ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ ΜΕ ΘΕΜΑ ΚΡΥΠΤΟΓΡΑΦΗΣΗ – ΔΗΜΟΣΙΟ ΚΑΙ ΙΔΙΩΤΙΚΟ ΚΛΕΙΔΙ

Ονοματεπώνυμο: Φωτεινιάς Μιχαήλ
Α.Μ.: 7650
Εξάμηνο: Πτυχίο Β'
Καθηγητής: Τσιρογιάννης Γιώργος

ΠΕΡΙΕΧΟΜΕΝΑ:

ΕΙΣΑΓΩΓΗ – ΕΥΧΑΡΙΣΤΗΡΙΟ ΣΗΜΕΙΩΜΑ

Είναι κοινώς αποδεκτό ότι η τεχνολογία και ειδικότερα, ο τομέας της πληροφορικής έχει εισχωρήσει δυναμικά στη ζωή και στη δράση των ανθρώπων σήμερα.

Επιπροσθέτως, η επιστήμη έχει κάνει αλματώδη βήματα στο τομέα της τεχνολογίας, ώστε σήμερα μπορούμε να μιλάμε για μεγάλη ασφάλεια αλλά και πολλούς κινδύνους όσον αφορά τα δεδομένα που ανταλλάσσονται καθημερινά. Σκοπός λοιπόν της εργασίας αυτής είναι η διερεύνηση των δυνατοτήτων και των λειτουργιών των Κρυπτογραφικών Αλγορίθμων Δημόσιου και Ιδιωτικού κλειδιού, μέσα από μία βιβλιογραφική ανασκόπηση.

Ουσιαστικά πρόκειται για μία περίληψη, η οποία περιλαμβάνει στοιχεία σχετικά με τους Κρυπτογραφικούς Αλγόριθμους από πέντε διαφορετικά βιβλία. Τα βιβλιογραφικά αυτά στοιχεία δόθηκαν σε εμένα από τον υπεύθυνο για την πτυχιακή μου εργασία καθηγητή κ. Τσιρογιάννη Γεώργιο.

Η εργασία περιλαμβάνει τέσσερα κεφάλαια. Το πρώτο κεφάλαιο αποτελεί την εισαγωγή και αναφέρομαι γενικά στους Κρυπτογραφικούς Αλγόριθμους, στο δεύτερο γίνεται λόγος γενικά για τη λειτουργία αλγόριθμων κατασκευής πρώτων αριθμών, στο τρίτο κεφάλαιο γίνεται μια περιγραφή των σημαντικότερων αλγόριθμων κρυπτογράφησης Δημόσιου Κλειδιού και τέλος, στο τέταρτο κεφάλαιο αναφέρω ένα παράδειγμα χρήσης του γνωστού αλγόριθμου R.S.A..

Σ' αυτό το σημείο θα ήθελα να ευχαριστήσω τον καθηγητή μου κ. Τσιρογιάννη Γεώργιο για την πολύτιμη βοήθεια και το χρόνο που μου προσέφερε προκειμένου να ολοκληρωθεί η εργασία αυτή.

Κεφάλαιο Πρώτο:

Εισαγωγή και γενική ανασκόπηση

1.1

Τι είναι η κρυπτογραφία;

Η κρυπτογραφία έχει μια μεγάλη και ενδιαφέρουσα ιστορία. Η πιο ολοκληρωμένη μη-τεχνική περιγραφή του θέματος είναι στο βιβλίο του Kahn, The Codebrakers. Αυτό το βιβλίο ερευνά την κρυπτογραφία από την πρώτη και περιορισμένη της χρήση από τους Αιγυπτίους περίπου 4.000 χρόνια πριν, έως και τον 20° αιώνα όπου διαδραμάτισε σημαντικό ρόλο και στους δύο Παγκοσμίους Πολέμους. Γραμμένο το 1963, το βιβλίο του Kahn καλύπτει τις πτυχές της ιστορίας που ήταν πιο σημαντικές (μέχρι εκείνα τα χρόνια) στην ανάπτυξη της κρυπτογραφίας. Αυτοί που χρησιμοποιούσαν πιο πολύ την κρυπτογραφία ήταν είχαν σχέση με το στρατό, τις διπλωματικές υπηρεσίες και την Κυβέρνηση γενικότερα. Η κρυπτογραφία λοιπόν χρησιμοποιούνταν σαν ένα εργαλείο για την προστασία των Εθνικών μυστικών και στρατηγικών.

Η ευρεία χρήση των υπολογιστών και των συστημάτων επικοινωνίας τη δεκαετία του 1960, δημιούργησε την απαίτηση από τον ιδιωτικό τομέα για μέσα τα οποία θα προστάτευαν τις πληροφορίες σε ψηφιακή μορφή καθώς και για δημιουργία υπηρεσιών ασφαλείας. Ξεκινώντας με τη δουλειά του Feistel στην I.B.M. στις αρχές της δεκαετίας του 1970 και καταλήγοντας το 1977 με την υιοθέτηση σαν Αμερικάνικο Ομοσπονδιακό Πρότυπο Επεξεργασίας για την κρυπτογράφηση μη μυστικών πληροφοριών του DES (Data Encryption Standard), έγινε ο πιο ευρέως διαδεδομένος μηχανισμός κρυπτογράφησης στην ιστορία της ανθρωπότητας.

Η πιο σημαντική εξέλιξη στην ιστορία της κρυπτογραφίας ήρθε το 1976 όταν ο Diffie και ο Hellman εξέδωσαν την εργασία New Directions in Cryptography. Αυτή η εργασία εισήγαγε την επαναστατική ιδέα της Κρυπτογραφίας Δημοσίου κλειδιού (public key cryptography) και παρείχε ένα νέο και έξυπνο μέθοδο για την ανταλλαγή κλειδιών, η ασφάλεια της οποίας είναι βασισμένη στην δυσκολία εντοπισμού του συγκεκριμένου λογαριθμικού προβλήματος. Αν και οι συγγραφείς δεν είναι μια μέθοδο πραγματοποίησης κρυπτογράφησης δημοσίου κλειδιού εκείνη τη περίοδο, η ιδέα τους ήταν σαφής και δημιούργησε μεγάλο ενδιαφέρον στην κρυπτογραφική κοινότητα. Το 1978 οι Rivest, Shamir και Adleman ανακάλυψαν την πρώτη πρακτική χρήση κρυπτογράφησης δημοσίου κλειδιού και χρήσης ιδιωτικής υπογραφής, που τώρα είναι γνωστή ως RSA. Η ιδέα του RSA βασίζεται σε ένα μαθηματικό πρόβλημα, την δυσκολία του να βρίσκουμε με ακρίβεια (factor) μεγάλους ακεραίους. Αυτή η χρήση ενός δύσκολου μαθηματικού προβλήματος στην κρυπτογραφία αναζωογόνησε τις προσπάθειες να βρεθούν πιο επαρκείς μέθοδοι για να factor. Η δεκαετία του 1980 έγιναν μεγάλες πρόοδοι σε αυτό το τομέα, όμως ο αλγόριθμος RSA παρέμεινε ασφαλής. Άλλη μία κλάση πολύ δυνατών και πρακτικών αλγορίθμων κρυπτογράφησης δημοσίου κλειδιού ανακαλύφθηκαν από τον ElGamal το 1985. Αυτά επίσης βασίζονται σε ένα ιδιαίτερο λογαριθμικό πρόβλημα.

Μία από τις πιο σημαντικές συνεισφορές που μας έδωσε η κρυπτογραφία δημοσίου κλειδιού είναι η ψηφιακή υπογραφή. Το 1991 το πρώτο παγκόσμιο πρότυπο για ψηφιακές υπογραφές (ISO/IEC 9796) υιοθετήθηκε. Είναι βασισμένη στον αλγόριθμο RSA. Το 1994 η Κυβέρνηση των Η.Π.Α. υιοθέτησε το Πρότυπο Ψηφιακής Υπογραφής, ένα μηχανισμό που βασίζεται στον κρυπτογραφικό αλγόριθμο που αναπτύχθηκε από τον ElGamal.

Η αναζήτηση για νέους κρυπτογραφικούς αλγόριθμους, αναβαθμίσεις και βελτιστοποιήσεις σε ήδη υπάρχοντες αλγόριθμους και η αύξηση της ασφάλειας των συστημάτων συνεχίζεται με μεγάλα βήματα και γρήγορους ρυθμούς. Πολλά πρότυπα και δομές σε διάφορους τομείς που έχουν σχέση με την κρυπτογραφία αναπτύσσονται και υιοθετούνται καθημερινά. Προϊόντα ασφάλειας αναπτύσσονται για να ικανοποιήσουν τις μεγάλες ανάγκες σε ασφάλεια μια κοινωνίας που βασίζεται στη Πληροφορική.

1.2

Ασφάλεια πληροφοριών και κρυπτογραφία

Η έννοια της πληροφορίας και η σχέση της με την κρυπτογραφία θα εξηγηθεί παρακάτω. Για να εισαγάγουμε την έννοια κρυπτογραφία, πρέπει να γίνουν κατανοητά θέματα που σχετίζονται με την ασφάλεια των πληροφοριών γενικότερα. Η ασφάλεια των πληροφοριών εμφανίζεται στις μέρες μας με πολλούς τρόπους ανάλογα με την κατάσταση και τις απαιτήσεις. Άσχετα με το ποιοι συμπεριλαμβάνονται, σε μικρότερο ή μεγαλύτερο βαθμό, όλα τα μέρη μιας συναλλαγής πρέπει να έχουν εμπιστοσύνη ότι ορισμένοι στόχοι που έχουν σχέση με την ασφάλεια των δεδομένων τηρούνται. Κάποιοι από αυτούς τους στόχους αναφέρονται στον πίνακα 1.1.

Μυστικότητα ή εμπιστευτικότητα (Privacy or confidentiality)	Να κρατάς τις πληροφορίες μυστικές από όλους εκτός από αυτούς που πρέπει να τις δουν
Ακεραιότητα δεδομένων (Data integrity)	Να είσαι σίγουρος ότι οι πληροφορίες δεν έχουν αλλαχθεί από οποιοδήποτε μη εξουσιοδοτημένο μέλος
Πιστοποίηση οντότητας ή αναγνώριση (Entity authentication or identification)	Η σωστή αναγνώριση της ταυτότητας μίας οντότητας (π.χ. ενός ανθρώπου, ενός τερματικού υπολογιστή, μίας πιστωτικής κάρτας)
Πιστοποίηση μηνύματος (Message authentication)	Η αναγνώριση της πηγής της πληροφορίας, που είναι επίσης γνωστή ως αναγνώριση πηγής δεδομένων
Υπογραφή (Signature)	Ένα μέσο που σχετίζει κάποιες πληροφορίες με μία οντότητα
Έγκριση (Authorization)	Η πιστοποίηση μίας οντότητας ότι είναι εγκεκριμένη να κάνει κάτι
Έλεγχος πρόσβασης (Access control)	Ο περιορισμός πρόσβασης πόρων μόνο σε εγκεκριμένες οντότητες

Πιστοποίηση (Validation)	Μία μέθοδος για να υπάρχει επικαιρότητα έγκρισης στο να χρησιμοποιείς ή να επεξεργάζεσαι πληροφορίες ή πόρους
Πιστοποίηση (Certification)	Η επικύρωση πληροφοριών από μία εμπιστευμένη οντότητα
Χρονοσφράγιση (Timestamping)	Η εγγραφή της ώρας της δημιουργίας ή της ύπαρξης πληροφοριών
Μαρτυρία (Witnessing)	Ο έλεγχος για τη δημιουργία πληροφοριών από μία οντότητα εκτός του δημιουργού
Απόδειξη (Receipt)	Η αναγνώριση ότι παρελήφθησαν οι πληροφορίες
Επιβεβαίωση (Confirmation)	Η αναγνώριση ότι έχει γίνει παροχή υπηρεσιών
Ιδιοκτησία (Ownership)	Ένα μέσο για να δώσεις σε μία οντότητα με το νόμιμο δικαίωμα της χρήσης ή της μεταβίβασης πόρων σε άλλους
Ανωνυμία (Anonymity)	Η απόκρυψη της ταυτότητας μιας οντότητας που παίρνει μέρος σε μια διαδικασία
Μη αποκήρυξη (Non-repudiation)	Η αποφυγή της άρνησης προηγούμενων δεσμεύσεων ή πράξεων
Ανάκληση (Revocation)	Η απόσυρση μιας πιστοποίησης ή έγκρισης

Πίνακας 1.1: Κάποιοι στόχοι ασφάλειας της πληροφορίας

Ανά τους αιώνες, πολλά πρωτόκολλα και μηχανισμοί δημιουργήθηκαν για να χρησιμοποιηθούν για θέματα ασφάλειας των πληροφοριών, όταν οι πληροφορίες μεταφέρονταν με τη χρήση εγγράφων. Συχνά, η ασφάλεια των πληροφοριών δεν μπορεί να επιτευχθεί μόνο μέσω της χρήσης μαθηματικών αλγορίθμων και πρωτοκόλλων, αλλά απαιτεί διάφορες τεχνικές διαδικασίες και την υπακοή στους νόμους για να έχουμε το επιθυμητό αποτέλεσμα. Για παράδειγμα, η μυστικότητα των γραμμάτων παρέχεται με τη χρήση σφραγισμένων γραμμάτων που παραδίδονται από μια υπηρεσία παράδοσης αλληλογραφίας. Η φυσική ασφάλεια του φακέλου είναι, για πρακτική ανάγκη, περιορισμένη και γι αυτό ψηφίστηκαν νόμοι που καθιστούν παράνομη την ανάγνωση γράμματος από οποιονδήποτε άλλο εκτός από τον τελικό παραλήπτη. Κάποιες φορές η ασφάλεια επιτυγχάνεται όχι μέσω της ίδιας της πληροφορίας αλλά μέσω του φυσικού εγγράφου που την καταγράφει. Για παράδειγμα, τα χαρτονομίσματα απαιτούν για τη δημιουργία τους ειδικά μελάνια και υλικό, πράγμα που αποτρέπει την εύκολη παραχάραξη τους.

Επομένως, ο τρόπος με τον οποίο καταγράφεται η πληροφορία δεν έχει αλλάξει δραματικά με την πάροδο του χρόνου. Ενώ η πληροφορία ήταν κλασσικά αποθηκευμένη και μεταδιδόταν σε χαρτί, μεγάλο μέρος της πλέον είναι καταγεγραμμένο σε μαγνητικά μέσα και μεταδίδεται μέσω τηλεπικοινωνιακών συστημάτων, κάποια από αυτά ασύρματα. Αυτό που έχει αλλάξει δραματικά είναι η ικανότητα να αντιγράφεις και να αλλάζεις πληροφορίες. Κάποιος μπορεί να κάνει χιλιάδες πανομοιότυπα αντίγραφα από μία πληροφορία που είναι αποθηκευμένη ηλεκτρονικά και κάθε ένα από αυτά είναι ίδιο με το αρχικό. Με την πληροφορία καταγεγραμμένη σε χαρτί, αυτό είναι πολύ πιο δύσκολο. Αυτό που χρειάζεται λοιπόν για μια κοινωνία που η πληροφορία είναι ως επί το πλείστον αποθηκευμένη και μεταδιδόμενη σε ηλεκτρονική μορφή είναι ένα μέσο για να εξασφαλιστεί η ασφάλεια

των πληροφοριών που θα είναι ανεξάρτητο από το φυσικό μέσο που είναι καταγεγραμμένη η πληροφορία. Έτσι, οι στόχοι της ασφάλειας των πληροφοριών θα στηρίζεται μόνο στη ίδια την ψηφιακή πληροφορία.

Ένα από τα θεμελιώδη εργαλεία που χρησιμοποιούνται στην ψηφιακή ασφάλεια είναι η υπογραφή. Είναι ένας θεμελιώδης λίθος για πολλές υπηρεσίες όπως η μη αποκήρυξη (non-repudiation), η πιστοποίηση προέλευσης δεδομένων (data origin authentication), η αναγνώριση (identification), και η μαρτυρία (witnessing), για να αναφέρουμε κάποιες. Έχοντας μάθει τα βασικά της γραφής, ένα άτομο μαθαίνει πώς να παράγει μία υπογραφή για το σκοπό της αναγνώρισης. Σε περιπτώσεις υπογραφής συμβολαίων, η υπογραφή εξελίσσεται και λαμβάνει ακέραια μορφή της ταυτότητας ενός ατόμου. Αυτή η υπογραφή προορίζεται να είναι μοναδική στο κάθε άτομο και εξυπηρετεί την ανάγκη της αναγνώρισης, έγκρισης και επικύρωσης. Με τις ηλεκτρονικές πληροφορίες η έννοια της υπογραφής πρέπει να αναθεωρηθεί; δεν αρκεί απλά να είναι κάτι το μοναδικό σε αυτόν που υπογράφει και ανεξάρτητο της πληροφορίας που μπαίνει. Η ηλεκτρονική αναπαραγωγή της είναι τόσο απλή που το να βάλεις μία υπογραφή σε ένα ανυπόγραφο κείμενο είναι κάτι το υπερβολικά απλό.

Πρέπει λοιπόν να δημιουργηθούν ανάλογα των "χάρτινων πρωτοκόλλων" σε ψηφιακή μορφή. Ελπίζουμε, λοιπόν, αυτά τα νέα ηλεκτρονικά πρωτόκολλα να είναι εξίσου καλά με αυτά που αντικαθιστούν. Υπάρχει μια μοναδική ευκαιρία για την κοινωνία να εισαχθούν νέοι και αποδοτικότεροι τρόποι για να εξασφαλιστεί η ασφάλεια των πληροφοριών. Πολλά μπορούμε να μάθουμε από την εξέλιξη του συστήματος βασισμένου σε χαρτί, μιμούμενοι αυτές τις πτυχές που μας έχουν υπηρετήσει καλά, ενώ παράλληλα αφαιρώντας και εξαλείφοντας τις διάφορες ανεπάρκειες.

Το να επιτύχουμε την ασφάλεια των πληροφοριών σε μία ηλεκτρονική κοινωνία απαιτεί ένα μεγάλο εύρος από τεχνικές και νομικές ικανότητες. Δεν υπάρχει, όμως, εγγύηση ότι όλοι οι στόχοι πληροφοριακής ασφάλειας που θα θεωρηθούν αναγκαίοι, μπορούν να επιτευχθούν επαρκώς. Τα τεχνικά μέσα παρέχονται μέσω της κρυπτογραφίας.

1.2.1

Ορισμός της Κρυπτογραφίας

Κρυπτογραφία είναι η μελέτη μαθηματικών τεχνικών που έχουν σχέση με πτυχές της ασφάλειας πληροφοριών όπως η εμπιστευτικότητα, η ακεραιότητα δεδομένων, η επικύρωση οντοτήτων και η επικύρωση προέλευσης των δεδομένων.
Η κρυπτογραφία δεν είναι το μοναδικό μέσο παροχής ασφάλειας πληροφοριών, αλλά ένα σύνολο από τεχνικές.

1.2.2.

Κρυπτογραφικοί στόχοι

Από όλα τα θέματα ασφάλειας της πληροφορίας που παρουσιάστηκαν στο πίνακα 1.1, τα ακόλουθα τέσσερα δημιουργούν ένα πλαίσιο πάνω στο οποίο τα υπόλοιπα απορρέουν:

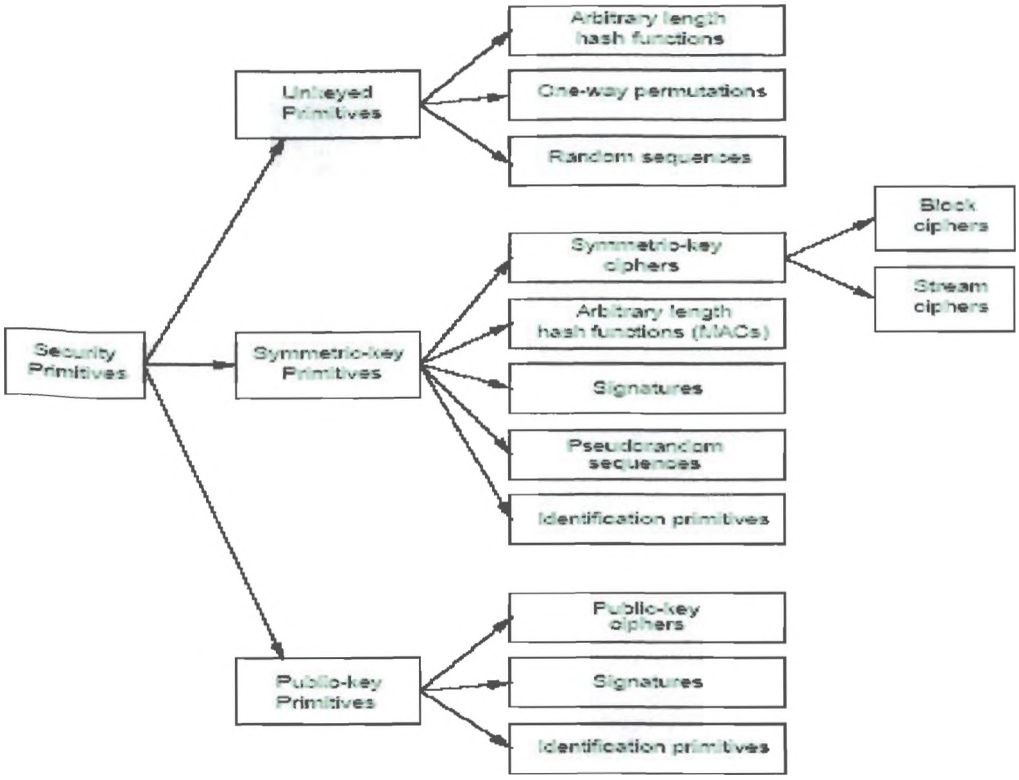
1) Μυστικότητα ή εμπιστευτικότητα
2) Ακεραιότητα δεδομένων
3) Αυθεντικότητα
4) Μη αποκήρυξη

1) Η *εμπιστευτικότητα* είναι μια υπηρεσία που χρησιμοποιείται για να κρατηθεί το περιεχόμενο της πληροφορίας μακριά από όλους, εκτός από αυτούς που έχουν βέβαια εξουσιοδότηση πρόσβασης. Η *μυστικότητα* είναι ένας όρος συνώνυμος με την εμπιστευτικότητα και την ιδιωτικότητα. Υπάρχουν πολλές προσεγγίσεις που χρησιμοποιούνται για να παρέχεται εμπιστευτικότητα, που κυμαίνονται από τη χρήση φυσικής προστασίας μέχρι τη χρήση μαθηματικών αλγορίθμων που καθιστούν τα δεδομένα ακατανόητα.
2) Η ακεραιότητα δεδομένων είναι μια υπηρεσία που απευθύνεται στην αναρμόδια αλλαγή δεδομένων. Για να βεβαιωθεί η ακεραιότητα δεδομένων, κάποιος πρέπει να έχει την ικανότητα να εντοπίζει την χρήση ή αλλαγή δεδομένων από μη εξουσιοδοτημένα άτομα. Η ακεραιότητα δεδομένων περιλαμβάνει την εισαγωγή, διαγραφή και αντικατάσταση δεδομένων.
3) Η αυθεντικότητα είναι μια υπηρεσία που σχετίζεται με την αναγνώριση. Αυτή η λειτουργία ισχύει στις οντότητες αλλά και στην ίδια την πληροφορία. Δύο ομάδες που ξεκινούν μία επικοινωνία μεταξύ τους, οφείλουν να αναγνωρίσουν η μία την άλλη. Η πληροφορία που παραδίδεται σε ένα κανάλι θα πρέπει να είναι αναγνωρισμένη όσον αφορά την προέλευση, την ημερομηνία προέλευσης, το περιεχόμενο δεδομένων, την ώρα που στάλθηκε, κ.τ.λ. Για αυτούς τους λόγους, αυτή η πτυχή της κρυπτογραφίας είναι συνήθως χωρισμένη σε δύο μεγάλες κατηγορίες: Την αναγνώριση οντότητας και την αναγνώριση προέλευσης δεδομένων. Η αναγνώριση προέλευσης δεδομένων παρέχει ακεραιότητα δεδομένων, αφού αν έχει αλλάξει ένα μήνυμα, τότε έχει αλλάξει και η πηγή προέλευσής του.
4) Η μη αποκήρυξη είναι μια υπηρεσία που αποτρέπει μια οντότητα από το να αρνηθεί προηγούμενες δεσμεύσεις ή ενέργειες. Όταν δημιουργούνται διαφωνίες κατά την άρνηση από μία οντότητα ότι έγιναν κάποιες ενέργειες, ένα μέσο που θα ξεκαθαρίσει την κατάσταση θα πρέπει να υπάρχει. Για παράδειγμα, μία οντότητα μπορεί να εγκρίνει την αγορά κάποιας ιδιοκτησίας από μία άλλη οντότητα, και αργότερα να αρνηθεί ότι δόθηκε τέτοια έγκριση. Μια διεργασία που αφορά ένα τρίτο μέλος που εμπιστεύονται και οι δύο οντότητες χρειάζεται για να λυθεί αυτή η διαφωνία.

Ένας θεμελιώδης στόχος της κρυπτογραφίας είναι να καλύπτει με επάρκεια αυτά τα τέσσερα θέματα τόσο στη θεωρία όσο και στη πράξη. Η κρυπτογραφία

σχετίζεται με την αποτροπή και τον εντοπισμό των παραβιάσεων και διάφορων άλλων κακόβουλων ενεργειών.

Το παρακάτω σχήμα παρέχει μια απεικόνιση που αναφέρει κάποιες αρχές της κρυπτογραφίας και πως σχετίζονται μεταξύ τους.



Σχήμα 1.1: Μια ταξινόμηση των αρχών της κρυπτογραφίας

Αυτές οι αρχές θα πρέπει να αξιολογηθούν σε σχέση με διάφορα κριτήρια όπως:

1) Επίπεδο της ασφάλειας: Αυτός ο όρος είναι δύσκολο να ποσολογηθεί. Συχνά το μεταφράζουμε σε σχέση με τον αριθμό των διεργασιών που χρειάζονται (χρησιμοποιώντας φυσικά τις καλύτερες γνωστές μεθόδους) για να καταλήξουμε στο επιθυμητό αποτέλεσμα. Τυπικά, το επίπεδο της ασφάλειας ορίζεται σαν το μέγιστο ποσό εργασίας που χρειάζεται για να ολοκληρωθεί η διεργασία. Αυτό συχνά ονομάζεται *παράγοντας εργασίας*.
2) Λειτουργικότητα: Οι κρυπτογραφικές αρχές θα πρέπει να συνδυαστούν για να επιτύχουμε διάφορους στόχους ασφάλειας. Ποιες αρχές είναι πιο αποτελεσματικές για το κάθε στόχο, θα αποφασιστεί από τις βασικές ιδιότητες των αρχών.
3) Μέθοδοι λειτουργίας: Οι αρχές της κρυπτογραφίας, όταν εφαρμόζονται με διάφορους τρόπους και με διάφορα δεδομένα, τυπικά θα επιδείξουν διαφορετικά χαρακτηριστικά, δηλαδή, μία αρχή μπορεί να μας δώσει πολύ διαφορετική λειτουργικότητα ανάλογα με τον τρόπο λειτουργίας της ή τη χρήση της.
4) Απόδοση: Αυτό το κριτήριο αναφέρεται στην αποδοτικότητα μιας αρχής σε ένα συγκεκριμένο τρόπο λειτουργίας. Για παράδειγμα, ένας αλγόριθμος κρυπτογράφησης μπορεί να αξιολογηθεί σε σχέση με τον αριθμό των bits ανά δευτερόλεπτο που μπορεί να κρυπτογραφήσει.

5) Ευκολία εφαρμογής: Το τελευταίο κριτήριο σχετίζεται με την δυσκολία πραγματοποίησης των αρχών σε μια πρακτική χρήση. Αυτό μπορεί να περιλαμβάνει την περιπλοκότητα εισαγωγής των αρχών είτε σε περιβάλλον λογισμικού, είτε σε περιβάλλον υλικού.

Η σημασία των διαφόρων κριτηρίων εξαρτάται άμεσα από τις εφαρμογές και τους πόρους που έχουμε στη διάθεσή μας. Για παράδειγμα, σε ένα περιβάλλον που η υπολογιστική ισχύς είναι περιορισμένη, ο χρήστης θα πρέπει να μειώσει το επίπεδο της ασφάλειας για να έχει καλύτερη γενική απόδοση συστήματος.

Η κρυπτογραφία, ανά τους αιώνες, είναι μία τέχνη που αξιοποιήθηκε από διάφορους που ανέπτυξαν πολλές τεχνικές για να επιτευχθεί ασφάλεια της πληροφορίας. Τα τελευταία είκοσι χρόνια ήταν μια μεταβατική περίοδος όπου η κρυπτογραφία εξελίχθηκε από μία τέχνη σε μία επιστήμη. Υπάρχουν πλέον πολλά διεθνή επιστημονικά συνέδρια αφιερωμένα αποκλειστικά στη κρυπτογραφία, καθώς επίσης και ένας διεθνής επιστημονικός οργανισμός, η Διεθνής Ένωση Κρυπτογραφικής Έρευνας (International Association for Cryptologic Research – I.A.C.R.), που σκοπό έχει την ανάπτυξη της έρευνας στο κρυπτογραφικό πεδίο.

Κεφάλαιο Δεύτερο:

2.1

Αλγοριθμικές τεχνικές κατασκευής πρώτων αριθμών

Αυτό το κεφάλαιο περιγράφει τους αλγορίθμους που χρησιμοποιούνται για την δημιουργία πρώτων αριθμών για κρυπτογραφικούς σκοπούς. Τέσσερις αλγόριθμοι παρουσιάζονται, και είναι οι παρακάτω:

α) Αλγόριθμος για τη δημιουργία πιθανών πρώτων αριθμών
β) Αλγόριθμος για τη δημιουργία δυνατών πρώτων αριθμών
γ) Αλγόριθμος για τη δημιουργία πιθανών πρώτων αριθμών p και q, κατάλληλους για χρήση στον Αλγόριθμο Ψηφιακής Υπογραφής (Digital Signature Algorithm – D.S.A.)
δ) Αλγόριθμος για τη δημιουργία αποδεδειγμένων πρώτων αριθμών.

Ας δούμε λοιπόν αναλυτικότερα τον κάθε αλγόριθμο ξεχωριστά:

2.1.1.

Τυχαία αναζήτηση για πιθανούς πρώτους αριθμούς

Σύμφωνα με το θεώρημα των πρώτων αριθμών, η αναλογία των (θετικών) ακεραίων <=x που είναι πρώτοι αριθμοί είναι περίπου 1 / lnx. Αφού οι μισοί ακέραιοι <= x είναι ζυγοί, η αναλογία των μονών ακεραίων <= x που είναι πρώτοι αριθμοί είναι περίπου 2 / lnx. Για παράδειγμα, η αναλογία όλων των μονών ακεραίων <= 2^{512} που είναι πρώτοι αριθμοί είναι περίπου 2 / (512 x ln(2)) =~ 1/777. Αυτό μας δείχνει ότι μία λογική στρατηγική για να επιλεχθεί ένας τυχαίος (πιθανός) πρώτος αριθμός k-ψηφίων είναι η επαναλαμβανόμενη τυχαία επιλογή k-ψηφίων περιττών ακεραίων n, μέχρι να βρεθεί ένας που θα ανακηρυχθεί ότι είναι "πρώτος" αριθμός από τον αλγόριθμο MILLER – RABIN (n,t), για μία κατάλληλη τιμή της παραμέτρου ασφάλειας t.

Αν ένας τυχαίος k-bit περιττός ακέραιος n είναι διαιρετέος από ένα μικρό πρώτο αριθμό, είναι λιγότερο υπολογιστικά "ακριβό" να αποκλείσεις τον υποψήφιο n με τη δοκιμαστική διαίρεση, παρά με το να χρησιμοποιήσουμε το τεστ Miller – Rabin. Αφού η πιθανότητα ότι ένας τυχαίος ακέραιος n έχει ένα μικρό πρώτο αριθμό ως διαιρέτη είναι αρκετά μεγάλη, πριν εφαρμόσουμε το Miller – Rabin τεστ, ο υποψήφιος αριθμός θα πρέπει να δοκιμαστεί για μικρούς διαιρέτες κάτω από ένα προκαθορισμένο όριο B. Αυτό μπορεί να γίνει με το να διαιρέσουμε το n με όλους τους πρώτους αριθμούς κάτω από τους πρώτους αριθμούς που είναι <= B. Η αναλογία των πιθανών περιττών ακεραίων n που δεν εξαλείφονται από αυτή τη δοκιμή είναι $\Pi_{3 <= p <= B} (1 - 1/p)$, που σύμφωνα με το θεώρημα του Merten, είναι περίπου 1.12 = lnB (εδώ το p κυμαίνεται αναμέσα στις πρώτες τιμές). Για παράδειγμα, αν το B = 256, τότε μόνο 20% από τους υποψήφιους περιττούς

ακέραιους n περνούν το στάδιο της δοκιμαστικής διαίρεσης, δηλ. το 80% απορρίπτονται πριν γίνει το τεστ Miller – Rabin.

2.1.2.

Αλγόριθμος για τυχαία αναζήτηση ενός πρώτου αριθμού χρησιμοποιώντας το τεστ Miller – Rabin.

Τυχαία – Αναζήτηση (k,t)
Είσοδος: Ένας ακέραιος k, και μία παράμετρος ασφάλειας t
Έξοδος: Ένας τυχαίος k-ψηφίων πιθανός πρώτος αριθμός

1. Δημιουργία ένα περιττό k-ψηφίων ακέραιο n τυχαία.
2. Χρησιμοποίηση της δοκιμαστικής διαίρεσης για να καθορίσουμε εάν το n είναι διαιρέσιμο από ένα περιττό πρώτο αριθμό <= B. Αν αυτό ισχύει τότε πάμε στο 1° βήμα.
3. Αν το τεστ Miller – Rabin (n,t) έχει σαν έξοδο "πρώτο αριθμό" τότε επέστρεψε μας τη τιμή n. Αλλιώς, πήγαινε στο 1° βήμα.

2.1.3

Ορισμός

Η πιθανότητα πως η τυχαία αναζήτηση (Random-search) (k,t) μας επιστρέφει ένα σύνθετο αριθμό μας δείχνεται από το $P_{lo,t}$.

2.2.1

Δυνατοί πρώτοι αριθμοί

Το κρυπτογραφικό σύστημα R.S.A. χρησιμοποιεί ένα συντελεστή της μορφής n = pq, όπου το p και το q είναι συγκεκριμένοι περιττοί πρώτοι αριθμοί. Οι πρώτοι αριθμοί p και q πρέπει να είναι ικανοποιητικού μεγέθους έτσι ώστε η παραγοντοποίηση του προϊόντος τους να είναι πέρα από την υπολογιστική ισχύ. Επιπλέον, θα πρέπει να είναι τυχαίοι πρώτοι αριθμοί με την έννοια ότι είναι επιλεγμένοι σαν μία λειτουργία μιας τυχαίας εισαγωγής μέσα σε μία διεργασία που οριστικοποιεί μια ομάδα υποψηφίων ικανοποιητικού αριθμού στοιχείων συνόλου, έτσι ώστε μία εξαντλητική επίθεση να είναι αδύνατη. Στη πρακτική εφαρμογή, οι πρώτοι αριθμοί που παίρνουμε σαν αποτέλεσμα πρέπει επίσης να είναι ενός προκαθορισμένου μεγέθους ψηφίων, για να πληροί της προϋποθέσεις του συστήματος.

Η ανακάλυψη του κρυπτογραφικού συστήματος R.S.A. οδήγησε στην εκτίμηση διάφορων επιπλέον περιορισμών στην επιλογή του p και του q που είναι αναγκαίοι για να εξασφαλιστεί ότι το σύστημα R.S.A. που θα καταλήξουμε θα είναι ασφαλές από κρυπταναλυτική επίθεση, και έτσι η έννοια του *δυνατού* πρώτου αριθμού δημιουργήθηκε και ορίστηκε. Πλέον πιστεύεται από τους ειδικούς ότι οι

δυνατοί πρώτοι αριθμοί προσφέρουν μικρή προστασία, πέρα από αυτή που ήδη προσφέρεται από τους τυχαίους πρώτους αριθμούς, αφού τυχαία επιλεγμένοι πρώτοι αριθμοί μεγεθών που τυπικά χρησιμοποιούνται στο R.S.A. σήμερα, θα ικανοποιήσουν τους περιορισμούς με υψηλή πιθανότητα. Από την άλλη, δεν είναι λιγότερο ασφαλής, και χρειάζονται μόνο μικρή επιπλέον υπολογιστική ισχύ και χρόνο για να υπολογιστούν. Έτσι, δεν υπάρχει ουσιαστικό παραπάνω κόστος από τη χρήση τους.

2.2.2

Αλγόριθμος Gordon για τη δημιουργία ενός δυνατού πρώτου αριθμού

Περίληψη: Ένα δυνατός πρώτος αριθμός p δημιουργείται

1. Δημιούργησε δύο μεγάλους πρώτους αριθμούς s και t σχεδόν με το ίδιο μέγεθος ψηφίων.
2. Διάλεξε ένα ακέραιο i_0. Βρες τον πρώτο αριθμό με την ακολουθία $2it+1$, όπου $i = i_0, i_0+1, i_0+2, \ldots$ Ονομάστε αυτό το πρώτο αριθμό με $r = 2it + 1$
3. Υπολογίστε $p_0 = 2(s^{r-2} \bmod r)\, s - 1$.
4. Διαλέξτε έναν ακέραιο j_0. Βρείτε τον πρώτο αριθμό στην ακολουθία $p0 + 2jrs$, όπου $j = j_0, j_0+1, j_0+2, \ldots$ Ονομάστε αυτό το πρώτο αριθμό με $p = p_0 + 2jrs$.
5. Επέστρεψε τιμή p.

2.2.3.

Ορισμός

Ένας πρώτος αριθμός p λέγεται ότι είναι ένας *δυνατός πρώτος αριθμός* αν οι ακέραιοι r,s και t υπάρχουν έτσι ώστε οι ακόλουθες τρεις προϋποθέσεις ικανοποιούνται:

(i) $p - 1$ έχει ένα μεγάλο πρώτο αριθμό σαν παράγοντα, ονομαζόμενο r
(ii) $p + 1$ έχει ένα μεγάλο πρώτο αριθμό σαν παράγοντα, ονομαζόμενο s
(iii) $r - 1$ έχει ένα μεγάλο πρώτο αριθμό σαν παράγοντα, ονομαζόμενο t.

2.3.1.

Μέθοδος NIST για τη δημιουργία πρώτων αριθμών D.S.A.

Κάποια σχέδια δημόσιου κλειδιού απαιτούν πρώτους αριθμούς που ικανοποιούν συγκεκριμένες συνθήκες. Για παράδειγμα, ο Αλγόριθμος Ψηφιακής Υπογραφής NIST απαιτεί δύο πρώτους αριθμούς p και q που ικανοποιούν τις ακόλουθες τρεις συνθήκες:

(i) $2^{159} < q < 2^{160}$, πράγμα που σημαίνει ότι το q είναι ένας πρώτος αριθμός 160 ψηφίων.

(ii) $2^{L-1} < p < 2^L$ για συγκεκριμένο L, όπου L = 512 + 64l, για τιμές $0 <= l <= 8$

(iii) Το q διαιρεί το p – 1

Αυτό το τμήμα περιγράφει έναν αλγόριθμο που δημιουργεί τέτοιους p και q πρώτους αριθμούς. Στα ακόλουθα, το H δείχνει τη λειτουργία SHA – 1, που χαρτογραφεί τις σειρές ψηφίων μεγέθους $< 2^{64}$ έως και 160 χαρακτήρων. Όπου απαιτείται, ένας ακέραιος x του εύρους $0 <= x <= 2^9$ του οποίου η δυαδική αναπαράσταση είναι $x = x_{g-1}2^{g-1} + x_{g-2}2^{g-2} + \ldots + x_2 2^2 + x_1 2 + x_0$, η οποία θα πρέπει να αντικατασταθεί στην ακολουθία g ψηφίων και αντίθετα.

2.3.2.

Μέθοδος αλγορίθμου NIST για τη δημιουργία πρώτων αριθμών D.S.A.

Είσοδος: Ένας ακέραιος l, όπου $0 <= l <= 8$
Έξοδος: Ένας πρώτος αριθμός 160 ψηφίων q και ένας πρώτος αριθμός L ψηφίων p, όπου L = 512 +64L και $q \mid (p - 1)$

1. Υπολόγισε L = 512 +64L. Χρησιμοποιώντας μεγάλη διαίρεση του (L – 1) με το 160, βρες το n, b έτσι ώστε L – 1 = 160n + b, όπου $0 <= b <= 160$.
2. Επανέλαβε τα ακόλουθα:
   2.1. Διάλεξε ένα τυχαίο σπόρο s (όχι απαραίτητα μυστικό) μεγέθους ψηφίων g $>= 160$.
   2.2. Υπολόγισε το U = H (s) + H ((s + 1) mod 2^9).
   2.3. Δημιούργησε το q από το U με το να βάλεις τιμή 1 στα πιο σημαντικά και στα λιγότερο σημαντικά ψηφία του U. (Να σημειωθεί ότι το U είναι ένας περιττός ακέραιος αριθμός 160 ψηφίων).
   2.4. Δοκίμασε το q αν είναι πρώτος αριθμός χρησιμοποιώντας το τεστ Miller – Rabin (q,t) για $t >= 18$, μέχρι να βρεθεί ότι το q είναι ένας (πιθανός) πρώτος αριθμός.
3. Θέσε i← 0, j ← 2.
4. Όσο το $i < 4096$ κάνε τα ακόλουθα:
   4.1. Για k από το 0 έως το n, κάνε τα ακόλουθα: Θέσε V_k ← H ((s + j + k) mod 2^9).
   4.2. Από τον ακέραιο W που περιγράφεται παρακάτω, θέσε όπου $X = W + 2^{L-1}$. (Ο X είναι ένας ακέραιος L ψηφίων).
   $W = V_0 + V_1 2^{160} + V_2 2^{320} + \ldots + V_{n-1} 2^{160(n-1)} + (V_n \bmod 2^b) 2^{160n}$.
   4.3. Υπολόγισε c = X mod 2q και θέσε p = X – (c – 1). (Σημείωσε ότι p ==1 mod 2q).)
   4.4. Αν το $p >= 2^{L-1}$ τότε κάνε τα ακόλουθα:
   Δοκίμασε αν το p είναι πρώτος αριθμός με το τεστ Miller – Rabin(p,t) για $t >= 5$. Αν είναι (πιθανός) πρώτος αριθμός τότε επέστρεψε τις τιμές (q,p).
   4.5. Θέσε i ← i + 1, j ← j + n + 1.
5. Πήγαινε στο βήμα 2.

2.4.1.

Δημιουργικές τεχνικές για την κατασκευή αποδεδειγμένων πρώτων αριθμών

Ο αλγόριθμος του Maurer δημιουργεί τυχαίους αποδεδειγμένους πρώτους αριθμούς που είναι σχεδόν γενικά διανεμημένοι πάνω στο γενικό πλαίσιο πρώτων αριθμών προκαθορισμένου μεγέθους. Ο χρόνος που χρειάζεται για να δημιουργηθεί ένας πρώτος αριθμός είναι λίγο μεγαλύτερος από αυτόν που χρειάζεται για να δημιουργηθεί ένας πιθανός πρώτος αριθμός ίδιου μεγέθους, θέτοντας στην παράμετρο ασφάλειας t = 1.

2.4.2.

Αλγόριθμος Maurer για την δημιουργία αποδεδειγμένων πρώτων αριθμών.

Αποδεδειγμένος πρώτος αριθμός (k)
Είσοδος: Ένας θετικός ακέραιος k.
Έξοδος: Ένας πρώτος αριθμός n, k ψηφίων.

1. (Αν το k είναι μικρός αριθμός, τότε δοκίμασε διάφορους ακεραίους με τυχαία διαίρεση. Ένας πίνακας μικρών πρώτων αριθμών μπορεί να έχει δημιουργηθεί για αυτό το σκοπό.)
   Αν το k <= 20 τότε συνέχεια κάνε τα ακόλουθα:
   1.1. Διάλεξε ένα τυχαίο περιττό ακέραιο n, k ψηφίων.
   1.2. Χρησιμοποίησε τη τυχαία διαίρεση όλων των πρώτων αριθμών μικρότερων από $\sqrt{n}$ για να καθοριστεί αν το n είναι πρώτος αριθμός.
   1.3. Αν το n είναι πρώτος αριθμός, τότε επέστρεψε τη τιμή του n.
2. Θέσε c ← 0.1 και m ← 20.
3. Θέσε B ← X*k^2
4. (Δημιούργησε r, το μέγεθος του q σχετικό με το n). Αν το k > 2m, τότε συνέχεια κάνε τα παρακάτω: Διάλεξε ένα τυχαίο αριθμό s που βρίσκεται ανάμεσα στο [0,1], θέσε r ← 2^s-1, μέχρι (k – rk) > m. Αλλιώς, αν για παράδειγμα k <= 2m, θέσε r ← 0.5.
5. Υπολόγισε q ← Αποδεδειγμένο πρώτο αριθμό([r*k] + 1).
6. Θέσε I ← [2^k-1 / (2q)].
7. Success ← 0.
8. Όσο (success = 0) κάνε τα ακόλουθα:
   8.1. (Διάλεξε ένα υποψήφιο ακέραιο n) Διάλεξε ένα τυχαίο ακέραιο R ο οποίος να βρίσκεται στα όρια [I + 1,2I] και θέσε n ← 2Rq + 1.
   8.2. Χρησιμοποίησε τη τυχαία διαίρεση για να καθορίσεις εάν το n είναι διαιρέσιμο από ένα πρώτο αριθμό < B. Εάν δεν είναι τότε κάνε τα παρακάτω:
   Διάλεξε ένα τυχαίο ακέραιο a που να βρίσκεται στα όρια [2, n - 2].
   Υπολόγισε b ← a^n-1 mod n.
   Αν b = 1 τότε κάνε τα ακόλουθα:
   Υπολόγισε b ← a^2R mod n και d ← gcd (b – 1,n).
   Αν d = 1 τότε success ← 1.
9. Επέστρεψε την τιμή του n.

Κεφάλαιο Τρίτο:

Αλγόριθμοι κρυπτογράφησης Δημόσιου Κλειδιού

3.1.

Εισαγωγή

Αυτό το κεφάλαιο ασχολείται με τις διάφορες τεχνικές που χρησιμοποιούνται στη κρυπτογράφηση Δημόσιου Κλειδιού, ή όπως λέγεται αλλιώς, ασσυμετρική κρυπτογράφηση. Στα συστήματα κρυπτογράφησης Δημόσιου Κλειδιού, κάθε οντότητα Α έχει ένα δημόσιο κλειδί e και ένα αντίστοιχο ιδιωτικό κλειδί d. Σε ασφαλή συστήματα, δεν είναι δυνατό να βρεθεί το d, εφόσον έχουμε το e. Το δημόσιο κλειδί ορίζει μία κρυπτογραφική μεταμόρφωση E_e, ενώ το ιδιωτικό κλειδί ορίζει και περιέχει τις ανάλογες πληροφορίες αποκρυπτογράφησης D_d. Κάθε οντότητα Β που επιθυμεί να στείλει ένα μήνυμα m στην οντότητα Α, αποκτά ένα αυθεντικό αντίγραφο του δημόσιου κλειδιού e της οντότητας – παραλήπτη Α. Έπειτα, χρησιμοποιεί τις πληροφορίες κρυπτογράφησης για να αποκτήσει το κρυπτογραφημένο μήνυμα $c = E_e(m)$, και μεταδίδει το c στον παραλήπτη Α. Για να αποκρυπτογραφήσει το c, η οντότητα Α, εφαρμόζει τις πληροφορίες αποκρυπτογράφησης για να πάρει έτσι το αρχικό μήνημα $m = D_d(c)$.

Το δημόσιο κλειδί δεν χρειάζεται να κρατηθεί μυστικό, και στην πραγματικότητα μπορεί να είναι ευρέως διαδεδομένο. Μόνο η αυθεντικότητά του είναι απαραίτητη για να βεβαιωθεί ότι ο παραλήπτης Α είναι όντως ο μόνος που γνωρίζει το αντίστοιχο ιδιωτικό κλειδί. Ένα σημαντικό πλεονέκτημα αυτών των συστημάτων είναι ότι το να παρέχονται αυθεντικά δημόσια κλειδιά είναι γενικότερα πιο εύκολο από το να διανέμονται μυστικά κλειδιά με ιδιωτικό τρόπο, πράγμα που απαιτείται από τα συστήματα συμμετρικού κλειδιού.

Ο βασικότερος στόχος της κρυπτογράφησης Δημόσιου Κλειδιού είναι να παρέχει ιδιωτικότητα και μυστικότητα. Αφού οι πληροφορίες κρυπτογράφησης της οντότητας Α είναι δημόσια γνώση, η κρυπτογράφηση Δημόσιου κλειδιού μόνο, δεν παρέχει επικύρωση προέλευσης δεδομένων ή ακεραιότητα δεδομένων. Τέτοιες επιβεβαιώσεις πρέπει να παρέχονται μέσω της χρήσης επιπλέον τεχνικών που χρησιμοποιούνται, όπως οι κωδικοί αυθεντικότητας μηνύματος και οι ψηφιακές υπογραφές.

Η κρυπτογράφηση Δημόσιου Κλειδιού και οι υλοποιήσεις της είναι γενικότερα σημαντικά αργότερη από ότι είναι οι αλγόριθμοι κρυπτογράφησης συμμετρικού κλειδιού όπως ο D.E.S. Για αυτό το λόγο, η κρυπτογράφηση Δημόσιου Κλειδιού χρησιμοποιείται πιο συχνά στη πράξη για τη μεταφορά κλειδιών που αργότερα χρησιμοποιούνται για τη κρυπτογράφηση δεδομένων από συμμετρικούς αλγόριθμους και άλλες εφαρμογές, αλλά και για την κρυπτογράφηση μικρών πακέτων δεδομένων όπως είναι τα P.I.N. και οι αριθμοί πιστωτικών καρτών. Η κρυπτογράφηση Δημόσιου Κλειδιού μπορεί επίσης να μας παρέχει εγγυήσεις αυθεντικότητας στην αναγνώριση οντοτήτων και κλειδιών προτοκόλλων.

3.2.

Βασικές αρχές

3.2.1.

Στόχοι των αντιπάλων

Ο βασικότερος στόχος ενός αντιπάλου που επιθυμεί να επιτεθεί σε ένα σύστημα δημοσίου κλειδιού, είναι η συστηματική ανάκτηση απλού κειμένου από το κρυπτογραφημένο κείμενο που προορίζεται για κάποια οντότητα Α. Αν αυτό επιτευχθεί, η κρυπτογράφηση λέμε ότι έχει σπάσει. Ένας πιο φιλόδοξος στόχος είναι η ανάκτηση του κλειδιού, η κλοπή δηλαδή του ιδιωτικού κλειδιού της οντότητας Α. Αν το καταφέρει αυτό ο επιτιθέμενος, τότε η κρυπτογράφηση λέμε ότι έχει σπάσει τελείως, αφού ο επιτιθέμενος έχει τη δυνατότητα να αποκρυπτογραφήσει όλα τα κρυπτογραφημένα κείμενα που στέλνονται στον Α.

3.2.2.

Τύποι επιθέσεων

Αφού οι κρυπτογραφικές μέθοδοι είναι δημόσια γνώση, κάποιος επιτιθέμενος μπορεί πάντα να δοκιμάσει μια επίθεση απλού αλλά συγκεκριμένου κειμένου σε ένα σύστημα κρυπτογράφησης Δημόσιου Κλειδιού. Μια ακόμα πιο δυνατή επίθεση, είναι αυτή όπου ο επιτιθέμενος επιλέγει κρυπτογραφημένο κείμενο και έπειτα, με τη χρήση άλλων μέσων αποσπά από την οντότητα Α το αντίστοιχο μη κρυπτογραφημένο κείμενο. Μπορούμε να διακρίνουμε δύο είδη αυτών των επιθέσεων.

1. Σε μία αδιάφορη επιλεγμένου κρυπτογραφημένου κειμένου επίθεση, ο επιτιθέμενος έχει αποκρυπτογραφήσεις από οποιοδήποτε κρυπτογραφημένη πληροφορία εκείνος επιθυμεί, αλλά αυτές πρέπει να είναι ήδη επιλεγμένες προτού ο στόχος να λάβει το κρυπτογραφημένο κείμενο c που επιθυμεί πραγματικά να αποκρυπτογραφήσει.
2. Σε μία προσαρμοσμένη επιλεγμένου κρυπτογραφημένου κειμένου επίθεση, ο επιτιθέμενος μπορεί να χρησιμοποιήσει ή να έχει πρόσβαση στην μηχανή αποκρυπτογράφησης του Α (αλλά όχι στο ίδιο το ιδιωτικό κλειδί), ακόμα και αφού έχει δει το κρυπτογραφημένο κείμενο c του στόχου. Ο επιτιθέμενος μπορεί να απαιτήσει αποκρυπτογραφήσεις κειμένου που μπορεί να έχουν σχέση τόσο με το κρυπτογραφημένο κείμενο της οντότητας Α, αλλά και αποκρυπτογραφήσεις από προηγούμενα κείμενα.

3.2.3.

Διανομή Δημόσιων Κλειδιών

Οι μέθοδοι κρυπτογράφησης Δημόσιου Κλειδιού που περιγράφονται παρακάτω, προαπαιτούν την ύπαρξη ενός μέσου για να αποκτήσει ο αποστολέας ενός μηνύματος ένα *αυθεντικό* αντίγραφο από το δημόσιο κλειδί του παραλήπτη. Κατά την απουσία ενός τέτοιου μέσου, η κρυπτογράφηση μπορεί να υποστεί μία επίθεση "προσωποποίησης". Υπάρχουν πολλές τεχνικές και μέθοδοι που μπορούν να χρησιμοποιηθούν πρακτικά, μέσω των οποίων αυθεντικά δημόσια κλειδιά μπορούν να διανεμηθούν, μέσα από ένα έμπιστο κανάλι επικοινωνίας και με τη χρήση πιστοποιητικών αυθεντικότητας.

Παρακάτω, θα δούμε μια παρουσίαση των πιο γνωστών και διαδεδομένων συστημάτων Δημοσίου Κλειδιού.

3.3.1.

Κρυπτογράφηση R.S.A.

Το κρυπτογραφικό σύστημα R.S.A., πήρε την ονομασία του από τους επιστήμονες που το ανακάλυψαν και είναι οι R. Rivest, A. Shamir και L. Adleman. Είναι το πιο ευρέως διαδεδομένο και με τη πιο μεγάλη χρήση, κρυπτογραφικό σύστημα. Μπορεί να χρησιμοποιηθεί για να παρέχει τόσο μυστικότητα, αλλά και ψηφιακές υπογραφές, και η ασφάλειά του βασίζεται στην δυσκολία εντοπισμού του προβλήματος παραγοντοποίησης των ακεραίων.

3.3.2.

Αλγόριθμος δημιουργίας κλειδιού κρυπτογράφησης του συστήματος R.S.A.

Περίληψη: Κάθε οντότητα δημιουργεί ένα δημόσιο κλειδί R.S.A. και ένα αντίστοιχο ιδιωτικό κλειδί. Κάθε οντότητα Α θα πρέπει να κάνει τα παρακάτω:

1. Δημιούργησε δύο μεγάλους και τυχαίους πρώτους αριθμούς p και q, με το ίδιο περίπου μέγεθος.
2. Υπολόγισε $n = pq$ και $\varphi = (p-1)(q-1)$.
3. Διάλεξε ένα τυχαίο ακέραιο e, $1 < e < \varphi$, έτσι ώστε $\gcd(e,\varphi) = 1$.
4. Χρησιμοποίησε το διευρυμένο Ευκλείδειο αλγόριθμο για να υπολογίσεις το μοναδικό ακέραιο d, $1 < d < \varphi$, έτσι ώστε $ed \equiv 1 \pmod{\varphi}$.
5. Το δημόσιο κλειδί του Α είναι (n,e), ενώ το ιδιωτικό του κλειδί είναι το d.

Ορισμός: Οι ακέραιο e και d στο σύστημα δημιουργίας κλειδιού R.S.A., ονομάζονται εκθέτης κρυπτογράφησης και αποκρυπτογράφησης αντίστοιχα, ενώ το n ονομάζεται συντελεστής.

3.3.3.

Αλγόριθμος κρυπτογράφησης δημόσιου κλειδιού R.S.A.

Περίληψη: Η οντότητα Β κρυπτογραφεί ένα μήνυμα m για την οντότητα Α, το οποίο ο Α αποκρυπτογραφεί.

1. Κρυπτογράφηση: Η οντότητα Β θα πρέπει να ακολουθήσει τα επόμενα βήματα.
   (a) Απέκτησε το αυθεντικό δημόσιο κλειδί του Α (n,e).
   (b) Αναπαράστησε το μήνυμα σαν ένα ακέραιο m στο διάστημα [0, n - 1]
   (c) Υπολόγισε $c = m^e \bmod n$.
   (d) Στείλε το κρυπτογραφημένο κείμενο c στην οντότητα Α.
2. Αποκρυπτογράφηση: Για να πάρουμε το κείμενο m από το c, η οντότητα Α θα πρέπει να κάνει τα εξής:
   (a) Χρησιμοποίησε το ιδιωτικό κλειδί d για να πάρουμε το $m = c^d \bmod n$.

3.3.4

Η κρυπτογράφηση R.S.A. στη πράξη

Υπάρχουν πολλοί τρόποι για να επιταχύνουμε την κρυπτογράφηση και την αποκρυπτογράφηση με το σύστημα R.S.A. τόσο από πλευράς λογισμικού όσο και από πλευράς υλικού. Κάποιες από αυτές τις τεχνικές είναι ο Γρήγορος Πολλαπλασιασμός Συντελεστή (Fast Modular Multiplication) και η χρήση του Θεωρήματος του Κινέζικου Υπολοίπου (Chinese Remainder Theory) για γρηγορότερη αποκρυπτογράφηση. Ακόμα και με αυτές τις βελτιώσεις, το σύστημα κρυπτογράφησης και αποκρυπτογράφησης R.S.A. είναι σημαντικά πιο αργό από την κοινά χρησιμοποιημένη κρυπτογράφηση συμμετρικού κλειδιού, όπως με τον αλγόριθμο D.E.S.

Στη πράξη, η κρυπτογράφηση R.S.A. χρησιμοποιείται συχνά για τη μεταφορά κλειδιών κρυπτογράφησης συμμετρικού κλειδιού και για τη κρυπτογράφηση μικρών πακέτων δεδομένων. Το σύστημα R.S.A. είναι κατοχυρωμένο με δίπλωμα ευρεσιτεχνίας στις Η.Π.Α. και τον Καναδά. Διάφοροι οργανισμοί έχουν γράψει ή είναι στη διαδικασία να γράψουν πρότυπα που απευθύνονται στη χρήση του συστήματος R.S.A. για κρυπτογράφηση, ψηφιακές υπογραφές, κ.α. Δεδομένου της τελευταίας προόδου των αλγορίθμων παραγοντοποίησης ακεραίων, ένας συντελεστής 512 ψηφίων n, παρέχει μόνο οριακή ασφάλεια από διάφορες επιθέσεις. Από το 1996, ένας συντελεστής n το λιγότερο με 768 ψηφία είναι προτεινόμενος, αν και για μακροπρόθεσμη ασφάλεια, θα πρέπει να χρησιμοποιηθεί συντελεστής της τάξης των 1024 ψηφίων.

3.4.1.

3.5.1.

Κρυπτογράφηση ElGamal

Η κρυπτογράφηση δημόσιου κλειδιού ElGamal μπορεί να θεωρηθεί ως συμφωνία κλειδιού Diffie – Hellman στη διαδικασία μεταφοράς κλειδιού. Η ασφάλειά της βασίζεται στη δυσκολία εντοπισμού του συγκεκριμένου λογαριθμικού προβλήματος και στο πρόβλημα Diffie – Hellman.

3.5.2.

Αλγόριθμος δημιουργίας κλειδιού για τη κρυπτογράφηση δημοσίου κλειδιού ElGamal.

Περίληψη: Κάθε οντότητα δημιουργεί ένα δημόσιο κλειδί και ένα αντίστοιχο ιδιωτικό κλειδί. Κάθε οντότητα Α θα πρέπει να ακολουθήσει τα παρακάτω βήματα:

1. Δημιούργησε ένα μεγάλο τυχαίο πρώτο αριθμό p και μία γεννήτρια α του πολλαπλασιαστικού συνόλου Z_p των ακεραίων p.
2. Διάλεξε ένα τυχαίο ακέραιο α, 1 <= α <= p – 2, και υπολόγισε $\alpha^{\wedge}\alpha$ mod p.
3. Το δημόσιο κλειδί του Α είναι (p, α, $\alpha^{\wedge}\alpha$), ενώ το ιδιωτικό κλειδί του Α είναι το α.

3.5.3.

Αλγόριθμος κρυπτογράφησης δημόσιου κλειδιού ElGamal

Περίληψη: Η οντότητα Β κρυπτογραφεί ένα μήνυμα m για την οντότητα Α, το οποίο ο Α αποκρυπτογραφεί.

1. Κρυπτογράφηση: Η οντότητα Β θα πρέπει να κάνει τα ακόλουθα:
   (a) Απέκτησε το αυθεντικό δημόσιο κλειδί της οντότητας Α (p, α, $\alpha^{\wedge}\alpha$).
   (b) Αναπαράστησε το μήνυμα σαν ένα ακέραιο m στο εύρος {0, 1,…, p - 1}
   (c) Διάλεξε ένα τυχαίο ακέραιο k, 1 <= k <= p – 2
   (d) Υπολόγισε γ = $\alpha^{\wedge}k$ mod p και δ = m * $(\alpha^{\wedge}\alpha)^{\wedge}k$ mod p.
   (e) Στείλε το κρυπτογραφημένο μήνυμα c = (γ, δ) στο Α.
2. Αποκρυπτογράφηση: Για να πάρεις το αποκρυπτογραφημένο κείμενο m από το c, η οντότητα Α θα πρέπει να κάνει τα παρακάτω:
   (a) Χρησιμοποίησε το ιδιωτικό κλειδί α για να υπολογίσεις $\gamma^{\wedge}p\text{-}1\text{-}\alpha$ mod p (Σημειώνουμε ότι $\gamma^{\wedge}p\text{-}1\text{-}\alpha = \gamma^{\wedge}\text{-}\alpha = \alpha^{\wedge}\text{-}\alpha k$).
   (b) Βρες το m υπολογίζοντας $(\gamma^{\wedge}\text{-}\alpha)$ * δ mod p.

Κεφάλαιο Τέταρτο:

4.1.

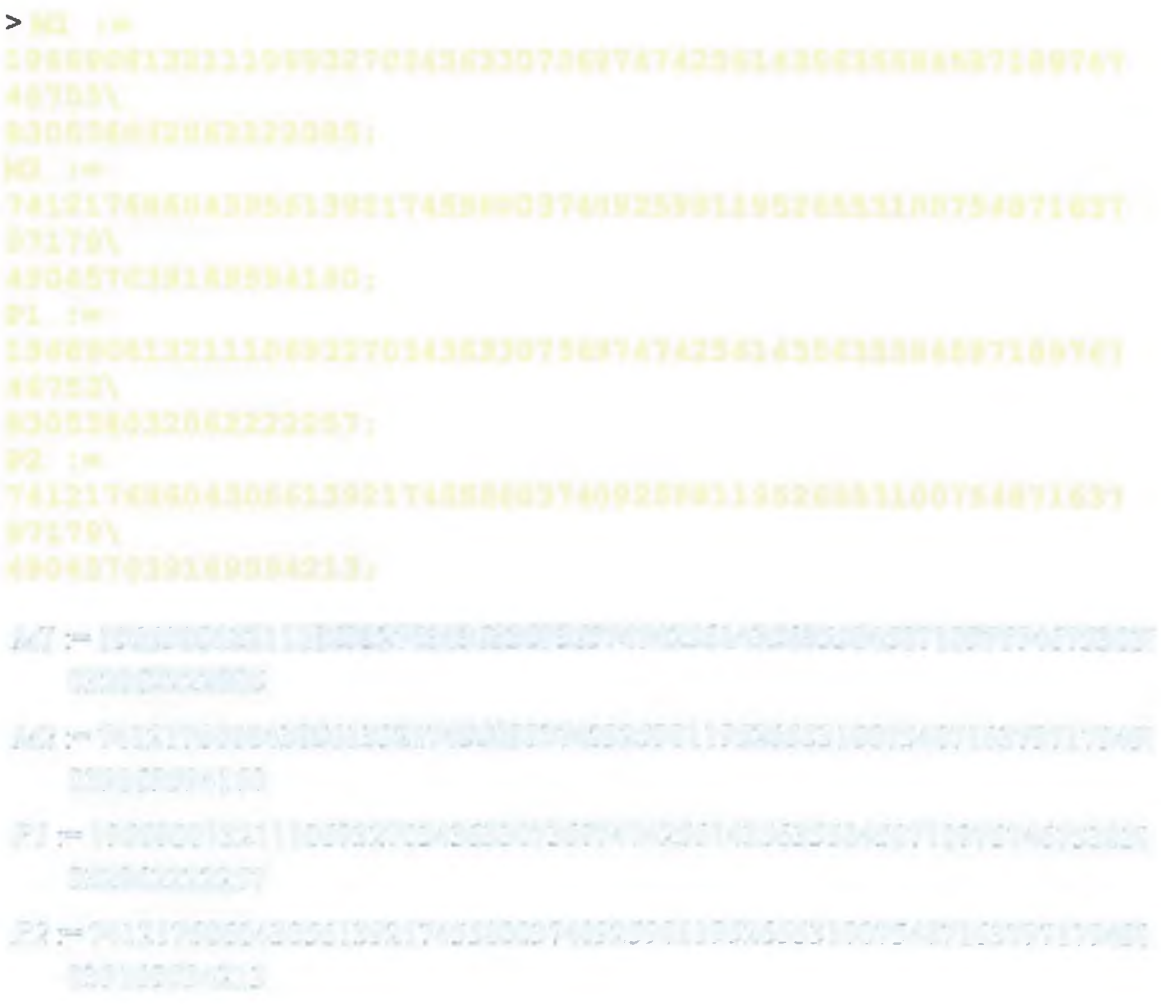
Χρησιμοποιώντας τον αλγόριθμο R.S.A.

Ετοιμάζοντας τον αλγόριθμο και διαλέγοντας τους μεγάλους πρώτους αριθμούς:

Το πρώτο πράγμα που πρέπει να κάνουμε για να χρησιμοποιήσουμε τον αλγόριθμο R.S.A. είναι το να βρούμε δύο μεγάλους πρώτους αριθμούς. Για αυτό το λόγο, το φύλλο εργασίας θα πρέπει να αναζητήσει πρώτους αριθμούς που είναι μεγέθους περίπου 80 ψηφίων. (Διαλέγουμε 80 ψηφία γιατί χωράνε εύκολα σε μία γραμμή κειμένου). Το κάνουμε αυτό με τις λειτουργίες rand και nextprime στο Maple. Έτσι έχουμε:

```
> M1 := rand(10^80)();
M2 := rand(10^80)();
P1 := nextprime(M1);
P2 := nextprime(M2);
```

Η χρήση μιας λειτουργίας τυχαίου αριθμού στην επιλογή των πρώτων αριθμών αποσκοπά στο να τους κάνουμε πιο δύσκολο στο να μπορούμε να τους βρούμε τυχαία. Η έξοδος έχει μετατραπεί σε είσοδο για το Maple για να μπορούμε να δουλέψουμε με επαναλαμβανόμενους υπολογισμούς. (Για να μετατρέψουμε σε είσοδο για Maple, πρέπει να αντιγράψουμε την έξοδο σε ένα αρχείο απλού κειμένου και έπειτα να το αντιγράψουμε πάλι στο Maple.)



Πρέπει να υπολογίσουμε το προϊόν των δύο πρώτων αριθμών και το προϊόν ενός λιγότερου από τον κάθε ένα πρώτο αριθμό.

>

Τώρα πρέπει να αποφασίσουμε για μία τιμή για το e, τον αριθμό κρυπτογράφησης. Αφού το e θα είναι δημόσια γνωστό, δε χρειάζεται να ασχοληθούμε με τυχαία δημιουργία του. Μπορούμε να χρησιμοποιήσουμε αριθμούς που θα είναι εύκολο να υπολογιστούν και να δουλέψουμε μαζί τους με μαθηματικό τρόπο. Φαίνεται πως το καλύτερο κριτήριο για μαθηματική ευκολία είναι ότι αν e αναπαριστάται με βάση το 2, θα έχει σχεδόν όλα τα ψηφία του 0.

>

Θυμηθείτε ότι έπρεπε να βεβαιωθούμε ότι το e είναι σχετικά πρώτος αριθμός σε σχέση με το n2. Αυτό είναι εύκολο γιατί επιλέξαμε το e να είναι πρώτος αριθμός. Τώρα πρέπει να υπολογίσουμε το d, το πολλαπλασιαστικό αντίστροφο του e mod n2. Θα μπορούσαμε να το κάνουμε αυτό απευθείας με το εκτεταμένο Ευκλείδειο αλγόριθμο, αλλά θα χρησιμοποιήσουμε απλά τις μαθηματικές και αριθμητικές λειτουργίες του Maple.

>

Είμαστε έτοιμοι να ορίσουμε τις διαδικασίες κωδικοποίησης και αποκωδικοποίησης.

>

Προφανώς θέλουμε απλά να ελέγξουμε ότι οι διαδικασίες αναιρούν η μία την άλλη, τουλάχιστον για ένα μικρό δείγμα μηνυμάτων.

>

Ασκήσεις:

1) Οι επιλεγμένοι πρώτοι αριθμοί μας επιτρέπουν να κωδικοποιήσουμε και να αποκωδικοποιήσουμε μηνύματα που είναι αριθμοί περίπου στο εύρος από 0 έως 10^159. Διάλεξε τυχαία πέντε αριθμούς σε αυτό το εύρος και επικύρωσε ότι η κωδικοποίηση και αποκωδικοποίηση λειτουργούν σαν αντίθετες διεργασίες σε αυτούς τους αριθμούς.
2) Από τους αριθμούς που βρήκαμε προς το παρόν, εξήγησε ποιοι αριθμοί που θέλουμε να δημοσιεύσουμε, πρέπει να σωθούν και να παραμείνουν μυστικοί και ποιοι πρέπει να καταστραφούν και να ξεχαστούν αφού χρησιμοποιούμε το σύστημα R.S.A. σαν ένα σύστημα δημόσιου κλειδιού.
3) Τυχαία επέλεξε δύο πρώτους αριθμούς στο εύρος 1 έως 10^80 και ετοίμασε τα δικά σου κλειδιά. Δοκίμασε αν τα κλειδιά σου κρυπτογραφούν και αποκρυπτογραφούν τους δύο αριθμούς της επιλογής σου. (Πιθανότατα δεν επιθυμούμε να ξαναχρησιμοποιήσουμε τα ονόματα n, e, ή d, αφού θα συνεχίσουμε να χρησιμοποιούμε αυτούς τους αριθμούς σε επόμενες ασκήσεις.
4) Δημοσίευσε το δημόσιο κλειδί και το modulus σε πίνακα ανακοινώσεων έτσι ώστε ο οποιοσδήποτε να μπορεί να στείλει μηνύματα. (Φυσικά μη δημοσιεύσεις το μυστικό κλειδί!)

Κρυπτογραφώντας μηνύματα αντί αριθμούς

Τώρα θέλουμε να εστιάσουμε την προσοχή μας στην κωδικοποίηση μηνυμάτων. Ακολουθώντας το σχέδιο από την προηγούμενη δουλειά μας, αν θέλουμε να μετατρέψουμε το μήνυμά μας σε ένα και μόνο αριθμό, η μέθοδος που θα χρησιμοποιήσουμε είναι η μετατροπή του μηνύματος από χαρακτήρες ASCII σε μία σειρά από δεκαδικά αντίτιμα και μετά η μετατροπή του κάθε ένα από τους δεκαδικούς αριθμούς σε ένα διψήφιο αριθμό hex. Έπειτα συνδέουμε τους αριθμούς hex σε ένα μεγάλο αριθμό και το ξαναμετατρέπουμε σε ένα δεκαδικό αριθμό. Μετά μπορούμε να κωδικοποιήσουμε το μήνυμά μας, να το μετατρέψουμε σε αριθμό hex ή να το αποθηκεύσουμε σε κάποια κατανοητή μορφή.

Θυμηθείτε ότι έχουμε συχνά προβλήματα με τη μετατροπή σε hex αριθμούς. Αν το δεκαδικό ανάλογο του χαρακτήρα ASCII είναι μικρότερο του 16, ο αριθμός hex είναι μεγέθους ενός ψηφίου και πρέπει να υποθέσουμε ότι οι χαρακτήρες συντελούν σε ψηφία δύο hex για να κρατηθεί η τοποθέτηση σωστή. (Συγκεκριμένα, ο χαρακτήρας που παίρνουμε είναι ισότιμος με 13.) Η διαδικασία μετατρέπει hex αριθμούς δύο ψηφίων με έξοδο δύο ψηφίων.

```
>
```

Είμαστε έτοιμοι να ξεκινήσουμε με ένα μικρό μήνυμα.

```
>
```

Θέλουμε μία διαδικασία που να μετατρέπει το κείμενο σε ένα αριθμό.

```
>
```

Έπειτα, θέλουμε να κωδικοποιήσουμε τον αριθμό μας και να τον μετατρέψουμε σε hex μορφή για δική μας ευκολία χρήσης.

```
>
```

Αυτό δεν φαίνεται πολύ εύκολο να αντιγραφεί από και προς το Maple. (Σίγουρα θα κάναμε λάθη αν προσπαθούσαμε να γράφαμε μια σειρά τόσο μεγάλη.) Για να δώσουμε μία ωραία μορφή στην έξοδο, βάζω αρχικά μηδενικά και μετά το χωρίζω σε κομμάτια ίσου μεγέθους. Θεωρούμε πως δέκα χαρακτήρες δημιουργούν ένα σωστό μέγεθος.

```
>
>
```

```
>
```

Τώρα θέλουμε να επιβεβαιώσουμε ότι μπορούμε να ξαναενώσουμε το μήνυμα και να το αποκωδικοποιήσουμε. Ορίζουμε μία διαδικασία για να μετατραπεί το διάνυσμα ενός κομματιού hex σε ένα απλό αριθμό.

```
>
```

Τώρα μπορούμε να μετατρέψουμε το μήνυμά μας ξανά σε ένα αποκωδικοποιημένο αριθμό. Θα πρέπει να πάρουμε σαν αποτέλεσμα το ίδιο που πήραμε από το messnum1 παραπάνω.

```
>
```

```
> convert(nmessmul,hex);
```

Θέλουμε επίσης μία διεργασία για να αλλάζει τον αποκωδικοποιημένο αριθμό και να τον μετατρέπει ξανά σε μήνυμα.

```
> numtostring := proc(nummul)
local hexstr, listlength, ascii, i;
#convert to a hex string
hexstr := convert(nummul,hex);
#make sure the hex string has even length
if (length(hexstr) mod 2) = 1 then hexstr := cat
cat("0",hexstr) fi;
#compute the number of characters
listlength := length(hexstr)/2;
#convert to a vector of decimal numbers
ascii := array(1..listlength);
for i from 1 to listlength do
ascii[i] := convert(substring(hexstr,2*i-
1..2*i),decimal,hex);
od;
#convert the vector to a list, then to an ASCII string
convert(convert(ascii,list),bytes);
end:
> numtostring(nmessmul);
```

Ασκήσεις:

5) Για να λειτουργήσουν οι παραπάνω διεργασίες, πρέπει να περιορίσουμε να μηνύματά μας σε μηνύματα τα οποία κωδικοποιούνται σαν νούμερα μικρότερα του n. Ποιο είναι το μέγιστο μέγεθος ενός μηνύματος που μπορούμε να κωδικοποιήσουμε;
6) Δοκίμασε να βάλεις ένα μήνυμα περίπου 50 χαρακτήρων και κωδικοποίησέ το χρησιμοποιώντας το nande που ορίζεται παραπάνω.
7) Επιβεβαίωσε ότι μπορείς να αποκωδικοποιήσεις το μήνυμα με το μυστικό κλειδί.
8) Για το υπόλοιπο αυτού του φύλλου εργασίας, το modulus είναι:
   14579070943426365719341081596858629803265159149118248616
   43397522980497550736230615496046802186876835611836753440
   52519958769801995483916593242784227837370699874 1
   και το κλειδί κρυπτογράφησης είναι: 65537.
   Κωδικοποίησε ένα μικρό μήνυμα και δοκίμασε να το στείλεις στο πίνακα ανακοινώσεων.

9) Απέκτησε τα δημόσια κλειδιά δύο άλλων ατόμων και στείλε τους ένα μικρό κρυπτογραφημένο μήνυμα μέσω του πίνακα ανακοινώσεων.
10) Κάνε ένα μικρότερο φύλλο εργασίας R.S.A. που μπορείς να το χρησιμοποιήσεις σαν εφαρμογή κρυπτογράφησης και αποκρυπτογράφησης.

Επίλογος:

Σε αυτή την εργασία είδαμε γενικά τις βασικότερες αρχές της κρυπτογραφίας. Ξεκινήσαμε με κάποια ιστορικά στοιχεία δηλαδή για το πώς ξεκίνησε σαν τέχνη και εξελίχθηκε στις μέρες μας σε επιστήμη. Στη σύγχρονη εποχή λοιπόν, η κρυπτογραφία χρησιμοποιεί εξελιγμένους αλγόριθμους για να κωδικοποιεί δεδομένα υψίστης σημασίας έτσι ώστε κατά τη μεταφορά τους να μην τύχουν παραβίασης. Υπάρχουν διάφοροι αλγόριθμοι, κάποιοι περισσότερο και κάποιοι λιγότερο γνωστοί, μερικούς από τους οποίους παρουσιάσαμε. Παρόλα αυτά, η προσπάθεια για αύξηση της ασφάλειας ποτέ δε σταματά, γιατί οι σημερινοί κίνδυνοι ασφάλειας είναι όλο και περισσότεροι. Στο μέλλον, αναμένουμε συγκλονιστικές εξελίξεις στο τομέα της ασφάλειας, τις οποίες θα δούμε να πραγματοποιούνται πολύ συντομότερα από ότι ίσως νομίζουμε!

ΒΙΒΛΙΟΓΡΑΦΙΑ:

Handbook of Applied Cryptography, by A. Menezes, P. van Oorschot, and S. Vanstone, CRC Press, 1996.

ΣΥΝΔΕΣΜΟΙ/ΙΣΤΟΣΕΛΙΔΕΣ:

Cryptography, Mathematical descriptions -
Cryptography from A-Z -
Cryptography FAQ index -
Cryptographic software and libraries -