
ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΠΕΛΟΠΟΝΝΗΣΟΥ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ Τ.Ε

# ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΑ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ
ΤΗΣ
**ΤΡΙΑΝΤΑΦΥΛΛΟΥ ΠΑΝΑΓΙΩΤΑΣ**

ΕΠΙΒΛΕΠΟΥΣΑ ΚΑΘΗΓΗΤΡΙΑ: **ΛΑΜΠΡΙΝΗ ΚΑΛΑΝΤΖΗ**

-

-

ΔΗΛΩΣΗ ΜΗ ΛΟΓΟΚΛΟΠΗΣ ΚΑΙ ΑΝΑΛΗΨΗΣ ΠΡΟΣΩΠΙΚΗΣ ΕΥΘΥΝΗΣ

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, δηλώνω ενυπογράφως ότι είμαι αποκλειστικός συγγραφέας της παρούσας Πτυχιακής Εργασίας, για την ολοκλήρωση της οποίας κάθε βοήθεια είναι πλήρως αναγνωρισμένη και αναφέρεται λεπτομερώς στην εργασία αυτή. Έχω αναφέρει πλήρως και με σαφείς αναφορές, όλες τις πηγές χρήσης δεδομένων, απόψεων, θέσεων και προτάσεων, ιδεών και λεκτικών αναφορών, είτε κατά κυριολεξία είτε βάση επιστημονικής παράφρασης. Αναλαμβάνω την προσωπική και ατομική ευθύνη ότι σε περίπτωση αποτυχίας στην υλοποίηση των ανωτέρω δηλωθέντων στοιχείων, είμαι υπόλογος έναντι λογοκλοπής, γεγονός που σημαίνει αποτυχία στην Πτυχιακή μου Εργασία και κατά συνέπεια αποτυχία απόκτησης του Τίτλου Σπουδών, πέραν των λοιπών συνεπειών του νόμου περί πνευματικών δικαιωμάτων. Δηλώνω, συνεπώς, ότι αυτή η Πτυχιακή Εργασία προετοιμάστηκε και ολοκληρώθηκε από εμένα προσωπικά και αποκλειστικά και ότι, αναλαμβάνω πλήρως όλες τις συνέπειες του νόμου στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δε μου ανήκει διότι είναι προϊόν λογοκλοπής άλλης πνευματικής ιδιοκτησίας.

Όνομα και Επώνυμο Συγγραφέα (Με Κεφαλαία): ΠΑΝΑΓΙΩΤΑ ΤΡΙΑΝΤΑΦΥΛΛΟΥ

Υπογραφή (Ολογράφως, χωρίς μονογραφή): 

Ημερομηνία (Ημέρα – Μήνας – Έτος): ΤΕΤΑΡΤΗ 30 ΜΑΪΟΥ 2018

-

# ΠΕΡΙΛΗΨΗ

Το αντικείμενο της παρούσας πτυχιακής εργασίας είναι η μελέτη των κρυπτοσυστημάτων δημοσίου κλειδιού. Τα κρυπτοσυστήματα δημοσίου κλειδιού χρησιμοποιούνται στην κρυπτογραφία και αποτελούν τεχνικές κρυπτογράφησης και αποκρυπτογράφησης ενός μηνύματος με στόχο την προστασία του περιεχόμενού του μηνύματος. Στα κρυπτοσυστήματα δημοσίου κλειδιού κάθε χρήστης διαθέτει δύο κλειδιά, το ένα είναι δημόσιο και χρησιμοποιείται κατά την κρυπτογράφηση, ενώ το άλλο είναι ιδιωτικό και χρησιμοποιείται κατά την αποκρυπτογράφηση. Πιο συγκεκριμένα, στην εργασία αναλύονται οι βασικές αρχές και μελετώνται ο αλγόριθμος RSA που βασίζεται στη δυσκολία παραγοντοποίησης μεγάλων αριθμών και ο αλγόριθμος ElGamal που βασίζεται στο πρόβλημα του διακριτού αλγορίθμου. Για τους αντίστοιχους αλγορίθμους, μελετώνται οι πιθανές επιθέσεις και πραγματοποιείται υλοποίηση τους στη γλώσσα προγραμματισμού C. Επιπρόσθετα, παρουσιάζονται αναλυτικά οι εφαρμογές τους και ειδικότερα οι ψηφιακές υπογραφές. Οι ψηφιακές υπογραφές υπάρχουν στα ψηφιακά έγγραφα, παίζουν σημαντικό ρόλο και σε πολλές χώρες αναγνωρίζονται και νομικά. Δεν μπορούν να πλαστογραφηθούν εύκολα έναντι των κανονικών υπογραφών και αυτό είναι που τις κάνει αρκετά σημαντικές και χρήσιμες.

**Λέξεις κλειδιά:** κρυπτοσυστήματα δημοσίου κλειδιού, RSA, ElGamal, ψηφιακές υπογραφές.

-

# ΠΕΡΙΕΧΟΜΕΝΑ

-

# *ΕΙΣΑΓΩΓΗ*

Στη παρούσα πτυχιακή εργασία μελετήθηκαν τα κρυπτοσυστήματα δημοσίου κλειδιού και πιο συγκεκριμένα οι δύο αλγόριθμοι RSA και ElGamal.
Στο πρώτο κεφάλαιο γίνεται μια ιστορική αναδρομή στην εξέλιξη της κρυπτογραφίας ανά τους αιώνες και αναλύονται οι βασικοί όροι της κρυπτογραφίας, οι στόχοι της και κάποιοι μαθηματικοί όροι που θα χρειαστούν στην συνέχεια . Επίσης δίνονται οι κατηγορίες των κρυπτοσυστημάτων και πιο συγκεκριμένα αναλύονται τα ασύμμετρα και συμμετρικά κυρίως ως προς τα πλεονεκτήματα και μειονεκτήματα τους .
Στο δεύτερο κεφάλαιο γίνεται η ανάλυση των βασικών αλγόριθμων της εργασίας δηλαδή των RSA και ElGamal δίνονται τα πλεονεκτήματα τους, τα μειονεκτήματα τους και τα είδη των επιθέσεων που πιθανόν δεχτούν.
Στο τρίτο κεφάλαιο έχει γίνει μελέτη πάνω στις εφαρμογές της κρυπτογραφίας αλλά και αυτών των αλγορίθμων και πιο συγκεκριμένα στις ψηφιακές υπογραφές. Έχουν αναλυθεί τα δύο είδη των σχημάτων των ψηφιακών υπογραφών και οι πιθανές επιθέσεις, τις οποίες μπορούν να δεχτούν. Επιπρόσθετα μελετήθηκαν οι ψηφιακές υπογραφές RSA και οι ψηφιακές υπογραφές ElGamal. Τέλος έγινε μια μελέτη πάνω στην αυθεντικοποίηση της ταυτότητας και στα ψηφιακά πιστοποιητικά που χρησιμοποιούνται στην αυθεντικοποίηση.
Στο τέταρτο κεφάλαιο έγινε η υλοποίηση σε γλώσσα C, των δυο αλγορίθμων που αναλύθηκαν στο δεύτερο κεφάλαιο και στο πέμπτο κεφάλαιο δόθηκαν μερικά συμπεράσματα σχετικά με την τις παραπάνω μελέτες.

-

# *1. ΚΡΥΠΤΟΓΡΑΦΙΑ*

Η κρυπτογραφία αρχικά έκανε την εμφάνιση της ως ένα είδος τέχνης και με την πάροδο των χρόνων μετεξελίχθηκε σε πεδίο της επιστήμης των υπολογιστών . Αυτό το πεδίο ασχολείται με τη μελέτη, την ανάπτυξη και την χρήση ειδικών τεχνικών προκειμένου να γίνεται απόκρυψη του περιεχομένου ενός μηνύματος.
Η κρυπτογραφία έχει μεγάλη σημασία στους τομείς της ασφάλειας υπολογιστικών συστημάτων και των τηλεπικοινωνιών καθώς παρέχει μηχανισμούς ώστε 2 ή περισσότερα άκρα επικοινωνίας όπως είναι οι άνθρωποι, τα προγράμματα υπολογιστών και άλλα να ανταλλάσσουν μηνύματα χωρίς κάποιος τρίτος να είναι ικανός να διαβάσει την πληροφορία που περιέχεται σε αυτά τα μηνύματα.

## *1.1 Ιστορικά στοιχεία*

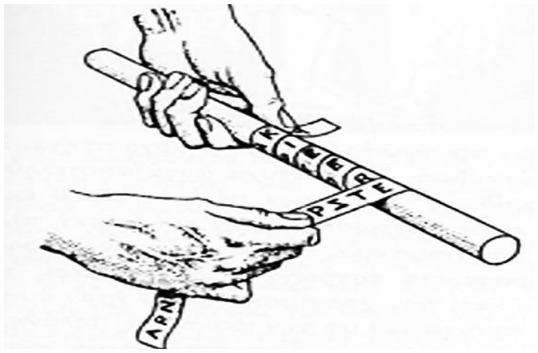
Η ιστορία της κρυπτογραφίας έχει διαιρεθεί σε 3 χρονικές περιόδους .Στην πρώτη περίοδο οι διαδικασίες απεικονίζονταν με μελάνι και χαρτί και είχαν την μορφή αντικατάστασης των γραμμάτων της αλφαβήτου και της αναδιάταξης τους. Στην δεύτερη περίοδο άρχισαν να χρησιμοποιούνται κρυπτογραφικές μηχανές και στην τελευταία περίοδο γίνεται συνδυασμός των μαθηματικών και των υπολογιστών άρα αρχίζει να δημιουργείται το σύγχρονο κρυπτογραφικό σύστημα. Παρότι η κρυπτογραφία μετεξελίχθηκε ο στόχος της, ο οποίος είναι η ασφαλής επικοινωνία, παρέμεινε ο ίδιος. Η κρυπτογραφία χωρίζεται χρονικά σε 3 περιόδους. Η πρώτη περίοδος ξεκινάει το 1900π.Χ και τελειώνει το 1900μ.Χ . Η δεύτερη περίοδος ξεκινάει το 1900μ.Χ και τελειώνει το 1950μ.Χ. Η τελευταία περίοδος ξεκινάει το 1950μ.Χ και συνεχίζεται μέχρι και σήμερα.

Ήδη από το 1500 π.Χ. η κρυπτογραφία έγινε αντικείμενο που απασχόλησε τους πολιτισμούς γύρω από την Μεσοποταμία. Σημαντικό εύρημα που δίνει στους μελετητές αυτό το στοιχείο είναι μια μικρή σφηνοειδής επιγραφή που βρέθηκε στις όχθες του ποταμού Τίγρη και χρονολογείτε στην τότε εποχή.
Το 1900 π.Χ χρησιμοποιήθηκε για πρώτη φόρα στην Αίγυπτο ένα άλλο είδος ιερογλυφικών με σκοπό την επικοινωνία. Λίγο αργότερα το 1908 π.Χ στην Κρήτη ανακαλύφθηκε μια πινακίδα κυκλικού σχήματος, γνωστή με το όνομα ο Δίσκος της Φαιστού. Η πινακίδα αυτή σύμφωνα με έρευνες δημιουργήθηκε το 1700 π.Χ και τα σύμβολα τα οποία έχει στην επιφάνεια της έχουν χαραχτεί με την χρήση διαφόρων σφραγίδων, γεγονός που τον καθιστά το αρχαιότερο δείγμα στοιχειοθεσίας. Τα σύμβολα αυτά δεν έχουν αποκρυπτογραφηθεί ακόμα και σήμερα και αυτού του είδους η γραφή αποτελεί την πιο μυστηριώδης αρχαία ευρωπαϊκή γραφή.

-

Στην Ελλάδα αναφορές στην κρυπτογραφία γίνονται και μέσα από βιβλία όπως η Ιλιάδα του Ομήρου, όπου ο Βελλερεφόντης πάει στη Λυκία μεταφέροντας κρυφό γραπτό μήνυμα, αλλά και στην Ιστορία του Ηροδότου, όπου ο Ιστιαίος, αιχμάλωτος του Δαρείου στέλνει κρυφό μήνυμα στην οικογένεια του γραμμένο στο κεφάλι ενός εμπίστου σκλάβου. Σημαντική αναφορά του Ηροδότου είναι επίσης η ιστορία του Δημάρατου, ο οποίος αν και εξόριστος στην Περσία προειδοποίησε τους Σπαρτιάτες για την εισβολή του Ξέρξη, στέλνοντας ένα μήνυμα καλυμμένο από κερί. Το μήνυμα αποκαλύφθηκε και ο Ξέρξης δεν μπόρεσε να έχει το πλεονέκτημα του αιφνιδιασμού. Υπάρχουν κι μερικές ακόμα ιστορίες αλλά η κωδικοποίηση γραμμάτων και η χρήση αριθμών μέσα σε πίνακες έγινε πρώτη φορά από τον Πολύβιο. Στην αρχαία Σπάρτη γύρω στο 5ο αιώνα π.Χ. γίνεται για πρώτη φορά χρήση της κρυπτογραφίας για στρατιωτικούς λόγους. Για πρώτη φορά φτιάχνεται μια συσκευή κρυπτογράφησης η λεγόμενη «σκυτάλη». Η συσκευή αυτή ήταν ουσιαστικά μια ξύλινη ράβδος με συγκεκριμένη διάμετρο γύρω από την οποία τύλιγαν ελικοειδώς μια λωρίδα περγαμηνής. Το κείμενο γραφόταν σε στήλες, σε κάθε έλικα γραφόταν ένα γράμμα, όταν ξετύλιγαν τη λωρίδα το κείμενο ήταν μη κατανοητό εξαιτίας της σειράς των γραμμάτων. Το «κλειδί» για να μπορέσει κάποιος να καταλάβει το σωστό κείμενο ήταν η διάμετρος της σκυτάλης.

Εικόνα 1. Δίσκος της Φαιστού



Εικόνα 2. Σκυτάλη

Η ιστορία της κρυπτογραφίας έχει ρίζες και από την αρχαία Αίγυπτο όπου οι ιερείς χρησιμοποιούσαν παρόμοια μέθοδο με αυτή της Σπαρτιάτικης σκυτάλης. Ακόμα και οι Φαραώ για να μεταφέρουν τα σημαντικά μηνύματα τους, ξύριζαν τα κεφάλια των σκλάβων έγραφαν το μήνυμα τους και τους έστελναν στον παραλήπτη. Επίσης οι Εβραίοι συγγραφείς χρησιμοποιούσαν ένα σύστημα κρυπτογραφίας προκειμένου να ‘’κρύψουν’’ τα κείμενα τους. Συνήθως αντέστρεφαν το αλφάβητο δηλαδή χρησιμοποιούσαν στην θέση του πρώτου γράμματος του αλφαβήτου το τελευταίο ,στην θέση του δεύτερου το προτελευταίο και ούτω καθεξής. Το ίδιο σύστημα χρησιμοποιήθηκε και στη Βίβλο για παρόμοιους λόγους.

Η κρυπτογραφία στην Ευρώπη ξεκίνησε από πολύ παλιά μέσω του Ιούλιου Καίσαρα. Ο Ιούλιος Καίσαρας ,προκειμένου να επικοινωνεί με τους επιτελείς με μηνύματα χωρίς να το καταλαβαίνουν οι εχθροί του, επινόησε έναν κρυπτογραφικό αλγόριθμο. Ο αλγόριθμος που χρησιμοποιούσε ήταν σχετικά

απλός και βασιζόταν στην αντικατάσταση κάθε γράμματος της αλφαβήτου με κάποιο άλλο, όχι όμως τυχαία αλλά με βάση ένα αριθμό που ονομάζαμε κλειδί. Με βάση αυτό το κλειδί πηγαίναμε δεξιά όσες θέσεις μας έλεγε. Ο αλγόριθμος αυτός ονομάστηκε «αλγόριθμος του Καίσαρα» προς τιμή του και είναι γνωστός μέχρι και σήμερα. Στα χρόνια όμως του Μεσαίωνα στην Ευρώπη η κρυπτογραφία αποτέλεσε απαγορευμένο τομέα και είδος μαύρης μαγείας, στοιχεία που συντέλεσαν στον να μην αναπτυχθεί όσο θα έπρεπε. Αυτά ίσχυαν μόνο στην Ευρώπη αντίθετα στον Αραβικό κόσμο η εξέλιξη της κρυπτογραφίας συνεχιζόταν κανονικά με αποτέλεσμα οι Άραβες να είναι οι πρώτοι που επινόησαν και χρησιμοποίησαν μεθόδους κρυπτανάλυσης.

Στους πιο σύγχρονους αιώνες η κρυπτογραφία χρησιμοποιήθηκε στις διπλωματικές σχέσεις μεταξύ των διαφόρων κρατών, κυρίως κατά την διάρκεια πολέμων. Μεγάλη εμφάνιση της κρυπτογραφίας υπήρξε κατά τη διάρκεια του 1$^{ου}$ και 2$^{ου}$ παγκοσμίου πολέμου όπου τα συστήματα κρυπτογράφησης γίνονται αρκετά πολύπλοκα και η διαδικασία για την αποκρυπτογράφηση των μηνυμάτων χρειαζόταν την συνεργασία πολλών ατόμων. Οι γερμανοί ήταν αυτοί που δημιούργησαν μια μηχανή κρυπτογράφησης γνωστή με το όνομα Enigma, της οποίας εφευρέτης ήταν ο γερμανός Άρθουρ Σέρμπιους. Το όνομα της μηχανής προερχόταν από την ελληνική λέξη αίνιγμα και ο κώδικας της θυμιζει τον κώδικα Vigener αλλά είναι πιο πολύπλοκος. Η πολεμική μορφή που πήρε μετά από μετατροπές την έκανε να θεωρηθεί από τους συμμάχους των γερμανών άθραυστη. Στην μηχανή αυτή εάν στην είσοδο δινόταν το κωδικοποιημένο κείμενο σαν έξοδο θα δινόταν το αρχικό κείμενο. Η κύρια μορφή της μηχανής αποτελούνταν από ένα πληκτρολόγιο μέσω του οποίου γινόταν η εισαγωγή του αποκρυπτογραφημένου κειμένου, μια μονάδα η οποία μετέτρεπε κάθε γράμμα του κειμένου που είχε εισαχθεί σε αντίστοιχο γράμμα του κρυπτογραφημένου κειμένου και τέλος από ένα πίνακα ηλεκτρικό ο οποίος έδειχνε το αντίστοιχο γράμμα του κρυπτογραφημένου κειμένου. Αυτό παρότι ήταν πολύ εύκολο για όσους την χρησιμοποιούσαν δημιουργούσε μεγάλο πρόβλημα γιατί δεν έδινε μεγάλη ασφάλεια. Εκείνα τα χρόνια ο στρατός της Γερμανίας αγόρασε πάνω από 30.000 συσκευές Enigma και έκανε τη Γερμανία να φαίνεται η χώρα που διέθετε τις πιο ασφαλής επικοινωνίες. Μία ομάδα όμως Πολωνών κρυπτολόγων με σημαντικό μαθηματικό το Μάριαν Ρεζέφσκι μπόρεσαν να σπάσουν το 1938 την μηχανή Enigma στην τότε απλή μορφή της. Τις πληροφορίες που ανακάλυψαν η κυβέρνηση τους τα έδωσε στους Άγγλους, οι οποίοι ήταν σύμμαχοι της, και με αυτό τον τρόπο τους απέδειξαν ότι τα μαθηματικά ήταν το πιο σημαντικό στοιχείο για το σπάσιμο των κωδικών. Σύμφωνα με ιστορικούς της Αγγλίας με το σπάσιμο του κωδικού της μηχανής Enigma συντομεύθηκε ο πόλεμος για 3 έτη και βοήθησε τα στρατεύματα τους να γλιτώσουν από βαριές απώλειες.

## 1.2 Βασικοί στόχοι κρυπτογραφίας

Η κρυπτογραφία ως βασικό στόχο έχει την ασφαλή επικοινωνία δύο οντοτήτων μέσα σε ένα κανάλι επικοινωνίας, ώστε να μην μπορεί μια άλλη οντότητα μη εξουσιοδοτημένη να μάθει το περιεχόμενο των μηνυμάτων που ανταλλάσουν οι δύο πρώτοι. Οι βασικοί στόχοι της κρυπτογραφίας είναι η εμπιστευτικότητα, η ακεραιότητα, η μη απάρνηση και η πιστοποίηση. Πιο αναλυτικά :

**Εμπιστευτικότητα** : Η πληροφορία, η οποία θα μεταδίδεται, είναι προσβάσιμη μόνο από εξουσιοδοτημένους χρήστες στους υπόλοιπους χρήστες είναι μη κατανοητή.

**Ακεραιότητα**: Η πληροφορία μπορεί να αλλοιωθεί μόνο από εξουσιοδοτημένους χρήστες και πάντα η αλλοίωση αυτή ανιχνεύεται.

**Μη απάρνηση**: Ο αποστολέας ή ο παραλήπτης της πληροφορίας δεν μπορεί να απαρνηθεί ότι έστειλε ή δημιούργησε αντίστοιχα την πληροφορία αυτή.

**Πιστοποίηση**: Ο αποστολέας και ο παραλήπτης μπορούν, με διαβεβαίωση ότι οι ταυτότητες τους δεν είναι πλαστές , να εξακριβώνουν τις ταυτότητες τους όπως επίσης και την πηγή και τον προορισμό της πληροφορίας.

## 1.3 Βασικές έννοιες

Σε αυτή την ενότητα αναλύονται έννοιες που χρησιμοποιούνται στις διάφορες διαδικασίες στο τομέα της κρυπτογραφίας. Επίσης αναλύονται οι στόχοι, τους οποίους θέλει να επιτύχει η κρυπτογραφία.

**Κρυπτογράφηση (Encryption)** ονομάζεται η διαδικασία μετασχηματισμού ενός μηνύματος σε μια άλλη μορφή μη-κατανοητή από μη εξουσιοδοτημένα άτομα.

**Αποκρυπτογράφηση (Decryption)** ονομάζεται η διαδικασία μετασχηματισμού του κρυπτογραφημένου κειμένου σε κανονικό μήνυμα.

**Αρχικό κείμενο (Plaintext)** είναι τα μήνυμα που θα έχω ως είσοδο στην διαδικασία της κρυπτογράφησης.

**Κλειδί (Key)** είναι ο αριθμός των bit που χρησιμοποιείται στην συνάρτηση κρυπτογράφησης σαν είσοδο.

**Κρυπτογραφημένο κείμενο (Cipher text)** είναι το κείμενο που δημιουργείται όταν εφαρμόσουμε το κρυπτογραφικό αλγόριθμο στο κείμενο.

**Κρυπτογραφικός αλγόριθμος (cipher)** είναι μια περίπλοκη μαθηματική συνάρτηση μέσω της οποίας μετασχηματίζονται τα δεδομένα σε μια μη-κατανοητή μορφή από μη- εξουσιοδοτημένα άτομα.

-

**Κρυπτανάλυση (cryptanalysis)** είναι η επιστήμη που μελετά μεθόδους ώστε να αποκρυπτογραφείται ένα μήνυμα χωρίς να είναι γνωστό το κλειδί.

**Κρυπτοσύστημα (cryptosystem)** είναι ο χώρος που αποτελείται από το σύνολο των διαδικασιών της κρυπτογράφησης και της αποκρυπτογράφησης. Αποτελείται ουσιαστικά από μια πεντάδα στοιχείων **P**, **C**, **k**, **enc**, **dec** όπου κάθε ένα έχει μια συγκεκριμένη λειτουργία.

Αναλυτικά :

Το **P** είναι ο χώρος όλων των αρχικών μηνυμάτων που μπορούν να σταλούν.

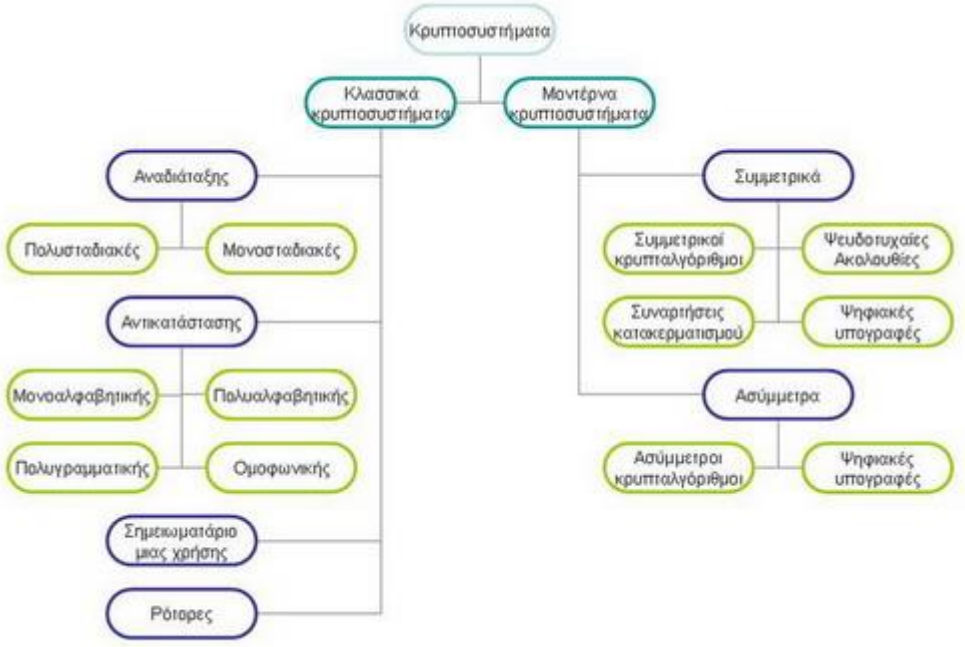
Το **C** είναι ο χώρος όλων των κρυπτογραφημένων κειμένων.

Το **k** είναι ο χώρος όλων των πιθανών κλειδιών που μπορούν να χρησιμοποιηθούν.

Το **enc( )** είναι η συνάρτηση, η οποία χρησιμοποιείται στη διαδικασία της κρυπτογράφησης των κειμένων.

Το **dec( )** είναι η συνάρτηση, η οποία χρησιμοποιείται στη διαδικασία της αποκρυπτογράφησης των κρυπτοκειμένων.

Τα κρυπτοσυστήματα χωρίζονται σε δύο μεγάλες κατηγορίες τα Συμμετρικά Κρυπτοσυστήματα και τα Ασύμμετρα Κρυπτοσυστήματα. Κάθε μια από αυτές τις κατηγορίες έχει και δικές της υποκατηγορίες κρυπτοσυστημάτων.



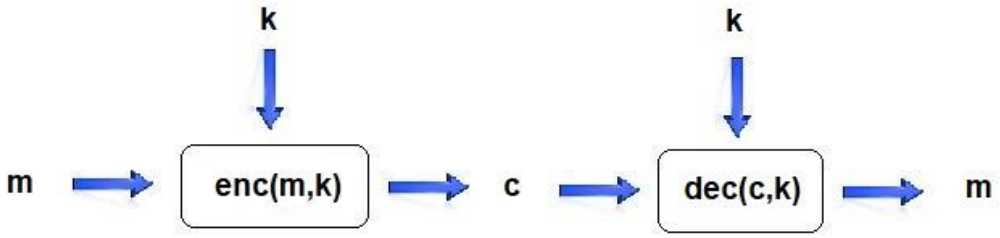

Εικόνα 3.Είδη κρυπτοσυστημάτων

-

## 1.4 Συμμετρικά κρυπτοσυστήματα

### 1.4.1 Γενικές αρχές

Τα συμμετρικά κρυπτοσυστήματα χρησιμοποιούνται από τα πολύ παλιά χρόνια, πριν από τα ασύμμετρα κρυπτοσυστήματα. Η κρυπτογράφηση και η αποκρυπτογράφηση των πληροφοριών γίνεται με τη χρήση ενός κλειδιού, το οποίο και ονομάζεται συμμετρικό. Το κλειδί αυτό το γνωρίζουν και το χρησιμοποιούν μόνο ο παραλήπτης και ο αποστολέας. Το μοίρασμα του κλειδιού στον αποστολέα και τον παραλήπτη γίνεται πριν από την αποστολή της πληροφορίας και αυτό αποτελεί σημαντικό στοιχείο για την ασφάλεια των συμμετρικών κρυπτοσυστημάτων.




### 1.4.2 Πλεονεκτήματα και Μειονεκτήματα συμμετρικών κρυπτοσυστημάτων

Τα πλεονεκτήματα αυτών των συστημάτων είναι ότι αρχικά έχουν υψηλές ταχύτητες κρυπτογράφησης και αποκρυπτογράφησης. Το μέγεθος του κρυπτογραφήματος είναι αρκετά μικρότερο από το αρχικό κείμενο και τα κλειδιά που χρησιμοποιεί έχουν μικρότερο μήκος. Επίσης έχει μικρές απαιτήσεις σε μνήμη αλλά και σε υπολογιστική ισχύ. Εφαρμόζεται σε περιβάλλοντα όπως τα κινητά τηλέφωνα ή οι έξυπνες κάρτες. Ακόμη οι κρυπταλγόριθμοι αυτών των συστημάτων μπορούν να χρησιμοποιηθούν στην κατασκευή γεννητριών ψευδοτυχαίων αριθμών και στις ψηφιακές υπογραφές.

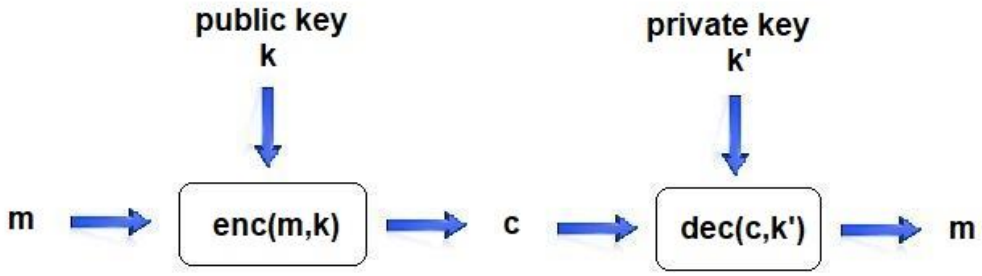
Τα μειονεκτήματα που έχουν είναι ότι ο αποστολέας και ο παραλήπτης πρέπει να κρατήσουν κρυφό το κοινό τους κλειδί από τους άλλους χρήστες. Γι' αυτό το λόγο το κλειδί πρέπει για λόγους ασφαλείας να αλλάζει αρκετά συχνά. Ακόμα σε πολύ μεγάλα δίκτυα χρειάζεται και ένα τρίτο άτομο έμπιστο και από τις δύο πλευρές, το οποίο θα διαχειρίζεται τα κλειδιά.

-

## 1.5 Ασύμμετρα κρυπτοσυστήματα

### 1.5.1 Γενικές αρχές

Στα ασύμμετρα κρυπτοσυστήματα έχουμε ως βάση ένα ζεύγος κλειδιών. Το ένα κλειδί του ζεύγους αυτού είναι δημόσιο και διαθέσιμο για την κρυπτογράφηση των δεδομένων και το άλλο είναι ιδιωτικό, δεν το γνωρίζουν όλοι και χρησιμοποιείται για την αποκρυπτογράφηση των δεδομένων. Τα κλειδιά αυτά τα συνδέει κάποια μαθηματική σχέση αλλά είναι ελάχιστα διαφορετικά μεταξύ τους. Παρόλα αυτά οι δύο αυτοί αριθμοί προκύπτουν με τέτοιο τρόπο ώστε να αποτρέπεται η παραγωγή του ιδιωτικού εάν ξέρουμε το δημόσιο και γενικά να είναι αδύναμο πρακτικά να γίνει αυτό από ένα σύγχρονο υπολογιστή.




Χαρακτηριστικά δημοσίου και ιδιωτικού κλειδιού

- Και τα δύο κλειδιά είναι δυαδικά αλφαριθμητικά
- Η δημιουργία και των δύο γίνεται από συναρτήσεις που δέχονται ως είσοδο ένα τυχαίο μεγάλο αριθμό και δίνουν ως έξοδο ένα ζεύγος κλειδιών
- Τα κλειδιά σχετίζονται με τέτοιο τρόπο μεταξύ τους ώστε να χρησιμοποιούνται για κρυπτογράφηση και αποκρυπτογράφηση
- Και οι δύο κατηγορίες που ανήκουν σε ένα ζεύγος είναι συμπληρωματικά δηλαδή εάν γίνεται κρυπτογράφηση με το ένα μπορεί να γίνει αποκρυπτογράφηση με το άλλο

Πιο συγκεκριμένα το ιδιωτικό κλειδί είναι προσβάσιμο μόνο από τον ιδιοκτήτη του και πρέπει να προστατεύεται από αυτόν. Επίσης χρησιμοποιείται για τις ψηφιακές υπογραφές. Αντίθετα το δημόσιο κλειδί είναι προσβάσιμο από όλους άρα δεν χρειάζεται κάποια ιδιαίτερη προστασία. Ακόμα χρησιμοποιείται για την κρυπτογράφηση των μηνυμάτων και την πιστοποίηση των ψηφιακών υπογραφών. Τέλος η αποθήκευση του γίνεται μέσα σε ψηφιακά πιστοποιητικά.

### 1.5.2 Πλεονεκτήματα και Μειονεκτήματα ασύμμετρων κρυπτοσυστημάτων

Τα πλεονεκτήματα των ασύμμετρων κρυπτοσυστημάτων είναι η υψηλή ασφάλεια τους καθώς η παραποίηση του ιδιωτικού τους κλειδιού είναι δυσκολότερη . Άλλο ένα πλεονέκτημα τους είναι ότι η διαχείριση των κλειδιών που χρησιμοποιούν είναι πολύ ευκολότερη. Αντίθετα τα μειονεκτήματα που έχουν τα ασύμμετρα κρυπτοσυστήματα είναι ότι τα κλειδιά τους έχουν μεγάλο μέγεθος όπως και οι ψηφιακές υπογραφές. Επίσης οι ασσύμετροι κρυπταλγόριθμοι είναι αρκετά αργοί και γενικά κανένα σχήμα δεν έχει αποδειχθεί ως ασφαλή.

## 1.6 Βασικοί αλγόριθμοι της θεωρίας αριθμών

Σε αυτό το κεφάλαιο θα μελετηθούν οι σχετικοί αλγόριθμοι, οι οποίοι χρησιμοποιούνται στη κρυπτογραφία. Πιο συγκεκριμένα θα αναλυθούν η modular αριθμητική, ο αλγόριθμος του Ευκλείδη. Επίσης θα δοθεί ο ορισμός του επεκτατικού αλγορίθμου καθώς και η συνάρτηση του Euler.

### 1.6.1 Αρχή της modular αριθμητικής

Στα μαθηματικά η modular αριθμητική ή αλλιώς αριθμητική υπολοίπων είναι μια λειτουργία εύρεσης αριθμητικών υπολοίπων που αφορούν την Ευκλείδεια διαίρεση και συμβολίζεται με τη λέξη mod. Στη κρυπτογραφία η αριθμητική υπολοίπων χρησιμοποιείται σε πολλούς αλγόριθμους συμμετρικών κλειδιών και κυρίως στις λειτουργίες που έχουν σχέση με τα δημόσια κλειδιά.

Για ένα θετικό ακέραιο αριθμό n, δυο ακέραιοι a και b είναι ισοδύναμοι modulo n, εάν η διαφορά τους a-b είναι ακέραιο πολλαπλάσιο του n, δηλαδή διαιρείται από το n ή υπάρχει ένας ακέραιος k τέτοιος ώστε να ισχύει ότι :

$$a - b = k * n$$

και συμβολίζονται

$$a \equiv b \pmod{n}.$$

*Παράδειγμα 1.* Για να δείξουμε ότι το $56 \equiv 2 \pmod 3$ ακολουθώ τα παρακάτω βήματα:

Κάνω αφαίρεση του αριθμού 2 από το 56 και εάν ο αριθμός που θα βρω είναι πολλαπλάσιο του αριθμού 3 τότε ισχύει το παραπάνω.

$56 - 2 = 54$, το 54 είναι ακέραιο πολλαπλάσιο του 3, αφού $54 = 3 * 18$, $k=18$ , άρα $56 \equiv 2 \pmod 3$.

*Παράδειγμα 2.* Για να δείξω ότι 38 ≡ 14 (mod 12) ακολουθώ τα παρακάτω βήματα :

Κάνω αφαίρεση του αριθμού 14 από το 38 και εάν ο αριθμός που θα βρω είναι πολλαπλάσιο του αριθμού 12 τότε ισχύει το παραπάνω.

38 - 14 = 24, το 24 είναι ακέραιο πολλαπλάσιο του 12, αφού 24 = 2 * 12, k=2, άρα 38 ≡ 14 (mod 12).

### 1.6.2 Ο αλγόριθμος του Ευκλείδη

Στην θεωρία των αριθμών ασχολούμαστε με τα σύνολα των ακεραίων **Z=** {…,-2,-1,0,1,2,….} και των φυσικών αριθμών **N=**{0,1,2,…}. Βασική έννοια αποτελεί η έννοια της διαιρετότητας.

Διαιρέτης ενός αριθμού **a** λέγεται κάθε φυσικός αριθμός **k** για τον οποίο υπάρχει αντίστοιχα ένας αριθμός **m** ώστε να ισχύει ότι :

$$a = m * k$$

Κοινός διαιρέτης των αριθμών a και b λέγεται κάθε αριθμός, ο οποίος είναι ταυτόχρονα διαιρέτης του a και του b. Να υπάρχουν κάποιοι φυσικοί αριθμοί m, p και να ισχύει ότι:

$$a = m * k \quad \text{και} \quad b = p * k$$

Κάθε τυχαίο ζεύγος αριθμών **a, b** έχουν σίγουρα κοινό διαιρέτη τον αριθμό 1. Υπάρχουν βέβαια και αριθμοί που έχουν μοναδικό κοινό διαιρέτη τον αριθμό 1 και ονομάζονται πρώτοι μεταξύ τους ή σχετικά πρώτοι. Γενικά ένας αριθμός είναι πρώτος εάν διαιρείται μόνο από την μονάδα και τον εαυτό του.

Ο μέγιστος κοινός διαιρέτης μεταξύ δύο ακέραιων αριθμών είναι ένας αριθμός ο οποίος είναι ο μεγαλύτερος κοινός διαιρέτης μεταξύ των αριθμών αυτών. Για 2 αριθμούς **a** ,**b** ο κοινός διαιρέτης είναι μικρότερος ή και ίσος με τους αριθμούς **a** και **b** και συμβολίζεται με **gcd(a,b)** .

Στα μαθηματικά για την εύρεση του Μέγιστου κοινού διαιρέτη χρησιμοποιείται ένας αλγόριθμος, ο οποίος ονομάζεται αλγόριθμος του Ευκλείδη. Το όνομα του προέρχεται από τον Έλληνα μαθηματικό Ευκλείδη, ο οποίος και περιγράφει αυτόν τον αλγόριθμο στο βιβλίο του Στοιχεία. Ο αλγόριθμος του Ευκλείδη, στην απλή μορφή του, ξεκινά με ένα ζεύγος θετικών ακεραίων και σχηματίζει ένα νέο ζευγάρι που αποτελείται από το μικρότερο αριθμό και το υπόλοιπο της διαίρεσης του μεγαλύτερου με το μικρότερο αριθμό. Η διαδικασία επαναλαμβάνεται μέχρι ο ένας αριθμός του ζεύγους να είναι 0. Τότε ο άλλος αριθμός είναι ο μέγιστος κοινός διαιρέτης του αρχικού ζεύγους.

*Ο αλγόριθμος του Ευκλείδη*

Είσοδος: δύο ακέραιοι $r_0$ και $r_1$, με $r_0 \geq r_1$
Έξοδος: gcd ($r_0$ , $r_1$)
1. i=1
2. do
3. i = i + 1
4. $r_i = r_{i-2} \bmod r_{i-1}$

5. while ( $r_i \neq 0$ )

6. gcd ($r_0$ , $r_1$) = $r_{i-1}$

*Παράδειγμα 1.* Για να βρω το gcd(11,14) ακολουθώ τα παρακάτω βήματα:

Ξεκινάω βρίσκοντας το gcd του μικρότερου αριθμού με το υπόλοιπο της διαίρεσης του μεγαλύτερου με το μικρότερο και συνεχίζω την ίδια διαδικασία μέχρι ο ένας αριθμός του ζεύγους να είναι 0.

gcd ( 11,14 ) = gcd ( 11 , 14 mod 11 )
= gcd ( 11 , 3 )
= gcd ( 3 , 11 mod 3 )
= gcd ( 3 , 2 )
= gcd ( 2 , 3 mod 2 )
= gcd ( 2 , 1 )
= gcd ( 1 , 2 mod 1 )
= gcd ( 1 , 0)
= 1

Ισοδύναμα τον παραπάνω είναι ο εξής:

14 = 1*11+3 ==> mod ( 14, 11) = 3 gcd(14,11) = gcd( 11, 3)
11 = 3*3+2 ==> mod ( 11, 3) = 2 gcd(11, 3) = gcd( 3, 2)
3 = 1*2+1 ==> mod ( 3, 2 ) = 1 gcd(3, 2) = gcd( 2, 1)
2 = 2*1+0 ==> mod ( 2, 1) = 0 gcd(2, 1) = gcd( 1, 0) = 1

*Παράδειγμα 2.* Για να βρω το gcd(973, 301) ακολουθώ τα παρακάτω βήματα:

Με τον πρώτο τρόπο είναι βρίσκοντας το gcd του 301 με το υπόλοιπο της διαίρεσης του 973 με το 301 και συνεχίζω να βρίσκω τα ζεύγη των gcd μέχρι ο ένας αριθμός από τα ζεύγη να είναι 0

gcd ( 973,301 ) = gcd ( 301 , 973 mod 301 )
= gcd ( 301 , 70 )
= gcd ( 70 , 301 mod 70)
= gcd ( 70 , 21 )
= gcd ( 21 , 70 mod 21 )
= gcd ( 21 , 7 )
= gcd ( 7 , 21 mod 7 )
= gcd ( 7 , 0)
= 7

### 1.6.3 Ορισμός αντιστρόφου

Στα μαθηματικά ως αντίστροφο ενός αριθμού x θεωρούμε τον αριθμό που εάν το πολλαπλασιάσουμε με το x μας δίνει τη μονάδα και συμβολίζεται $x^{-1}$

$$x * x^{-1} = 1.$$

Ένας αριθμός a έχει αντίστροφο modulo m όταν ισχύει ότι gcd(a,m)=1 με m>1 και ισχύει ότι:

$$a * b \equiv 1 \bmod m,$$

όπου b είναι ο αντίστροφος του a και τον συμβολίζουμε $a^{-1} \bmod m$

*Παράδειγμα*. Για να βρω τον αντίστροφο του 4 modulo 15 λύνω ως εξής:

Αρχικά για να υπάρχει ο αντίστροφος του θα πρέπει το gcd(4,15) να ισούνται με το 1. Οπότε βρίσκω το gcd(4,15):

gcd( 4, 15) = gcd( 4, 15 mod 4)
= gcd( 4, 3)
= gcd( 3, 4 mod 3)
= gcd( 3, 1)
= gcd( 1, 3 mod1)
= gcd( 1, 0)
= 1

Αφού ισχύει η παραπάνω προϋπόθεση , θα πρέπει να βρω έναν αριθμό, ο οποίος εάν τον πολλαπλασιάσω με το 4 θα ισούται με 1 (mod 15).

$4 * b \equiv 1 \pmod{15} \rightarrow 4 * 4 \equiv 1 \pmod{15}$ άρα ο αντίστροφος $4^{-1} \equiv 4 \bmod 15$

### 1.6.4 Επεκτατικός αλγόριθμος του Ευκλείδη & υπολογισμός αντιστρόφου

Έστω ότι θέλουμε να βρούμε το μέγιστο κοινό διαιρέτη g = gcd(a,b) για δύο αριθμούς a, b και να βρούμε και δύο ακεραίους x, y για τους οποίους ισχύει ότι:

$$a * x+b * y = g.$$

Τότε χρησιμοποιούμε τον επεκτατικό αλγόριθμο του Ευκλείδη, ο οποίος ακολουθεί τα παρακάτω βήματα. Αρχικά κάνει διαίρεση των δύο αριθμών a και b και δίνει το a = k* b+r. Εάν ο αριθμός r είναι διάφορος του μηδενός, θέτουμε a=b και b=r και κάνουμε πάλι ίδια διαίρεση όπως με το a και b. Αυτή η διαδικασία συνεχίζεται μέχρι να βρεθεί ένα r που να είναι 0. Το τελευταίο μη μηδενικό υπόλοιπο που θα πάρουμε θα είναι ο μέγιστος κοινός διαιρέτης g.

Από τις σχέσεις που θα έχουν δημιουργηθεί μέχρι να βρεθεί ο μέγιστος κοινός διαιρέτης, εάν τις χρησιμοποιήσουμε ανάποδα, ξεκινώντας από την προτελευταία θα βρούμε τα x και y που θέλουμε.

*Παράδειγμα 1.* Για να βρούμε για δύο αριθμούς a=1925 και b=693, τους αριθμούς x,y για τους οποίους ισχύει ότι:

$$ax+by = g$$

κάνουμε τα εξής βήματα. Αρχικά βρίσκουμε το μέγιστο κοινό διαιρέτη των αριθμών a,b μέσω του αλγορίθμου του Ευκλείδη .

$$1925 = 2 * 693 + 539 \quad (1)$$
$$693 = 1 * 539 + 154 \quad (2)$$
$$539 = 3 * 154 + 77 \quad (3)$$
$$154 = 2 * 77 \quad (4)$$

Άρα ο μέγιστος κοινός διαιρέτης είναι το 77.

Έπειτα ξεκινάω από την προτελευταία σχέση και αναλύω το υπόλοιπο της, με βάση αυτή τη σχέση δηλαδή στο παράδειγμα μας

$$77 = 539 – 3 * 154$$

Συνεχίζω και αναλύω τα άγνωστα στοιχεία, με τη σειρά που τα βρίσκω στις αμέσως προηγούμενες σχέσεις και έχουμε ότι:

$$77 = 539 – 3 * 154$$
$$= 539 – 3 * (693 – 1 * 539)$$
$$= 539 – 3 * 693 + 3*539$$
$$= 4 * 539 – 3 * 693$$
$$= 4 * (1925 – 2 * 693) – 3 * 693$$

$= 4 * 1925 – 8 * 693 – 3 * 693$
$= \mathbf{4} * 1925 – \mathbf{11} * 693$

Άρα με βάση τη μορφή ax+by=g το x = 4 και το y = -11

*Παράδειγμα 2.* Για να βρούμε για δύο αριθμούς a=1210 και b=340, τους αριθμούς x,y για τους οποίους ισχύει ότι:

$$ax+by=g$$

κάνουμε τα εξής βήματα. Αρχικά βρίσκουμε το μέγιστο κοινό διαιρέτη των αριθμών a,b μέσω του αλγορίθμου του Ευκλείδη .

$1210 = 3 * 340 + 190$ (1)
$340 = 1 * 190 + 150$ (2)
$190 = 1 * 150 + 40$ (3)
$150 = 3 * 40 + 30$ (4)
$40 = 1 * 30 + 10$ (5)
$30 = 3 * 10$ (6)

Άρα ο μέγιστος κοινός διαιρέτης είναι το 10.

Έπειτα ξεκινάω από την προτελευταία σχέση και αναλύω το υπόλοιπο της, με βάση αυτή τη σχέση δηλαδή στο παράδειγμα μας

$$10 = 40 – 1 * 30$$

Συνεχίζω αναλύωντας τα άγνωστα στοιχεία, με τη σειρά που τα βρίσκω στις αμέσως προηγούμενες σχέσεις και έχουμε ότι:

$10 = 40 – 1 * 30$
$= 40 – 1 * ( 150 – 3 * 40 )$
$= 4 * 40 – 1 * 150$
$= 4 * ( 190 – 1 * 150 ) – 1 * 150$
$= 4 * 190 – 4 * 150 – 1 * 150$
$= 4 * 190 – 5 * 150$
$= 4 * 190 – 5 * ( 340 – 1 * 190 )$
$= 4 * 190 – 5 * 340 + 5 * 190$
$= 9 * 190 – 5 * 340$
$= 9 * ( 1210 – 3 * 340 ) – 5 * 340$
$= 9 * 1210 – 27 * 340 – 5 * 340$
$= \mathbf{9} * 1210 – \mathbf{32} * 340$

Άρα με βάση τη μορφή ax+by=g το x= 9 και το y= -32

### 1.6.5 Συνάρτηση Euler

| Η συνάρτηση φ(n), για κάθε θετικό ακέραιο n, δηλώνει τον αριθμό των θετικών ακεραίων που είναι μικρότεροι ή ίσοι με το n και σχετικά πρώτοι με τον n. |
|---|

Η συνάρτηση του Euler έχει και κάποιες ιδιότητες . Αρχικά εάν ο n είναι πρώτος αριθμός τότε:

$$\varphi(n)=n-1 .$$

Εάν το φ(n)=0 τότε το n=0 και αντίστροφα και το ίδιο ισχύει για το φ(1)=1.

Επίσης εάν ο p και ο q είναι πρώτοι αριθμοί με $p \neq q$ , τότε το γινόμενο τους είναι :

$$n = p * q$$

και $$\varphi(n) = \varphi(p * q) = \varphi(p) * \varphi(q) = (p - 1) * (q - 1)$$

Εάν ο p είναι πρώτος και το $k \geq 1$, τότε :

$$\varphi(p^k)=p^k - p^{k-1} = p^{k-1}(p-1)$$

Ακόμη εάν gcd(a, b)=1, τότε:

$$\varphi(a * b)=\varphi(a) * \varphi(b)$$

δηλαδή η συνάρτηση φ(n) είναι πολλαπλασιαστική.

Τέλος εάν ισχύει ότι gcd(a, n)=1 και a είναι φυσικός αριθμός τότε:

$$a^{\varphi(n)} \equiv 1 \pmod n$$

*Παράδειγμα 1.* Για να βρω το φ(n) για ακέραιο n=6 ακολουθώ τα εξής βήματα:

Αρχικά βρίσκω τη συσχετισμένη ομάδα, η οποία αποτελείται από τους αριθμούς 0 εώς n-1 , άρα για το παράδειγμα αυτό είναι το Z6={0,1,2,3,4,5}. Έπειτα βρίσκω το gcd για τα ζεύγη που αποτελούνται από τους παραπανω αριθμούς και το n . Άρα :

gcd(0,6)=6
gcd(1,6)=1 *1ο*
gcd(2,6)=2
gcd(3,6)=3
gcd(4,6)=2
gcd(5,6)=1 *2ο*

Στην ομάδα αυτή υπάρχουν 2 αριθμοί, οι οποίοι είναι μικρότεροι και σχετικά πρώτοι με το 6 δηλαδή το n, άρα φ(6)=2 .

*Παράδειγμα 2.* Για να βρω το φ(n) για ακέραιο n=8 ακολουθώ τα εξής βήματα:

Αρχικά βρίσκω τη συσχετισμένη ομάδα, η οποία είναι η Z8={0,1,2,3,4,5,6,7}
Μετά υπολογίζω τα gcd για τα ζεύγη που αποτελούνται από τους παραπανω αριθμούς και το 8, άρα :

gcd(0,8)=8
gcd(1,8)=1 *1ο*
gcd(2,8)=2
gcd(3,8)=1 *2ο*
gcd(4,8)=4
gcd(5,8)=1 *3ο*
gcd(6,8)=2
gcd(7,8)=1 *4ο*

Στην ομάδα αυτή υπάρχουν 4 αριθμοί, οι οποίοι είναι μικρότεροι και σχετικά πρώτοι με το 8, άρα φ(8)=4

Ο υπολογισμός της συνάρτησης Euler όταν οι αριθμοί είναι μικροί, υπολογίζονται εύκολα όπως στα παραπάνω παραδείγματα. Εάν οι αριθμοί είναι μεγάλοι τότε η διαδικασία υπολογισμού του gcd, θα είναι πολύ αργή. Για αυτό το λόγο χρησιμοποιείται ένα άλλο θεώρημα.

**Θεώρημα**

Έστω ότι n ένας ακέραιος αριθμός με την εξής παραγοντοποίηση

$$n = p_1^{k_1} * p_2^{k_2} * .... * p_i^{k_i}$$

όπου pi είναι πρώτοι αριθμοί και ki πιθανοί ακέραιοι, τότε ισχύει ότι :

$$\varphi(n) = p_1^{k_1-1}(p_1-1) * p_2^{k_2-1}(p_2-1) * .... * p_i^{k_i-1}(p_i-1)$$

$$= n\left(1-\frac{1}{p_1}\right) * \left(1-\frac{1}{p_2}\right) * .... * \left(1-\frac{1}{p_i}\right)$$

Άρα ισχύει ότι :

$$\phi(n) = n\prod_{p|n}\left(1-\frac{1}{p}\right)$$

*Παράδειγμα.* Για να υπολογίσω το φ(n) για n=240 κάνω τις εξής ενέργειες:

Για αρχή βρίσκω για τον αριθμό n, ο οποίος στο παράδειγμα μας είναι το 240, πως μπορώ να το παραγοντοποιήσω για να έχει τη μορφή αριθμών με δυνάμεις τύπου

$$p_1^{k_1} * p_2^{k_2} * p_3^{k_3}$$

Άρα

$$n = 240 = 16 * 15 = 2^4 * 3^1 * 5^1$$

Για να υπολογίσω το φ(240) θα ακολουθήσω τους πολλαπλασιασμούς που ορίζει το παραπάνω θεώρημα. Άρα:

$$\begin{aligned}\varphi(n) &= 240\left(1-\frac{1}{2}\right) * \left(1-\frac{1}{3}\right) * \left(1-\frac{1}{5}\right) \\ &= 240\left(\frac{2}{2}-\frac{1}{2}\right) * \left(\frac{3}{3}-\frac{1}{3}\right) * \left(\frac{5}{5}-\frac{1}{5}\right) \\ &= 240\left(\frac{1}{2}\right) * \left(\frac{2}{3}\right) * \left(\frac{4}{5}\right) = 240\left(\frac{8}{30}\right) = 64\end{aligned}$$

Αυτό σημαίνει ότι ο αριθμός των ακεραίων στο διάστημα [0,239], οι οποίοι είναι σχετικά πρώτοι με το 240 είναι 64.

-

-

# *2. ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΑ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ*

Σε αυτό το κεφάλαιο αναλύονται οι αλγόριθμοι RSA και ElGamal, οι οποίοι είναι οι δύο βασικοί αλγόριθμοι αυτής της εργασίας. Δίνονται τα βήματα που ακολουθούν κατά τη διάρκεια της κρυπτογράφησης και αποκρυπτογράφησης των διάφορων μηνυμάτων. Επίσης δίνονται τα πλεονεκτήματα και τα μειονεκτήματα των αντίστοιχων αλγορίθμων καθώς και τα είδη των επιθέσεων που μπορούν να δεχτούν.

## 2.1 Γενικές αρχές

Η δημιουργία αυτού του είδους των κρυπτοσυστημάτων αποτελεί σημαντική ανακάλυψη στην ιστορία της κρυπτογραφίας. Ως ιδέα η κρυπτογραφία δημοσίου κλειδιού διατυπώθηκε από τους Diffie και Hellman το 1976. Στα ασύμμετρα κρυπτοσυστήματα έχουμε ως βάση ένα ζεύγος κλειδιών. Το ένα κλειδί του ζεύγους αυτού είναι δημόσιο και διαθέσιμο για την κρυπτογράφηση των δεδομένων και το άλλο είναι ιδιωτικό, δεν το γνωρίζουν όλοι και χρησιμοποιείται για την αποκρυπτογράφηση των δεδομένων. Τα κλειδιά αυτά τα συνδέει κάποια μαθηματική σχέση αλλά είναι ελάχιστα διαφορετικά μεταξύ τους. Παρόλα αυτά οι δύο αυτοί αριθμοί προκύπτουν με τέτοιο τρόπο ώστε να αποτρέπεται η παραγωγή του ιδιωτικού εάν ξέρουμε το δημόσιο και γενικά να είναι αδύναμο πρακτικά να γίνει αυτό από ένα σύγχρονο υπολογιστή. Για την επικοινωνία των διαφόρων οντοτήτων μέσα σε ένα κρυπτοσύστημα χρειάζεται κάποιος αριθμός κλειδιών ανάλογος του $n^2$ .

## 2.2 Κρυπτοσύστημα RSA

Ένα από τα πιο διαδεδομένα κρυπτοσυστήματα δημοσίου κλειδιού είναι το κρυπτοσύστημα RSA. Το όνομα του προέρχεται από τα αρχικά των ονομάτων των δημιουργών του, τους Ron Rivest, Adi Shamir και Leonard Adleman. Ο αλγόριθμος αυτός χρησιμοποιείται για την κρυπτογράφηση και την αποκρυπτογράφηση δεδομένων, την ασφαλή μεταφορά κλειδιών και την δημιουργία ψηφιακών υπογραφών. Επίσης έχει ως βάση την θεωρία των αριθμών.

### 2.2.1 Αλγόριθμος Κρυπτογράφησης και Αποκρυπτογράφησης

ΚΡΥΠΤΟΓΡΑΦΗΣΗ

1. Ζητάμε το δημόσιο κλειδί Kpub=(n,e)
2. Αναπαριστάμε το μήνυμα m που θέλουμε να στείλουμε ως ακέραιο στο Zn=$\{0,1,\ldots,n-1\}$
3. Υπολογίζουμε το κρυπτοκείμενο $c=m^e \bmod n$
4. Στέλνουμε το c στον παραλήπτη

ΑΠΟΚΡΥΠΤΟΓΡΑΦΗΣΗ

Υπολογίζουμε το $m=c^d \bmod n$ με το ιδιωτικό κλειδί Kpr=d

### 2.2.2 Παραγωγή κλειδιών

Το ιδιωτικό κλειδί είναι το Kpr=d και το δημόσιο κλειδί είναι το Kpubl=(n,e) .

Επιλέγουμε δύο μεγάλους πρώτους αριθμούς p και q ίδιου μεγέθους
Υπολογίζουμε το n όπου

$$n = p * q$$

Υπολογίζουμε την συνάρτηση φ(n)

$$\varphi(n)= (p-1) * (q-1)$$

Επιλέγουμε έναν ακέραιο e, όπου $1 < e < \varphi(n)$, έτσι ώστε να ισχύει ότι

$$gcd(e,\varphi(n))=1$$

Υπολογίζουμε το ιδιωτικό κλειδί d, έτσι ώστε να είναι αντίστροφος του e mod φ(n), δηλαδή να ισχύει:

$$d * e = 1 \bmod \varphi(n)$$
$$d = e^{-1} \bmod \varphi(n)$$

Ο αλγόριθμος RSA είναι αρκετά ασφαλής όσο το n δεν μπορεί να παραγοντοποιηθεί εύκολα μιας και η ασφάλεια αυτού του αλγορίθμου βασίζεται στη δυσκολία να παραγοντοποιήσει σε πρώτους παράγοντες πολύ μεγάλους αριθμούς. Για το λόγο αυτό θέλουμε να παράγουμε πολύ μεγάλους πρώτους αριθμούς. Τα κλειδιά που χρησιμοποιούνται σήμερα είναι πολύ μεγάλα (>768 bits) με ελάχιστο προτεινόμενο μέγεθος σήμερα τα 2048 bits. Δεδομένου ότι το n=p*q , τότε οι δύο αυτοί πρώτοι αριθμοί p,q θα πρέπει να έχουν το μισό σε μήκος bit από το n.

Εάν θέλουμε να ρυθμίσουμε για παράδειγμα το RSA με μέτρο μήκους

$$\log_2 n = 1024 \text{ bit},$$

τότε τα p και q πρέπει να έχουν μήκος bit περίπου 512 bit.

### 2.2.3 Γρήγορη ύψωση σε δύναμη

Στην κρυπτογράφηση και αποκρυπτογράφηση RSA παρατηρούμε ότι βασίζονται σε δυνάμεις modular.

$$c = m^e \bmod n \quad \text{και} \quad m = c^d \bmod n$$

Ένας γρήγορος τρόπος δυνάμεων θα ήταν

$$x \xrightarrow{sq} x^2 \xrightarrow{mul} x^3 \xrightarrow{mul} x^4$$

όπου sq είναι ο τετραγωνισμός (squaring) δηλαδή η ύψωση σε δύναμη του 2 (squaring) και mul είναι ο πολλαπλασιασμός (multiplication).

*Παράδειγμα 1.* Για να βρω πόσοι πολλαπλασιασμοί χρειάζονται για να υπολογίσουμε την έκθεση $x^8$ όπου είναι δύναμη του 2 κάνω το εξής:

$$x \xrightarrow{sq} x^2 \xrightarrow{mul} x^3 \xrightarrow{mul} x^4 \xrightarrow{mul} x^5 \xrightarrow{mul} x^6 \xrightarrow{mul} x^7 \xrightarrow{mul} x^8$$

Με αυτό τον τρόπο χρειαζόμαστε 7 πολλαπλασιασμούς και 1 τετραγωνισμό.
Εναλλακτικά, με ένα πιο γρήγορο τρόπο:

$$x \xrightarrow{sq} x^2 \xrightarrow{sq} x^4 \xrightarrow{sq} x^8$$

άρα με αυτό τον τρόπο χρειαζόμαστε μόνο 3 τετραγωνισμούς.

Δυστυχώς οι αριθμοί e και d είναι πολύ μεγάλοι και οι εκθέσεις τους και δεν είναι τόσο απλοί υπολογισμοί όσο οι εκθέσεις που είναι δυνάμεις του 2. Βέβαια υπάρχει μία μέθοδος, η οποία ονομάζεται αλγόριθμος square and multiply, ο οποίος είναι πιο γρήγορος και αποδοτικός για τέτοιους υπολογισμούς.
Ο αλγόριθμος βασίζεται στη σάρωση του bit του εκθέτη από τα αριστερά προς τα δεξιά. Σε κάθε επανάληψη, δηλαδή, για κάθε δυφίο εκθέτων, το τρέχον αποτέλεσμα είναι τετράγωνο. Εάν και μόνο εάν το bit του εκθέματος που έχει σαρωθεί έχει την τιμή 1, ένας πολλαπλασιασμός του τρέχοντος αποτελέσματος με το x εκτελείται ακολουθώντας τετραγωνισμό.

**Αλγόριθμος square and multiply**

Είσοδος: στοιχείο βάσης x, εκθέτες

$$\sum_{i=0}^{t} h_i\, 2^i \qquad , \qquad h_i \in 0, 1 \;\; \kappa\alpha\iota \;\; h_t = 1$$

και modulus n.

ΒΗΜΑΤΑ
1. for i=t-1 to 0
2. $r=r^2$ mod n
3. if hi=1
4. $r=r * x$ mod n
5. return (r)

Έξοδος: $x^H$ mod n

*Μετατροπή από δεκαδική σε δυαδική μορφή.*

Το δεκαδικό σύστημα έχει ως βάση το 10, χρησιμοποιεί δηλαδή τα δέκα ψηφία (0,1,…,9) ενώ το δυαδικό σύστημα χρησιμοποιεί τα δύο ψηφία το 0 και το 1, τα οποία αποτελούν δυνάμεις του 2. Για να μετατρέπουμε έναν αριθμό από το δεκαδικό σύστημα στο δυαδικό ακολουθούμε το παρακάτω αλγόριθμο:

1. Κάνουμε διαίρεση του αρχικού αριθμού με το 2

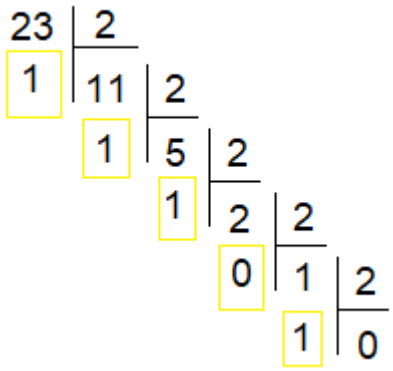
2. Σημειώνουμε το υπόλοιπο και διαιρούμε πάλι το πηλίκο με το 2

3. Επαναλαμβάνουμε το 2ο βήμα για όσο το πηλίκο είναι μεγαλύτερο του 0

4.Ο δυαδικός αριθμός που ψάχνουμε αποτελείται από τα υπόλοιπα των διαιρέσεων ξεκινώντας από το τελευταίο και πηγαίνοντας προς το πρώτο.

*Παράδειγμα 1.* Για να μετατρέψω το 23 σε δυαδικό εργάζομαι ως εξής :

Ξεκινάω με διαίρεση του αρχικού αριθμού με το 2 και συνεχίζω με διαδοχικές διαιρέσεις των πηλίκων τους.




Άρα το 23 γίνεται 10111.

*Παράδειγμα 2.* Για να υπολογίσω το $4^{13}$ mod 5 ακολουθώ τα εξής βήματα :

Αρχικά μετατρέπω τον εκθέτη από δεκαδικό σε δυαδικό δηλαδή 13= 1101

Ο αριθμός 0 αντιπροσωπεύει την ύψωση στο τετράγωνο και ο αριθμός 1 αντιπροσωπεύει την ύψωση στο τετράγωνο μαζί με πολλαπλασιασμό.

$0=S \rightarrow (\ ^2)$
$1=SM \rightarrow (\ ^2 * x)$

S=square (τετραγωνισμός) , M=multiply (πολλαπλασιασμός)

Έπειτα αναλύω τον εκθέτη με βάση τα σύμβολα που αντιπροσωπεύει :

1 1 0 1 → SM SM S SM

Άρα

$( ( (1^2 * x)^2 * x )^2 )^2 * x$

Το x είναι η βάση της δύναμης άρα αντικαθιστώ όπου x το 4.

$((1^2 * 4)^2 * 4)^2 )^2 * 4 = ((4)^2 * 4)^2 )^2 * 4$

$= ((16 * 4)^2 )^2 * 4$

$= ((64)^2 )^2 * 4$

$= (4096)^2 * 4$

$= 16777216 * 4 = 67108864$

Όταν στις δυνάμεις έχουμε modulo n=5 τότε χρησιμοποιούμε το mod 5 σε κάθε σχέση άρα :

((((((4$^2$ mod 5) * 4) mod 5)$^2$ mod 5)$^2$ mod 5) * 4) mod 5

= ((((((16 mod 5) * 4) mod 5)$^2$ mod 5)$^2$ mod 5) * 4) mod 5

= ((((((1) * 4) mod 5)$^2$ mod 5)$^2$ mod 5) * 4) mod 5

= (((((4) mod 5)$^2$ mod 5)$^2$ mod 5) * 4) mod 5

= ((((4)$^2$ mod 5)$^2$ mod 5) * 4) mod 5

= (((16 mod 5)$^2$ mod 5) * 4) mod 5

= (((1)$^2$ mod 5) * 4) mod 5

= ((1 mod 5) * 4) mod 5

= ((1 mod 5) * 4) mod 5

= ((1 mod 5) * 4) mod 5

= (1* 4) mod 5 = 4 mod 5 = 4

### 2.2.4 Κινέζικο θεώρημα

Έστω

$m_1, \ldots, m_k$

θετικοί ακέραιοι, οι οποίοι ανά δύο σχετικά πρώτοι μεταξύ τους και μεγαλύτεροι του 1. Για οποιοδήποτε ακεραίους

$a_1,\ldots,a_k$

υπάρχει x, το οποίο επαληθεύει τις παρακάτω ισοδυναμίες:

$$x \equiv a_1 \pmod{m_1} \ , \ x \equiv a_2 \pmod{m_2} \ , \ldots , \ x \equiv a_k \pmod{m_k}$$

Και έχει μοναδική λύση modulo n = $n_1$* $n_2$ * …* $n_k$.

Ο αλγόριθμος Gauss μπορεί να υπολογίσει τη λύση των παραπάνω ισοδυναμιών μέσω του τύπου:

$$\sum_{i=1}^{k} a_i N_i M_i \pmod{n} \quad , \text{όπου} \ \ N_i = \frac{n}{n_i} \ \ \text{και} \ \ M_i = N^{-1}_{n} \pmod{n_i}$$

Μέσω της παραπάνω σχέσης ουσιαστικά μπορούμε να βρούμε τον αριθμό x εάν είναι σπασμένος σε r μέρη με την προϋπόθεση το κάθε μέρος r να ανήκει σε μία κυκλική ομάδα Zmi .
Παράδειγμα 1. Βρες την λύση του παρακάτω συστήματος .

$x \equiv 1 \bmod 3$
$x \equiv 2 \bmod 4$
$x \equiv 3 \bmod 5$

Επειδή οι αριθμοί 3,4,5 είναι πρώτοι μεταξύ τους το σύστημα έχει μοναδική λύση το mod 60 γιατί 3*4*5=60.

$N_1 = 60/3 = 20$
$N_2 = 60/4 = 15$
$N_3 = 60/5 = 12$

Βρίσκουμε και τα αντίστροφα των παραπάνω στοιχείων $N_1$, $N_2$, $N_3$.

Για τον αντίστροφο $N_1$ αναζητούμε ένα $M_1$, τέτοιο ώστε:

$$N_1 * M_1 \equiv 1 \bmod 3.$$

Βρίσκουμε ότι $M_1 = 2$.
Αντίστοιχα οι αντίστροφοι των $N_2$ και $N_3$ είναι $M_2 = 3$ και $M_3 = 3$.
Συνεπώς η λύση του αρχικού συστήματος είναι:

$x \equiv 1 * 20 * 2 + 2 * 15 * 3 + 3 * 12 * 3 \pmod{60}$
$\equiv 40 + 90 + 108 \pmod{60}$
$\equiv 10 + 30 + 48 \bmod 60$
$\equiv 118 \pmod{60} \equiv 58 \pmod{60}$

## 2.2.5 Το μικρό θεώρημα του Fermat και το τεστ πρωτοτυπίας του.

Για να αποφασίσουμε ποιοι τυχαίοι μεγάλοι ακέραιοι είναι και πρώτοι προκειμένου να τους χρησιμοποιήσουμε στην παραγωγή κλειδιών μπορούμε να χρησιμοποιήσουμε το τεστ πρωτοτυπίας του Fermat, το οποίο βασίζεται στο μικρό θεώρημα του Fermat . Το μικρό θεώρημα του Fermat είναι χρήσιμο για δοκιμές πρωτοτυπίας και σε πολλές άλλες πτυχές της κρυπτογραφίας δημόσιου κλειδιού.

**Θεώρημα**

Έστω a ένας ακέραιος και p ένας πρώτος αριθμός τότε θα ισχύει ότι :

$$a^p \equiv a \pmod p$$

Βέβαια στη κρυπτογραφία μπορεί να δοθεί με τη μορφή:

$$a^{p-1} \equiv 1 \pmod{p}$$

## 2.2.6 Παράδειγμα Κρυπτογράφησης- Αποκρυπτογράφησης RSA

*ΠΑΡΑΔΕΙΓΜΑ.* Για να κρυπτογραφήσω και να αποκρυπτογραφήσω ένα μήνυμα m=4 με $k_{pub}$ και $k_{pr}$ της επιλογής μου ακολουθώ τα παρακάτω βήματα:

Για τη δημιουργία κλειδιών αρχικά επιλέγω δύο αριθμούς p, q , οι οποίοι να είναι μεταξύ τους πρώτοι δηλαδή να έχουν μέγιστο κοινό διαιρέτη μεταξύ τους τον αριθμό 1.

Θέτω :

$$p=4 \quad \text{και} \quad q=9$$

gcd(4,9) = gcd (4 , 9 mod 4)
= gcd (4 , 1)
= gcd (1 , 4 mod 1)
= gcd (1 , 0)
= 1

Άρα είναι μεταξύ τους πρώτοι.

Έπειτα υπολογίζω :

$$n = p * q = 4 * 9 = 36$$

$$\varphi(n) = (p-1) * (q-1) = (4-1) * (9-1) = 3 * 8 = 24$$

Επιλέγω έναν ακέραιο e όπου

$$1 < e < \varphi(n) \rightarrow 1 < e < 24$$

και για τον οποίο ισχύει ότι :

$$\gcd(e, \varphi(n)) = 1 \rightarrow \gcd(e,24) = 1$$

Επιλέγω e=5

gcd(5,24) = gcd (5 , 24 mod 5)
= gcd (5 , 4)
= gcd (4 , 5 mod 4)
= gcd (4 , 1)
= gcd (1 , 4 mod 1)
= gcd (1 , 0)
= 1 Άρα σωστή επιλογή

-

Μέχρι στιγμής βρήκα το Kpub ( n , e) → Kpub=(36,5)

Για να βρω το Kpr(d) κάνω τις εξής ενέργειες :

Για τον αριθμό d ισχύει ότι:

$$1< d < \varphi(n)$$

$d * e = 1 \bmod \varphi(n) \rightarrow d * 5 = 1 \bmod 24$

για d=5

$5 * 5 = 1 \bmod 24$

$25 = 1 \bmod 24$ ισχύει

άρα Kpr=(5)

Αφού βρήκαμε τα κλειδιά συνεχίζουμε στις διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης του μηνύματος.

**ΚΡΥΠΤΟΓΡΑΦΗΣΗ**

Το κρυπτοκείμενο c προκύπτει ως :

$c= m^e \bmod n$ άρα $c= 4^5 \bmod 36$

επειδή το 5 είναι μεγάλος αριθμός για δύναμη θα χρησιμοποιήσω τον αλγόριθμο square and multiply

το 5 στο δυαδικό είναι 101 → SM S SM

$$(((1^2 * x)^2)^2 * x)$$

Το x είναι η βάση μας άρα το 4

$$(((1^2 * 4)^2)^2 * 4) = (((4)^2)^2) * 4)$$

$$= (16)^2 * 4 = 256 * 4$$

$$= 1024$$

άρα $c= 1024 \bmod 36 = 16$

**ΑΠΟΚΡΥΠΤΟΓΡΑΦΗΣΗ**

Με βάση το d για να αποκρυπτογραφήσουμε το κρυπτοκείμενο υπολογίζω :

$m= c^d \bmod n$ άρα $m= 16^5 \bmod 33$

επειδή το 5 είναι μεγάλος αριθμός για δύναμη θα χρησιμοποιήσω τον αλγόριθμο square and multiply μαζί με modulus 33

το 5 στο δυαδικό είναι 101 → SM S SM

$$(((1^2 * x)^2)^2 * x)$$

Μαζί με το mod 36 γίνεται :

$$(((((((\ 1^2\ ) \bmod 36) * x\ ) \bmod 36\ )^2 \bmod 36\ )^2 \bmod 36) * x) \bmod 36)$$

Το x είναι η βάση μας άρα το 16

$= (((((((\ 1^2\ ) \bmod 36\ ) * 16\ ) \bmod 36\ )^2 \bmod 36\ )^2 \bmod 36\ ) * 16\ ) \bmod 36\ )$

$= (((((((\ 1\ ) * 16\ ) \bmod 36\ )^2 \bmod 36\ )^2 \bmod 36\ ) * 16\ ) \bmod 36\ )$

$= (((((\ 16\ ) \bmod 36\ )^2 \bmod 36\ )^2 \bmod 36\ ) * 16\ ) \bmod 36\ )$

$= (((((\ 16\ \ )^2 \bmod 36\ )^2 \bmod 36\ ) * 16\ ) \bmod 36\ )$

$= ((((\ 256 \bmod 36\ )^2 \bmod 36\ ) * 16\ ) \bmod 36\ )$

$= ((((\ 4\ )^2 \bmod 36\ ) * 16\ ) \bmod 36\ )$

$= (((\ 16 \bmod 36\ ) * 16\ ) \bmod 36\ )$

$= (((\ 16\ ) * 16\ ) \bmod 36\ )$

$= ((\ 256\ ) \bmod 36\ ) = 4$

άρα c = 4

## 2.2.7 Πλεονεκτήματα και Μειονεκτήματα RSA

Ο αλγόριθμος RSA παρέχει κάποια πλεονεκτήματα, τα οποία βοηθούν σε διάφορες λειτουργίες. Αρχικά ο αριθμός των χρηστών και ο αριθμός των κλειδιών συνδέονται μεταξύ τους γραμμικά και αυτό έχει ως αποτέλεσμα η διαχείριση των κλειδιών να γίνεται με πιο εύκολο τρόπο. Άρα βασικό πλεονέκτημα είναι η απλοποίηση που προσφέρει στο πρόβλημα διαχείρισης των κλειδιών. Ακόμα είναι πιο ενισχυμένη η ασφάλεια των συναλλαγών καθώς

κάθε χρήστης μπορεί να δημιουργεί το δικό του ζεύγος κλειδιών. Το ένα κλειδί είναι ιδιωτικό, το ξέρει μόνο ο χρήστης, άρα δεν χρειάζεται ένα ασφαλές μέσο για να σταλεί στον παραλήπτη. Το άλλο κλειδί είναι δημόσιο άρα μπορεί να μεταφερθεί με οποιοδήποτε τρόπο.

Τα μειονεκτήματα του αλγορίθμου RSA είναι ότι θεωρείται αρκετά αργός εν σχέση με τους αλγορίθμους των μυστικών κλειδιών και αυτό γιατί είναι αργοί οι υπολογισμοί που χρειάζονται, ιδιαίτερα όταν γίνονται και από τον ίδιο υπολογιστή. Επίσης δεν έχει δοθεί κάποια απόδειξη ότι ο κώδικας του δεν ‘’σπάει ‘’ άρα δεν μπορεί να θεωρηθεί και τέλειος αλγόριθμος.

### 2.2.7 Πιθανές επιθέσεις στον RSA

Μία επίθεση κατά του RSA είναι η επίθεση επανάληψης όπου κατά την διάρκεια αυτής της επίθεσης, το κείμενο αποκρυπτογραφείται συνέχεια προσπαθώντας να βρεθεί το αρχικό κείμενο. Πολλές επαναλήψεις μπορούν να κάνουν σωστά αποκρυπτογράφηση. Η ταχύτητα αυτής της μεθόδου όμως είναι πολύ μικρή και πολλές φορές μη-πρακτική ιδιαίτερα εάν το μήκος του κλειδιού είναι πολύ μεγάλο.

Επίσης μια ακόμα επίθεση είναι η παραγοντοποίηση δημοσίου κλειδιού όπου κάθε εισβολέας θέλει να ανακτήσει μέσω ενός κρυπτοκειμένου και του δημοσίου κλειδιού του παραλήπτη (e,n), το αρχικό κείμενο. Για να επιλύσει αυτό το πρόβλημα θα πρέπει αρχικά να παραγοντοποιήσει το n. Εάν ο εισβολέας μπορέσει να υπολογίσει το ιδιωτικό κλειδί (d) τότε θα μπορεί να αποκρυπτογραφήσει οτιδήποτε στέλνεται στο παραλήπτη.

Επιπρόσθετα μια τελευταία επίθεση, είναι η επίθεση στον συντελεστή RSA. Μια τέτοιου είδους επίθεση μπορεί να γίνει σε περιπτώσεις όπου άτομα τα οποία επικοινωνούν μεταξύ τους έχουν κλειδιά με ίδιο n. Για να αποφευχθεί αυτό το πρόβλημα υπάρχει μια κεντρική αρχή, η οποία διανέμει το συντελεστή n του RSA και έπειτα διάφορα ζεύγη κλειδιών στους διάφορους χρήστες. Με κάποια τεχνική όμως κάποιος που γνωρίζει ένα ζεύγος κλειδιών μπορεί να παραγοντοποιήσει το n και να βρει τελικά το αρχικό μήνυμα.

## 2.3 ElGamal

Στην κρυπτογραφία, το σύστημα κρυπτογράφησης ElGamal είναι ένας ασύμμετρος αλγόριθμος κρυπτογράφησης κλειδιών και βασίζεται στην ανταλλαγή κλειδιού Diffie-Hellman. Περιγραφή αυτού του αλγορίθμου έχει γίνει από τον Αιγύπτιο κρυπτογράφο Taher Elgamal το 1985. Η κρυπτογράφηση ElGamal χρησιμοποιείται στο δωρεάν λογισμικό GNU Privacy Guard, στις πρόσφατες εκδόσεις του PGP και σε άλλα κρυπτοσυστήματα.

### 2.3.1 Αλγόριθμος Κρυπτογράφησης και Αποκρυπτογράφησης

ΚΡΥΠΤΟΓΡΑΦΗΣΗ

1. Ζητάμε το δημόσιο κλειδί $K_{pub}=(p,g,y)$
2. Αναπαριστάμε το μήνυμα m που θέλουμε να στείλουμε ως ακέραιο στο $Zn=\{0,1,\ldots,n-1\}$
3. Διαλέγουμε ένα τυχαίο k τέτοιο ώστε $1 < k < p-1$
4. Υπολόγισε το κρυπτοκείμενο :

$$z= m * y^k \pmod p$$

5. Στέλνουμε το (y,z) στον παραλήπτη, το οποίο αποτελεί το κρυπτοκείμενο

Ο k πρέπει να διαφέρει σε κάθε κρυπτογράφηση – αποκρυπτογράφηση ενός El Gamal, διότι εάν παραμείνει ο ίδιος, τότε υπάρχει ο κίνδυνος ανάγνωσης και άλλων μηνυμάτων με το ίδιο k.

ΑΠΟΚΡΥΠΤΟΓΡΑΦΗΣΗ

1. Αφού ο αποστολέας λάβει το κρυπτοκείμενο, με τη χρήση του ιδιωτικού κλειδιού $K_{pr}=a$ υπολογίζω

$$y^{-a} \equiv y^{p-1-a} \bmod p$$

2. Επίσης υπολογίζω το αρχικό κείμενο μέσω του τύπου:

$$m = y^{-a} * y \bmod p$$

### 2.3.2 Παραγωγή Κλειδιών

$K_{pub}=(p,g,y)$ $K_{pr}=a$

Αρχικά επιλέγουμε έναν μεγάλο πρώτο αριθμό p

Μετά επιλέγω έναν αριθμό g , ο οποίος είναι αριθμός γεννήτορας στο $Z_p^*$ και ισχύει ότι:

$$g^k \neq 1 \pmod p \text{ , για όλα τα } k< p-1$$

Έπειτα επιλέγω έναν τυχαίο ακέραιο αριθμό a ανάμεσα στο διάστημα

$$1 < a < p-1$$

και με αυτόν υπολογίζω τον αριθμό y που προκύπτει από το τύπο:

$$y = g^a \bmod p$$

### 2.3.3 Παράδειγμα κρυπτογράφησης-αποκρυπτογράφησης ElGamal

*ΠΑΡΑΔΕΙΓΜΑ.* Για να κρυπτογραφήσω και να αποκρυπτογραφήσω ένα μήνυμα m=4 με $k_{pub}$ και $k_{pr}$ της επιλογής μου ακολουθώ τα παρακάτω βήματα:

Για τη δημιουργία κλειδιών αρχικά επιλέγω έναν πρώτο αριθμό p, ο οποίος διαιρείται μόνο από τον εαυτό του και τον αριθμό 1 άρα p=5.

Μετά επιλέγω έναν αριθμό g , ο οποίος είναι αριθμός γεννήτορας και ισχύει ότι:

$$g^k \neq 1 \pmod p \text{ , για όλα τα } k< p-1$$

για g= 2

$$2^1 \neq 1 \pmod 5 \text{ , } 2^2 \neq 1 \pmod 5 \text{ , } 2^3 \neq 1 \pmod 5$$

αφού ισχύουν τα παραπάνω μπορώ να συνεχίσω.

Έπειτα επιλέγω έναν τυχαίο ακέραιο αριθμό a ανάμεσα στο διάστημα

$$1 < a < p-1 \rightarrow 1< a < 4$$

οπότε επιλέγω a=3 και με αυτόν υπολογίζω τον αριθμό y που προκύπτει από το τύπο:

$$y = g^a \bmod p$$

άρα υπολογίζω :

$$y = 2^3 \bmod 5 = 8 \bmod 5 = 3$$

Το ιδιωτικό κλειδί είναι το a και το δημόσιο κλειδί είναι η τριάδα p,g,y

$$K_{pr}=(3) \qquad K_{pub}=(5,2,3)$$

Προκειμένου να γίνει η διαδικασία της κρυπτογράφησης επιλέγω έναν τυχαιο ακέραιο k , όπου

$$1 < k < p-1 \rightarrow 1 < k < 4$$

και υπολογίζω το :

$$z= m * y^k \pmod p$$

Για k= 2

$$z= 4 * 3^2 \pmod 5 = 4 * 9 \pmod 5 = 27 \bmod 5 = 2$$

Το ζεύγος ( y , z ) αποτελεί το κρυπτοκείμενο άρα

$$c= (3 , 2 )$$

Για την αποκρυπτογράφηση του κρυπτοκειμένου c υπολογίζω το τύπο:

$$y^{-a} \equiv y^{p-1-a} \bmod p$$

άρα $m = y^{-a} * y \bmod p$

με βάση τα κλειδιά που έφτιαξα

$$3^{-3} \equiv 3^{5-1-3} \bmod 5 = 3^1 \bmod 5 = 3 \bmod 5 =3$$

Άρα $m= 3 * 3 \bmod 5 = 9 \bmod 5 = 4$

### 2.3.4 Πρόβλημα διακριτού λογαρίθμου

Δίνεται ο ορισμός του προβλήματος διακριτού λογαρίθμου:

Έστω G μια πεπερασμένη ομάδα τάξης n, g ένας γεννήτορας της G και $b \in G$. Διακριτός λογάριθμος του b με βάση g και συμβολίζεται με $\log_a b$ είναι ο μοναδικός ακέραιος x για τον οποίο ισχύει ότι $0 \le x \le n-1$ , με $g^x=b$

Ως πρόβλημα του διακριτού λογαρίθμου ονομάζεται το πρόβλημα εύρεσης του αριθμού x όταν είναι γνωστοί οι αριθμοί g και b. Η δυσκολία επίλυσης αυτού του προβλήματος στηρίζεται στον αριθμό των υπολογισμών που θα πρέπει να γίνουν από ένα άτομο προκειμένου να βρει αυτόν τον αριθμό.

ΙΔΙΟΤΗΤΕΣ

Έστω G μια πολλαπλασιαστική ομάδα τάξης n , h και h' γεννήτορες της G , b και $a \in G$ και $s \in \mathbf{Z}$

- $\log_h(a*b) \equiv (\log_h b+\log_h a) \bmod n$

- $\log_h(b^s) \equiv s*\log_h b \bmod n$
- $\log_h b \equiv (\log_h b)*(\log_h h')^{-1} \bmod n$

### 2.3.5 Χαρακτηριστικά αλγορίθμου ELGAMAL

Αρχικά το κρυπτοκείμενο είναι δύο φορές πιο μεγάλο από το αρχικό κείμενο, το οποίο αποτελεί και το βασικό του μειονέκτημα έναντι στον αλγόριθμο RSA .
Η ασφάλεια του στηρίζεται στη δυσκολία επίλυσης των προβλημάτων διακριτού λογαρίθμου DLP.
Ακόμα ο αλγόριθμος έχει ως στόχο να διατηρήσει ασφαλή την ανταλλαγή ενόςμυστικού κλειδιού μεταξύ δύο χρηστών, το οποίο θα χρησιμοποιηθεί κατά τη διαδικασία της κρυπτογράφησης. Τέλος η αποτελεσματικότητα του στηρίζεται στην δυσκολία υπολογισμού διακριτών λογαρίθμων.

### 2.3.6 Πιθανές επιθέσεις στον ELGAMAL

Ενεργές επιθέσεις

Στο σύστημα Elgamal όπως και στα άλλα ασύμμετρα σχήματα πρέπει το δημόσιο κλειδί να είναι αυθεντικό. Αυτό σημαίνει ότι στην πραγματικότητα το κλειδί που χρησιμοποιεί ο αποστολέας είναι το δημόσιο κλειδί του παραλήπτη. Εάν ο επιτιθέμενος μπορεί να πείσει τον αποστολέα ότι το κλειδί του αποστολέα που αναζητά είναι το δικό του κλειδί, τότε μπορεί να επιτεθεί στο σύστημα. Προκειμένου να αποφευχθεί αυτή η επίθεση τότε μπορούν αν

χρησιμοποιηθούν πιστοποιητικά, τα οποία θα αναλυθούν στο επόμενο κεφάλαιο.
Μία ακόμα αδυναμία της κρυπτογράφησης Elgamal είναι ότι ο μυστικός εκθέτης δεν πρέπει να χρησιμοποιηθεί ξανά. Έστω ότι ο αποστολέας χρησιμοποίησε την τιμή i για να κρυπτογραφήσει δύο μηνύματα $x_1$ και $x_2$. Σε αυτή τη περίπτωση τα δύο κλειδιά κάλυψης θα είναι τα ίδια και ισχύει ότι :

$$k_m = \beta^i$$

Τέλος άλλη μια επίθεση εναντίον του ElGamal γίνεται εάν ο επιτιθέμενος παρατηρήσει το κρυπτοκείμενο και μπορέσει να το αντικαταστήσει , όπου s ένας ακέραιος αριθμός. Ο δέκτης θα υπολογίσει

$$\begin{aligned} Dk_{pr}(kE, sy) &\equiv sy^{-1}{}_M \bmod p \\ &\equiv s(x * k_M) * k^{-1}{}_M \bmod p \\ &\equiv sx \bmod p \end{aligned}$$

-

Παθητικές επιθέσεις

Η ασφάλεια του συστήματος ElGamal έναντι παθητικών επιθέσεων βασίζεται στο πρόβλημα Diffie-Hellman. Η πιο γνωστή μέθοδος για την επίλυση του προβλήματος Diffie Hellman είναι ο υπολογισμός των διακριτών λογαρίθμων. Εάν υποθέσουμε ότι ο επιτιθέμενος είχε υπερφυσικές δυνάμεις και μπορούσε τα DLPs, τότε θα μπορούσε να επιτεθεί με δύο τρόπους.

Ο ένας τρόπος είναι ανακτώντας το x μέσω της εύρεσης του μυστικού κλειδιού d του παραλήπτη:

$$d = \log_a \beta \bmod p$$

αυτό το βήμα λύνει το πρόβλημα Diffie Hellman εάν επιλεγούν σωστά οι παράμετροι κι έτσι ο επιτιθέμενος μπορεί να αποκρυπτογραφήσει το κρυπτοκείμενο κάνοντας τα ίδια βήματα με τον παραλήπτη:

$$x \equiv y * (k^d_E)^{-1} \bmod p$$

Ο άλλος τρόπος είναι να μπορέσει ο επιτιθέμενος να ανακτήσει το τυχαίο εκθέτη i του αποστολέα:

$$i = \log_a k \bmod p$$

Αυτό το βήμα είναι η επίλυση του προβλήματος του διακριτού λογαρίθμου και μόνο εάν ο επιτιθέμενος μπορέσει να το πετύχει θα μπορεί να υπολογίσει το απλό κείμενο ως εξής:

$$x \equiv y * (\beta^i)^{-1} \bmod p$$

Και στις δύο παραπάνω περιπτώσεις ο επιτιθέμενος θα πρέπει να λύσει το πρόβλημα διακριτού λογαρίθμου στην πεπερασμένη κυκλική ομάδα Z*p . Επίσης προκειμένου να διασφαλιστεί η ασφάλεια του συστήματος Elgamal θα πρέπει το p να έχει μήκος τουλάχιστον 1024 bits.

## 2.4 Πολυπλοκότητα αλγορίθμων

Με τον όρο πολυπλοκότητα αναφερόμαστε στο βέλτιστο χρόνο που μπορεί να λυθεί ένα πρόβλημα χρησιμοποιώντας έναν συγκεκριμένο αλγόριθμο αλλά και στο χώρο που χρειάζεται αυτός ο αλγόριθμος. Κάνοντας αναφορά στο χρόνο ουσιαστικά εννοούμε το σύνολο των βημάτων που χρειάζεται να κάνει ένας αλγόριθμος με βάση τα στοιχεία εισόδου του . Επίσης κάνοντας αναφορά στο χώρο εννοούμε το σύνολο της μνήμης που χρειάζεται ο αλγόριθμος με βάση τα στοιχεία εισόδου του.

## 2.5 Σύγκριση αλγορίθμων RSA και ELGAMAL

Βασική διαφορά των αλγορίθμων είναι ότι αλγόριθμος rsa βασίζεται στην παραγοντοποίηση ενώ ο elgamal στο πρόβλημα διακριτού λογαρίθμου. Ο rsa δεν μπορεί να γίνει πιο αποτελεσματικός αντίθετα ο elgamal μπορεί να υλοποιηθεί μέσω ελλειπτικών καμπυλών με αποτέλεσμα να αυξήσει την απόδοση του και να μειώσει τα απαιτούμενα μεγέθη κλειδιών. Επίσης ο rsa είναι ντετερμινιστικός αλγόριθμος και κάθε κλειδί του είναι ανεξάρτητο με μοναδικό p ,q ενώ ο elgamal είναι τυχαιοποιημένος αλγόριθμος και έχει μια παράμετρο, την ομάδα με την οποία μοιράζεται πολλά κλειδιά. Ακόμη ο rsa είναι πλήρως τυποποιημένος και σχεδόν κάθε εφαρμογή του είναι αμοιβαία συμβατή αντίθετα ο elgamal διαθέτει ένα ευρύ φάσμα υλοποιήσεων, χρησιμοποιώντας διαφορετικές παραστάσεις και αλγεβρικές ομάδες, οι περισσότερες από τις οποίες είναι αμοιβαία ασύμβατες. Ορισμένα από αυτά είναι στην πραγματικότητα τυποποιημένα. Τέλος υπάρχουν λιγότερα κρυπτογραφικά σχήματα που είναι παρόμοια με τον rsa από ότι είναι με τον elgamal.
Βέβαια μπορεί να ο rsa να έχει αδύναμα κλειδιά αλλά ο elgamal έχει αδύναμη ομάδα όμως κάθε κλειδί που χρησιμοποιεί αυτή την ομάδα είναι εξίσου ασφαλές. Και οι δύο αλγόριθμοι απαιτούν παρόμοια μεγέθη κλειδιών και μπορούν να ‹σπάσουν› χρησιμοποιώντας ίδιες προσεγγίσεις. Επιπρόσθετα και οι δύο υλοποιούνται με τη χρήση αριθμητικής αριθμητικής, αλλά:
ο RSA χρησιμοποιεί μια διαφορετική αριθμητική δομή για κάθε κλειδί (mod n), ενώ ο ElGamal χρησιμοποιεί την ίδια αριθμητική δομή για κάθε κλειδί μέσα στο σύστημα (mod p).

-

# *3. ΕΦΑΡΜΟΓΕΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ*

Σε αυτό το κεφάλαιο γίνεται μια μελέτη σχετικά με τις εφαρμογές της κρυπτογραφίας σε διάφορους τομείς της τεχνολογίας και περισσότερη ανάλυση γίνεται πάνω στις ψηφιακές υπογραφές. Αρχικά αναλύονται τα δύο είδη των σχημάτων των ψηφιακών υπογραφών και τα είδη των επιθέσεων τα οποία μπορούν να δεχτούν. Επίσης μελετήθηκαν οι ψηφιακές υπογραφές των δύο βασικών αλγορίθμων της εργασίας RSA και ElGamal. Ακόμη σε αυτό το κεφάλαιο έγινε μελέτη πάνω στην αυθεντικοποίηση της ταυτότητας και στα ψηφιακά πιστοποιητικά που χρησιμοποιούν .

## 3.1 Γενικές Εφαρμογές

Η εξέλιξη της χρησιμοποίησης της κρυπτογραφίας ολοένα αυξάνεται καθιστώντας πλέον αξιόπιστη τη μεταφορά της πληροφορίας για διάφορους λειτουργικούς σκοπούς

- Ασφάλεια συναλλαγών σε τράπεζες δίκτυα – ATM
- Κινητή τηλεφωνία (ΤΕΤΡΑ-ΤΕΤΡΑΠΟΛ-GSM)
- Σταθερή τηλεφωνία (cryptophones)
- Διασφάλιση Εταιρικών πληροφοριών
- Στρατιωτικά δίκτυα (Τακτικά συστήματα επικοινωνιών μάχης)
- Διπλωματικά δίκτυα (Τηλεγραφήματα)
- Ηλεκτρονικές επιχειρήσεις (πιστωτικές κάρτες, πληρωμές)
- Ηλεκτρονική ψηφοφορία
- Ηλεκτρονική δημοπρασία
- Ηλεκτρονικό γραμματοκιβώτιο
- Συστήματα συναγερμών
- Συστήματα βιομετρικής αναγνώρισης
- Ιδιωτικά δίκτυα (VPN)
- Word Wide Web
- Δορυφορικές εφαρμογές (δορυφορική τηλεόραση)
- Δορυφορικές εφαρμογές (δορυφορική τηλεόραση)
- Ασύρματα δίκτυα (Hipperlan, bluetooth, 802.11x) Συστήματα ιατρικών δεδομένων και άλλων βάσεων δεδομένων
- Τηλεσυνδιάσκεψη - Τηλεφωνία μέσω διαδικτύου (VOIP)

-

## 3.2 Ψηφιακές υπογραφές

### 3.2.1 Γενικές αρχές

Η ψηφιακή υπογραφή είναι ένα μαθηματικό σύστημα, το οποίο χρησιμοποιείται για την απόδειξη γνησιότητας ενός ψηφιακού μηνύματος ή εγγράφου .Η ψηφιακή υπογραφή πιστοποιεί ότι το μήνυμα που δημιουργήθηκε ανήκει στον αποστολέα, ο οποίος το έχει ψηφιακά υπογράψει, και δεν έχει υποστεί κατά τη διάρκεια της μεταφοράς κάποια αλλοίωση ή παραποίηση. Ως ιδέα οι ψηφιακές υπογραφές παρουσιάστηκαν για πρώτη φορά το 1976 από τους Whitfield Diffie και Martin Hellman. Όταν παρουσιάστηκε ο αλγόριθμος RSA, άρχισε και να χρησιμοποιείται ο αλγόριθμος αυτός στις πρώτες υπογραφές. Για το λόγο ότι οι πρώτες αυτές υπογραφές δεν ήταν καθόλου ασφαλείς, άρχισε να χρησιμοποιείται η συνάρτηση κατατεμαχισμού. Ολοκληρωμένη μελέτη για τις απαιτήσεις ασφαλείας των ψηφιακών υπογραφών ήταν το 1988 από τους Shafi Goldwasser, Silvio Micali και Ronald Rivest. Οι ψηφιακές υπογραφές στα ψηφιακά έγγραφα είναι παρόμοιες με τις χειρόγραφες υπογραφές αλλά είναι πολύ πιο δύσκολο κάποιος να τις πλαστογραφήσει. Σε πολλές χώρες οι ψηφιακές υπογραφές έχουν νομική υπόσταση .

Σήμερα οι ψηφιακές υπογραφές εφαρμόζονται στη σύνοψη του μηνύματος και όχι σε ολόκληρο το έγγραφο γιατί με αυτό τον τρόπο έχουμε τα παρακάτω θετικά.

*Αποτελεσματικότητα* (Efficiency):Η ψηφιακή υπογραφή είναι πολύ μικρότερη σε μέγεθος από ένα ολόκληρο το κείμενο άρα απαιτεί και πολύ λίγο χρόνος για να εφαρμοστεί.

*Συμβατότητα* (Compartibility ):Τα αρχικά κείμενα αποτελούν δέσμες bit, οι οποίες δεν αλλάζουν και μέσω του αλγορίθμου κατατεμαχισμού έχουν τη δυνατότητα να μετατραπούν σε συγκεκριμένο αριθμό bit.

*Ακεραιότητα* (Integrity):Αν η συνάρτηση κατακερματισμού δεν εφαρμοστεί σε όλο το αρχικό κείμενο, τότε το κείμενο θα πρέπει να διαιρεθεί σε κομμάτια μικρότερου bits έτσι ώστε να μπορεί να εφαρμοστεί ο αλγόριθμος ψηφιακών υπογραφών πάνω σε αυτά τα κομμάτια των bits. Παρόλα αυτά ο αποδέκτης των πακέτων αυτών δεν μπορεί να γνωρίζει ποιος είναι ο αριθμός αυτών των πακέτων και ποια είναι η σειρά των πακέτων αυτών.

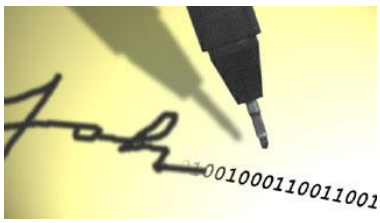
-

### 3.2.2 Σύγκριση χειρόγραφων – ψηφιακών υπογραφών

Παρότι οι ψηφιακές υπογραφές και οι χειρόγραφες υπογραφές δημιουργήθηκαν για ίδιους σκοπούς, παρουσιάζουν κάποιες σημαντικές διαφορές. Οι διαφοροποιήσεις που παρουσιάζουν, αναγράφονται επιγραμματικά στο πίνακα παρακάτω.

| **Χειρόγραφη υπογραφή** | **Ψηφιακή υπογραφή** |
|---|---|
| Πάνω στο κείμενο | Ξεχωριστό αρχείο το οποίο συνδέεται με το κείμενο |
| Χρήση της ίδιας υπογραφής για όλους τους σκοπούς | Χρήση διαφορετικών υπογραφών για διαφορετικούς σκοπούς |
| Εύκολη η πλαστογράφηση | Δύσκολη η πλαστογράφηση |
| Πιστοποιεί την ταυτότητα του ατόμου που υπογράφει | Πιστοποιεί την ταυτότητα του ατόμου που υπογράφει και τη γνησιότητα του περιεχομένου της πληροφορίας |
| Δεν απαιτείται ειδικό λογισμικό για τη δημιουργία της | Απαιτείται ειδικό λογισμικό για τη δημιουργία της |
| Απευθείας ορατή | Απαιτείται ειδικό λογισμικό για την ορατότητα της |
| Ο τρόπος δημιουργίας της παραμένει ο ίδιος και δεν μπορεί να αλλάξει | Ο μηχανισμός δημιουργίας, επαλήθευσής της μπορεί να καταστραφεί και να αντικατασταθεί από κάποιον άλλο |

-



Εικόνα 4. Από χειρόγραφη σε ψηφιακή υπογραφή

### 3.2.3 Συναρτήσεις κατακερματισμού

Οι συναρτήσεις κατακερματισμού είναι μαθηματικές συναρτήσεις, οι οποίες χρησιμοποιούνται στην κρυπτογραφία, κυρίως στις ψηφιακές υπογραφές και σε κωδικούς πρόσβασης. Ως είσοδο δέχονται δεδομένα ανεξάρτητου μεγέθους και ως έξοδο δίνουν μια στοιχειοσειρά σταθερού μεγέθους. Οι συναρτήσεις αυτές είναι μίας κατεύθυνσης δηλαδή για οποιαδήποτε είσοδο υπολογίζεται η έξοδος αλλά όχι το αντίστροφο και επίσης δεν μπορεί να βρεθεί ίδια έξοδος για διαφορετικές εισόδους. Η έξοδος ενός μηνύματος M ονομάζεται σύνοψη του μηνύματος, συμβολίζεται h(M) και για οποιαδήποτε αλλαγή στην είσοδο μιας συνάρτησης κατακερματισμού αλλάζει αμέσως μορφή και η σύνοψη.

## 3.3 Κατηγορίες ψηφιακών υπογραφών

Οι ψηφιακές υπογραφές χωρίζονται σε 2 μεγάλες κατηγορίες ανάλογα με το εάν απαιτούν το πρωτότυπο μήνυμα στον αλγόριθμο επαλήθευσης. Η μία κατηγορία είναι οι ψηφιακές υπογραφές με παράρτημα, οι οποίες απαιτούν το αρχικό μήνυμα ως είσοδο και είναι η πιο συχνά χρησιμοποιούμενες. Σε αυτή την κατηγορία οι υπογραφές βασίζονται σε συναρτήσεις κατακερματισμού και δεν τους γίνονται πολλές επιθέσεις. Ο αλγόριθμος ElGamal δημιουργεί υπογραφές τέτοιου είδους. Η άλλη κατηγορία είναι οι ψηφιακές υπογραφές με ανάκτηση μηνύματος, οι οποίες ανακτούν το αρχικό μήνυμα από την ίδια υπογραφή. Σε αυτή την κατηγορία οι υπογραφές βασίζονται κυρίως σε συναρτήσεις πλεονασμού(R) και σε αυτή ανήκουν και οι υπογραφές του αλγορίθμου RSA. Και στις 2 παραπάνω κατηγορίες εάν το |R|>1 τότε το σχήμα ονομάζεται τυχαίας ψηφιακής υπογραφής αλλιώς ονομάζεται ντετερμινιστικής υπογραφής.

ΧΡΗΣΙΜΟΙ ΣΥΜΒΟΛΙΣΜΟΙ

- M : ο χώρος των μηνυμάτων
- $M_S$ : ο χώρος που εφαρμόζονται οι μετασχηματισμοί της υπογραφής
- S : ο χώρος των υπογραφών που έχουν σχέση με τα μηνύματα στο M
- R : συνάρτηση πλεονασμού, η απεικόνιση από το M στο $M_S$

- $M_R$ : η εικόνα του R δηλαδή $M_R$=Im(R)
- $R^{-1}$: η αντίστροφη της R
- h: μια μονόδρομη συνάρτηση με πεδίο ορισμού το M
- $M_b$: εικόνα του h , M->$M_h$ όπου $M_h$ υποσύνολο του $M_b$ και ο χώρος των τιμών κατακερματισμού

### 3.3.1 Ψηφιακές υπογραφές με παράρτημα

1.Δημιουργία κλειδιών

Κάθε οντότητα A δημιουργεί το δημόσιο ($V_A$) και ιδιωτικό ($S_A$) κλειδί της, το οποίο θα χρησιμοποιηθεί για την επαλήθευση των υπογραφών από άλλους χρήστες και την υπογραφή μηνυμάτων αντίστοιχα.

- Η οντότητα A διαλέγει ένα ιδιωτικό κλειδί για ένα σύνολο μετασχηματισμών $S_A$={ $S_{A,k}$ : k $\in$ R}. Κάθε μετασχηματισμός $S_{A,k}$ ονομάζεται μετασχηματισμός υπογραφής και αποτελεί μια 1-1 απεικόνιση από το $M_h$ στο S.

- Το $S_A$ καθορίζει μια απεικόνιση $V_A$ από το $M_h$ στο S, η οποία ονομάζεται μετασχηματισμός επαλήθευσης

$$V_A(m',s^*)= \begin{cases} \text{-Αληθές , αν } S_{A,k}(m)=s^* \\ \text{-Ψευδής , διαφορετικά} \end{cases}$$

για κάθε m' $\in$ $M_h$ , s* $\in$ S όπου m' =h(m) για κάθε m $\in$ M

2.Δημιουργία υπογραφής

Η οντότητα A δημιουργεί μια υπογραφή s $\in$ S για ένα μήνυμα m $\in$ M και κάνει τα εξής :

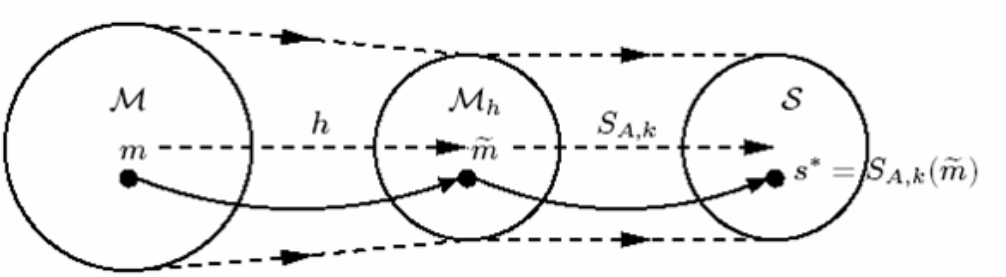
- Επιλέγει ένα k $\in$ R
- Υπολογίζει το m'=h(m) και s*= $S_{A,k}$(m')
- Το m και s* δίνονται στις οντότητες που θέλουν να επαληθεύσουν την υπογραφή

Η υπογραφή του A για το m είναι το s*

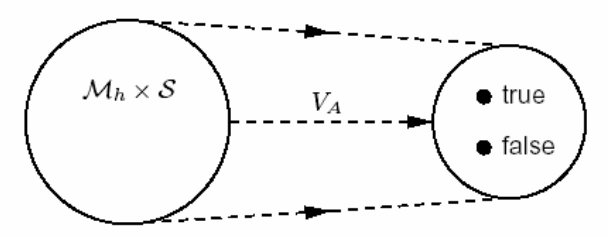
3.Επαλήθευση υπογραφής

Η οντότητα B ,η οποία θέλει να κάνει την επαλήθευση της υπογραφής κάνει τα εξής:

- Παίρνει το αυθεντικό δημόσιο κλειδί του A , το $V_A$
- Υπολογίζει το m'=h(m) και u= $V_A$(m',s*)
- Εάν το u είναι αληθές τότε δέχεται την υπογραφή




Εικόνα 5. Δημιουργία υπογραφής




Εικόνα 6. Επαλήθευση υπογραφής

### 3.3.2 Ψηφιακές υπογραφές με ανάκτηση μηνύματος

1.Δημιουργία κλειδιών
Κάθε οντότητα A δημιουργεί το δημόσιο ($V_A$) και ιδιωτικό ($S_A$) κλειδί της ,το οποίο θα χρησιμοποιηθεί για την επαλήθευση των υπογραφών από άλλους χρήστες και την υπογραφή μηνυμάτων αντίστοιχα.

- Η οντότητα A διαλέγει ένα ιδιωτικό κλειδί για ένα σύνολο μετασχηματισμών $S_A$={ $S_{A,k}$ : k $\in$ R} . Κάθε μετασχηματισμός $S_{A,k}$ ονομάζεται μετασχηματισμός υπογραφής και αποτελεί μια 1-1 απεικόνιση από το $M_h$ στο S.

- Το $S_A$ καθορίζει μια απεικόνιση $V_A$ ,η οποία ονομάζεται μετασχηματισμός επαλήθευσης και έχει την ιδιότητα ότι $V_A$ $S_A$ είναι ταυτοτική απεικόνιση στο $M_S$ για κάθε k $\in$ R .

2.Δημιουργία υπογραφής

Η οντότητα Α δημιουργεί μια υπογραφή s $\in$ S για ένα μήνυμα m $\in$ M και κάνει τα εξής :

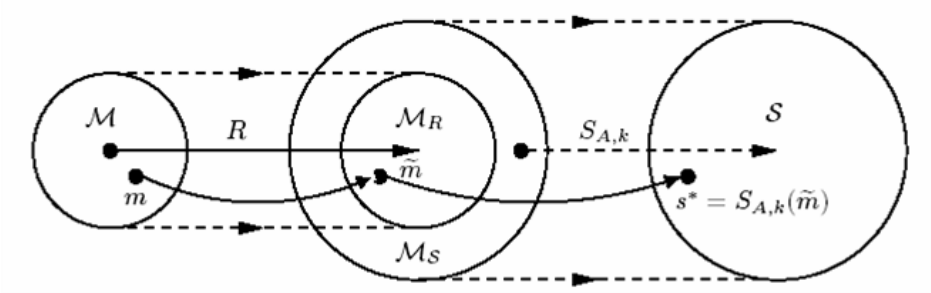
- Επιλέγει ένα k $\in$ R
- Υπολογίζει το m'=R(m) και s*= $S_{A,k}$ (m') όπου R είναι μια συνάρτηση πλεονασμού
- Το m και s* δίνονται στις οντότητες που θέλουν να επαληθεύσουν την υπογραφή και να ανακτήσουν το αρχικό μήνυμα

Η υπογραφή του Α για το m είναι το s*.

3.Επαλήθευση υπογραφής

Η οντότητα Β, η οποία θέλει να κάνει την επαλήθευση της υπογραφής κάνει τα εξής:

- Παίρνει το αυθεντικό δημόσιο κλειδί του Α, το $V_A$
- Υπολογίζει το m'= $V_A$(s*)
- Εάν το m' $\in$ $M_R$ τότε δέχεται την υπογραφή
- Υπολογίζει το $R^{-1}$(m')
- Ανακτά το αρχικό μήνυμα m από τον προηγούμενο υπολογισμό




Εικόνα 7. Δημιουργία υπογραφής

## 3.4 Ψηφιακές υπογραφές RSA

Αρχικά δημιουργούνται τα αντίστοιχα κλειδιά που χρειάζονται, όπως έχει αναφερθεί στο προηγούμενο κεφάλαιο ,δηλαδή το ιδιωτικό κλειδί (d) και το δημόσιο κλειδί (n,e). Η οντότητα Α για να δημιουργήσει την υπογραφή κάνει τις παρακάτω ενέργειες.
Αρχικά υπολογίζει το m=R(m), το οποίο είναι ένας ακέραιος στο διάστημα [0,n-1] και μετά υπολογίζει το

$$s = m^d \bmod n,$$

το οποίο είναι η υπογραφή του Α

Η οντότητα Β προκειμένου να επαληθεύσει την υπογραφή κάνει τις εξής ενέργειες :

-Υπολογίζει το

$$m = s^e \bmod n ,$$

χρησιμοποιώντας το δημόσιο κλειδί του Α

-Επαληθεύει ότι m ανήκει στο $M_R$ κι εάν αυτό δεν ισχύει απορρίπτει την υπογραφή

-Ανακτά το μήνυμα $m=R^{-1}(m)$

*ΠΑΡΑΔΕΙΓΜΑ.* Για να βρω και να επαληθεύσω τη ψηφιακή υπογραφή ενός μηνύματος m= 4 , με κλειδί Kpub=(36,5) , Kpr=(5) , χώρος υπογραφής M = Zn ,συνάρτηση πλεονασμού R: M →Zn και ταυτοτική απεικόνιση R(m)=m λειτουργώ ως εξής :

Σχετικά με την παραγωγή της ψηφιακής υπογραφής ο αποστολέας

- Υπολογίζει:

$$m' = R(m) = 4$$

-Υπολογίζει

$$s = m'^d \bmod n = 4^5 \bmod 36$$

χρησιμοποιώ αλγόριθμο squaring and multiply

$5 \rightarrow 101 \rightarrow$ SM S SM

$$(((((( 1^2 ) \bmod 36 ) * 4 ) \bmod 36 )^2 \bmod 36 )^2 \bmod 36 ) * 4 ) \bmod 36$$

$$= ((( 4 \bmod 36 )^2 \bmod 36 )^2 \bmod 36 ) * 4 ) \bmod 36$$

$$= (( 16 \bmod 36 )^2 \bmod 36 ) * 4 ) \bmod 36$$

$$= (( 256 \bmod 36 ) * 4 ) \bmod 36$$

$$= 16 \bmod 36 = 16$$

Άρα s = 16 και αποτελεί την υπογραφή του αποστολέα για το μήνυμα m

Για να επαληθεύσει ο παραλήπτης την ψηφιακή υπογραφή:

Μέσω του δημοσίου κλειδιού του αποστολέα αρχικά υπολογίζει

$m' = s^e \bmod n = 16^5 \bmod 36$

χρησιμοποιώ αλγόριθμο squaring and multiply

$5 \rightarrow 101 \rightarrow SM\ S\ SM$

$(((((( 1^2 ) \bmod 36 ) * 16 ) \bmod 36 )^2 \bmod 36 )^2 \bmod 36 ) * 16 ) \bmod 36$

$= ((( 16 \bmod 36 )^2 \bmod 36 )^2 \bmod 36 ) * 16 ) \bmod 36$

$= ((( 256 \bmod 36 )^2 \bmod 36 ) * 16 ) \bmod 36$

$= (( 16 \bmod 36 ) * 16 ) \bmod 36$

$= 256 \bmod 36 = 4$

Άρα m'= 4

Επαληθεύει ότι m' $M_R$ , έτσι ανακτά το m υπολογίζοντας m = R-1(m') = 4

## 3.5 Ψηφιακές υπογραφές ELGAMAL

Αφού δημιουργηθούν το δημόσιο κλειδί (p,q,y) και το ιδιωτικό κλειδί (b), η οντότητα Α κάνει τις παρακάτω λειτουργίες. Αρχικά επιλέγει έναν ακέραιο k, ο οποίος θα είναι τυχαίος και μυστικός και θα ισχύει ότι:

$$1 \le k \le p-2 \qquad \text{και} \qquad gcd(k,p-1)=1$$

Επίσης υπολογίζω τον αριθμό r για τον οποίο ισχύει ότι:

$$r = q^k \bmod p$$

Ακόμη υπολογίζω το

$$k^{-1} \bmod (p-1)$$

και τέλος υπολογίζω έναν αριθμό s για τον οποίο ισχύει ότι :

$$s = k^{-1}\{ h(m) – br \} \bmod (p-1)$$

Η ψηφιακή υπογραφή για το m αποτελείται από το ζεύγος (r,s).

Η οντότητα Β για να κάνει επαλήθευση στην υπογραφή κάνει τα εξής :

-Επαληθεύει ότι 1<=k<= p-1

-Υπολογίζει το

$$u_1 = y^r r^s \bmod p$$

$$u_2 = q^m \bmod p$$

-Εάν ισχύει ότι u1=u2 τότε δέχεται την υπογραφή

*Παράδειγμα* . Για την δημιουργία υπογραφής ενός μηνύματος m=11 και την επαλήθευση της με $K_{pub}$= (13,2,8) ,$K_{pr}$=(3) ακολουθώ τα παρακάτω βήματα

Από τα παραπάνω στοιχεία έχω

p=13 , q=2 , d=3 , m=11

Βρίσκω k για το οποίο ισχύει ότι 1<= k <= p-2 και gcd(k,p-1)=1

Έστω k=5

- 1<=5<=11
- gcd (5,12) = gcd ( 5 , 12 mod 5 )
  = gcd ( 5 , 2 )
  = gcd ( 2 , 5 mod 2 )
  = gcd ( 2 , 1 )
  = gcd ( 1 , 2 mod 1 )
  = gcd ( 1 , 0 )
  = 1

Ισχύουν οι προϋποθέσεις άρα συνεχίζω

$r = q^k \bmod p \rightarrow r = 2^5 \bmod 13 = 6$

5 → 101 → SM S SM

$(((((((1^2) \bmod 13) * 2) \bmod 13)^2 \bmod 13)^2 \bmod 13) * 2) \bmod 13$

$= ((((2 \bmod 13)^2 \bmod 13)^2 \bmod 13) * 2) \bmod 13$

$= (((4 \bmod 13)^2 \bmod 13) * 2) \bmod 13$

$= ((16 \bmod 13) * 2) \bmod 13$

$= 6 \bmod 13 = 6$

$s = (k^{-1})(m - d * r) \bmod (p-1) = 1$

Η υπογραφή του μηνύματος m είναι το ζεύγος (r,s)

Ο παραλήπτης για να επαληθεύσει την υπογραφή ελέγχει ότι :

$0 < r < p$ και $0 < s < p-1$
$0 < 9 < 13$ και $0 < 1 < 12$ ισχύουν

Και υπολογίζει :

$u_1 = y^r r^s \bmod p = 8^6 * 6^1 \bmod 13 = 262144 * 6 \bmod 13 = 1572864 \bmod 13 = 7$

6 → 110 → SM SM S

$(((1^2) * 8)^2 * 8)^2 = (64 * 8)^2 = (512)^2 = 262144$

$u_2 = q^m \bmod p = 2^{11} \bmod 13 = 7$

11 → 1011 → SM S SM SM

$((((((((((1^2) \bmod 13) * 2) \bmod 13)^2 \bmod 13)^2 \bmod 13) * 2) \bmod 13)^2 \bmod 13) * 2) \bmod 13$

$= (((((((2) \bmod 13)^2 \bmod 13)^2 \bmod 13) * 2) \bmod 13)^2 \bmod 13) * 2) \bmod 13$

$= ((((((4) \bmod 13)^2 \bmod 13) * 2) \bmod 13)^2 \bmod 13) * 2) \bmod 13$

$= (((((16 \bmod 13) * 2) \bmod 13)^2 \bmod 13) * 2) \bmod 13$

$= ((((6) \bmod 13)^2 \bmod 13) * 2) \bmod 13$

$= ((36 \bmod 13) * 2) \bmod 13 = 20 \bmod 13 = 7$

$u_1 = u_2$ Άρα σωστή η επαλήθευση

## 3.6 Τύποι επιθέσεων στις ψηφιακές υπογραφές

Συνήθως ο στόχος της επίθεσης σε μια ψηφιακή υπογραφή είναι η πλαστογράφηση της. Τα είδη των επιθέσεων σε σχήματα ψηφιακών υπογραφών είναι δύο, οι επιθέσεις κλειδιού, όπου ο αντίπαλος γνωρίζει το δημόσιο κλειδί και οι επιθέσεις μηνύματος. Στις επιθέσεις μηνύματος ανήκουν οι επιθέσεις γνωστού μηνύματος, όπου ο αντίπαλος γνωρίζει τις ψηφιακές υπογραφές για ένα σύνολο μηνυμάτων, οι επιθέσεις επιλεγμένου μηνύματος,

όπου ο αντίπαλος πριν την παραβίαση λαμβάνει από μια λίστα υπογραφές για μια ομάδα μηνυμάτων και τέλος οι προσαρμόσιμες επιθέσεις επιλεγμένου μηνύματος, όπου ο αντίπαλος ζητάει υπογραφές που έχουν εξάρτηση από το δημόσιο κλειδί ή από άλλες υπογραφές.

### 3.6.1 Τύποι επιθέσεων στις ψηφιακές υπογραφές RSA

*-Επίθεση που βασίζεται στην παραγοντοποίηση ακεραίων*
Εάν ο επιτιθέμενος μπορέσει να βρει τους παράγοντες του n δηλαδή τους αριθμούς p και q, τότε θα μπορεί να υπολογίσει τη τιμή του φ(n). Έπειτα θα μπορέσει να υπολογίσει και το ιδιωτικό κλειδί d μιας και το δημόσιο κλειδί είναι γνωστό.

*-Πολλαπλασιαστική ιδιότητα RSA*
Έστω m1 m2 δύο μηνύματα και s1=m1d mod n ,s2=m2d mod n οι υπογραφές τους, τότε ισχύει η ιδιότητα ότι s=s1s2=(m1m2)mod n. Εάν το m1 και m2 ανήκουν στο MR τότε η s είναι έγκυρη υπογραφή για το m.

### 3.6.2 Τύποι επιθέσεων στις ψηφιακές υπογραφές ELGAMAL

Ο επιτιθέμενος μπορεί να προσπαθήσει να πλαστογραφήσει την υπογραφή του μήνυμα m επιλέγοντας έναν τυχαίο ακέραιο k και υπολογίζοντας το $r = \alpha^k \bmod p$. Ο αντίπαλος πρέπει μετά να προσδιορίσει το $s = k^{-1}\{h(m) - ar\} \bmod (p - 1)$. Αν το πρόβλημα διακριτού λογαρίθμου δεν είναι υπολογιστικά εφικτό, ο αντίπαλος δεν μπορεί παρά να διαλέξει ένα τυχαίο s όπου η πιθανότητα επιτυχίας είναι 1/p αμελητέα δηλαδή για μεγάλα p.

Επίσης για κάθε υπογεγραμμένο μήνυμα θα πρέπει να επιλέγεται διαφορετικό k· αλλιώς το ιδιωτικό κλειδί μπορεί να προσδιοριστεί εύκολα ως εξής. Υποθέτουμε ότι :

$$s_1 = k^{-1}\{h(m_1) - ar\} \bmod (p - 1) \qquad \text{και}$$
$$s_2 = k^{-1}\{h(m_2) - ar\} \bmod (p - 1).$$

Τότε :

$$(s_1 - s_2)k \equiv (h(m_1) - h(m_2)) \pmod{p - 1}.$$

Αν $s_1 - s_2 \not\equiv 0 \pmod{p - 1}$, τότε

$$k = (s_1 - s_2) - 1(h(m_1) - h(m_2)) \bmod (p - 1).$$

Εάν το k είναι γνωστό, τότε μπορεί να βρεθεί εύκολα το a.

Ακόμη αν δεν γίνεται χρήση της συνάρτησης h, η εξίσωση υπογραφής είναι

$$s = k^{-1}\{m - ar\} \bmod (p - 1)$$

άρα είναι πολύ εύκολο για έναν αντίπαλο να κάνει μια επίθεση πλαστογράφησης ως εξής. Επιλέγει ένα ζεύγος ακεραίων (u, υ) με

$$\gcd(u, p - 1) = 1.$$

Υπολογίζει

$$r = \alpha^u y^u \bmod p = \alpha^{u+au} \bmod p \quad \text{και}$$

$$s = -ru^{-1} \bmod (p - 1).$$

Το ζεύγος (r, s) είναι μια έγκυρη υπογραφή για το μήνυμα

$$m = su \bmod (p - 1),$$

αφού

$$\left(a^m\ a^{-ar}\right)^{s^{-1}}$$

## 3.7 Αυθεντικοποίηση ταυτότητας

Αυθεντικοποίηση θεωρείται η διαδικασία κατά την οποία αναγνωρίζεται και επιβεβαιώνεται η ταυτότητα ενός χρήστη μέσω των πληροφοριών που δίνει σε ένα σύστημα. Οι πληροφορίες αυτές συσχετίζονται με τις πληροφορίες που έχουν δοθεί κατά την ταυτοποίηση αυτού του χρήστη. Η ταυτοποίηση είναι μια άλλη διαδικασία όπου ο χρήστης δίνει τα στοιχεία του, τα οποία απαιτούνται προκειμένου να συσχετιστεί με τα αντικείμενα που δικαιούνται προσπέλαση στους πόρους του.

### 3.7.1 Τεχνικές εφαρμογής ελέγχων αυθεντικοποίησης

Αρχικά η πρώτη κατηγορία είναι κάτι που ο χρήστης γνωρίζει. Σε αυτή τη κατηγορία ανήκουν οι κωδικοί πρόσβασης, τα PIN και γενικά πληροφορίες τις οποίες εισάγει ο χρήστης κατά την είσοδο του στο σύστημα και είναι δύσκολο να αποκαλύψει ο ίδιος. Βέβαια υπάρχουν πολλοί μέθοδοι για να “σπάσει” κάποιος αυτές τις πληροφορίες οπότε καλό θα ήταν να έχουν κάποια συγκεκριμένα χαρακτηριστικά, τα οποία θα έχουν να κάνουν με το μήκος τους, τη διάρκεια ζωής τους και τη διανομή τους.

Ακόμα η επόμενη κατηγορία είναι κάτι που ο χρήστης κατέχει. Σε αυτή τη κατηγορία ανήκουν αντικείμενα , τα οποία μπορεί να έχει στη κατοχή του ο χρήστης όπως για παράδειγμα ένα ψηφιακό πιστοποιητικό ή μια έξυπνη κάρτα. Παρότι έχουν υψηλό κόστος και υπάρχει μεγάλος κίνδυνος να χαθούν , έχουν το μεγάλο πλεονέκτημα ότι λόγω της κατασκευής τους είναι δύσκολο να αντιγραφούν από άλλους χρήστες. Ιδιαίτερα κάποιες έξυπνες κάρτες έχουν ενσωματωμένους αισθητήρες ανίχνευσης επιθέσεων πράγμα που τις κάνει πολύ ασφαλείς.

Η τελευταία κατηγορία είναι κάτι που χαρακτηρίζει το χρήστη. Πρόκειται για σωματικά χαρακτηριστικά, τα οποία χρησιμοποιούνται σε συστήματα βιομετρικής τεχνολογίας. Σε αυτά τα συστήματα ανήκουν εφαρμογές δακτυλικών αποτυπωμάτων ,αναγνώρισης ίριδας ματιού κ.α Βέβαια και αυτά τα συστήματα έχουν πολύ υψηλό κόστος αλλά είναι από τα πιο ασφαλή.

Όλοι οι μηχανισμοί αυθεντικοποίησης χρησιμοποιούν 2 τύπους κλειδιών. Ο ένας είναι τα μυστικά κλειδιά, στα οποία συμπεριλαμβάνονται τα συνθηματικά, οι κωδικοί και τα συμμετρικά κλειδιά και ο άλλος τα ασύμμετρα κλειδιά , στα οποία συμπεριλαμβάνονται τα ζεύγη κλειδιών όπου το ένα είναι δημόσιο και το άλλο ιδιωτικό.

Ένα σύστημα αυθεντικοποίησης αποτελείται από διάφορα σύνολα. Αυτά είναι τα εξής :

-Το σύνολο A : Εδώ εμπεριέχονται πληροφορίες όπου ο χρήστης αποδεικνύει την ταυτότητα του
-Το σύνολο C : Εδώ εμπεριέχονται συμπληρωματικές πληροφορίες ,τις οποίες αποθηκεύει το σύστημα για την επικύρωση της αυθεντικοποίησης
-Το σύνολο F : Εδώ υπάρχουν συναρτήσεις ,οι οποίες δημιουργούν τις συμπληρωματικές πληροφορίες για την αυθεντικοποίηση
-Το σύνολο L : Αυτό είναι το σύνολο των συναρτήσεων αυθεντικοίησης που αναγνωρίζουν ένα χρήστη
-Το σύνολο S : Αυτό είναι το σύνολο των λοιπών συναρτήσεων επιλογής που δίνουν στο χρήστη την δυνατότητα να τροποποιήσει τις πληροφορίες αυθεντικοποίησης ή τις συμπληρωματικές πληροφορίες.

### 3.7.2 Ψηφιακά πιστοποιητικά

Για να διασφαλιστεί όμως η ταυτότητα του αποστολέα και να μπορεί να είναι σίγουρος ο παραλήπτης ότι χρησιμοποιεί το σωστό δημόσιο κλειδί για τις διάφορες λειτουργίες υπάρχει ένας Πάροχος Υπηρεσιών Πιστοποίησης. Οι πάροχοι εκδίδουν βεβαιώσεις ηλεκτρονικής μορφής, τα λεγόμενα πιστοποιητικά ηλεκτρονικής υπογραφής, τα οποία στέλνονται μαζί με το μήνυμα ως συννημένα αρχεία. Ως στόχο έχουν να συσχετίζουν ένα δημόσιο κλειδί με τον αντίστοιχο δικαιούχο. Οι εταιρείες που παρέχουν υπηρεσίες πιστοποίησης ελέγχονται από την Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων (Hellenic Telecommunications & Post Commission) Ε.Ε.Τ.Τ., η οποία είναι υπεύθυνη για τον έλεγχο όλων των Παρόχων Υπηρεσιών Πιστοποίησης που είναι εγκατεστημένοι στην Ελλάδα και επιβάλλει πρόστιμα σε όσους Παρόχους ενεργούν χωρίς να είναι διαπιστευμένοι. Υπάρχουν δύο είδη ψηφιακών πιστοποιητικών ανάλογα με τη χρήση τους. Το ένα είναι για ψηφιακή υπογραφή μηνυμάτων και εγγράφων και το άλλο για κρυπτογράφηση μηνυμάτων και εγγράφων. Το πιο διαδεδομένο πρότυπο πιστοποιητικού είναι το X.509 και περιλαμβάνει τα εξής βασικά πεδία :

-Το όνομα και άλλες σχετικές πληροφορίες του κατόχου
-Το δημόσιο κλειδί του κατόχου

-

-Την ημερομηνία λήξης του πιστοποιητικού
-Το όνομα της αρχής που το εξέδωσε
-Την ψηφιακή υπογραφή της αρχής που το εξέδωσε
-Τον αριθμό σειράς και έκδοσης του πιστοποιητικού

# *4. ΥΛΟΠΟΙΗΣΗ*

Σε αυτό το κεφάλαιο γίνεται η υλοποίηση σε γλώσσα C των δύο βασικών αλγορίθμων της εργασίας. Αρχικά παρουσιάζεται ο αλγόριθμος RSA σε γλώσσα C και δίνεται κι ο τρόπος επίλυσης μέσω ενός παραδείγματος σε εικόνα. Έπειτα δίνεται ο δεύτερος αλγόριθμος, ο ElGamal, σε γλώσσα C και ένα παράδειγμα και για αυτόν .

## 4.1 RSA σε γλώσσα C

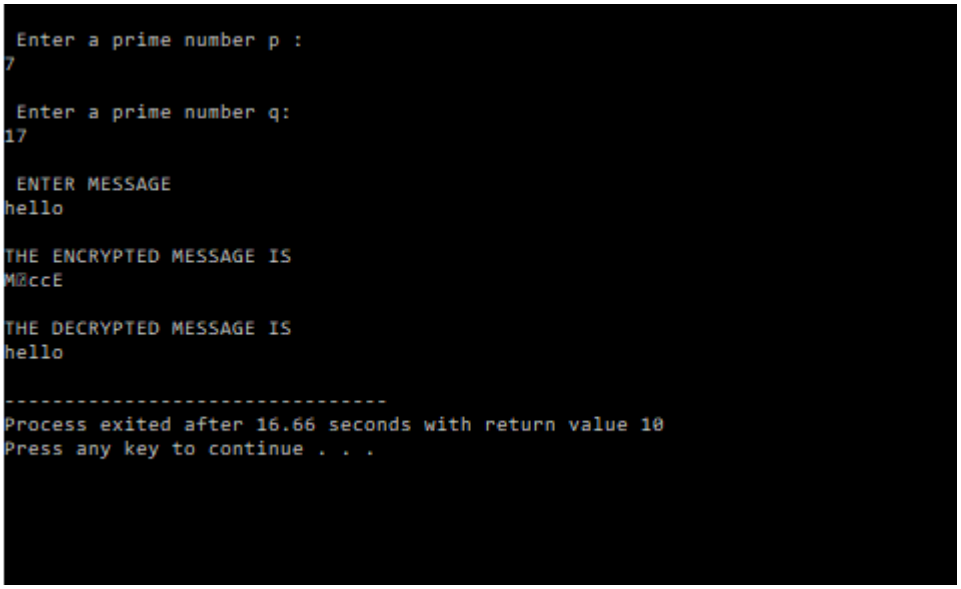
```
1.    #include<stdio.h>
2.    #include<stdlib.h>
3.    #include<math.h>
4.    #include<string.h>

      /*  δηλώνω τα στοιχεία που θα χρησιμοποιήσω στον κώδικα*/

5.    long int  p, q, flag, n, t, i, j, m[100], en[100], pr;
6.    long int temp[100], e, count, d, k ;

7.    char msg[100];

8.    int  prime (long int);
9.    int gcd(int , int );


10.   void encrypt();
11.   void decrypt();

12.   int main()
13.   {

/*  σε αυτή τη δομή επανάληψης, ζητείται ένας πρώτος αριθμός από το
χρήστη αλλά μέσω της συνάρτησης prime() ελέγχεται αν είναι όντως
πρώτος και η ερώτηση θα συνεχίζεται όσο κάποιος δίνει σαν αριθμό το 0*/

14.   do{

15.     printf("\n Enter a prime number p :\n");
16.     scanf("%ld",&p);
17.     flag=prime(p);
```

```
18.          }while(flag==0) ;

/*  αυτή τη δομή επανάληψης είναι ίδια με την παραπάνω αλλά η ερώτηση
θα συνεχίζεται όσο κάποιος δίνει σαν αριθμό το 0 ή ίδιο με το p */

19.          do{
20.               printf("\n Enter a prime number q:\n");
21.              scanf("%ld",&q);
22.              flag=prime(q);
23.          }while(flag==0||p==q);



/*  ζητείται το μήνυμα */
24.          printf("\n ENTER MESSAGE\n");
25.          scanf("%s",msg);

/*  26-27. εδώ μετατρέπω το αλφαριθμητικό που έδωσα σε πίνακα
χαρακτήρων */

26.          for(i=0; msg[i]!='\0'; i++)
27.           m[i]=msg[i];
28.
29.          n=p*q;
30.          t=(p-1)*(q-1);

/*  31-39 .  δίνω μια τυχαία τιμή στο e και μέσω τον ελέγχων που κάνω ,
κάνει μόνο του αύξηση */

31.          e=2;
32.          while(e<t)
33.          {
34.           count=gcd(e,t);

35.            if (count==1)
36.             break;
37.            else
38.              e=e+1;
39.          }


40.          k=2;

41.          d= (1 + (k*t))/e;

42.          encrypt();
43.          decrypt() ;
```

```
44.         }

            /*  η συνάρτηση prime ελέγχει εάν το όρισμα της είναι πρώτος
            αριθμός  */

45.         int prime(long int pr)
46.         {
47.            int i;
               int j=sqrt(pr); /*  το sqrt βρίσκει τη ρίζα του ορίσματος της  */
48.

49.            for(i=2; i<=j; i++)
50.           {
51.             if(pr%i==0)
52.             return 0;
53.           }
54.            return 1;
55.         }

            /*  η συνάρτηση gcd μας δίνει το μέγιστο κοινό διαιρέτη δύο
            αριθμών */

56.         int gcd(int a, int h)
57.         {
58.         int temp;
59.         while(1)
60.         {
               temp = a%h; /*  εδώ βρίσκω το υπόλοιπο της διαίρεσης των
            δύο αριθμών*/

               if(temp==0) /*  εάν τα υπόλοιπο της διαίρεσης είναι 0
            σταματάω ,αλλιώς συνεχίζω μέχρι να είναι 0 */
61.               return h;
62.            a = h;
63.            h = temp;
64.         }
65.         }


66.         void encrypt()
67.         {
68.           long int pt,ct,key=e,k,len;
69.            i=0;

/*  το strlen δίνει τη τελευταία θέση του πίνακα χαρακτήρων */

70.            len=strlen(msg);

              while(i!=len) /*  'όσο το i δεν είναι η τελευταία θέση */
71.           {
```

```
   pt=m[i];   /*  το pt είναι η θέση i του μηνύματος */
   pt=pt-96; /*  κάνω αφαίρεση το 96 γιατί από αυτό τον αριθμό
και μετά ξεκινάνε τα μικρά γράμματα στο ascii  */

72.    k=1;
   for(j=0;j<key;j++) /*  μέσω αυτή της επανάληψης βρίσκω ποιο
γράμμα βγαίνει  την ύψωση (77) και το mod n(78) */

73.    {
74.      k=k*pt;
75.      k=k%n;
76.    }


   temp[i]=k; /*  αποθηκεύω σε αυτό το πίνακα τις τιμές του k σε
κάθε θέση*/
77.

   ct=k+96; /*  'προσθέτω τον αριθμό από την αφαίρεση
παραπάνω */

   en[i]=ct; /*  αποθηκεύω σε αυτό το πίνακα τον τελικό
κρυπτογραφημένο γράμμα*/
78.
79.    i++;
80.    }
81.
82.  en[i]=-1;

83.  printf("\nTHE ENCRYPTED MESSAGE IS\n");

   for(i=0; en[i]!=-1; i++)
84.      printf("%c",(char)en[i]);

85.  printf("\n");
86.  }



87.  void decrypt()
88.  {
89.    long int pt,ct,key=d,k;
90.    i=0;
91.    while(en[i]!=-1)
92.    {
       ct=temp[i];  /*  χρησιμοποιώ το πίνακα που έφτιαξα στην
encrypt , γιατί αυτό το πίνακα θέλω να κάνω
αποκρυπτογράφηση */
93.
94.      k=1;
```

```
95.                for(j=0;j<key;j++)
96.                {
97.                  k=k*ct;
98.                  k=k%n;
99.                }
100.               pt=k+96;
101.               m[i]=pt;
102.               i++;
103.             }
104.             m[i]=-1;
105.             printf("\nTHE DECRYPTED MESSAGE IS\n");
106.             for(i=0;m[i]!= -1;i++)
107.                 printf("%c",(char)m[i]);

108.              printf("\n");

109.         }
```



-

## 4.2 ELGAMAL σε γλώσσα C

```
1.      #include<stdio.h>
2.      #include<stdlib.h>
3.      #include<math.h>
4.      #include<string.h>

        /* δηλώνω τα στοιχεία που θα χρησιμοποιήσω στο κώδικα */

5.      long int p,flag,a,x,pr,k,m,d,q,r,y,z;

        /* δηλώνω τις απαραίτητες συναρτήσεις */

6.      int  prime(long int);
7.      int ipow( long int ,long int  );

8.      void encrypt();
9.      void decrypt();

10.     int main()
11.     {

        /* ζητάμε από το χρήστη να δώσει έναν αριθμό, ο οποίος μέσα από
        την prime ελέγχουμε εάν είναι πρώτος, και η ερώτηση
        επαναλαμβάνεται εάν ο αριθμός δεν είναι πρώτος.  */
12.      do{

13.        printf("\n Enter a prime number p :\n");
14.        scanf("%ld",&p);
15.        flag=prime(p);
16.      }while(flag==0) ;

        /* ζητάμε από το χρήστη να δώσει έναν αριθμό γεννήτορα, ο
        οποίος θα είναι μεγαλύτερος της μονάδας και μικρότερος του p-1.
        */

17.      do{
18.
19.        printf("\n choose a generation number :\n");
20.        scanf("%ld",&a);
21.     }while(a<1|| a>(p-1)) ;

        /* ζητάμε από το χρήστη να δώσει έναν τυχαίο αριθμό x, ο οποίος
        θα είναι μεγαλύτερος της μονάδας, μικρότερος του p-2 και θα
        αποτελεί το ιδιωτικό του κλειδί  */

22.        do{

23.          printf("\n Enter a number x:\n");
```

```
24.          scanf("%ld",&x);

25.        }while(x>(p-2));

           /* εδώ μέσω της συνάρτησης βρίσκω τη δύναμη a^x και έπειτα
           υπολογίζω το κλειδί d*/

26.        d = ipow(a, x) % p;

27.        printf( "public key is: (%ld, %ld, %ld)\n", a ,p , d);
28.        printf( "the private key is: (%ld)\n", x);

29.      encrypt();
30.      decrypt();
31.      }


32.      int prime (long int pr)
33.      {
34.        int i;
35.        int j = sqrt (pr);

36.        for(i=2; i<=j; i++)
37.       {
38.          if(pr%i == 0)
39.          return 0;
40.       }
41.      return 1;
42.      }

           /* η συνάρτηση αυτή υπολογίζει το τη δύναμη με βάση το base και
           εκθέτη exp*/

43.      int ipow ( long int base, long  int exp )
44.      {
45.        if (exp != 0)
46.           return (base * ipow (base, exp-1));
47.        else
48.           return 1;
49.      }

50.      void encrypt()
51.      {

52.      do{
53.         printf("\n Enter a number k:\n");
54.         scanf("%ld",&k);

55.      }while(x<1 && x>(p-2));
```

-

```
56.     y = ipow (a, k) % p;

57.     do{
58.       printf ("\n Enter message m:\n");
59.       scanf ("%ld", &m);

60.     }while (m<0 || m>(p-1));

61.     printf("\n");

62.     y = ipow(a,k) % p;
63.     z = (ipow(d,k)*m) % p;

64.     printf("The ciphertext is c = (%ld , %d)", y, z);

65.     printf("\n");
66.     }

67.     void decrypt( )
68.     {
69.       q = p-1-x;
70.       r = ipow (y, q) % p;
71.       m = (r * z) % p;
72.       printf ("the message is :%ld \n",m);
73.     }
```

```
 Enter a prime number p:
7

 choose a generation number :
3

 Enter a number x:
5
public key is: (3,7,5)
the private key is: (5)

 Enter a number k:
4

 Enter message m:
6
the ciphertext is C=(4,5)
the message is :6

--------------------------------
Process exited after 22.65 seconds with return value 19
Press any key to continue . . .
```

-

# *5. ΣΥΜΠΕΡΑΣΜΑ*

Η ιστορία της κρυπτογραφίας ξεκινά από τα πολύ παλιά χρόνια πριν καν δημιουργηθούν οι πρώτοι υπολογιστές και διαδίκτυο . Τα τελευταία χρόνια έχει αναπτυχθεί σημαντικά και η χρήση της είναι απαραίτητη ακόμα και σε μικρά πράγματα της καθημερινότητας μας.
Μέσω των διάφορων μεθόδων κρυπτογράφησης τα προσωπικά δεδομένα και οι προσωπικές πληροφορίες , οι οποίες χρειάζονται σε διάφορες εφαρμογές όπως είναι οι τραπεζικές συναλλαγές , οι συναλλαγές μέσω internet και άλλα , προστατεύονται από τυχόν παραβιάσεις και αλλοιώσεις .
Οι υπογραφές , οι οποίες χρησιμοποιούνται για να πιστοποιούν την ταυτότητα ενός ατόμου ,ενώ τα περισσότερα χρόνια ήταν χειρόγραφες τώρα παίρνουν και ψηφιακή μορφή και χρησιμοποιούνται και σε ψηφιακά έγγραφα. Οι τρόποι για την δημιουργία τους είναι πολλοί ανάλογα με τον αλγόριθμο που χρησιμοποιούν .
Ο αλγόριθμος RSA είναι ο πιο γνωστός αλγόριθμος δημοσίου κλειδιού και είναι από τους αλγόριθμους που χρησιμοποιούνται πιο πολύ. Παρότι όπως και άλλοι αλγόριθμοι έχει πολλές αδυναμίες κυρίως ως προς την ασφάλεια χρησιμοποιείται συχνά.
Όλα δείχνουν ότι με την ανάπτυξη της τεχνολογίας , ο άνθρωπος θα ψάχνει συνεχώς να βρίσκει τρόπους για να προστατεύσει τα προσωπικά του δεδομένα, μιας και η τεχνολογία όπως φαίνεται θα αναπτυχθεί σε ακόμα μεγαλύτερο βαθμό στο μέλλον. Αυτό θα έχει σαν αποτέλεσμα να αναπτυχθούν και άλλοι αλγόριθμοι κρυπτογράφησης και ίσως μια μέρα να βρεθεί ο καλύτερος όλων , ο οποίος θα έχει την καλύτερη ασφάλεια.

-

# *ΒΙΒΛΙΟΓΡΑΦΙΑ*


[1] "Understanding Cryptography: A Textbook for Students and Practitioners " Christof Paar ,Jan Pelzl, Heidelberg Springer,2014

[2] "Handbook of Applied Cryptography ", A. Menezes, P. van Oorschot, and S. Vanstone, CRC Press, 1996.

[3] "Τεχνικές κρυπτογραφίας και Κρυπτανάλυσης ", Κάτος Β. ,Στεφανίδης Γ. , εκδόσεις ΖΥΓΟΣ 2003

[4] Wikipedia: Κρυπτογραφία. Διαθέσιμο στο δικτυακό τόπο: https://el.wikipedia.org/wiki/%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%AF%CE%B1

[5] Wikipedia: RSA. Διαθέσιμο στο δικτυακό τόπο: https://el.wikipedia.org/wiki/RSA

[6] Wikipedia: Υπογραφή ElGamal. Διαθέσιμο στο δικτυακό τόπο: https://el.wikipedia.org/wiki/%CE%A5%CF%80%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%AE_ElGamal

[7] Wikipedia: Κρυπτογραφία Ψηφιακή υπογραφή. Διαθέσιμο στο δικτυακό τόπο: https://el.wikipedia.org/wiki/%CE%A8%CE%B7%CF%86%CE%B9%CE%B1%CE%BA%CE%AE_%CF%85%CF%80%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%AE

[8] Εργαστηριακό μάθημα κρυπτογραφίας. Διαθέσιμο στο δικτυακό τόπο: http://cgi.di.uoa.gr/~klimn/cryptography/Lab/lab-1.pdf

[9] Εθνική επιτροπή τηλεπικοινωνιών-ψηφιακή υπογραφή. Διαθέσιμο στο δικτυακό τόπο: https://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/IntroEsign.html

[10] Ταυτοποίηση και αυθεντικοποίηση. Διαθέσιμο στο δικτυακό τόπο: http://www.icsd.aegean.gr/website_files/proptyxiako/527437721.pdf

[11] Κρυπτογραφία και ασφάλεια υπολογιστών. Διαθέσιμο στο δικτυακό τόπο: https://openeclass.teimes.gr/modules/document/file.php/CIED194/lecture03.pdf

[12] Ψηφιακές υπογραφές. Διαθέσιμο στο δικτυακό τόπο: http://utopia.duth.gr/vkatos/documents/the_book/ch8.pdf

[13] Εγχειρίδιο Εφαρμοσμένης Κρυπτογραφίας A. Menezes, P. Van Oorschot, S. Vanstone. Διαθέσιμο στο δικτυακό τόπο:
http://users.uom.gr/~steph/material/crypto/HAC_Ch11.pdf

[14] Ελληνικά ηλεκτρονικά συγγράματα Κάλλιπος. Διαθέσιμο στο δικτυακό τόπο:
https://repository.kallipos.gr/bitstream/11419/1033/1/05_Chapter_09.pdf