική συσκευή) χρησιμοποιώντας θεωρητικά μαθηματικά το 1932. Ήταν η μεγαλύτερη σημαντική ανακάλυψη στην κρυπτολογική ανάλυση της εποχής. Οι Πολωνοί συνέχισαν να αποκρυπτογραφούν τα μηνύματα που βασίζονταν στην κρυπτογράφηση με το Enigma μέχρι το 1939. Τότε, ο γερμανικός στρατός έκανε ορισμένες σημαντικές αλλαγές και οι Πολωνοί δεν μπόρεσαν να τις παρακολουθήσουν, επειδή η αποκρυπτογράφηση απαιτούσε περισσότερους πόρους από όσους μπορούσαν να διαθέσουν. Έτσι, εκείνο το καλοκαίρι μεταβίβασαν τη γνώση τους, μαζί με μερικές μηχανές που είχαν κατασκευάσει, στους Βρετανούς και τους Γάλλους. Ακόμη και ο Rejewski και οι μαθηματικοί και κρυπτογράφοι του, όπως ο Biuro Szyfrow, κατέληξαν σε συνεργασία με τους Βρετανούς και τους Γάλλους μετά από αυτή την εξέλιξη. Η συνεργασία αυτή συνεχίστηκε από τον Alan Turing, τον Gordon Welchman και από πολλούς άλλους στο Bletchley Park, κέντρο της Βρετανικής Υπηρεσίας από/κρυπτογράφησης, και οδήγησε σε συνεχείς αποκρυπτογραφήσεις των διαφόρων παραλλαγών του Enigma, με τη βοήθεια και ενός υπολογιστή, που κατασκεύασαν οι Βρετανοί επιστήμονες, ο οποίος ονομάσθηκε Colossus και, δυστυχώς, καταστράφηκε με το τέλος του Πολέμου. Οι

αποκρυπογραφήσεις αυτές οδήγησαν σε σημαντικές νίκες και έπαιξαν καθοριστικό ρόλο στην αίσια, για τις χώρες των Συμμαχικών Δυνάμεων, έκβαση του πολέμου. Οι συμμαχικές κρυπτομηχανές που χρησιμοποιήθηκαν στον δεύτερο παγκόσμιο πόλεμο περιλάμβαναν το βρετανικό TypeX και το αμερικανικό SIGABA. Και τα δύο ήταν ηλεκτρομηχανικά σχέδια παρόμοια στο πνεύμα με το Enigma, με σημαντικές εν τούτοις βελτιώσεις. Κανένα δεν έγινε γνωστό ότι παραβιάστηκε κατά τη διάρκεια του πολέμου. Τα στρατεύματα στο πεδίο μάχης χρησιμοποίησαν το M-209 και τη λιγότερη ασφαλή οικογένεια κρυπτομηχανών M-94. Μερικά χρόνια νωρίτερα, οι Πολωνοί είχαν προετοιμαστεί για την εμπόλεμη περίοδο κατασκευάζοντας την κρυπτομηχανή LCD Lacida, η οποία κρατήθηκε μυστική ακόμη και από τον Rejewski. Όταν τον Ιούλιο του 1941 ελέγχθηκε από τον Rejewski η ασφάλειά της, του χρειάστηκαν μερικές μόνον ώρες για να την "σπάσει" και έτσι αναγκάστηκαν να την αλλάξουν βιαστικά. Τα μηνύματα που εστάλησαν με Lacida δεν ήταν, εντούτοις, συγκρίσιμα με αυτά του Enigma, αλλά η παρεμπόδιση θα μπορούσε να έχει σημάνει το τέλος της κρίσιμης κρυπταναλυτικής Πολωνικής προσπάθειας.

Τρίτη Περίοδος κρυπτογραφίας (1950 μ.Χ. - Σήμερα)

Η τρίτη περίοδος χαρακτηρίζεται από τη ραγδαία ανάπτυξη των επιστημονικών κλάδων των μαθηματικών, της μικροηλεκτρονικής και των υπολογιστικών συστημάτων. Η εποχή της σύγχρονης κρυπτογραφίας ξεκινάει, ουσιαστικά, με τον Claude Shannon, αναμφισβήτητα ο πατέρας των μαθηματικών συστημάτων κρυπτογραφίας. Το 1949 δημοσίευσε το έγγραφο «Communication Theory of Secrecy Systems» στο τεχνικό περιοδικό Bell System και λίγο αργότερα το βιβλίο του, «Mathematical Theory of Communication», μαζί με τον Warren Weaver. Αυτά, εκτός από τις άλλες εργασίες του επάνω στη θεωρία δεδομένων και επικοινωνίας καθιέρωσαν μια στερεά θεωρητική βάση για την κρυπτογραφία και την κρυπτανάλυση. Εκείνη την εποχή η κρυπτογραφία εξαφανίζεται και φυλάσσεται από τις μυστικές υπηρεσίες κυβερνητικών επικοινωνιών όπως η NSA. Πολύ λίγες εξελίξεις δημοσιοποιήθηκαν ξανά μέχρι τα μέσα της δεκαετίας του '70, όταν όλα άλλαξαν.



εικόνα 1.2.3

Πηγή:
https://steemit.com/popularscience/@krishtopa/data-encryption-standard-des-as-a-guardian-of-our-privacy

Στα μέσα της δεκαετίας του '70 έγιναν δύο σημαντικές δημόσιες πρόοδοι. Πρώτα, ήταν η δημοσίευση του σχεδίου προτύπου κρυπτογράφησης DES (Data Encryption Standard) (εικόνα 1.2.3) στον ομοσπονδιακό κατάλογο της Αμερικής στις 17 Μαρτίου 1975. Το προτεινόμενο DES υποβλήθηκε από την IBM, στην πρόσκληση του Εθνικού Γραφείου των Προτύπων (τώρα γνωστό ως NIST). Η ενέργεια αυτή έγινε στα πλαίσια μιας προσπάθειας ανάπτυξης ασφαλών ηλεκτρονικών εγκαταστάσεων επικοινωνίας για επιχειρήσεις, όπως τράπεζες και άλλες μεγάλες οικονομικές οργανώσεις. Μετά από συμβουλές και την τροποποίηση από την NSA, αυτό το πρότυπο υιοθετήθηκε και δημοσιεύθηκε ως ένα ομοσπονδιακή τυποποιημένο πρότυπο επεξεργασίας πληροφοριών το 1977 (αυτήν την περίοδο αναφέρεται σαν FIPS 46-3). Ο DES ήταν ο πρώτος δημόσια προσιτός αλγόριθμος κρυπτογράφησης που εγκρίνεται από μια εθνική αντιπροσωπεία όπως η NSA. Η απελευθέρωση της προδιαγραφής της από την NBS υποκίνησε μια έκρηξη δημόσιου και ακαδημαϊκού ενδιαφέροντος για τα συστήματα κρυπτογραφίας.

Ο DES αντικαταστάθηκε επίσημα από τον AES το 2001 όταν ανήγγειλε ο NIST το FIPS 197. Έπειτα από έναν ανοικτό διαγωνισμό, ο NIST επέλεξε τον αλγόριθμο Rijndael, που υποβλήθηκε από δύο Φλαμανδούς κρυπτογράφους, για να είναι το AES. Ο DES και οι ασφαλέστερες παραλλαγές του όπως ο 3DES ή TDES χρησιμοποιούνται ακόμα σήμερα, ενσωματωμένος σε πολλά εθνικά και οργανωτικά πρότυπα. Εντούτοις, το βασικό μέγεθος των 56-bit έχει αποδειχθεί ότι είναι ανεπαρκές να αντισταθεί στις επιθέσεις ωμής βίας (μια τέτοια επίθεση πέτυχε να σπάσει τον DES σε 56 ώρες ενώ το άρθρο που αναφέρεται ως το σπάσιμο του DES δημοσιεύτηκε από τον O'Reilly and Associates). Ως συνέπεια, η χρήση απλής κρυπτογράφησης με τον DES είναι τώρα χωρίς την αμφιβολία επισφαλής για χρήση στα νέα σχέδια των κρυπτογραφικών συστημάτων και μηνύματα που προστατεύονται από τα παλαιότερα κρυπτογραφικά συστήματα που χρησιμοποιούν DES, και όλα τα μηνύματα που έχουν αποσταλεί από το 1976 με τη χρήση DES, διατρέχουν επίσης σοβαρό κίνδυνο αποκρυπτογράφησης. Ανεξάρτητα από την έμφυτη ποιότητά του, το βασικό μέγεθος του DES (56-bit) ήταν πιθανά πάρα πολύ μικρό ακόμη και το 1976, πράγμα που είχε επισημάνει ο Whitfield Diffie. Υπήρξε επίσης, η υποψία ότι κυβερνητικές οργανώσεις είχαν ακόμα και τότε ικανοποιητική υπολογιστική δύναμη ώστε να σπάσουν μηνύματα που είχαν κρυπτογραφηθεί με τον DES.

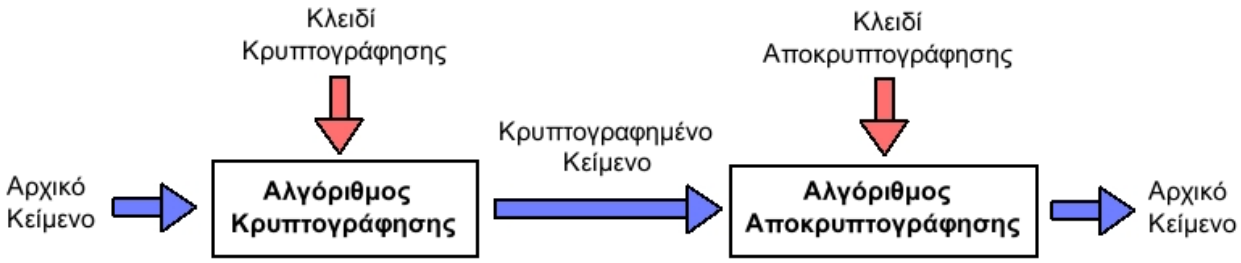
1.2 Βασικοί Ορισμοί

Η κρυπτογραφία είναι ένας από τους δύο κλάδους στους οποίους αναλύεται η κρυπτολογία (ο άλλος είναι η κρυπτανάλυση), η οποία ασχολείται με τη μελέτη της ασφαλούς επικοινωνίας.

Πιο συγκεκριμένα κρυπτογραφία ονομάζεται η διαδικασία μετασχηματισμού ενός μηνύματος σε μία ακατανόητη μορφή με τη χρήση κάποιου κρυπτογραφικού αλγορίθμου ούτως ώστε να μην μπορεί να διαβαστεί από κανέναν εκτός του νόμιμου παραλήπτη.

Αντίστοιχα, η αντίστροφη διαδικασία όπου από το κρυπτογραφημένο κείμενο παράγεται το αρχικό μήνυμα ονομάζεται αποκρυπτογράφηση.

Στη συνέχεια φαίνεται ένα διάγραμμα (εικόνα 1.1) που παρουσιάζει σχηματικά όλη τη διαδικασία της κρυπτογράφησης ενός μηνύματος.



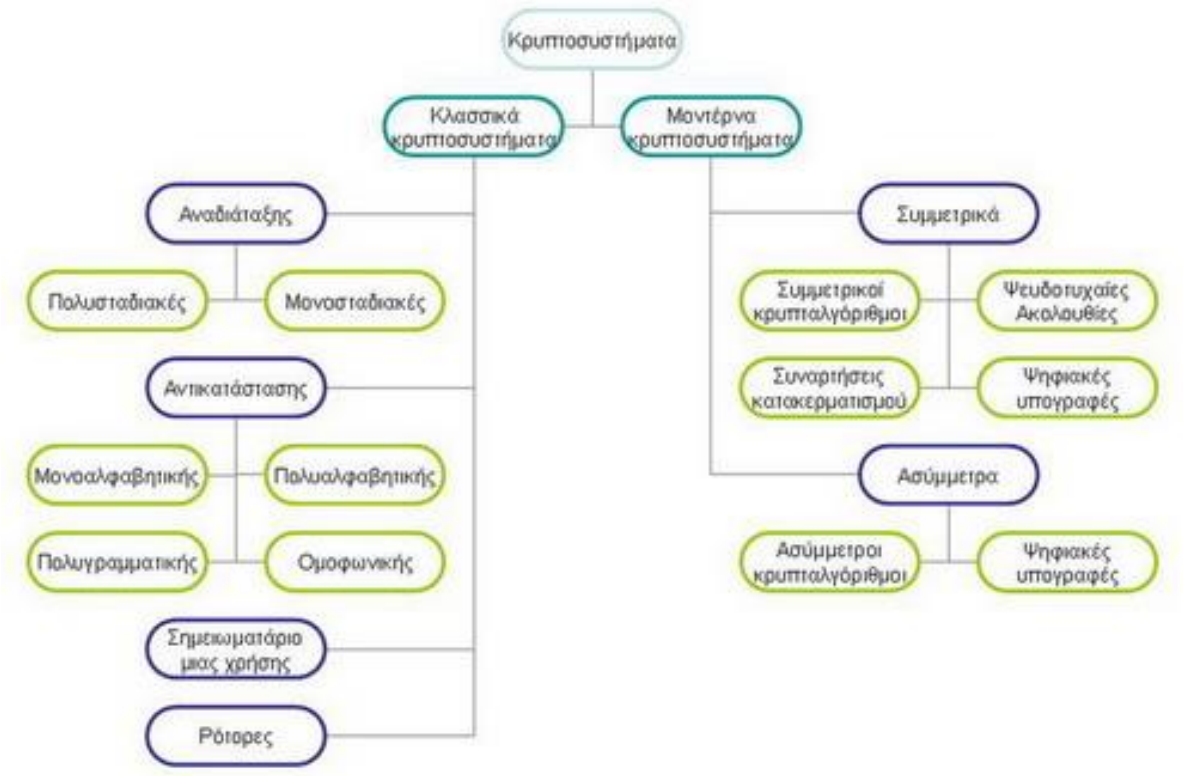
εικόνα 1.2 Πηγή: https://el.wikipedia.org/wiki/Κρυπτογραφία

Οι όροι κλειδί κρυπτογράφησης και αποκρυπτογράφησης αναφέρονται σε έναν αριθμό αρκετών bit που χρησιμοποιείται ως είσοδος στη συνάρτηση κρυπτογράφησης.

Κεφάλαιο 2ο: Συστήματα Κρυπτογραφίας, Αλγόριθμοι, Κλειδιά

2.1 Είδη Κρυπτοσυστημάτων

Τα κρυπτοσυστήματα που έχουν αναπτυχθεί χωρίζονται σε δυο κατηγορίες, τα Κλασσικά ή αλλιώς Συμμετρικά Κρυπτοσυστήματα και τα Μοντέρνα ή Ασύμμετρα Κρυπτοσυστήματα. Παρακάτω παρουσιάζεται και ένα αναλυτικό διάγραμμα των βασικών συστατικών στοιχείων κάθε κρυπτογραφικού είδους.



εικόνα 2.1.1 Πηγή: https://el.wikipedia.org/wiki/Κρυπτογραφία

2.1.1 Κλασσικά – Συμμετρικά Κρυπτοσυστήματα

Συμμετρικό κρυπτοσύστημα είναι το σύστημα εκείνο το οποίο χρησιμοποιεί κατά τη διαδικασία της κρυπτογράφησης ή αποκρυπτογράφησης ένα κοινό κλειδί. Η ασφάλεια αυτών των αλγορίθμων βασίζεται στη μυστικότητα του κλειδιού. Τα συμμετρικά κρυπτοσυστήματα 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.

Έστω ότι έχουμε δυο χρήστες. Τα στάδια της επικοινωνίας τους μέσω του συμμετρικού μοντέλου είναι τα ακόλουθα:

1. Οι χρήστες του συστήματος αποφασίζουν για ένα κλειδί το οποίο το επιλέγει τυχαία μέσα από τον κλειδοχώρο.
2. Ο πρώτος χρήστης αποστέλλει το κλειδί στον δεύτερο μέσα από ένα ασφαλές κανάλι.
3. Ο δεύτερος δημιουργεί ένα μήνυμα όπου τα σύμβολα m ανήκουν στον χώρο των μηνυμάτων.
4. Κρυπτογραφεί το μήνυμα με το κλειδί που έλαβε από τον πρώτο χρήστη και η παραγόμενη κρυπτοσυμβολοσειρά αποστέλλεται.
5. Ο πρώτος χρήστης λαμβάνει την κρυπτοσυμβολοσειρά και στη συνέχεια με το ίδιο κλειδί την αποκρυπτογραφεί και η έξοδος που παράγεται είναι το αρχικό μη κρυπτογραφημένο μήνυμα.

εικόνα 2.1.2 Πηγή: https://el.wikipedia.org/wiki/Κρυπτογραφία

Οι βασικοί αλγόριθμοι αυτού του μοντέλου χωρίζονται σε τέσσερις υποκατηγορίες με βάση τον τρόπο κρυπτογράφησης μηνυμάτων και είναι οι εξής:

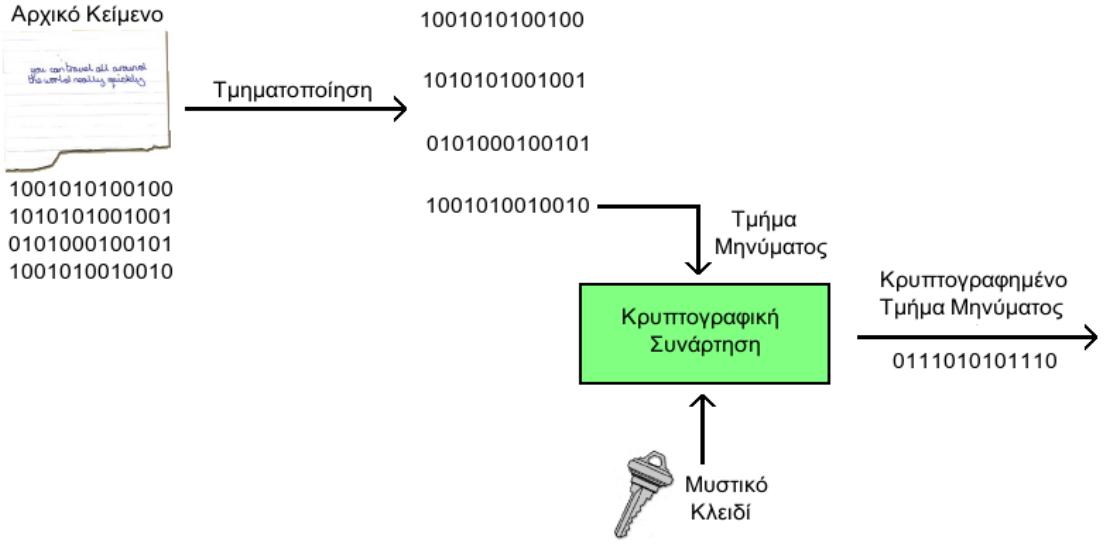
- **Δέσμης (Block Ciphers)**, οι οποίοι χωρίζουν το μήνυμα σε κομμάτια και κρυπτογραφούν κάθε ένα από τα κομμάτια αυτά χωριστά.

  Χαρακτηριστικός αλγόριθμος αυτής της κατηγορίας είναι ο DES (Data Encryption Standard). Ο DES υιοθετήθηκε το 1977 από τον NIST (National Institute of Standards and Technology) ως το επίσημο πρότυπο για κρυπτογράφηση μη απορρήτων πληροφοριών. Αναπτύχθηκε από την IBM και βασίστηκε στον προϋπάρχοντα αλγόριθμο, Lucifer. Ο DES έχει μήκος τμήματος 64 bits και μήκος κλειδιού 56 bits (στην πραγματικότητα έχει μήκος κλειδιού 64 bits αλλά τα 8 bits είναι bits ισοτιμίας). Ο αλγόριθμος αρχικά αντιμεταθέτει τα δυο υποτμήματα μήκους 32 bits το κάθε ένα (Αρχική Αντιμετάθεση) και στην συνέχεια 7 για 16 γύρους χρησιμοποιεί ένα υποκλειδί από το αρχικό κλειδί μήκους 48 bits για να υλοποιήσει την εξής πράξη :

  $$Li = Ri{-}1 \; και \; Ri = Li{-}1 \oplus f(Ri{-}1, Ki)$$

  $με \; i$ = 1, … ,16 όπου με L και R συμβολίζουμε το εκάστοτε αριστερά και δεξιά υποτμήματα των 32 bits. Τέλος, ο αλγόριθμος μετά το πέρας των 16 γύρων κάνει την αντίστροφη της Αρχικής Αντιμετάθεσης και αυτό είναι το τελικό αποτέλεσμα. Η αποκρυπτογράφηση ενός τμήματος γίνεται εφόσον ακολουθηθεί η ακριβώς αντίστροφη διαδικασία. Το 1977 οι Diffie και Hellman χρησιμοποίησαν ένα μήνυμα και την κρυπτογράφηση του και σχεδίασαν ένα μηχάνημα το οποίο μπορούσε να ανακαλύψει το κλειδί κάνοντας εξαντλητική αναζήτηση σε λιγότερο από μια ημέρα, κάτι το όποιο ήταν αρκετά πρωτοποριακό για δεδομένα της εποχής.

  Επιπλέον χαρακτηριστικά παραδείγματα αλγορίθμων αυτής της υποκατηγορίας αποτελούν οι εξής αλγόριθμοι: 3Way ,Blowfish, CAST ,CMEA , TripleDES, DEAL FEAL, GOST, IDEA,LOKI, Lucifer, MacGuffin, TwofishMARS, MISTY, MMB, NewDES, RC2, RC5, RC6 REDOC, Rijndael, Safer, Serpent, SQUARE, Skipjack, Tiny Encryption Algorithm



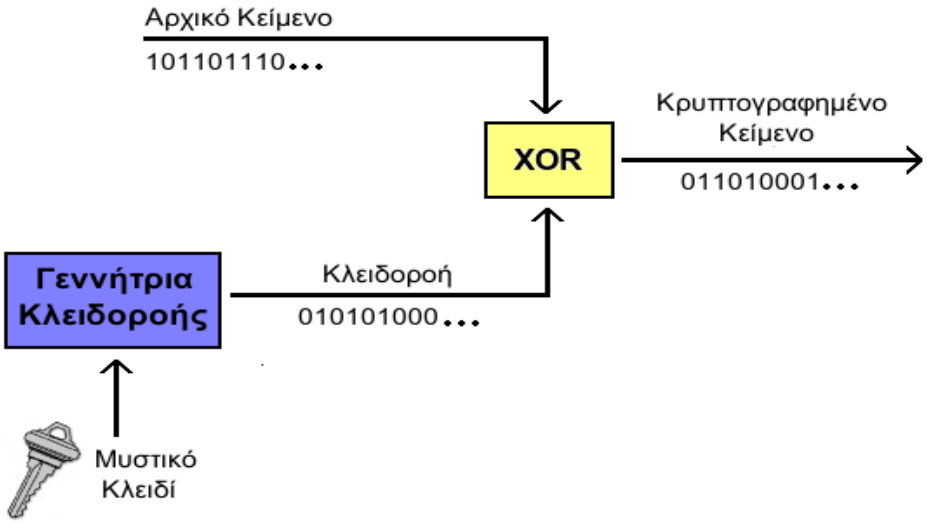
εικόνα 2.1.3 Πηγή: https://el.wikipedia.org/wiki/Κρυπτογραφικοί_Αλγόριθμοι_Δέσμης

- **Ροής (Stream Ciphers)**, οι οποίοι κρυπτογραφούν μία ροή μηνύματος (stream) χωρίς να τη διαχωρίζουν σε τμήματα.

  Οι κρυπταλγόριθμοι αυτοί εμφανίζονται τόσο σε συμμετρική όσο και ασύμμετρη μορφή, εμείς όμως θα αναλύσουμε μόνο την ασύμμετρη μορφή καθώς μόνο αυτή περιορίζεται στα πλαίσια της παρούσας εργασίας. Η βασική διαφορά των αλγορίθμων αυτής της κατηγορίας έγκειται στο γεγονός ότι η κρυπτογράφηση γίνεται κάθε χρονική στιγμή όχι όμως σε επίπεδο τμήματος, αλλά σε επίπεδο συμβόλου. Χρησιμοποιείται μια ψευδοτυχαία ακολουθία συμβόλων η οποία ονομάζεται κλειδοροή, η οποία συνδυάζεται με το αρχικό κείμενο προκειμένου να παραχθεί το κρυπτογραφημένο μήνυμα. Όπως θα αναλυθεί και σε επόμενο κεφάλαιο, οι κρυπταλγόριθμοι ροής είναι ιδανικοί για τηλεπικοινωνιακές εφαρμογές καθώς χαρακτηρίζονται από χαμηλές απαιτήσεις μνήμης αλλά και μικρή διάδοση σφαλμάτων.

  Ο RC4 είναι ένας από τους πιο δημοφιλείς κρυπταλγορίθμους ροής. Σχεδιάστηκε από τον Ron Rivest και κυκλοφόρησε πρώτη φορά το 1994. Ο αλγόριθμος χρησιμοποιεί κλειδιά μήκους από 40 μέχρι 2048 bits και η λειτουργία του βασίζεται σε μεταθέσεις και πράξεις αποκλειστικής διάζευξης (XOR). Η απλή δομή του καθώς και οι μικρές απαιτήσεις σε μνήμη, τον έκαναν ευρέως διαδεδομένο και έτσι χρησιμοποιήθηκε σε πρωτόκολλα όπως το WEP και το TLS [4]. Παρόλα αυτά, σήμερα δεν προτιμάται καθώς δεν είναι πλέον ασφαλής.

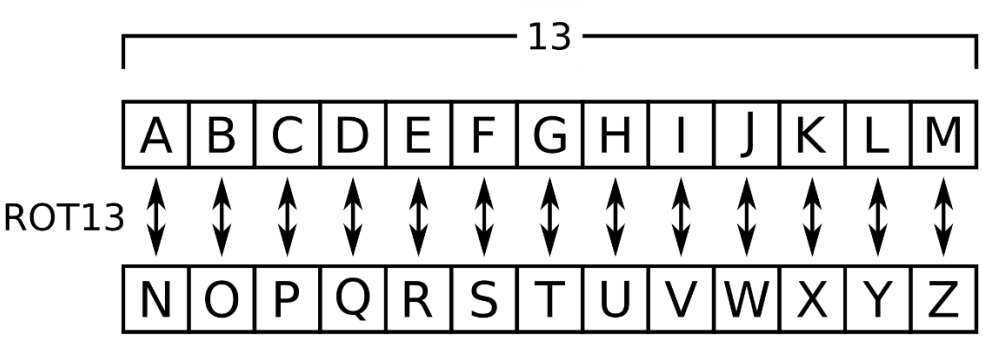
  Επιπλέον χαρακτηριστικά παραδείγματα αλγορίθμων αυτής της υποκατηγορίας αποτελούν οι αλγόριθμοι ORYX και SEAL.



εικόνα 2.1.4 Πηγή: https://el.wikipedia.org/wiki/Κρυπτογραφικοί_Αλγόριθμοι_Ροής

- **Αντικατάστασης (substitution ciphers)**
  Οι κρυπταλγόριθμοι αυτοί αντιστοιχίζουν και στη συνέχεια αντικαθιστούν κάθε σύμβολο-γράμμα που αρχικού μηνύματος με κάποιο άλλο γράμμα ή ακολουθία γραμμάτων. Ο δέκτης λαμβάνοντας το μήνυμα για να το αποκρυπτογραφήσει ακολουθεί την ανάστροφη διαδικασία. Υπάρχουν αρκετά είδη αντικατάστασης, το πιο γνωστό όμως και αυτό που αντικαθιστά μονά γράμματα είναι η απλή κρυπτογραφική αντικατάσταση που περιεγράφηκε παραπάνω. Η απλή κρυπτογραφική αντικατάσταση έχει και αυτή διάφορα είδη. Μια από τι πιο γνωστές είναι η αντικατάσταση ROT13. Σύμφωνα μ αυτή

χωρίζουμε στη μέση το αλφάβητο και αντιστοιχίζουμε τα γράμματα όπως παρουσιάζεται στην παρακάτω εικόνα.



εικόνα 2.1.5 Πηγή: https://commons.wikimedia.org/wiki/File:ROT13_table.svg

Ας δούμε ένα παράδειγμα για καλύτερη κατανόηση. Έστω ότι το μήνυμα είναι: “Hello”. Μετά την αντικατάσταση των γραμμάτων όπως υποδεικνύει η παραπάνω εικόνα το μήνυμα θα γίνει “Uryyb”.

Ένα ακόμα παράδειγμα είναι το σύστημα zebra, το οποίο κατά την αντιστοίχιση έχει στην αρχή τη λέξη zebra και μετά ακολουθούν στην κανονική τους σειρά τα γράμματα που υπολείπονται. Έτσι λοιπόν έχουμε:

Κανονικό Αλφάβητο: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Αλφάβητο Αντικατάστασης: ZEBRASCDFGHIJKLMNOPQTUVWXY

Έστω ότι το μήνυμα είναι: “We are discovered”. Μετά την αντικατάσταση zebra θα έχουμε “Va zoa repbluaoar”.

Με αντίστοιχο τρόπο μπορούμε να δημιουργήσουμε πολλούς τέτοιους κρυπταλγορίθμους.

Επιπλέον σ’ αυτή την κατηγορία αλγορίθμων υπόκεινται και αλγόριθμοι-συναρτήσεις κατακερματισμού. Οι κρυπτογραφικές συναρτήσεις κατακερματισμού, έρχονται να δώσουν λύση, μεταξύ άλλων, στο πρόβλημα της ακεραιότητας ενός μηνύματος, γιατί τόσο η αλλοίωση λόγω της μεταφοράς μέσα από κανάλια επικοινωνίας, όσο και κακόβουλοι χρήστες, πολλές φορές μπορούν να διαφοροποιήσουν σε μικρό ή μεγάλο βαθμό ένα μήνυμα προβλημάτων. Αυτό που κάνουν είναι να αντιστοιχίζουν το μήνυμα σε μια συμβολοσειρά προκαθορισμένου μεγέθους (message digests). Ο τελικός χρήστης που παραλαμβάνει ένα μήνυμα, μπορεί να το δώσει σαν όρισμα στην ίδια συνάρτηση και αν οι συμβολοσειρές (message digests) ταυτίζονται, τότε ξέρει ότι δεν υπήρξε αλλοίωση.

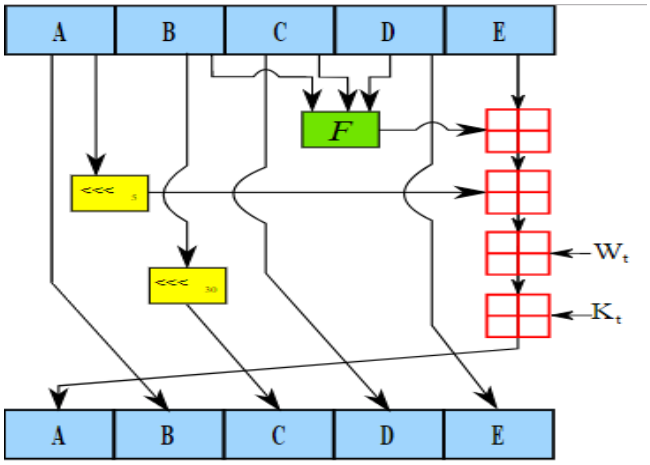
Προκειμένου να θεωρηθεί μια συνάρτηση κατακερματισμού αποδεκτή για χρήση στην κρυπτογραφία πρέπει να πληροί συγκεκριμένες προϋποθέσεις :

- Το κείμενο εισόδου να μπορεί να έχει οσοδήποτε μήκος.
- Η συνάρτηση να μπορεί να υπολογιστεί γρήγορα (σε πολυωνυμικό χρόνο) συναρτήσει του μήκους της εισόδου.
- Η συμβολοσειρά εξόδου πρέπει να έχει σταθερό μήκος, με ελάχιστο τα 128 bits και συνηθισμένο τα 160 bits.
- Να μην μπορεί να βρεθεί $x \neq y$ με $H(x) = H(y)$ σε πολυωνυμικό χρόνο.
- Να είναι αδύνατο δεδομένης της τιμής H(x) να μπορεί να ανακτηθεί το x.

Μερικοί χαρακτηριστικοί αλγόριθμοι αυτής της κατηγορίας είναι η οικογένεια των MD(Message Direct) όπως οι MD2, MD4, MD5, η οικογένεια των SHA όπως οι SHA-1, SHA-2 και SHA-3, Snefru, RIPEMD. Παρακάτω θα αναλύσουμε μια από τις βασικές οικογένειες αλγορίθμων.

Οικογένεια SHA

Η συνάρτηση κατακερματισμού SHA-1 δημιουργήθηκε από την NSA (National Security Agency) και υιοθετήθηκε από τον NIST ως στάνταρ για μη απόρρητες πληροφορίες (FIPS).Το μέγιστο μέγεθος κειμένου που δέχεται η συνάρτηση είναι 264 και παράγει έξοδο των 160 bits. Η επεξεργασία γίνεται σε block των 512 bits, το οποίο χωρίζεται σε λέξεις των 32 bits και στις οποίες εφαρμόζονται προσαυξήσεις, ολισθήσεις και προσθέσεις σε τέσσερις γύρους των είκοσι βημάτων. Σχηματικά, ένα γύρος αναπαρίσταται στο παρακάτω σχήμα όπου με A,B,C,D,E αναπαρίστανται λέξεις των 32 bits, F είναι μια συνάρτηση η οποία διαφοροποιείται ανά γύρο, Wt είναι η προσαυξημένη λέξη στον γύρο t, ενώ Kt είναι μια σταθερά που και αυτή αλλάζει ανά γύρο. Τέλος, τα προσομοιώνουν πρόσθεση mod 2 32 .



εικόνα 2.1.6 Πηγή: http://www.unixwiz.net/techtips/iguide-crypto-hashes.html

Αντίστοιχα οι SHA-2 και SHA-3 αποτελούν νεότερες εκδόσεις SHA-1. Στην SHA-2 δημιουργούνται συμβολοσειρές μήκους 224,256,384 και 512 bits, ενώ παράλληλα υποστηρίζονται τμήματα εισόδου εώς 21024 καθώς και τμήματα υπολογισμού των 64 bits.

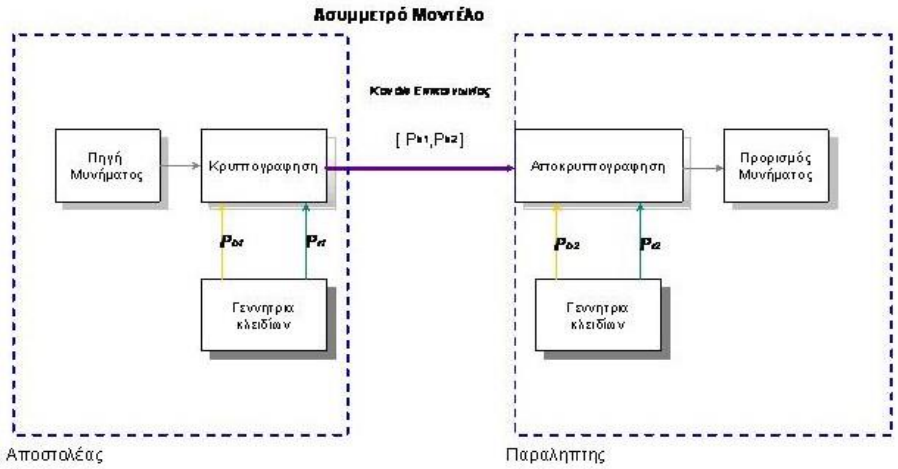
Επίσης, στην SHA-3 υποστηρίζονται διαφορετικά μεγέθη εξόδου μήκους 224, 256, 384, και 512 bits ενώ τα τμήματα που χρησιμοποιούνται για τον υπολογισμό έχουν μέγεθος 1600 bits (σε επιμέρους μέρη λέξεων των 64 bits) και το μέγεθος της εισόδου δεν περιορίζεται σε κάποιο μέγεθος.

2.1.2 Μοντέρνα – Ασύμμετρα Κρυπτοσυστήματα

Το ασύμμετρο κρυπτοσύστημα ή κρυπτοσύστημα δημοσίου κλειδιού (Κρυπτογράφηση Δημόσιου Κλειδιού) αποτελεί τη νεότερη μορφή κρυπτογραφίας και δημιουργήθηκε για να καλύψει την αδυναμία μεταφοράς κλειδιών που παρουσίαζαν τα συμμετρικά συστήματα. Εμφανίστηκε για πρώτη φορά το 1976 από τους Diffie και Hellman και βασίζεται στην μαθηματική σχέση των κλειδιών κρυπτογράφησης και αποκρυπτογράφησης, τα οποία πλέον δεν ταυτίζονται. Γι' αυτό έχει δυο είδη κλειδιών, ένα ιδιωτικό και ένα δημόσιο. Το δημόσιο είναι διαθέσιμο σε όλους ενώ το ιδιωτικό είναι μυστικό. Η βασική σχέση μεταξύ τους είναι: ό,τι κρυπτογραφεί το ένα, μπορεί να το αποκρυπτογραφήσει μόνο το άλλο, ενώ παρά το γεγονός ότι τα κλειδιά σχετίζονται μαθηματικά, δεν υπάρχει τρόπος να υπολογιστεί το ιδιωτικό με βάση το δημόσιο. Οι δυνατότητες της ασύμμετρης κρυπτογραφίας οδήγησαν στη δημιουργία των ψηφιακών υπογραφών και ακολούθως στην ανάπτυξη της Υποδομής Δημόσιου Κλειδιού (Public Key Infrastructure) και στα Ψηφιακά πιστοποιητικά.

Έστω πάλι ότι έχουμε δυο χρήστες. Τα στάδια της επικοινωνίας τους μέσω του ασύμμετρου μοντέλου είναι τα ακόλουθα:

1. Η γεννήτρια κλειδιών του πρώτου χρήστη παράγει 2 ζεύγη κλειδιών,
2. Η γεννήτρια κλειδιών του δεύτερου χρήστη παράγει 2 ζεύγη κλειδιών
3. Οι χρήστες ανταλλάσσουν τα δημόσια ζεύγη
4. Ο πρώτος δημιουργεί ένα μήνυμα όπου τα σύμβολα m ανήκουν στον χώρο των μηνυμάτων.
5. Κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί του δεύτερου και η παραγόμενη κρυπτοσυμβολοσειρά αποστέλλεται
6. Ο δεύτερος λαμβάνει την κρυπτοσυμβολοσειρά και στη συνέχεια με το ιδιωτικό του κλειδί την αποκρυπτογραφεί και η έξοδος που παράγεται είναι το αρχικό μη κρυπτογραφημένο μήνυμα.



εικόνα 2.1.7 Πηγή: https://el.wikipedia.org/wiki/Κρυπτογραφία

Μερικοί χαρακτηριστικοί ασύμμετροι κρυπταλγόριθμοι είναι οι εξής: RSA, DSA, Paillier, Πρωτόκολλο Diffie-Hellman, Πρότυπο ElGamal ή αλλιώς Υπογραφή ElGamal, Κρυπτογραφία

ελλειπτικών καμπύλων (ECC). Από αυτά θα αναλύσουμε λίγο περισσότερο τον αλγόριθμο RSA καθώς υπήρξε η αφετηρία της χρήσης των ψηφιακών υπογραφών οι οποίες τείνουν να αντικαταστήσουν πλήρως τις σημερινές.

Το 1976 ο Whitfield Diffie και ο Martin Hellman για πρώτη φορά παρουσίασαν την ιδέα των ψηφιακών υπογραφών, αν και η κεντρική ιδέα των τέτοιων συστημάτων προϋπήρχε. Ένα χρόνο αργότερα, ο Ronald Rivest, ο Adi Shamir και ο Len Adleman παρουσίασαν τον αλγόριθμο RSA ο οποίος χρησιμοποιήθηκε στις πρώτες ψηφιακές υπογραφές. Οι πρώτες ψηφιακές υπογραφές με τον αλγόριθμο RSA αποδείχθηκαν ότι δεν ήταν ασφαλείς. Το πρώτο, ευρέος γνωστό στην αγορά, λογισμικό που χρησιμοποίησε τέτοιες ψηφιακές υπογραφές ήταν τον Lotus Notes 1.0, το οποίο κυκλοφόρησε το 1989.

Η γενική ιδέα υλοποίησης του αλγορίθμου είναι η εξής:

Ένας χρήστης για να δημιουργήσει τα δυο κλειδιά του, επιλέγει δυο μεγάλους τυχαίους αριθμούς, έστω p και q, για τους οποίους πρέπει η διαφορά p-q να είναι επίσης μεγάλη. Στη συνέχεια, υπολογίζει το γινόμενο τους $n = p * q$, καθώς και την τιμή $\varphi(n) = (p - 1)(q - 1)$. Ύστερα, επιλέγει ένα αριθμό e, ο οποίος πρέπει να είναι σχετικά πρώτος με το φ(n) και μεγαλύτερος του 1. Τέλος, υπολογίζει d τέτοιο ώστε $d * e \equiv 1 \ mod \ \varphi(n)$. Από τα παραπάνω, το ιδιωτικό του κλειδί είναι το d και το δημόσιο του, το ζευγάρι n,e. Προκειμένου να κρυπτογραφήσει κάποιος ένα μήνυμα m, υπολογίζει το $c = memod \ n$, ενώ η αποκρυπτογράφηση γίνεται υπολογίζοντας την ποσότητα $m = c \ dmod \ n$.

Κεφάλαιο 3: Σύγχρονες εφαρμογές της κρυπτογραφίας

3.1 Κρυπτογραφία και DNA

Η κρυπτογραφία παίζει βασικό ρόλο στην ασφάλεια των πληροφοριών. Πολλοί νέοι αλγόριθμοι και τεχνικές έχουν χρησιμοποιηθεί με το ίδιο σκεπτικό. Η κρυπτογραφία με τη χρήση του DNA είναι πολύ πρόσφατη και σύγχρονη τεχνολογία. Ανεβαίνουμε ένα επίπεδο πιο πάνω στο κομμάτι της ακεραιότητας και της εμπιστευτικότητας των δεδομένων για την προστασία των πληροφοριών από εισβολές. Στην εργασία του Mazhar Karimi (Ιούνιος 2017) προτείνεται μια λύση κρυπτογράφησης με ένα νέο μοντέλο συμμετρικής δημιουργίας κλειδιών βασισμένο στο DNA, στα νουκλεοτίδια, στα κωδικόνια κανόνων ζευγών βάσεων και μετάλλαξης καθώς και στη μετατροπή του DNA σε mRNA. Η λύση που προτάθηκε από τον Mazhar Karimi τονίζει τη χρήση βιολογικών διεργασιών και τις τυχαίες αλλαγές που εντοπίστηκαν στο DNA οι οποίες προσομοιώνουν αυτές τις διαδικασίες στη δημιουργία κλειδιών όπως ακριβώς και στη κρυπτογραφία.

Αρχικά το DNA προσομοιώνεται ως μια τρισδιάστατη διπλή έλικα, σαν μια σπειροειδή σκάλα. Κάθε έλικα αποτελείτε από άλλα μονομερή τα οποία ονομάζονται νουκλεοτίδια. Κάθε νουκλεοτίδιο έχει ζάχαρη και φωσφορικά σε ομάδες και η βάση του είναι αζώτου. Αυτές οι βάσεις αζώτου είναι αδενίνη (A), Θυμίνη (T), Γουανίνη (G) και Κυτοσίνη (C).

Όταν ο Adleman ξεκίνησε την έρευνα του στη μοριακή βιολογία, συνειδητοποίησε ότι αυτά τα 4 γράμματα (A, T, G και C) κατέχουν όλες τις πληροφορίες που απαιτούνται για έναν οργανισμό, και με αντίστοιχο τρόπο μπορεί να χρησιμοποιηθεί για τον επιτυχή υπολογισμό ενός μαθηματικού προβλήματος πολυπλοκότητας NP πλήρες. Το πρόβλημα αυτό ήταν πολυπλοκότητας O(n) σε τσιπ πυριτίου και το ίδιο επιλύθηκε σε O(1) χρησιμοποιώντας DNA. Αυτή ήταν η αρχή της χρήσης του DNA στην κρυπτογραφία.

Η κρυπτογραφία του DNA είναι ένα θεωρητικό πεδίο πληροφορικής όπου το DNA χρησιμοποιείται για την απόκρυψη πληροφοριών. Το μικρότερο DNA αποτελείται από 30 νουκλεοτίδια. Το DNA δηλαδή είναι μια αποθήκη πληροφοριών η οποία μεταφράζεται σύμφωνα με τον παρακάτω πίνακα.

Bits	Nucleotide
00	A
11	C
01	G
10	T

Μετά τη μετατροπή του δυαδικού αριθμού σε Νουκλεοτίδια, εφαρμόζεται η διαδικασία της αντιγραφής εάν το μήκος των νουκλεοτιδίων είναι μικρότερο από 60. Στη συνέχεια εάν το μήκος των νουκλεοτιδίων δεν είναι τέλεια διαιρούμενο με το μήκος ενός κωδικονίου, το τελευταίο κωδικόνιο τροποποιείται επαναλαμβάνοντας το τελευταίο νουκλεοτίδιο στην αλληλουχία. Στη συνέχεια της διαδικασίας η ενιαία έλικα συνδέεται με το ζεύγος της σύμφωνα με τον συμπληρωματικό κανόνα. Δημιουργείται λοιπόν, ένα πλήρες DNA. Ακολουθεί η μετατροπή του

DNA στο mRNA. Οι πρωτεΐνες καλούνται κλειδιά του DNA. Ο αριθμός των κλειδιών DNA εξαρτάται από το πόσα κωδικονικά σφάλματα βρίσκονται και πώς τα αμινοξέα τύπου τρυπτοφάνης (UGG), γλουταμίνης (CAG), αργινίνης (CGA), Αλανίνη (GCC) και Ασπαρτικό Οξύ (GAU) που προκύπτουν από τη μετάλλαξη του DNA σε mRNA μετατρέπονται σε κωδικόνια τερματισμού ή άλλα αμινοξέα. Όταν δημιουργηθούν όλα τα τελικά κλειδιά DNA, αποκωδικοποιούνται σε μπλόκ των 8 bits.

Ας δούμε όμως ένα παράδειγμα για να γίνει πιο κατανοητή η όλη διαδικασία.

Έστω ότι έχουμε το παρακάτω μήνυμα σε δυαδικά ψηφία
01101101011001010111001101110011011000010110011101 100101

Όταν αυτά μεταφραστούν σε νουκλεοτίδια θα έχουμε
GAAAATAAGGCCATAAATTCATAAACATATCGGAAA ATAAGGCCATAAATTCATAAACAT

Όταν η διαδικασία της μετάλλαξης εφαρμοστεί και οι δύο έλικες ενωθούν θα έχουμε
GAAAATAAGGCCATAAATTCATAAACATATCGGAAAATAAGGCCATAAATTCATAAACATCTT
TTATTCCGGT ATTTAAGTATTTGTATAGCCTTTTATTCCGGTATTTA AGTATTTGTA

Όταν ξεκινά η διαδικασία της μεταγραφής, η ακολουθία γίνεται ως εξής
GAAAAUAAGGCCAUAAAUUCAUAAACAUAUCGGAAAAUAAGGCCAUAAAUUCAUAAACAC
UUUUAUUCCGGUAUUUAAGUAUUUGUAUAGCCUUUUAUUCCGGUAUUUAAGUAUUUGUA

Όταν γίνεται η μετατροπή σε mRNA και δημιουργούνται οι πρωτεΐνες-κλειδιά έχουμε
GAAAAUAAGGCCAUAAAUUCAUAAACAUAUCGGAAAAUAAGGCCAUAAAUUCAUAAACAC
UUUUAUUCCGGUAUUUAAGUAUUUGUAUAGCCUUUUAUUCCGGUAUUUAAGUAUUUGUA

ACAUAUCGGAAAAUAAGGCCAUAAAUUCAUAAACAUCUUUUAUUCCGGUAUUUAAGUAUU
UGUAUAGCCU UUUAUUCCGGUAUUUAAGUAUUUGUA

AUUCAUAAACAUCUUUUAUUCCGGUAUUUAAGUAUUUGUAUAGCCUUUUAUUCCGGUAU
UUAAGUAUUUGUA

GUAUUUGUAAAA

Το οποίο όταν το μεταφράσουμε σε bits θα έχουμε

01000000011100000010000000000011010000000111000000100000000011101010110110101000111101010 1101101010100010101010

00000011010000000111000000100000000011101010110110101000101010101001111010101101101010100010101010

00100000000011101010110110101000101010101001111010 10110110101000101010100010010000

Κάθε DNA κλειδί δημιουργεί ένα δυαδικό block

$$B = \{b_1, b_2 \dots b_n\}$$

Σε κάθε δυαδικό block, κάθε 8 bits blocks ομαδοποιούνται στα

$$b_i = \{k_1, k_2 \dots k_n\}$$

Για την κρυπτογράφηση τα πρώτα 8 ψηφία του μηνύματος συλλέγονται και μετατοπίζονται αριστερά κατά 1 bit και εφαρμόζεται η λειτουργία XOR με καθένα στο μπλοκ 1, αυτό συνεχίζεται για όλα τα {k1, k2 ... kn} στο b1.

$$CM = (M << 1) \oplus b1kj$$

Το δεύτερο δυαδικό μπλοκ μετατοπίζει το μήνυμα κατά 2 bits και εφαρμόζει XOR με καθένα πλήκτρο στο μπλοκ 2, και αυτό επίσης συνεχίζεται για όλα τα πλήκτρα στο μπλοκ b2.

$$CM = (CM << 2) \oplus b2kj$$

Ο γενικός τύπος που προκύπτει είναι:

$$CM = (CM << i) \oplus bikj$$

Επομένως το τελικό κρυπτογραφημένο μήνυμα είναι :

11101001111010011110100111101001111010011110100111 101001

3.2 Κρυπτογραφία και κινητά τηλέφωνα

Αρχικά για λόγους ευκολίας από εδώ και στο εξής θα αναφερόμαστε στον κλιμακωτό πολλαπλασιασμό ελλειπτικής καμπύλης ως ECSM (elliptic curve scalar multiplication).

Στο άρθρο τους με τίτλο “A NEW ALGORITHM FOR SIGNED BINARY REPRESENTATION AND APPLICATION IN MOBILE PHONES”, οι συγγραφείς μας παρουσιάζουν και προτείνουν έναν αλγόριθμο ο οποίος μπορεί να αντικαταστήσει το πρωτόκολλο ελλειπτικής καμπύλης της κρυπτογραφίας πάνω στο οποίο βασίζονται τα κινητά μας τηλέφωνα έχοντας έτσι καλύτερη απόδοση κυρίως από άποψη χρόνου.

Η πιο σημαντική λειτουργία στην ελλειπτική καμπύλη είναι ο βαθμιαίος πολλαπλασιασμός. Αυτή μπορεί να αναπαρασταθεί μαθηματικά ως F=rG όπου F,G είναι σημεία στην ελλειπτική καμπύλη και r είναι οποιοσδήποτε θετικός ακέραιος αριθμός. Η χρήση της δυαδικής επέκτασης για την αναπαράσταση του r όπως είναι ένα άθροισμα από n-1 μέχρι s=0, θεωρείται ο πιο συνηθισμένος τρόπος. Εδώ, rs είναι ένα στοιχείο ενός πεπερασμένου σετ στοιχείων, του Dk.

Το ζητούμενο, λοιπόν, είναι η βελτιστοποίηση του βαθμιαίου πολλαπλασιασμού. Αυτή μπορεί να πραγματοποιηθεί με την εισαγωγή γρήγορων σύνθετων μεθόδων και με τη χρήση συστημάτων συντεταγμένων (coordinates systems) αντί για συντεταγμένες συγγενών (affine coordinates). Μπορεί επίσης να επιταχυνθεί μέσω τεχνικών προεπεξεργασίας (precomputations techniques), αλλά και μετατροπών του hardware.

Η δυαδική αναπαράσταση του μήκους του κλιμακωτού k και το πλήθος των “1” σε αυτό, ελέγχουν την απόδοση και το κόστος του ECSM. Έχουν γίνει αρκετές μελέτες για την εύρεση του βέλτιστου τρόπου αναπαράστασης του k και οι συγγραφείς μας σ’ αυτή την περίπτωση χρησιμοποιούν την πιο απλή από αυτές τις μεθόδους, τη δυαδική μέθοδο. Ορίζεται, λοιπόν, ως $(k_{l-1}, k_{l-2},\ldots, k_0)_2$ όπου ki ∈ (0,1), i=0, 1, 2, …, l-4. Επιπλέον, κάθε ακέραιος μπορεί να εκφραστεί ως ένα άθροισμα από το 0 μέχρι το l-1 του $k_i 2^i P_i$ και όλο αυτό το ονομάζουμε P_2 και έχουμε άλλο ένα σημείο στην ελλειπτική καμπύλη. Ο αλγόριθμος που περιγράφει τη διαδικασία αυτή παρουσιάζεται παρακάτω.

Είσοδος: $k = (k_{l-1}, k_{l-2},\ldots, k_0)_2$, $P_1 \in E(F_p)$

Έξοδος: Q = kP

Βήμα 1: Q = P

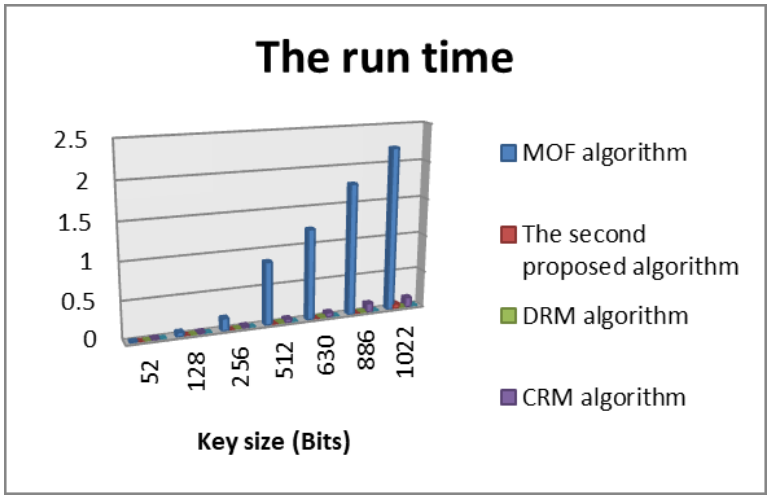
Βήμα 2: for i = l – 1 down to 0 do

Βήμα 2.1: If $k_i = 1$ then Q = Q + P

Βήμα 2.2: Q = 2P

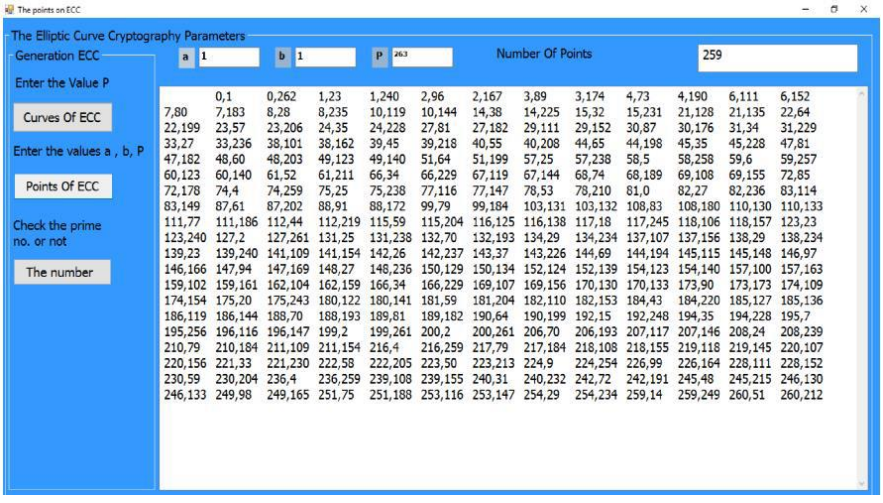
Βήμα 3: Return Q

Στη συνέχεια προτείνουν και άλλους αλγορίθμους όπως ο δεξιά-προς-τα-αριστερά της αμοιβαίας αντίθετης μορφής (Mutual Opposite Form - MOF) σε ECSM, τη Συμπληρωματική Αναγνωριστική Μέθοδο (Complementary Recognition Method - CRM), τη Μη Γειτονική Μορφή (Non Adjacent Form - NAF) του κλιμακωτού k, τη μη προσημασμένη δυαδική αναπαράσταση του κλιμακωτού k για την άμεση μέθοδο αναγνώρισης (Direct Recognition Method - DRM), οι οποίοι συνοδεύονται και από παραδείγματα και αποτελέσματα εκτελέσεων. Οι τέσσερις αυτοί αλγόριθμοι συγκρίνονται σύμφωνα με τον χρόνο εκτέλεσης για τη δημιουργία μη προσημασμένων δυαδικών αναπαραστάσεων. Τα αποτελέσματα αυτής της σύγκρισης παρουσιάζονται συνοπτικά στην παρακάτω εικόνα.



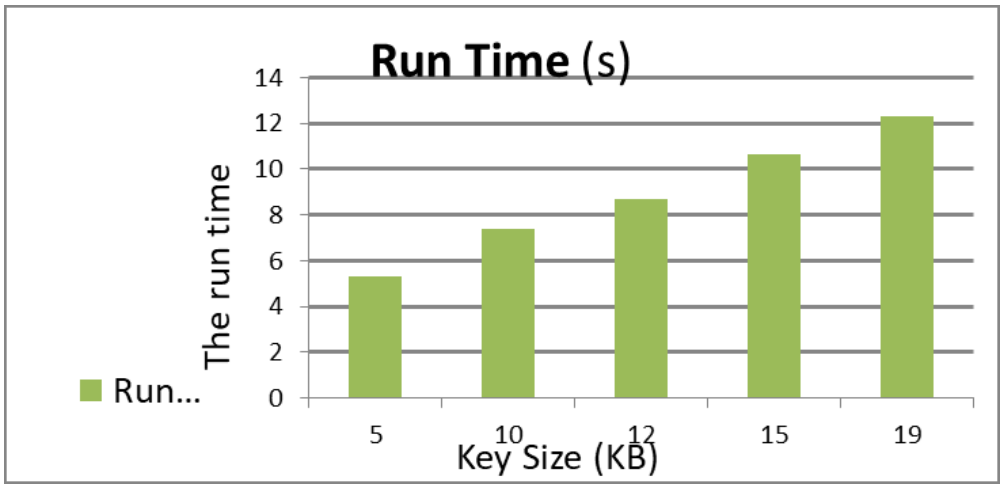
εικόνα 3.2.1 Πηγή: άρθρο ενότητας “A new algorithm for signed binary representation and application in mobile phones”

Στη συνέχεια μας παρουσιάζουν τις εφαρμογές που σχεδίασαν. Αυτή που έχει αρκετό ενδιαφέρον για τη κρυπτογραφία είναι αυτή που υπολογίζει τις ελλειπτικές καμπύλες πάνω από μια δοσμένη δίνοντας μόνο τη τιμή του πρώτου αριθμού, ο οποίο έχει ήδη υπολογιστεί σε προηγούμενη εφαρμογή. Κάθε αποτέλεσμα αποτελείται από δύο τιμές οι οποίες αντικαθίστανται στην εξίσωση της ελλειπτικής καμπύλης. Τα αποτελέσματα δίνονται στην παρακάτω εικόνα.



εικόνα 3.2.2 Πηγή: άρθρο ενότητας “A new algorithm for signed binary representation and application in mobile phones”

Προφανώς όλα αυτά τα δεδομένα πρέπει να κρυπτογραφηθούν για να μεταφερθούν και ο χρόνος που χρειάζονται για να κρυπτογραφηθούν είναι ένας πολύ σημαντικός παράγοντας. Παρακάτω φαίνεται τα δευτερόλεπτα που χρειάζονται για την κρυπτογράφηση αντίστοιχων KB.



εικόνα 3.2.3 Πηγή: άρθρο ενότητας “A new algorithm for signed binary representation and application in mobile phones”

Αντίστοιχα με την κρυπτογράφηση για την αποστολή, χρειάζεται και η αποκρυπτογράφηση για την παραλαβή του μηνύματος. Επομένως έχουμε μετρήσεις και για την αποκρυπτογράφηση.

εικόνα 3.2.4 Πηγή: άρθρο ενότητας “A new algorithm for signed binary representation and application in mobile phones”

Συνοψίζοντας, οι συγγραφείς μας παρουσιάζουν έναν νέο αλγόριθμο ο οποίος μετά την εφαρμογή του για την κατασκευή ενός νέου κρυπτοσυστήματος EC, παρουσιάζει καλύτερους χρόνους απόκρισης από αυτόν που χρησιμοποιείται τώρα. Φυσικά μπορεί να εφαρμοστεί σε οποιαδήποτε κινητή συσκευή που χρησιμοποιεί Android, αφού αυτός ήταν και ο σκοπός της παρούσας εργασίας.

3.3 Quantum Computing και Κρυπτογραφία

Στη παράγραφο αυτή θα ασχοληθούμε με το άρθρο του Tim Moses με τίτλο “Quantum Computing and Cryptography ”. Αρχικά όμως τι είναι το Quantum Computing; Πρόκειται για ένα μοντέλο υπολογισμού που εκμεταλλεύεται τις περίεργες αλλά συνάμα και υπέροχες ιδιότητες των κβαντικών αντικειμένων. Ορισμένα προβλήματα, των οποίων η δυσκολία αυξάνεται εκθετικά με το μέγεθος του προβλήματος στο κλασικό μοντέλο, κλιμακώνονται πολυωνυμικά (ή ακόμα και γραμμικά) στο το κβαντικό μοντέλο, καθιστώντας έτσι δυνατή μια λύση ακόμα και για μεγάλα συστήματα.

Στο κλασικό υπολογιστικό μοντέλο, η βασική μονάδα πληροφοριών είναι ένα "bit", το οποίο μπορεί να υιοθετήσει μια από τις δύο αμοιβαία αποκλειστικές καταστάσεις, είτε το "0" είτε το "1". Η πιο στοιχειώδης λειτουργία που μπορεί να πραγματοποιηθεί με αυτά είναι μια πύλη, η οποία παίρνει κάποιο αριθμό bits στις εισόδους της και παράγει ένα bit στην έξοδο της. Αυτές οι πύλες μπορούν να συνδυάζονται σε κυκλώματα για την πραγματοποίηση πιο σύνθετων λειτουργιών, όπως είναι μια μονάδα επεξεργασίας δεδομένων.

Ομοίως, στο μοντέλο κβαντικού υπολογισμού, η βασική μονάδα πληροφοριών ονομάζεται "quantum bit "ή" qubit ", το οποίο μπορεί να υπάρξει σε οποιοδήποτε από όσα οι φυσικοί ονομάζουν "ιδανικό quantum σύστημα δύο καταστάσεων". Παραδείγματα τέτοιων συστημάτων περιλαμβάνουν φωτόνια (με κάθετη και οριζόντια πόλωση που αντιπροσωπεύουν τις δύο ορθογώνιες καταστάσεις), ηλεκτρόνια και άλλα συστήματα spin-1/2 (με περιστροφή επάνω και αριστερά που αντιπροσωπεύουν τις δύο ορθογώνιες καταστάσεις) και συστήματα που ορίζονται από δύο ενεργειακά επίπεδα ατόμων ή ιόντα.

Κάθε κατάσταση αντιστοιχεί στις γνωστές τιμές "0" και "1" bit. Τα qubits όμως μπορούν να λάβουν τιμές που είναι υπερθέσεις αυτών των δύο καταστάσεων. Έτσι, μπορεί να θεωρηθεί ότι καταλαμβάνουν μια κατάσταση που είναι ένας συνδυασμός τόσο της κατάστασης "0" όσο και της κατάστασης "1". Ενώ η κβαντομηχανική περιγράφει αρκετά ενδιαφέροντα φαινόμενα, η υπέρθεση είναι αυτή έχει λάβει την μεγαλύτερη προσοχή λόγω της καταλληλότητά της ως βάση ενός κβαντικού υπολογιστή.

Με την κατασκευή μεγάλων κβαντικών υπολογιστών, θα υπάρξουν τουλάχιστον δύο σημαντικές επιπτώσεις για την ασφάλεια των πληροφοριών. Οι κβαντικοί υπολογιστές θα επηρεάσουν την ασφάλεια και των αλγορίθμων συμμετρικού κλειδιού (π.χ., κρυπτογράφηση μπλοκ) αλλά και τους αλγορίθμους δημόσιου κλειδιού (όπως RSA), αν και η σοβαρότητα των επιπτώσεων θα είναι διαφορετική για κάθε μία περίπτωση. Όσων αναφορά την κρυπτογραφία δημόσιου κλειδιού οι συνέπειες είναι πιο σοβαρές. Οι κβαντικοί υπολογιστές μπορούν να τρέξουν αλγόριθμους που σπάζουν όλα τα δημοφιλή συστήματα δημόσιου κλειδιού σε ασήμαντα χρονικά διαστήματα. Για παράδειγμα, ο κβαντικός αλγόριθμος Shor μπορεί να ανακτήσει ένα κλειδί RSA σε πολυωνυμικό χρόνο.

Για την αντιμετώπιση αυτού του προβλήματος δημιουργήθηκε η κβαντική κρυπτογραφία. Πρόκειται για μια άλλη βασική μέθοδο διανομής που θα ήταν απρόσβλητη από τις κβαντικές υπολογιστικές επιθέσεις, στα περιβάλλοντα όμως τα οποία εφαρμόζεται η κβαντική κρυπτογραφία. Αυτό ισχύει γιατί η κβαντική κρυπτογραφία παρέχει "απόλυτη ασφάλεια". Σημειώστε, ωστόσο, ότι υπάρχουν ορισμένες βοηθητικές λειτουργίες εντός κβαντικών

κρυπτογραφικών σχημάτων που εξαρτώνται από τη συμμετρική ή δημόσιου κλειδιού κρυπτογράφηση και αυτές θα επηρεαστούν ακριβώς όπως περιγράφεται παραπάνω.

Υπάρχουν δύο περιοχές της κρυπτογραφίας που μπορούν να επωφεληθούν από την εφαρμογή των κβαντικών μηχανών: η παραγωγή τυχαίων αριθμών και η διανομή κλειδιών.

Παραγωγή τυχαίων αριθμών

Πολλές από τις διαδικασίες που συνήθως θεωρούμε τυχαίες δεν είναι πραγματικά τυχαίες, απλώς εμείς δεν διαθέτουν τα δεδομένα ή την υπολογιστική ισχύ για να προβλέψουμε τις μελλοντικές τους τιμές. Για παράδειγμα, αν είχαμε επαρκείς πληροφορίες σχετικά με ένα κομμάτι βουτυρωμένο τοστ που πέφτει προς ένα δάπεδο με μοκέτα θα είμαστε σε θέση να προβλέψουμε εάν θα προσγειωθεί με την πλευρά του βουτύρου προς τα κάτω ή με την πλευρά του βουτύρου προς τα πάνω (στην πραγματικότητα, ο νόμος του Murphy ρυθμίζει την κατάσταση και το τοστ θα προσγειώνεται πάντα από την πλευρά του βουτύρου).

Οι κβαντικές διεργασίες, από την άλλη πλευρά, είναι πραγματικά τυχαίες. Καμία ποσότητα υπολογιστικής ισχύος δεν θα μας επιτρέψει να κάνουμε προβλέψεις για τις μελλοντικές τους τιμές. Οι περισσότεροι κρυπτογραφικοί μηχανισμοί χρησιμοποιούν κλειδιά για να προστατεύσουν είτε την εμπιστευτικότητα είτε την ακεραιότητα των δεδομένων. Αυτά τα κλειδιά πρέπει να μην είναι προβλέψιμα από έναν εισβολέα, οπότε συνήθως παράγονται με τυχαία σειρά. Βέβαια, είναι πολύ δύσκολο να αποδείξουμε την ποσότητα της εντροπίας που παρουσιάζεται μόνο από ένα λογισμικό γεννήτρια τυχαίων αριθμών.

Διανομή κλειδιών

Το πρόβλημα της διανομής κλειδιών αντιμετωπίζεται από οποιαδήποτε δύο μέρη που θέλουν να επικοινωνήσουν ασφαλώς. Αν δυο χρήστες θέλουν να χρησιμοποιήσουν ένα παραδοσιακό κωδικό κρυπτογράφησης μπλοκ και μηνύματος για να προστατεύσουν τις επικοινωνίες τους, πρέπει πρώτα απ' όλα να συμφωνήσουν σε ένα κλειδί. Σήμερα, αυτό το πρόβλημα συνήθως λύνεται με κρυπτογραφία δημόσιου κλειδιού.

Οι δυο χρήστες δημιουργούν ένα ζεύγος δημόσιου-ιδιωτικού κλειδιού και καταγράφουν το δημόσιο μέρος με μια αρχή πιστοποίησης (certification authority - CA). Στη συνέχεια, η CA δημιουργεί ένα πιστοποιητικό για κάθε δημόσιο κλειδί και το διανέμει στο άλλο. Οι χρήστες μπορούν πλέον να χρησιμοποιούν το δικό τους ιδιωτικό κλειδί και το δημόσιο κλειδί από το άλλο CA, και να συμφωνήσουν σε ένα κοινό συμμετρικό κλειδί με το οποίο θα προστατεύσουν την επικοινωνία τους. Υπάρχει ένας αριθμός αλγορίθμων και πρωτοκόλλων για αυτό, συμπεριλαμβανομένης της συμφωνίας κλειδιού Diffie-Hellman και της βασικής μεταφοράς RSA.

Η κρυπτογραφία δημόσιου κλειδιού είναι επί του παρόντος ένας ασφαλής τρόπος για την προστασία των πληροφοριών. Χρησιμοποιώντας τα μεγέθη των πλήκτρων που χρησιμοποιούνται σήμερα, φαίνεται ότι δεν είναι εφικτό για έναν εισβολέα να αποκτήσει αποκλειστικά το ιδιωτικό κλειδί ενός χρήστη με την ανάλυση του δημόσιου κλειδιού του, το οποίο συνήθως απαιτείται για να σπάσει ένα δημόσιο κλειδί.

Η κβαντική κρυπτογραφία δεν είναι μια νέα μέθοδος κρυπτογραφίας και δεν μπορεί να αντικαταστήσει πλήρως όλες τις χρήσεις του συμμετρικού και του δημόσιου κλειδιού κρυπτογράφηση. Ωστόσο, παρέχει μια ριζικά διαφορετική προσέγγιση στο βασικό πρόβλημα διανομής. Στη κρυπτογραφία δημόσιου κλειδιού, με το πέρας της επικοινωνίας των δύο χρηστών το κλειδί μπορεί να χρησιμοποιηθεί σε συμβατικό συμμετρικό κρυπτογράφο, σε κωδικό ελέγχου ταυτότητας μηνύματος ή σε κάποιο άλλο μεμονωμένο πεδίο.

Στη κβαντική κρυπτογραφία παρέχεται απόλυτη ασφάλεια επειδή, σε αντίθεση με τα παραδοσιακά κρυπτογραφικά συστήματα τα οποία βασίζονται σκληρά μαθηματικά προβλήματα, βασίζεται στο φυσικό νόμο, γνωστό ως Αρχή αβεβαιότητας του Heisenberg. Στην αρχική του διατύπωση, ο νόμος αυτός δηλώνει ότι η μετρούμενη θέση και η ορμή ενός σωματιδίου δεν μπορούν να είναι γνωστές με ακρίβεια. Δηλαδή, η περισσότερη βεβαιότητα υπάρχει για τη θέση του σωματιδίου, τόσο μεγαλύτερη αβεβαιότητα υπάρχει για την ορμή του και αντίστροφα.

Ας αφήσουμε όμως τους αριθμούς να μιλήσουν μόνοι τους. Η κβαντική κρυπτογραφία έχει ήδη εφαρμοστεί και κλειδιά της έχουν εναλλαγή σε αποστάσεις μεγαλύτερες των 100χλμ. Μια βασική συμφωνία είναι εφικτή σε περίπου 2Kb ανά δευτερόλεπτο στον πραγματικό κόσμο όχι μόνο στις προσομοιώσεις.

Παρόλα αυτά υπάρχουν και αρνητικά σημεία. Αρχικά, δεν παρέχει επί του παρόντος ικανοποιητική μέθοδο απόκτησης ψηφιακής υπογραφή. Οι ψηφιακές υπογραφές και η προστασία ακεραιότητας και αυθεντικότητας που παρέχουν είναι μια από τις πιο σημαντικές χρήσεις της κρυπτογραφίας δημόσιου κλειδιού. Επιπλέον, δεν φαίνεται να είναι πρακτική, εκτός από πολύ περιορισμένες καταστάσεις όπου είναι πρακτική για χρήση μεταξύ δύο σταθερών θέσεων με σημαντικό όγκο δεδομένων για ανταλλαγή και με πολύ υψηλές απαιτήσεις εμπιστευτικότητας.

3.4 Post-Quantum Κρυπτογραφία

Για να καλύψουμε τις ανάγκες της κβαντικής υπολογιστικής ισχύος έχουμε πλέον περάσει στη μέτα-κβαντική κρυπτογραφία (Post-Quantum Cryptography). Έχει αναδειχθεί μια μεγάλη διεθνής κοινότητα για να αντιμετωπίσει το ζήτημα της ασφάλειας των πληροφοριών σε ένα κβαντικό υπολογιστικό μέλλον, με την ελπίδα ότι η υποδομή δημόσιου κλειδιού μας μπορεί να παραμείνει ανέπαφη χρησιμοποιώντας νέα πρωτόνια ανθεκτικά στα κβάντα. Στον ακαδημαϊκό κόσμο, αυτή η νέα επιστήμη φέρει το όνομα "μετά-κβαντική κρυπτογραφία". Προσοχή όμως η μετά-κβαντική κρυπτογραφία δεν πρέπει να συγχέεται με την κβαντική κρυπτογραφία (ή την κβαντική διανομή κλειδιού), η οποία χρησιμοποιεί ιδιότητες της κβαντομηχανικής για να δημιουργήσει ένα ασφαλές κανάλι επικοινωνίας.

Στην εικόνα που ακολουθεί φαίνεται η επίδραση της κβαντικής υπολογιστικής στους κοινούς κρυπτογραφικούς αλγόριθμους, μερικούς από τους οποίους αναλύσαμε στο Κεφάλαιο 2.

Table 1 - Impact of Quantum Computing on Common Cryptographic Algorithms

Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	----------	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

Πηγή: άρθρο ενότητας "Report on Post-Quantum Cryptography

Στη συνέχεια θα δούμε συνοπτικά τις κύριες οικογένειες για τις οποίες έχουν προταθεί μετα-κβαντικά στοιχεία. Αυτές οι οικογένειες, περιλαμβάνουν αυτές που βασίζονται σε πλέγματα, κωδικούς και πολυώνυμα με πολλές μεταβλητές, καθώς και μερικές ακόμα.

Κρυπτογραφία βασιζόμενη σε πλέγμα

Τα κρυπτοσυστήματα που βασίζονται σε προβλήματα πλέγματος έχουν κερδίσει το ενδιαφέρον, για σχετικά λίγους λόγους. Συναρπαστικές νέες εφαρμογές (όπως η πλήρως ομομορφική κρυπτογράφηση, κωδικοποίηση του κώδικα και κρυπτογράφηση με βάση τα χαρακτηριστικά) έχουν καταστεί δυνατές χρησιμοποιώντας τη χρήση πλέγματος κρυπτογράφηση. Οι περισσότεροι αλγόριθμοι δημιουργίας κλειδιών βασισμένοι σε πλέγμα είναι σχετικά απλοί,

αποδοτικοί, και εξαιρετικά παραλληλοποιημένοι. Επίσης, η ασφάλεια ορισμένων συστημάτων που βασίζονται σε πλέγματα είναι προφανώς ασφαλής κάτω από μια υπόθεση χειρότερης περίπτωσης, αντί για τη μέση περίπτωση. Από την άλλη πλευρά, έχει αποδειχθεί δύσκολο να δώσει κανείς ακριβείς εκτιμήσεις για την ασφάλεια των συστημάτων πλέγματος ενάντια ακόμη και σε γνωστές τεχνικές κρυπτοανάλυσης.

Κρυπτογραφία βασισμένη στον κώδικα

Το 1978, προτάθηκε το πρώτο κρυπτοσύστημα βασισμένο σε κώδικα, το κρυπτοσύστημα McEliece και δεν έχει σπάσει από τότε. Βέβαια, από τότε, έχουν προταθεί και άλλα συστήματα βασισμένα σε συστήματα διόρθωσης λαθών κώδικα. Ενώ είναι αρκετά γρήγοροι, τα περισσότερα βασισμένα στο κώδικα στοιχεία υποφέρουν από τα πολύ μεγάλα μεγέθη κλειδιών. Οι νεότερες παραλλαγές έχουν εισαγάγει περισσότερη δομή στους κώδικες σε μια προσπάθεια να μειωθεί το μέγεθος του κλειδιού, ωστόσο η προστιθέμενη δομή έχει επίσης οδηγήσει σε επιτυχείς επιθέσεις σε ορισμένες προτάσεις. Ενώ έχουν υπάρξει κάποιες προτάσεις για κωδικοποιημένες υπογραφές, η κρυπτογραφία βάσει κώδικα έχει δει μεγαλύτερη επιτυχία με τα προγράμματα κρυπτογράφησης.

Πολλαπλασιαστική πολυωνυμική κρυπτογραφία

Τα συστήματα αυτά βασίζονται στη δυσκολία επίλυσης πολυωνυμικών συστημάτων πολλών μεταβλητών σε πεπερασμένα πεδία. Αρκετά κρυπτοσυστήματα με πολλές μεταβλητές έχουν προτάθηκε τις τελευταίες δεκαετίες, ενώ πολλά έχουν σπάσει. Επιπλέον, ενώ έχουν υπάρξει μερικές προτάσεις για πολυπαραγοντικά συστήματα κρυπτογράφησης, η πολυπαραγοντική κρυπτογραφία, ιστορικά, ήταν πιο επιτυχημένη ως προσέγγιση των υπογραφών.

Hash βασισμένες υπογραφές

Hash-based υπογραφές είναι ψηφιακές υπογραφές που κατασκευάζονται χρησιμοποιώντας hash συναρτήσεις. Η ασφάλεια τους, ακόμη και ενάντια στις κβαντικές επιθέσεις, είναι αρκετά κατανοητή. Πολλά ακόμα και από τα πιο αποδοτικά συστήματα υπογραφής με βάση το hash έχουν το μειονέκτημα ότι ο υπογράφων πρέπει να κρατά αρχείο με τον ακριβή αριθμό των μηνυμάτων που έχει υπογράψει γιατί οποιοδήποτε λάθος σε αυτό το μέτρημα θα έχει ως αποτέλεσμα ανασφάλεια. Ένα άλλο μειονέκτημα είναι ότι μπορούν να παράγουν μόνο περιορισμένο αριθμό υπογραφών. Ο αριθμός των υπογραφών μπορεί να αυξηθεί, ακόμα και στο σημείο να είναι πραγματικά απεριόριστος. Αυτό βέβαια, αυξάνει το μέγεθος υπογραφής.

Άλλο

Έχουν προταθεί διάφορα συστήματα που δεν εμπίπτουν στις παραπάνω οικογένειες. Μια τέτοια πρόταση βασίζεται στην αξιολόγηση των ισογονιδιών σε υπερηχητικές ελλειπτικές καμπύλες. Ενώ το διακριτό πρόβλημα καταγραφής των ελλειπτικών καμπυλών μπορεί να λυθεί αποτελεσματικά με αλγόριθμο Shor σε κβαντικού υπολογιστή, το πρόβλημα της ισογονικότητας στις υπερκείμενες καμπύλες δεν έχει κάποια παρόμοια γνωστή κβαντική επίθεση. Μερικές άλλες προτάσεις, όπως για παράδειγμα εκείνες που βασίζονται στο πρόβλημα αναζήτησης συζυγικής

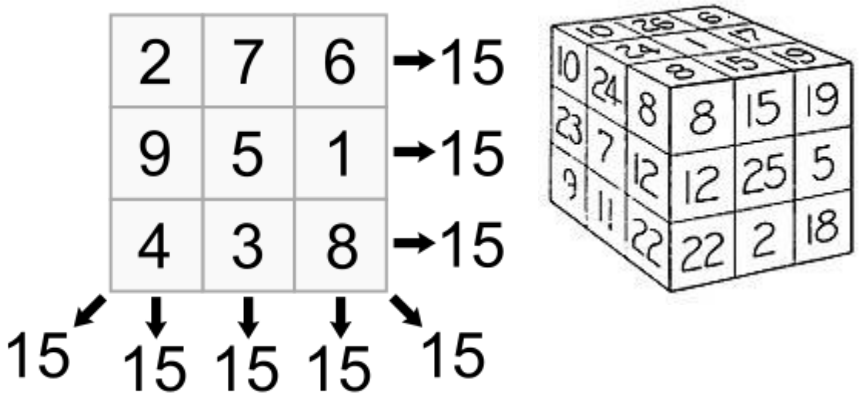
σύνδεσης και τα σχετικά προβλήματα σε ομάδες πλεξούδες, δεν έχουν αναλυθεί αρκετά ώστε να έχουμε εμπιστοσύνη στην ασφάλειά τους.

Φαίνεται απίθανο οποιοσδήποτε από τους γνωστούς αλγόριθμους μπορεί να χρησιμεύσει ως drop-in αντικατάσταση αυτού που χρησιμοποιείται σήμερα. Μία πρόκληση που πιθανόν θα πρέπει να ξεπεραστεί είναι αυτή ότι οι περισσότεροι από τους κβαντικούς ανθεκτικούς αλγόριθμους έχουν μεγαλύτερα μεγέθη κλειδιών από τους αλγορίθμους που καλούμαστε να αντικαταστήσουμε. Αυτό μπορεί να έχει ως αποτέλεσμα την ανάγκη αλλαγής διαφόρων πρωτοκόλλων του Internet, όπως το πρωτόκολλο μεταφοράς επιπέδου (Transport Layer Security – TLS), ή το Internet Key Exchange (IKE). Οι τρόποι με τους οποίους αυτό θα πραγματοποιηθεί πρέπει να γίνουν πολύ προσεκτικά.

Συνοψίζοντας, δεν είναι σαφές πότε θα είναι διαθέσιμοι οι κλιμακωτοί κβαντικοί υπολογιστές. Ωστόσο, στο παρελθόν, οι ερευνητές που εργάστηκαν για την κατασκευή ενός κβαντικού υπολογιστή έχουν εκτιμήσει ότι είναι πιθανό ότι ο κβαντικός υπολογιστής που μπορεί να σπάσει τον RSA 2000-bit σε λίγες ώρες θα μπορούσε να κατασκευαστεί μέχρι το 2030 με προϋπολογισμό περίπου ενός δισεκατομμυρίου δολαρίων. Πρόκειται για μια σοβαρή μακροπρόθεσμη απειλή για τα κρυπτοσυστήματα που επί του παρόντος τυποποιούνται από την NIST. Είναι χρήσιμο να συγκρίνουμε τις παραπάνω προβλέψεις με το κόστος διάσπασης αυτών των κρυπτοσυστημάτων στους κλασικούς υπολογιστές. Κρυπτοσυστήματα που προσφέρουν 80 bit ασφαλείας ή λιγότερα, τα οποία καταργήθηκαν σταδιακά το 2011-2013, διατρέχουν τον μεγαλύτερο κίνδυνο: μπορούν να σπάσουν τώρα με κόστος που κυμαίνεται από δεκάδες χιλιάδες έως εκατοντάδες εκατομμύρια δολάρια. Κρυπτοσυστήματα που προσφέρουν 112 bits ασφάλειας είναι πιθανό να παραμείνουν ασφαλή για κάποιο χρονικό διάστημα. Μπορεί βέβαια, να είναι παραμείνουν εύθραυστα για έναν προϋπολογισμό δισεκατομμυρίων δολάρια σε 30 έως 40 χρόνια (χρησιμοποιώντας κλασσικούς υπολογιστές). Έτσι, η μετάβαση από 112 σε 128 (ή υψηλότερα) bits ασφαλείας είναι ίσως λιγότερο επείγουσα από τη μετάβαση των υπαρχόντων κρυπτοσυστήματων σε μετα-κβαντικά κρυπτοσυστήματα. Αυτή η μετα-κβαντική μετάβαση εγείρει πολλές θεμελιώδεις προκλήσεις.

3.5 Μαγικό Τετράγωνο

Το μαγικό τετράγωνο αποτελεί διάταξη αριθμών σε συστοιχία ίσου συνόλου γραμμών και στηλών, όπου η αριθμητική πράξη μεταξύ των αριθμών στην ίδια σειρά ή στήλη ή διαγώνιο του τετραγώνου επιστρέφει πάντα το ίδιο αποτέλεσμα. Το κοινό αποτέλεσμα ονομάζεται μαγική σταθερά του μαγικού τετραγώνου. Η πλέον συνήθης αριθμητική πράξη στα μαγικά τετράγωνα είναι η πρόσθεση μεταξύ των αριθμών. Ένα χαρακτηριστικό μαγικό τετράγωνο είναι αυτό που φαίνεται στην παρακάτω εικόνα και αθροίζεται στο 15. Επιπλέον, υπάρχουν και άλλες εκδοχές τους όπως η τέλεση αφαίρεσης ή πολλαπλασιασμού, καθώς και είναι δυνατό να αναπαρασταθούν σε τρισδιάστατη μορφή ως μαγικοί κύβοι ή ορθογώνια, ή να υπάρξουν τροποποιήσεις όπου αντί για αριθμούς χρησιμοποιούνται σχήματα.



εικόνα 3.5.1

Πηγή: https://el.wikipedia.org/wiki/Μαγικό_τετράγωνο

Η πρώτη περιγραφή μαγικού τετραγώνου υπήρξε στην Κίνα από την 3η χιλιετία π.Χ., κατόπιν μεταφέρθηκε στους Ινδούς κατά την ύστερη αρχαιότητα και μετέπειτα στους Άραβες, και από εκεί στους Βυζαντινούς από όπου μεταδόθηκε στην υπόλοιπη Ευρώπη. Κατά τον Μεσαίωνα τα μαγικά τετράγωνα ήταν ιδιαίτερα δημοφιλή ως φυλακτά και αποτροπαϊκά σύμβολα. Στην σύγχρονη εποχή αποτελούν συχνό πεδίο ενασχόλησης των ψυχαγωγικών μαθηματικών και των μαθηματικών κλάδων της συνδυαστικής και στατιστικής, καθώς επίσης της τέχνης και του μυστικισμού, και επίσης σε ότι αφορά τις πρακτικές εφαρμογές τους χρησιμοποιούνται για τους σκοπούς της κρυπτογράφησης ψηφιακών εικόνων, ενώ στην μηχανική ρευστών για τον υπολογισμό κατακράτησης υδάτων σε επιφάνειες.

Στο άρθρο, λοιπόν, που εξετάζουμε σ αυτή την ενότητα με τίτλο “A Research on Enhancing Public Key Cryptography by The Use of MRGA with RSA and N-Prime RSA” , οι συγγραφείς μας παρουσιάζουν μια μεθοδολογία χρήσης του μαγικού ορθογώνιου για την εξασφάλιση μεγαλύτερης ασφάλειας. Όπως αναφέρουν η χρήση του μαγικού τετραγώνου εξαρτάται εντελώς από τον μαθηματικό υπολογισμό του πίνακα. Στο μαγικό ορθογώνιο, η άθροιση όλων των στηλών είναι ίδια όπως επίσης και στις στήλες. Αυτός ο τύπος πίνακα χρησιμοποιείται και μπορεί να κάνει στα δεδομένα μια ακόμα χαρτογράφηση στον χρόνο και έτσι να δημιουργήσει ένα ακόμα επίπεδο ασφάλειας στην επικοινωνία. Έτσι, με τη χρήση του μαγικού ορθογώνιου μπορούμε να ενισχύσουμε το κρυπτοσύστημα δημόσιου κλειδιού και τους αλγορίθμους που χρησιμοποιούνται στην κρυπτογραφία.

Η μεθοδολογία του προτεινόμενου περιγράφεται στα ακόλουθα βήματα:

1) Κατασκευάστε ένα μαγικό ορθογώνιο άρτιου πλήθους τετραγώνων, διαστάσεων 32x48 και χρησιμοποιήστε αντί του πίνακα ASCII με 128 τιμές. Το μαγικό ορθογώνιο περιέχει συνολικά 1536 τιμές. Έχει χωριστεί σε 12 τεταρτημόρια, όπου το καθένα αποτελείται από 128 χαρακτήρες.

2) Κάθε χαρακτήρας του απλού κειμένου μετατρέπεται σε αριθμούς με βάση τη θέση του στο μαγικό ορθογώνιο σε διαφορετικά τεταρτημόρια. Οι αριθμοί κρυπτογραφούνται και αποκρυπτογραφούνται με RSA και N-prime RSA αλγόριθμο.

Φάση Πρώτη: Δημιουργία του μαγικού ορθογωνίου

Μαγικά ορθογώνια είναι τα ορθογώνια που έχουν άθροισμα όλων των στοιχείων των σειρών ίσα και άθροισμα των στοιχείων των στηλών επίσης ίσα. Θα μας δοθούν οι μέγιστες και ελάχιστες τιμές και από αυτό θα δημιουργήσουμε τον πίνακα 4x6. Θα εφαρμοστούν δύο διαφορετικούς τύπους υπολογισμού μητρώων. Σύμφωνα με τους πίνακες που δίνονται στο μητρώο-1 και στο μητρώο -2, πρώτα θα δημιουργηθεί το μητρώο 4x6 και στη συνέχεια θα υπολογίσουμε το μέγιστο και το ελάχιστο του μητρώου αυτού. Στη συνέχεια θα εφαρμοστεί το δεύτερο είδος μητρώου. Έτσι, η διαδικασία θα συνεχιστεί και εναλλακτικά ο υπολογισμός θα γίνει για μητρώο 4x6. Μετά από την παραγωγή τεσσάρων τετραγώνων 4x6 η συναρμολόγηση θα έρθει και θα δημιουργήσει μητρώο 8x12. Η διαδικασία αυτή συνεχίζεται μέχρι να έχουμε τέσσερα μητρώα 8x12 δημιουργώντας έτσι έναν πίνακα 16x24. Στη συνέχεια οι τέσσερις πίνακες 16x24 θα ενωθούν και τελικά θα δημιουργηθούν πίνακες 32x48.

Φάση Δεύτερη: Χαρτογράφηση μαγικού ορθογωνίου

Από το μητρώο 32x48 θα υπάρχουν συνολικά 1536 τιμές και υπάρχουν συνολικά 128 ASCII τιμές. Θα χωρίσουμε αυτή το μητρώο σε 12 υπομητρώα έτσι ώστε να έχουμε σε κάθε μητρώο 128 τιμές. Για κάθε δεδομένο μήνυμα κάθε χαρακτήρας θα είναι εκεί με την τιμή ASCII του. Και σε κάθε χαρακτήρα θα δοθεί ένας πίνακας με 128 τιμές. Έτσι, 1*1 χαρακτήρας θα έχει 1*1 μητρώο. Ο πρώτος χαρακτήρας θα πάει στο πρώτο μητρώο και ο δεύτερος πηγαίνει στο δεύτερο μητρώο και ούτω καθεξής, ώστε η εμφάνιση δύο ίδιων χαρακτήρων δεν θα έχει το ίδιο κρυπτογραφικό κείμενο. Η αποκρυπτογράφηση θα γίνει ακολουθώντας την αντίστροφη διαδικασία.

Φάση Τρίτη: Κρυπτογράφηση με RSA και N-prime RSA

Το πρότυπο RSA θα εφαρμοστεί ώστε η χαρτογραφημένη τιμή να ληφθεί από το μαγικό ορθογώνιο ως είσοδο και στη συνέχεια θα υπάρχει διαδικασία κρυπτογράφησης. Ομοίως, η διαδικασία αποκρυπτογράφησης θα γίνει με την αντίστροφη σειρά. Την ίδια στιγμή το αποκρυπτογραφημένο μήνυμα θα ληφθεί ως είσοδος και η τιμή του μαγικού ορθογωνίου θα είναι η έξοδος του αλγορίθμου.

1) Κάθε χρήστης δημιουργεί ένα ζεύγος δημόσιου / ιδιωτικού κλειδιού με:

- επιλογή δύο τυχαίων μεγάλων δειγμάτων - p, q
- υπολογίζει τον συντελεστή του συστήματος τους N = p.q
- σημείωση ø (N) = (p-1) (q-1)

- επιλογή τυχαίου κλειδιού κρυπτογράφησης e, όπου 1 <e <ø (N), gcd (e, ø (N)) = 1
- επιλύει την ακόλουθη εξίσωση για να βρει το κλειδί αποκρυπτογράφησης d, d = 1 mod ø (N) και 0≤d≤N
- δημοσιεύει το δημόσιο κλειδί κρυπτογράφησης του: KU = {e, N}
- κρατάει μυστικό το ιδιωτικό κλειδί αποκρυπτογράφησης: KR = {d, p, q}

2) N-Prime RSA:
Ο N-Prime RSA είναι παρόμοιο με τον RSA, αλλά μπορούμε να πάρουμε περισσότερους από δύο πρώτους αριθμούς για τη δημιουργία κλειδιών για κρυπτογράφηση και αποκρυπτογράφηση. Οπως φαίνεται παρακάτω,

- Επιλέξτε δύο ή περισσότερους ξεχωριστούς πρωτεύοντες αριθμούς p, q, r και ούτω καθεξής.
- Υπολογίστε n = p * q * r; "N" ενεργεί ως η τιμή modulus τόσο του δημόσιου όσο και του ιδιωτικού κλειδιού.
- Υπολογισμός της συνάρτησης Attendance του Euler, Φ (n) = (p - 1) * (q - 1) * (r - 1) και ούτω καθεξής.
- Τα υπόλοιπα βήματα είναι παρόμοια με το Standard RSA.

Φάση Τέταρτη: Πιθανά Αποτέσματα
(Οι πίνακες που ακολουθούν προέρχονται από το άρθρο A Research on Enhancing Public Key Cryptography by The Use of MRGA with RSA and N-Prime RSA")

1) Magic rectangle 1 (MR _sub1): Minstart=4, Maxstart=1539, S1=0

1539	6	8	1533	1523	20	4629
12	1529	1527	18	28	1515	4629
1525	16	14	1531	1509	34	4629
10	1535	1537	4	26	1517	4629
3086	3086	3086	3086	3086	3086	

2) Magic rectangle 2 (MR _sub2): Minstart=36, Maxstart=1507; S2=0

1507	38	40	1501	22	1521	4629
44	1497	1495	50	1513	30	4629
1493	48	46	1499	32	1511	4629
42	1503	1505	36	1519	24	4629
3086	3086	3086	3086	3086	3086	

3) Magic rectangle 3 (MR _sub3): Minstart=52, Maxstart=1491 S3=1

1491	54	56	1485	1475	68	4629
60	1481	1479	66	76	1467	4629
1477	64	62	1483	1461	82	4629
58	1487	1489	52	74	1469	4629
3086	3086	3086	3086	3086	3086	

Αυτή η εργασία απαγορεύει σε κάθε εισβολέα να αποκτά το απλό κείμενο σε μια ευανάγνωστη μορφή. Η ασφαλείας βελτιώνεται καθώς δεν υπάρχει επανάληψη των τιμών στο μαγικό ορθογώνιο. Υπάρχουν αρκετές παράμετροι που χρησιμοποιούνται για την αύξηση της πολυπλοκότητας του χρόνου για την κατασκευή του μαγικού ορθογωνίου όπως το άθροισμα των στηλών, οι τιμές Minstart και Maxstart. Ακόμη και αν οι εισβολείς βρουν τις αρχικές τιμές του MR, είναι πολύ δύσκολο να εντοπιστεί η σειρά ή η στήλη. Παίζει ζωτικό ρόλο στην αύξηση της τυχαιότητας και της ασφάλειας του αλγορίθμου. Η χρήση του RSA έχει το πρόβλημα ότι οι πρώτοι αριθμοί που χρησιμοποιούνται θα πρέπει να είναι πάνω από 100. Έτσι έχουν χρησιμοποιήσει τον N-prime RSA, έτσι ώστε να χρησιμοποιηθούν περισσότεροι από δύο πρωταρχικοί αριθμοί και αυτό μπορεί να κάνει την πρόβλεψη των πρώτων αριθμών πιο εύκολη.

Β Ι Β Λ Ι Ο Γ Ρ Α Φ Ι Α

[1] Βικιπαίδεια: https://el.wikipedia.org/wiki/Κρυπτογραφία

[2] M. Burmester, Σ. Γκρίτζαλης, Σ. Κάτσικας και Β. Χρυσακόπουλος, Σύχγρονη Κρυπτογραφία : Θεωρία και Εφαρμογές, Αθήνα: Εκδόσεις Παπασωτηρίου, 2011.

[3] A. S. Tanenbaum, Computer Networks, Prentice Hall, 2003.

[4] Β. Α. Κάτος και Γ. Χ. Στεφανίδης, Τεχνικές Κρυπτογραφίας & Κρυπτανάλυσης, Θεσσαλονίκη: Εκδόσεις Ζυγός, 2003.

[5] Mazhar Karimi, Waleej Haider, “Cryptography using DNA Nucleotides”, June 2017

[6] N.M.G. Al-Saidi, M.A. Magamiss, S.F. Ibraheem, A. Kh. Faraj, “A new algorithm for signed binary representation and application in mobile phones”, Journal of Mathematical and Computational Science, Vol 8, 03 January 2018

[7] Βικιπαίδεια https://en.wikipedia.org/wiki/Substitution_cipher

[8] Tim Moses, Quantum Computing and Cryptography – “Their impact on cryptographic practice”, Entrust Inc, January 2009

[9] V. Dubois, P. Fouque, A. Shamir and J. Stern, Practical cryptanalysis of SFLASH, “Advances in Cryptology” — CRYPTO 2007, Lecture Notes in Comput. Sci. 4622, Springer-Verlag, 2007, pp. 1–12., http://dx.doi.org/10.1007/978-3-540-74143-5_1.

[10]Lily Chen, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray Perlner and Daniel Smith-Tone - “Report on Post-Quantum Cryptography”, April 2016

[11] M. Mariantoni, Building a Superconducting Quantum Computer, Invited Talk PQCrypto 2014, October 2014 Waterloo, Canada. https://www.youtube.com/watch?v=wWHAs--HA1c [accessed 4/20/2016].

[12] Hardik Gandhi, Vinit Gupta, Indra Rajput – “A Research on Enhancing Public Key Cryptography by The Use of MRGA with RSA and N-Prime RSA”, IJIRST - International Journal for Innovative Research in Science & Technology, May 2015

[13] krishtopa (username) - “Data Encryption Standard (DES) as a Guardian of Our Privacy”, https://steemit.com/popularscience/@krishtopa/data-encryption-standard-des-as-a-guardian-of-our-privacy, 2017