ΕΥΚΛΕΙΔΗΣ *γ΄*, Τεύχος 101(1–2), 2025

Εισαγωγή στην Κρυπτολογία

Δημήτριος Πουλάκης

Τμήμα Μαθηματικών

Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης

poulakis@math.auth.gr

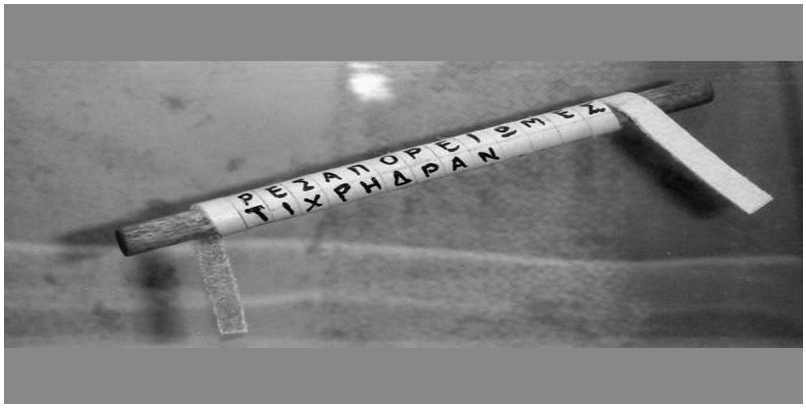
Περίληψη

Το παρόν κείμενο αποτελεί μία συνοπτική εισαγωγή στη σύγχρονη Κρυπτολογία μαζί με το απαραίτητο υπόβαθρο της Θεωρίας Αριθμών για την κατανόησή της. Ειδικότερα, δίνονται βασικές έννοιες της Κρυπτογραφίας και Κρυπτανάλυσης και περιγράφονται μερικά ιστορικά κρυπτοσυστήματα. Εισάγονται τα δύο είδη συμμετρικών κρυπτοσυστημάτων, τα κρυπτοσυστήματα ροής και τμήματος, και περιγράφεται η λειτουργίας τους. Στη συνέχεια δίνονται οι βασικές έννοιες και αποτελέσματα της Θεωρίας Αριθμών που χρειάζονται για την παρουσίαση της Κρυπτογραφίας Δημοσίου Κλειδιού. Τέλος, περιγράφεται η λειτουργία των κρυπτοσυστημάτων δημοσίου κλειδιού RSA και ElGamal, καθώς και του πρωτοκόλλου των Diffie-Hellman.

Λέξεις Κλειδιά: Κρυπτολογία, Κρυπτογραφία, Κρυπτανάλυση, Συμμετρικά Κρυπτοσυστήματα, Κρυπτοσυστήματα Δημοσίου Κλειδιού.

1. ΕΙΣΑΓΩΓΗ

Από την αρχαιότητα μέχρι σήμερα, σε πολλές ανθρώπινες δραστηριότητες υπάρχει η ανάγκη της μετάδοσης ή αποθήκευσης πληροφοριών. Η πλέον σημαντική ιδιότητα την οποία θα πρέπει να έχουν οι ενέργειες αυτές είναι η εμπιστευτικότητα, δηλαδή η πρόσβαση σε αυτές τις πληροφορίες θα πρέπει να είναι δυνατή μόνον από εξουσιοδοτημένα άτομα. Από την αρχαιότητα είχαν αναπτυχθεί μέθοδοι γι' αυτό τον σκοπό. Για παράδειγμα, μία τέτοια μέθοδος η οποία ανάγεται στον 5ο π.Χ. αιώνα, όπως αναφέρεται από τον Πλούταρχο, ήταν η Σπαρτιατική Σκυτάλη (βλ. Εικόνα 1). Ο αποστολέας[1] ενός μηνύματος τυλίγει γύρω από μία σκυτάλη μια λωρίδα από δέρμα ή περγαμηνή και κατόπιν γράφει το μήνυμα κατά μήκος της. Ο παραλήπτης, για να διαβάσει το μήνυμα, απλώς τυλίγει τη δερμάτινη λωρίδα γύρω από μια σκυτάλη ίσης διαμέτρου με αυτήν που χρησιμοποίησε ο αποστολέας.



Εικόνα 1. Η Σπαρτιατική Σκυτάλη (Πηγή: Noesis[2])

Καλούμε Κρυπτογραφία τη μελέτη των μαθηματικών μεθόδων οι οποίες εξασφαλίζουν την εμπιστευτικότητα των δεδομένων και Κρυπτανάλυση τη μελέτη των μαθηματικών μεθόδων οι οποίες επιχειρούν την αναίρεσή της. Καλούμε Κρυπτολογία τη μελέτη της Κρυπτογραφίας και της Κρυπτανάλυσης.

---

1 Από το σημείο αυτό και εξής, για λόγους οικονομίας χώρου και μόνο, χρησιμοποιείται ένα μόνο γραμματικό γένος.

2 http://archive.noesis.edu.gr/default.aspx?bridge=jpeg&c=true&m=AltaB2xUi&height=800&width=800&imageFile=/inst/noesis/gallery/Katagrafes/3182.jpg

Ας σημειωθεί ότι η Κρυπτογραφία εξασφαλίζει επίσης την αυθεντικότητα, την ακεραιότητα και την αδυναμία αποκήρυξης των δεδομένων (βλ. Πουλάκης, 2004). Η ανάπτυξη αυτών των ιδιοτήτων εκφεύγει των στόχων του κειμένου μας και γι' αυτό θα περιοριστούμε μόνο στην ιδιότητα της εμπιστευτικότητας.

Σήμερα σε πάρα πολλές τεχνολογικές εφαρμογές είναι απαραίτητη η εμπιστευτικότητα, όπως, για παράδειγμα, οι διάφορες βάσεις δεδομένων, εμπιστευτικές βιομηχανικές πληροφορίες, ηλεκτρονικό ταχυδρομείο, μετάδοση στρατιωτικών απορρήτων, ηλεκτρονικό εμπόριο, ασφάλεια τραπεζικών συναλλαγών κ.ά. Η Κρυπτογραφία αποτελεί βασικό εργαλείο για τη διαφύλαξη της εμπιστευτικότητας σε όλους αυτούς τους τομείς.

Την τελευταία πεντηκονταετία, η Κρυπτογραφία και η Κρυπτανάλυση έχουν γνωρίσει αλματώδη ανάπτυξη και πλήθος μαθηματικών αντικειμένων έχουν χρησιμοποιηθεί για την εξέλιξή τους. Κλάδοι της Θεωρίας Αριθμών, όπως οι πρώτοι αριθμοί, οι ισοτιμίες, τα πεπερασμένα σώματα, η αριθμητική των ελλειπτικών καμπυλών, τα αλγεβρικά σώματα αριθμών, η αριθμητική των πολυωνύμων, η γεωμετρία αριθμών κ.ά., έχουν αποτελέσει τη βάση για την ανάπτυξη κρυπτοσυστημάτων, αλλά και μεθόδων κρυπτανάλυσής τους.

Ας σημειωθεί ότι η Κβαντική Υπολογιστική έχει δώσει πλήθος Κβαντικών μεθόδων κρυπτογράφησης και κρυπτανάλυσης. Μία συνέπεια της αναμενόμενης ανάπτυξης των κβαντικών υπολογιστών είναι η κρυπτανάλυση πολλών κρυπτοσυστημάτων δημοσίου κλειδιού τα οποία χρησιμοποιούνται ευρέως σήμερα. Αυτό είχε ως αποτέλεσμα την ανάπτυξη της Μετα-Κβαντικής Κρυπτογραφίας, δηλαδή κρυπτοσυστημάτων τα οποία ανθίστανται στις κβαντικές επιθέσεις. Τέτοιοι κλάδοι της κρυπτογραφίας είναι οι: Συμμετρική Κρυπτογραφία, Πολυμεταβλητή Κρυπτογραφία, Κρυπτογραφία με πλέγματα, Κρυπτογραφία με Κώδικες Διορθωτές Λαθών, Κρυπτογραφία με Συναρτήσεις Κατακερματισμού κ.ά. (Bernstein κ.ά., 2009).

Το κείμενο αυτό παρουσιάζει μία συνοπτική εισαγωγή στο αντικείμενο της Κρυπτολογίας μαζί με την ύλη της Θεωρίας Αριθμών η οποία είναι απαραίτητη για την κατανόησή της. Το κείμενο είναι οργανωμένο σε έξι ενότητες. Στη δεύτερη ενότητα δίνονται βασικές έννοιες της Κρυπτογραφίας και της Κρυπτανάλυσης. Στην τρίτη ενότητα περιγράφονται μερικά ιστορικά κρυπτοσυστήματα. Στην τέταρτη ενότητα παρουσιάζονται δύο κρυπτοσυστήματα τα οποία σκιαγραφούν αντίστοιχα την λειτουργία των δύο ειδών συμμετρικών κρυπτοσυστημάτων: των κρυπτοσυστημάτων ροής και

των κρυπτοσυστημάτων τμήματος. Η πέμπτη ενότητα περιέχει την ύλη της Θεωρίας Αριθμών, η οποία απαιτείται για την περιγραφή των κρυπτοσυστημάτων δημοσίου κλειδιού, καθώς και δύο σχετικά συμμετρικά κρυπτοσυστήματα. Η έκτη ενότητα είναι αφιερωμένη στην Κρυπτογραφία Δημοσίου Κλειδιού και ειδικότερα στη παρουσίαση του πρωτοκόλλου κατασκευής κοινού κλειδιού των Diffie – Hellman και των κρυπτοσυστημάτων RSA και ElGamal. Σημειώνεται ότι στο Παράρτημα παρατίθεται μία συλλογή ασκήσεων για την καλύτερη κατανόηση των περιγραφόμενων εννοιών.

Στο Νέο Πρόγραμμα Σπουδών για τα Μαθηματικά του Λυκείου (Φ.Ε.Κ. 2023, σελ. 11565) υπογραμμίζεται ότι:

> Μια κεντρική διδακτική πρακτική του/της εκπαιδευτικού αφορά την επιλογή και διαχείριση του κατάλληλου μαθηματικού έργου που θα πυροδοτήσει την επιθυμητή μαθηματική δραστηριότητα. Πρόκειται για την εργασία που αναθέτει ο εκπαιδευτικός σε μαθητές/-τριες [...], καλείται να μην περιορίζει τις επιλογές του σε έργα που εστιάζουν στην εφαρμογή αλγορίθμων και μαθηματικών τύπων, αλλά να επιλέγει έργα που ανταποκρίνονται στα ενδιαφέροντα και τις εμπειρίες των μαθητών/-τριών, αντλούν προβληματισμούς από πραγματικές καταστάσεις της καθημερινότητας, επιδέχονται διαφορετικές μεθόδους επίλυσης και απαιτούν τεκμηριωμένες επεξηγήσεις και παραδοχές.

Θεωρούμε ότι το θεωρητικό πλαίσιο, αλλά και τα συγκεκριμένα παραδείγματα και προβλήματα που προσφέρουμε στην εργασία αυτή για την Κρυπτολογία, δίνουν μία βάση στην οποία ο εκπαιδευτικός θα σχεδιάσει πώς θα οδηγήσει τους μαθητές του για να ασχοληθούν με προβλήματα που αφορούν πραγματικές καταστάσεις τα οποία έχουν ενδιαφέρον για αυτούς.

2. ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ

Σε αυτή την ενότητα δίνουμε βασικές έννοιες της Κρυπτολογίας και υπενθυμίζουμε απλές μαθηματικές έννοιες τις οποίες θα χρειαστούμε παρακάτω.

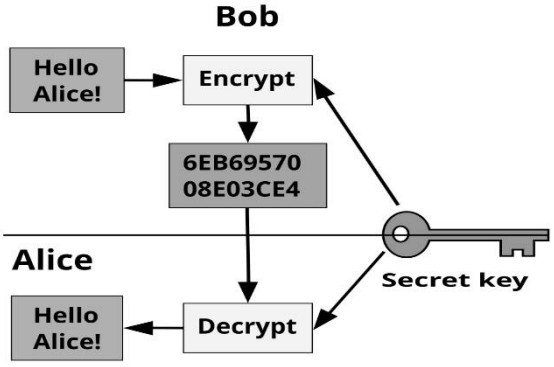
2.1 Κρυπτογράφηση

Η διασφάλιση της εμπιστευτικότητας των πληροφοριών επιτυγχάνεται με τον μετασχηματισμό τους σε μορφή κατανοητή μόνο από κάθε εξουσιοδοτημένο παραλήπτη. Η ενέργεια αυτή καλείται *κρυπτογράφηση*. Ένα σχήμα *κρυπτογράφησης* ή *κρυπτοσύστημα* είναι μία πεντάδα συνόλων $(\boldsymbol{\mathcal{P}},\boldsymbol{\mathcal{C}},\boldsymbol{\mathcal{K}},\boldsymbol{\mathcal{E}},\boldsymbol{\mathcal{D}})$.

Τα σύνολα $\boldsymbol{\mathcal{P}}$, $\boldsymbol{\mathcal{C}}$, $\boldsymbol{\mathcal{K}}$ καλούνται, αντίστοιχα, *χώρος των απλών κειμένων, χώρος των κρυπτογραφημένων κειμένων* ή *κρυπτοκειμένων* και *χώρος των κλειδιών*. Για κάθε $k \in \boldsymbol{\mathcal{K}}$, υπάρχουν συναρτήσεις $E_k : \boldsymbol{\mathcal{P}} \rightarrow \boldsymbol{\mathcal{C}}$ και $D_k : \boldsymbol{\mathcal{C}} \rightarrow \boldsymbol{\mathcal{P}}$ οι οποίες καλούνται *συνάρτηση κρυπτογράφησης* και *συνάρτηση αποκρυπτογράφησης* οι οποίες αντιστοιχούν στο κλειδί k. Οι συναρτήσεις E_k αποτελούν το *σύνολο των συναρτήσεων κρυπτογράφησης* $\boldsymbol{\mathcal{E}}$ και οι συναρτήσεις D_k το *σύνολο των συναρτήσεων αποκρυπτογράφησης* $\boldsymbol{\mathcal{D}}$. Επίσης, για κάθε $e \in \boldsymbol{\mathcal{K}}$ υπάρχει $d \in \boldsymbol{\mathcal{K}}$ με $D_d(E_e(m)) = m$, για κάθε $m \in \boldsymbol{\mathcal{P}}$. Το e καλείται *κλειδί κρυπτογράφησης* και το d *κλειδί αποκρυπτογράφησης* το οποίο αντιστοιχεί στο e.

Αν ένας χρήστης A επιθυμεί να κρυπτογραφήσει ένα μήνυμα $m \in \boldsymbol{\mathcal{P}}$ και να το στείλει σ' έναν άλλο χρήστη B, τότε χρησιμοποιεί ένα κλειδί κρυπτογράφησης e και στέλνει στον B το κρυπτογραφημένο μήνυμα $E_e(m)$. Ο B χρησιμοποιεί το αντίστοιχο κλειδί αποκρυπτογράφησης d και βρίσκει το m υπολογίζοντας $D_d(E_e(m)) = m$.

Ένα κρυπτοσύστημα καλείται *συμμετρικό,* αν για κάθε $e \in \boldsymbol{\mathcal{K}}$ το κλειδί αποκρυπτογράφησης d το οποίο αντιστοιχεί στο e είναι δυνατόν να υπολογιστεί πολύ εύκολα από το e. Οι χρήστες ενός τέτοιου σχήματος θα πρέπει να διαφυλάττουν το e μυστικό και να το ανταλλάσσουν πριν την επικοινωνία τους.

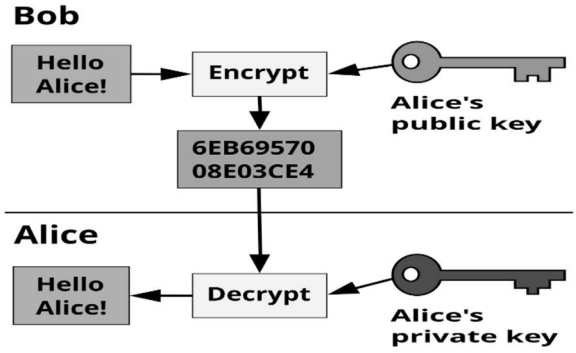


Εικόνα 2. Μορφή ενός συμμετρικού κρυπτοσυστήματος (Πηγή: Wikipedia[3])

[3] https://commons.wikimedia.org/wiki/File:Symmetric_key_encryption.svg

Βασικό πρόβλημα: Η ασφαλής διανομή κλειδιού για συμμετρικά κρυπτοσυστήματα.

Ένα κρυπτοσύστημα καλείται *ασύμμετρο*, αν ο υπολογισμός του d από το e είναι πρακτικά αδύνατος. Σε τέτοια σχήματα κρυπτογράφησης το κλειδί κρυπτογράφησης e δημοσιοποιείται, ενώ το αντίστοιχο κλειδί αποκρυπτογράφησης d κρατείται μυστικό. Έτσι, οποιοσδήποτε μπορεί να στείλει κρυπτογραφημένο μήνυμα στον χρήστη στον οποίο αντιστοιχεί το κλειδί κρυπτογράφησης e, ο οποίος το αποκρυπτογραφεί με την χρήση του d το οποίο μόνο αυτός γνωρίζει. Τα ασύμμετρα κρυπτοσυστήματα καλούνται επίσης και *κρυπτοσυστήματα δημόσιου κλειδιού.* \



Εικόνα 3. Μορφή ενός ασύμμετρου κρυπτοσυστήματος (Πηγή: Wikipedia[4]).

Ας σημειωθεί ότι συνήθως, η κρυπτογράφηση μεγάλης ποσότητας δεδομένων με ένα ασύμμετρο σχήμα κρυπτογράφησης απαιτεί πολύ περισσότερο χρόνο από ότι με ένα συμμετρικό. Έτσι, συχνά στην πράξη, πολλές φορές χρησιμοποιείται ένα συμμετρικό σχήμα για την κρυπτογράφηση ενός μηνύματος και ένα σχήμα δημοσίου κλειδιού για την αποστολή του κλειδιού που θα χρησιμοποιηθεί.

2.2 Είδη κρυπταναλυτικών επιθέσεων

Η ασφάλεια ενός σχήματος κρυπτογράφησης, σύμφωνα με την αρχή του Kerckhoffs (Kerckhoffs, 1883a· Kerckhoffs, 1883b), δεν πρέπει να εξαρτάται από τη μυστική διαφύλαξη της μεθόδου κρυπτογράφησης, αλλά μόνο από τη μυστική διαφύλαξη των κλειδιών. Επομένως, υποθέτουμε πάντα ότι ένας

4 https://en.wikipedia.org/wiki/Public-key_cryptography#/ media/File:Public_key_encryption.svg

κρυπταναλυτής γνωρίζει τον τύπο του σχήματος κρυπτογράφησης που θέλει να προσβάλει. Οι πλέον συνήθεις τύποι κρυπταναλυτικών επιθέσεων είναι οι εξής:

1. *Επίθεση κρυπτογραφημένου κειμένου.* Ο κρυπταναλυτής έχει στην κατοχή του κρυπτογραφημένα κείμενα και προσπαθεί να βρει το κλειδί αποκρυπτογράφησης ή τα αντίστοιχα απλά κείμενα.
2. *Επίθεση γνωστού απλού κειμένου.* Στην περίπτωση ενός συμμετρικού κρυπτοσυστήματος, ο κρυπταναλυτής έχει στην κατοχή του ζεύγη από απλά κείμενα και τα αντίστοιχα κρυπτογραφημένα με το ίδιο κλειδί. Σκοπός του είναι η αποκρυπτογράφηση άλλων κειμένων ή η εύρεση του κλειδιού αποκρυπτογράφησης.
3. *Επίθεση επιλεγμένου απλού κειμένου.* Στην περίπτωση ενός συμμετρικού κρυπτοσυστήματος, ο κρυπταναλυτής έχει την δυνατότητα να κρυπτογραφεί επιλεγμένα απλά κείμενα, χωρίς όμως να γνωρίζει το κλειδί της κρυπτογράφησης. Σκοπός του είναι η εύρεση του κλειδιού αποκρυπτογράφησης ή η αποκρυπτογράφηση άλλων κειμένων.
4. *Επίθεση επιλεγμένου κρυπτογραφημένου κειμένου.* Ο κρυπταναλυτής έχει την δυνατότητα να αποκρυπτογραφεί κάποια επιλεγμένα από τον ίδιο κρυπτοκείμενα χωρίς όμως να γνωρίζει το κλειδί της αποκρυπτογράφησης. Σκοπός του είναι η αποκρυπτογράφηση ενός συγκεκριμένου κρυπτοκειμένου το οποίο δεν έχει την δυνατότητα να αποκρυπτογραφήσει ή η εύρεση του κλειδιού αποκρυπτογράφησης.

Στην επόμενη ενότητα θα παρουσιάσουμε τέσσερα ιστορικά κρυπτοσυστήματα. Για τον σκοπό αυτό θα χρειαστούμε την έννοια της μετάθεσης και της πράξης XOR τις οποίες εισάγουμε παρακάτω.

2.3 Μεταθέσεις

Ας είναι $f : A \rightarrow B$ μία συνάρτηση. Λέμε ότι η f είναι *ένεση,* αν για κάθε $x,y \in A$ με $x \neq y$ έχουμε $f(x) \neq f(y)$. Εύκολα βλέπουμε ότι η f είναι *ένεση,* αν και μόνον αν, για $x,y \in A$ με $f(x) = f(y)$ συνεπάγεται ότι $x = y$. Λέμε ότι η f είναι *έφεση,* αν για κάθε $y \in B$ υπάρχει $x \in A$ με $f(x) = y$. Επίσης, η f καλείται *αμφίεση* αν είναι ένεση και έφεση. Η f είναι αμφίεση αν και μόνον αν υπάρχει μία συνάρτηση $g : B \rightarrow A$ τέτοια, ώστε να ισχύει $f(g(x)) = x$, για κάθε $x \in B$, και $g(f(x) = x$, για κάθε $x \in A$. Η συνάρτηση g είναι μοναδική, συμβολίζεται με f^{-1} και καλείται *αντίστροφη* συνάρτηση της f.

Παράδειγμα 2.1. Ας θεωρήσουμε το σύνολο των φυσικών αριθμών $\mathbb{N}$ και την συνάρτηση $h : \mathbb{N} \to \mathbb{N}$ με $h(n) = n+1$, για κάθε $n \in \mathbb{N}$. Παρατηρούμε ότι αν $m,n \in \mathbb{N}$ με $h(m) = h(n)$, τότε $m+1 = n+1$ και επομένως $m = n$. Άρα, η συνάρτηση h είναι ένεση. Επίσης, παρατηρούμε ότι δεν υπάρχει $n \in \mathbb{N}$ τέτοιο, ώστε $n+1 = 0$, το οποίο ισοδυναμεί με $h(n) = 0$. Επομένως, η συνάρτηση h δεν είναι έφεση.

Παράδειγμα 2.2. Ας θεωρήσουμε στη συνέχεια το σύνολο των ακεραίων αριθμών $\mathbb{Z}$ και την συνάρτηση $g : \mathbb{Z} \to \mathbb{N}$ με $g(z) = |z|$, για κάθε $z \in \mathbb{Z}$. Καθώς για κάθε $n \in \mathbb{N}$ έχουμε $g(n) = n$, η g είναι έφεση. Επίσης, παρατηρούμε ότι ισχύει $g(1) = 1 = g(-1)$ και επομένως η g δεν είναι ένεση.

Παράδειγμα 2.3. Ας είναι $\mathbb{R}$ το σύνολο των πραγματικών αριθμών και $a, b \in \mathbb{R}$ με $a \neq 0$. Θεωρούμε την συνάρτηση $f : \mathbb{R} \to \mathbb{R}$, με $f(x) = ax+b$ για κάθε $x \in \mathbb{R}$. Αν $x,y \in \mathbb{R}$ με $f(x) = f(y)$, τότε $ax+b = ay+b$ και επομένως παίρνουμε $x = y$. Άρα, η συνάρτηση f είναι ένεση. Επίσης, αν $y \in \mathbb{R}$, τότε για $z = (y-b)/a$ έχουμε $f(z) = y$ και επομένως, η συνάρτηση f είναι έφεση. Συνεπώς, η συνάρτηση f είναι αμφίεση με αντίστροφο συνάρτηση την $g : \mathbb{R} \to \mathbb{R}$ με $g(y) = (y-b)/a$, για κάθε $y \in \mathbb{R}$.

Καλούμε *μετάθεση* ενός πεπερασμένου συνόλου A κάθε αμφίεση του A στον εαυτό του. Συμβολίζουμε με S(A) το σύνολο των μεταθέσεων του A. Ας είναι $A = \{a_1,\ldots,a_n\}$. Για να ορίσουμε μία μετάθεση σ του A μπορούμε να πάρουμε ως $\sigma(\alpha_1)$ οποιοδήποτε από τα $a_1, \ldots, a_n$ και επομένως υπάρχουν n τρόποι για να γίνει αυτό. Κατόπιν, μπορούμε να πάρουμε ως $\sigma(\alpha_2)$ οποιοδήποτε από τα υπόλοιπα $n-1$ στοιχεία και υπάρχουν $n-1$ τρόποι για να γίνει αυτό. Δηλαδή, υπάρχουν $n(n-1)$ τρόποι για να επιλέξουμε τα στοιχεία $\sigma(\alpha_1)$ και $\sigma(\alpha_2)$. Συνεχίζοντας αυτή την διαδικασία, βλέπουμε ότι υπάρχουν $n(n-1) \cdots 3 \cdot 2 \cdot 1 = n!$ τρόποι για να επιλέξουμε τα στοιχεία $\sigma(\alpha_1),\ldots,\sigma(\alpha_n)$. Συνεπώς, το πλήθος των στοιχείων του S(A) είναι $n!$.

Αν $A = \{1,\ldots,n\}$, τότε θα γράφουμε πιο απλά S_n αντί S(A). Επίσης, θα παριστάνουμε μία μετάθεση του S_n με μία αντιστοίχιση όπως παρακάτω:

$$\sigma = \begin{pmatrix} 1 & \ldots & n \\ \sigma(1) & \ldots & \sigma(n) \end{pmatrix}$$

Για παράδειγμα, ο πίνακας

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

παριστάνει την μετάθεση σ με $\sigma(1) = 2$, $\sigma(2) = 4$, $\sigma(3) = 3$, $\sigma(4) = 1$.

2.4 Η πράξη XOR

Ας είναι $B = \{0,1\}$. Στο σύνολο αυτό θα ορίσουμε μία πράξη την οποία συμβολίζουμε με $\oplus$ και είναι γνωστή ως πράξη XOR. Αυτό γίνεται ως εξής:

$$0\oplus 0 = 1\oplus 1 = 0 \quad \text{και} \quad 1\oplus 0 = 0\oplus 1 = 1.$$

Ας είναι m θετικός ακέραιος. Η παραπάνω πράξη μπορεί να επεκταθεί στα στοιχεία του καρτεσιανού γινομένου B^m. Για κάθε ζεύγος στοιχείων $x = (x_1,\ldots,x_m)$ και $y = (y_1,\ldots,y_m)$ του B^m θέτουμε:

$$x\oplus y = (x_1\oplus y_1,\ldots,x_m\oplus y_m)$$

Θα συμβολίζουμε πιο απλά με 0 το στοιχείο $(0,\ldots,0)$ του B^m. Συχνά, ένα στοιχείο $(x_1,\ldots,x_m)$ του B^m θα συμβολίζεται με $x_1\ldots x_m$. Επαληθεύουμε εύκολα ότι ισχύουν οι ακόλουθες ιδιότητες:

1. $(x\oplus y)\oplus z = x\oplus(y\oplus z)$, για κάθε $x,y,z\in B^m$
2. $x\oplus y = y\oplus x$, για κάθε $x,y\in B^m$
3. $x\oplus 0 = x$, για κάθε $x\in B^m$
4. $x\oplus x = 0$, για κάθε $x\in B^m$

Παράδειγμα 2.4. Θα υπολογίσουμε το αποτέλεσμα της πράξης XOR μεταξύ των στοιχείων (1,0,0,1,1) και (0,0,1,1,0) του B^5. Έχουμε:

$$(1,0,0,1,1)\oplus(0,0,1,1,0) = (1\oplus 0,0\oplus 0,0\oplus 1,1\oplus 1,1\oplus 0) = (1,0,1,0,1).$$

3. ΜΕΡΙΚΑ ΙΣΤΟΡΙΚΑ ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΑ

Στην ενότητα αυτή θα παρουσιάσουμε τέσσερα κλασικά κρυπτοσυστήματα: το κρυπτοσύστημα αντικατάστασης, το κρυπτοσύστημα του Vigenère, το κρυπτοσύστημα μετάθεσης και το σημειωματάριο της μίας χρήσης.

3.1 Το κρυπτοσύστημα αντικατάστασης

Ένα από τα πλέον γνωστά και ευρέως χρησιμοποιημένα κρυπτοσυστήματα επί σειρά αιώνων είναι το *κρυπτοσύστημα αντικατάστασης*. Οι χώροι των απλών και κρυπτογραφημένων κειμένων αυτού του κρυπτοσυστήματος είναι ένα πεπερασμένο σύνολο A. Ο χώρος κλειδιών είναι το σύνολο S(A). Για κάθε $\sigma\in S(A)$ ορίζουμε την συνάρτηση κρυπτογράφησης

$$E_\sigma: A \to A,\ x \mapsto \sigma(x)$$

και τη συνάρτηση αποκρυπτογράφησης

$$D_\sigma: A \to A,\ x \mapsto \sigma^{-1}(x)$$

οι οποίες αντιστοιχούν στη μετάθεση σ.

Αν το σύνολο Α έχει n στοιχεία, τότε ο χώρος κλειδιών, δηλαδή το σύνολο S(A), έχει n! στοιχεία. Στην περίπτωση του λατινικού αλφαβήτου έχουμε n = 26 και επομένως υπάρχουν περισσότερα από $4 \cdot 10^{26}$ κλειδιά. Έτσι, ακόμη και για έναν υπολογιστή, η μέθοδος της δοκιμής όλων των δυνατών κλειδιών για την αποκρυπτογράφηση ενός κειμένου δεν είναι πρακτικά αποδοτική.

Παράδειγμα 3.1. Ας υποθέσουμε ότι θέλουμε να χρησιμοποιήσουμε το κρυπτοσύστημα αντικατάστασης με χώρο απλών μηνυμάτων το λατινικό αλφάβητο. Θεωρούμε τη μετάθεση η οποία δίνεται από τον παρακάτω Πίνακα 1. Η πρώτη στήλη περιέχει το λατινικό αλφάβητο και κάτω από κάθε γράμμα το γράμμα στο οποίο αντιστοιχεί.

Πίνακας 1. Μορφή ενός κρυπτοσυστήματος δημοσίου κλειδιού

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

Χρησιμοποιώντας την παραπάνω μετάθεση, κρυπτογραφούμε το μήνυμα

THE PIN IS TEN TWO SIX

και παίρνουμε το κρυπτοκείμενο

TCBUXJXRTBJKJBRXG

(κατά την κρυπτογράφηση δεν διατηρήθηκε το διάστημα μεταξύ των λέξεων). Η αποκρυπτογράφηση του μηνύματος γίνεται με την εφαρμογή σ' αυτό της αντίστροφης απεικόνισης.

Ας είναι $A = \{a_1,\ldots,a_n\}$ και $k \in \{1,\ldots,n\}$. Καλούμε *μετατόπιση* κατά k θέσεις τη μετάθεση μ_k του Α η οποία ορίζεται ως εξής:

$$\mu_k(a_i) = a_{k+i} \quad (i = 1,\ldots,n-k)$$

$$\mu_k(a_i) = a_{i-n+k} \quad (i = n-k+1,\ldots,n)$$

Δηλαδή, η μετάθεση μ_k απεικονίζει τα στοιχεία $a_1,\ldots,a_{n-k},\ldots,a_n$ στα $a_{k+1},\ldots,a_n,a_1,\ldots,a_k$, αντίστοιχα. Παρατηρούμε ότι $\mu_k^{-1} = \mu_{n-k}$, δηλαδή η αντίστροφος συνάρτηση μίας μετατόπισης είναι επίσης μία μετατόπιση. Ένα κρυπτοσύστημα αντικατάστασης που χρησιμοποιεί τέτοιες μεταθέσεις καλείται *κρυπτοσύστημα μετατόπισης*.

Αν Α είναι το λατινικό αλφάβητο και k = 3, τότε προκύπτει το ιστορικό κρυπτοσύστημα του Ιούλιου Καίσαρα. Το πλήθος των κλειδιών σ' ένα κρυπτοσύστημα μετατόπισης ισούται με το πλήθος των στοιχείων του συνόλου Α. Έτσι, στην περίπτωση όπου το Α έχει λίγα στοιχεία, για

παράδειγμα στην περίπτωση όπου είναι το αλφάβητο μίας φυσικής γλώσσας, τότε το κρυπτοσύστημα μετατόπισης μπορεί πολύ εύκολα να κρυπταναλυθεί αφού όλα τα δυνατά κλειδιά μπορούν να δοκιμαστούν με εξαντλητικό τρόπο.

Στη γενική περίπτωση, όπως είδαμε παραπάνω, ο χώρος κλειδιών ενός κρυπτοσυστήματος αντικατάστασης είναι αρκετά μεγάλος και επομένως η μέθοδος της εξαντλητικής αναζήτησης του κλειδιού δεν είναι αποτελεσματική. Από την άλλη πλευρά, το κρυπτοσύστημα αντικατάστασης είναι πολύ ευάλωτο στην κρυπτανάλυση γνωστού απλού κειμένου. Πράγματι, αν ένα απλό κείμενο το οποίο περιλαμβάνει όλα τα στοιχεία του Α και το αντίστοιχο κρυπτογραφημένο του είναι γνωστά, η μετάθεση η οποία χρησιμοποιήθηκε για την κρυπτογράφηση προσδιορίζεται πολύ εύκολα.

Στην περίπτωση όπου το Α είναι το αλφάβητο μίας φυσικής γλώσσας, οι στατιστικές ιδιότητες αυτής της γλώσσας χρησιμοποιούνται για την κρυπτανάλυση αυτού του σχήματος. Αυτό βασίζεται στο γεγονός ότι το κρυπτογραφημένο κείμενο το οποίο δημιουργείται μετά την εφαρμογή του κρυπτοσυστήματος αντικατάστασης διατηρεί την κατανομή συχνότητας εμφάνισης των γραμμάτων του απλού κειμένου. Η παρατήρηση αυτή διατυπώθηκε τον 9ο μ.Χ. αιώνα από τον Άραβα Φιλόσοφο Αλ Κιντί.

Ας θεωρήσουμε την αγγλική γλώσσα. Η πιθανότητα εμφάνισης των γραμμάτων της έχει υπολογιστεί δια μέσου των περιοδικών, εφημερίδων, βιβλίων κ.λπ. και τα γράμματα του αγγλικού αλφαβήτου έχουν ταξινομηθεί σε πέντε ομάδες:

1. E, με πιθανότητα εμφάνισης 0.127.
2. T, A, O, I, N, S, H, R, με πιθανότητα εμφάνισης μεταξύ 0.06 και 0.09.
3. D, L, με πιθανότητα εμφάνισης 0.043 και 0.040 αντίστοιχα.
4. C, U, M, W, F, G, Y, P, B, με πιθανότητα εμφάνισης μεταξύ 0.015 και 0.028.
5. V, K, J, X, Q, Z, με πιθανότητα εμφάνισης μικρότερη του 0.01.

Τα 30 ζεύγη γραμμάτων με την μεγαλύτερη πιθανότητα εμφάνισης είναι κατά σειρά συχνότερης εμφάνισης τα εξής: TH, HE, IN, ER, AN, RE, ED,ON,ES,ST, EN, AT, TO, NT, HA, ND,OU, EA, NG, AS, OR, TI, IS, ET, IT, AR, TE, SE, HI και OF. Επιπλέον, οι 12 τριάδες γραμμάτων με την μεγαλύτερη πιθανότητα εμφάνισης είναι κατά σειρά συχνότερης εμφάνισης οι εξής: THE, ING, AND, HER, ERE, ENT, THA, NTH, WAS, ETH, FOR και DTH. Ανάλογα αποτελέσματα υπάρχουν και για άλλες φυσικές γλώσσες.

Έτσι, το σύμβολο που έχει το μεγαλύτερο πλήθος εμφανίσεων στο κρυπτογραφημένο κείμενο αντιστοιχεί με μεγάλη πιθανότητα στο Ε. Το σύμβολο με το αμέσως μικρότερο πλήθος εμφανίσεων θα είναι κάποιο από τα T, A, O, I, N, S, H, R. Συνεχίζοντας μ' αυτό τον τρόπο και εξετάζοντας επίσης την εμφάνιση ζευγών, τριάδων κ.λπ. είναι δυνατόν μετά από δοκιμές να υπολογιστεί το κλειδί κρυπτογράφησης. Αναγκαία προϋπόθεση είναι η ύπαρξη αρκετής ποσότητας κρυπτογραφημένου κειμένου.

Παράδειγμα 3.2. Το παρακάτω κείμενο έχει προκύψει από την κρυπτογράφηση ενός κειμένου στην αγγλική γλώσσα και την χρήση του κρυπτοσύστημα αντικατάστασης:

RJJY ZXYT RTWW TBFY KNAJ HTRJ FQTS JYMN WYJJ SNRU TWYF SYIT HZRJ SYXR ZXYG JJCH MFSL JIMJ WHZQ JUTN WTY

Καθώς τα γράμματα τα οποία έχουν το μεγαλύτερο πλήθος εμφάνισης είναι το J (13 φορές) και το Y (10 φορές), τα αντιστοιχούμε στα Ε και Τ. Παρατηρούμε ότι η μετατόπισή των Ε και Τ κατά 5 θέσεις δίνει τα J και Y. Έτσι, υποθέτουμε ότι το παραπάνω κείμενο έχει κρυπτογραφηθεί με την χρήση της μετατόπισης μ_5 και εφαρμόζουμε σε αυτό την αντίστροφη μετατόπιση μ_{21} η οποία μας δίνει τελικά το εξής κείμενο:

MEET US TOMORROW AT FIVE COME ALONE THIRTEEN IMPORTANT DOCUMENTS MUST BE EXCHANGED HERCULE POIROT

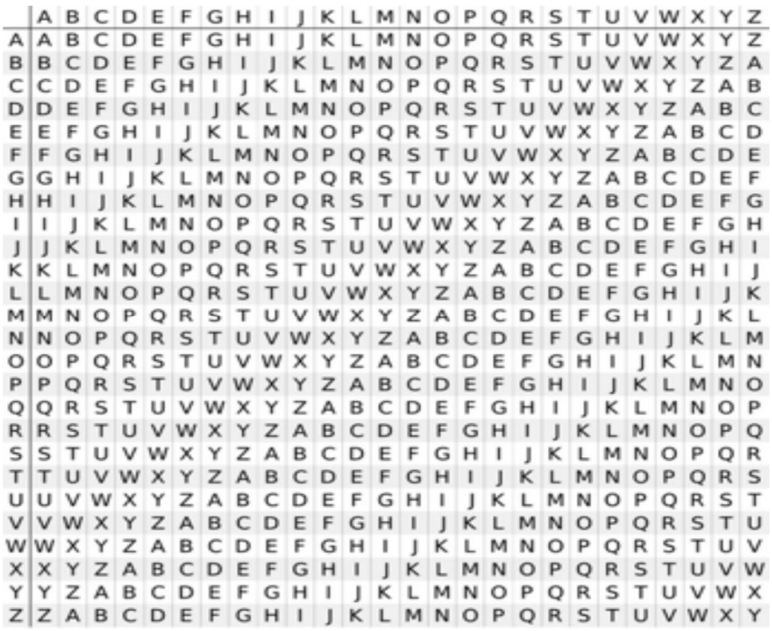
3.2 Το κρυπτοσύστημα του Vigenère

Το *κρυπτοσύστημα του Vigenère* το οποίο θα παρουσιάσουμε σ' αυτή την ενότητα περιεγράφηκε για πρώτη φορά το 1553 από τον Giovan Battista Bellaso σε ένα βιβλίο του και στη συνέχεια το 1596 από τον Γάλλο διπλωμάτη Blaise de Vigenère στον οποίο και αποδόθηκε.

Το πρότυπο κρυπτοσύστημα του Vigenère χρησιμοποιεί το λατινικό αλφάβητο και τον πίνακα της Εικόνας 4. Οι ενέργειες της κρυπτογράφησης και αποκρυπτογράφησης των κειμένων γίνονται ως εξής:

1. Επιλέγουμε μία λέξη-κλειδί.
2. Για την κρυπτογράφηση ενός κειμένου γράφουμε την λέξη-κλειδί πάνω από το κείμενο τόσες φορές ώστε να το καλύψει. Για κάθε γράμμα του κειμένου βρίσκουμε το γράμμα που είναι στη τομή της στήλης του πίνακα που αρχίζει από αυτό και της γραμμής που αρχίζει από το αντίστοιχο γράμμα του κλειδιού.

3. Για την αποκρυπτογράφηση ενός κειμένου γράφεται η λέξη-κλειδί πάνω από το κρυπτογραφημένο κείμενο τόσες φορές ώστε να το καλύψει. Για κάθε γράμμα του κρυπτοκειμένου θεωρούμε την στήλη του πίνακα που ορίζει το αντίστοιχο γράμμα του κλειδιού και την κατεβαίνουμε μέχρι να το βρούμε. Το γράμμα που ορίζει την γραμμή είναι το αντίστοιχο γράμμα του απλού κειμένου.



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

Εικόνα 4. Πίνακας του Vigenère (Πηγή: Wikipedia[5]).

Στη συνέχεια δίνουμε ένα παράδειγμα χρήσης του κρυπτοσυστήματος.

Παράδειγμα 3.3. Θα χρησιμοποιήσουμε το κρυπτοσύστημα του Vigenère για να κρυπτογραφήσουμε το εξής κείμενο:

TO BE OR NOT TO BE THAT IS THE QUESTION

Επιλέγουμε ως λέξη-κλειδί την λέξη RELATIONS και την γράφουμε πάνω από το κείμενο ώστε να το καλύψουμε. Έτσι, έχουμε:

Λέξη – κλειδί: RELAT IONSR ELATI ONSRE LATIO NSREL

5 https://en.wikipedia.org/wiki/Tabula_recta#/media/File:Vigenère_square_shading.svg

Απλό Κείμενο: TOBEO RNOTT OBETH ATIST HEQUE STION

Για να κρυπτογραφήσουμε το πρώτο γράμμα Τ θεωρούμε την στήλη η οποία αρχίζει από αυτό και την κατεβαίνουμε μέχρι να συναντήσουμε την γραμμή την οποία ορίζει το αντίστοιχο γράμμα R του κλειδιού το οποίο υπάρχει πάνω από το Τ. Το γράμμα το οποίο βρίσκεται στην τομή αυτής της στήλης και γραμμής είναι το Κ. Επομένως, η κρυπτογράφηση του Τ είναι το Κ. Συνεχίζοντας με αυτό τον τρόπο βρίσκουμε το κρυπτοκείμενο:

KSMEH ZBBLK SMEMP OGAJX SEJCS FLZSY

Για να αποκρυπτογραφήσουμε αυτό το κείμενο, γράφουμε τη λέξη RELATIONS τόσες φορές πάνω από το κρυπτοκείμενο ώστε να το καλύψουμε και έτσι παίρνουμε την αντιστοιχία:

Λέξη – κλειδί: RELAT IONSR ELATI ONSRE LATIO NSREL

Κρυπτοκείμενο: KSMEH ZBBLK SMEMP OGAJX SEJCS FLZSY

Για να αποκρυπτογραφήσουμε το πρώτο γράμμα Κ θεωρούμε την στήλη την οποία ορίζει το γράμμα του κλειδιού το οποίο βρίσκεται πάνω από το Κ, δηλαδή το R, και την κατεβαίνουμε μέχρι να βρούμε το Κ. Η γραμμή στην οποία βρίσκεται το Κ ορίζεται από το Τ. Συνεπώς, η αποκρυπτογράφηση του Κ είναι το Τ. Συνεχίζοντας αυτή την διαδικασία βρίσκουμε το απλό κείμενο.

Ας δούμε τώρα με λεπτομέρεια τη διαδικασία της κρυπτογράφησης στο παραπάνω παράδειγμα. Για την κρυπτογράφηση του Τ θεωρήσαμε την στήλη του πίνακα που αρχίζει από αυτό και την κατεβήκαμε μέχρι να συναντήσουμε την γραμμή που ορίζει το αντίστοιχο γράμμα R του κλειδιού το οποίο βρίσκεται στη 18η θέση του αγγλικού αλφαβήτου. Άρα, η κρυπτογράφηση του Τ έγινε με την κυκλική μετατόπισή του μέσα στο αγγλικό αλφάβητο κατά 17 θέσεις. Ομοίως, η κρυπτογράφηση του Ο έγινε με την μετατόπιση του κατά 4 θέσεις, του Β κατά 10 θέσεις, το Ε δεν μετατοπίστηκε, του Ο κατά 19 θέσεις, του R κατά 8 θέσεις, του Ν κατά 14 θέσεις, του Ο κατά 13 θέσεις και του Τ κατά 11 θέσεις. Το ίδιο συμβαίνει και με τα γράμματα του κειμένου τα οποία βρίσκονται κάτω από την επόμενη γραφή της λέξης - κλειδί κ.ο.κ. Δηλαδή, τα γράμματα του κλειδιού ορίζουν την κρυπτογράφηση των αντιστοίχων γραμμάτων του κειμένου με ένα κρυπτοσύστημα μετατόπισης και τις απεικονίσεις μ_{17}, μ_4, μ_{10}, μ_0, μ_{19}, μ_8, μ_{14}, μ_{13}, μ_{11}, αντίστοιχα. Η αποκρυπτογράφηση δεν είναι παρά η εφαρμογή της αντίστοιχης αντίστροφης μετατόπισης. Το ίδιο βέβαια συμβαίνει και στη γενική περίπτωση. Κάθε γράμμα της λέξης – κλειδί ορίζει ένα κρυπτοσύστημα μετατόπισης που κρυπτογραφεί το γράμμα του κειμένου που υπάρχει κάτω από αυτό. Έτσι, το

κρυπτοσύστημα του Vigenère μπορεί να οριστεί πιο γενικά, όπως δίνεται παρακάτω.

Ας είναι $A = \{a_1,\ldots,a_n\}$ ένα πεπερασμένο σύνολο και m θετικός ακέραιος. Οι χώροι των απλών και κρυπτογραφημένων κειμένων είναι το σύνολο A^m και ο χώρος των κλειδιών είναι το σύνολο $K = \{1,\ldots,n\}^m$. Για κάθε κλειδί $k = (k(1),\ldots,k(m))$ ορίζουμε την συνάρτηση κρυπτογράφησης

$$E_k : A^m \rightarrow A^m,\ (x_1,\ldots,x_m) \mapsto (\mu_{k(1)}(x_1),\ldots,\mu_{k(m)}(x_m))$$

και τη συνάρτηση αποκρυπτογράφησης

$$D_k : A^m \rightarrow A^m,\ (x_1,\ldots,x_m) \mapsto (\mu_{n-k(1)}(x_1),\ldots,\mu_{n-k(m)}(x_m))$$

Η κρυπτογράφηση κάθε στοιχείου του A εξαρτάται από τη θέση στην οποία βρίσκεται. Έτσι, αυτό μπορεί να κρυπτογραφηθεί με τόσους διαφορετικούς τρόπους όσα είναι και τα διαφορετικά στοιχεία του συνόλου $\{k(1),\ldots,k(m)\}$.

Το πρώτο βήμα για την κρυπτανάλυση του σχήματος του Vigenère είναι ο υπολογισμός του μήκους m του κλειδιού. Αυτό μπορεί να επιτευχθεί με την εφαρμογή ενός κριτηρίου το οποίο διατυπώθηκε στα 1863 από τον Friedrich Kasiski (αν και είχε ανακαλυφθεί στα 1854 από τον Charles Babbage) και βασίζεται στην παρατήρηση ότι δύο ίδια τμήματα μηνύματος τα οποία απέχουν d θέσεις, όπου d είναι πολλαπλάσιο του m, δίνουν ίδια τμήματα κρυπτοκειμένου.

Έτσι, το κριτήριο του Kasiski εφαρμόζεται ως εξής: Αναζητούμε στο κρυπτογραφημένο μήνυμα ίδια τμήματα μήκους > 2 και καταγράφουμε την απόσταση των θέσεων εμφάνισης του πρώτου γράμματός των. Αν $d_1,\ldots,d_m$ είναι τέτοιες αποστάσεις, τότε μπορούμε να εικάσουμε ότι ο m διαιρεί τους ακέραιους $d_1,\ldots, d_m$. Άρα, αν έχουμε αρκετά τέτοια τμήματα μπορούμε να οδηγηθούμε αρκετά εύκολα στον προσδιορισμό του m. Περισσότερες πληροφορίες για τον m μπορούμε να πάρουμε από το δεύτερο κριτήριο το οποίο διατυπώθηκε στα 1925 από τον William Frederick Friedman (Πουλάκης, 2004· Sinkov, 2009).

Εάν γνωρίζουμε το μήκος m του κλειδιού, τότε τα τμήματα κειμένου τα οποία σχηματίζονται από τα στοιχεία του κρυπτογραφημένου κειμένου τα οποία βρίσκονται σε θέσεις των οποίων η απόστασή τους είναι πολλαπλάσιο του m είναι κρυπτογραφημένα μ' ένα κρυπτοσύστημα μετατόπισης και κατά συνέπεια εφαρμόζοντας την τεχνική κρυπτανάλυσης ενός τέτοιου σχήματος μπορούμε να προσδιορίσουμε το κλειδί αποκρυπτογράφησης.

Παράδειγμα 3.4. Το παρακάτω κείμενο έχει κρυπτογραφηθεί με το κρυπτοσύστημα του Vigenère και έχουν χρησιμοποιηθεί μόνο τα γράμματα του αγγλικού αλφαβήτου:

KWCSS GXYUT ZBZWU DXYYJ NPRPW OPVJJ JXVLL TBYUL VOZPW IKZJZ ZZKYP OTVNL ZZDUQ MMGLW NMENE JZVNZ VVFHW KTRCF OMOND ZBKYJ CWNYN ZZNYE PAKHG ONFLY ZBKBS OEVHW ZLKBW XQGBW MBVRL OWUYL ZZDCF ZBYYU GMRLL ZFKOF DYLYD TEVWS IVFNX JZVRS HXCYZ VDVUF VTXIJ DBYGA IEYCU CITCH CMINW SBOLW KZVMW IBJYA OPVLH GIZHL ZFKYG MANCL CWLNZ VDZHY VZLFW OWKYD GBYYV ZKZJZ ZZVLH MMTCK ZTPQZ ZVZNJ ZXIYK ZVKMW VVUQZ ZVZNJ ZXIYK ZVKMK DBZMU MCTCS GBYUL VBVUU CXFMA OQFHG ABYYU MGGNG BZRGC FWNFW YOVIX OPVEW TCECI PMCSV ZNZHW NBYYH GIZHL ZFKYI PQMUD ZVKIX ZITBU DXYYJ OMOND ZBKYJ

Παρατηρούμε ότι η ακολουθία LZZD επαναλαμβάνεται μετά από 90 θέσεις και η ακολουθία OPV μετά από 215 θέσεις. Καθώς ο μοναδικός κοινός διαιρέτη των αριθμών 90 και 215 είναι ο 5, έχουμε μία ισχυρή ένδειξη ότι το μήκος του κλειδιού είναι $m = 5$. Ας είναι $k = (k_1, \ldots, k_5)$ το ζητούμενο κλειδί. Στα τμήματα του κρυπτοκειμένου τα οποία έχουν κρυπτογραφηθεί με την χρήση των $k_1, \ldots, k_5$, τα γράμματα με το μεγαλύτερο πλήθος εμφανίσεων είναι τα Z, M, V, Y, W, αντίστοιχα. Επομένως, υποθέτοντας ότι το E αντιστοιχεί σε κάθε ένα από τα προηγούμενα γράμματα, παίρνουμε $k = (21,8,17,20,18)$. Αποκρυπτογραφούμε το παραπάνω κείμενο μ' αυτό το κλειδί και παίρνουμε το εξής κείμενο:

POLYALPHABETIC CIPHER SHAVE THE PROPERTY THAT A GIVEN CIPHERTEXT LETTER MAY REPRESENT MORE THAN ONE PLAIN TEXT LETTER HOWEVER WE MUST NOT FORGET THAT WE NEED THE CIPHERTEXT TO DETERMINE THE CLEAR TEXT UNIQUELY WE CANNOT FOR EXAMPLE HAVE AN ALGORITHM IN WHICH A CIPHERTEXT X REPRESENTS EITHER PLAIN TEXT E OR S WITHOUT HAVING A RULE TO TELL THE DECIPHERER PRECISELY WHEN IT REPRESENTS E AND WHEN IT REPRESENTS S IT IS CRUCIAL THAT AT EACH POSITION OF THE CRYPTOGRAM KNOWLEDGE OF THE KEY UNIQUELY DEFINES THE PLAIN TEXT EQUIVALENT OF EACH CIPHER TEXT LETTER

3.3 Το κρυπτοσύστημα μετάθεσης

Ένα κρυπτοσύστημα το οποίο χρησιμοποιήθηκε για αρκετούς αιώνες είναι το *κρυπτοσύστημα μετάθεσης* το οποίο θα ορίσουμε στη συνέχεια. Ας είναι m ένας θετικός ακέραιος και A ένα πεπερασμένο σύνολο. Ο χώρος των απλών κειμένων και ο χώρος των κρυπτοκειμένων είναι το σύνολο A^m. Ο χώρος κλειδιών είναι το σύνολο $K = S_m$. Για κάθε $\sigma \in K$ έχουμε την συνάρτηση κρυπτογράφησης

$$E_\sigma : A^m \to A^m,\ (x_1,\ldots,x_m) \mapsto (x_{\sigma(1)},\ldots,x_{\sigma(m)})$$

και την αντίστοιχη συνάρτηση αποκρυπτογράφησης

$$D_\sigma : A^m \to A^m,\ (x_1,\ldots,x_m) \mapsto (x_{\sigma^{-1}(1)},\ldots,x_{\sigma^{-1}(m)})$$

Αν το πλήθος των στοιχείων του A τα οποία εμφανίζονται στο κείμενο το οποίο πρόκειται να κρυπτογραφηθεί δεν είναι πολλαπλάσιο του m, τότε προστίθενται στο κείμενο μερικά τυχαία στοιχεία ώστε το πλήθος όλων των στοιχείων του να είναι πολλαπλάσιο του m.

Παράδειγμα 3.5. Ας είναι m = 6 και το κλειδί η παρακάτω μετάθεση:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 1 & 6 & 4 & 2 \end{pmatrix}$$

Παίρνουμε ως σύνολο A το σύνολο το οποίο αποτελείται από τα γράμματα του Ελληνικού αλφαβήτου και το κενό διάστημα το οποίο συμβολίζεται με ⊔. Για να κρυπτογραφήσουμε το μήνυμα

ΕΠΙΘΕΣΗ ΣΤΙΣ ΔΕΚΑ

το χωρίζουμε σε ομάδες των έξι συμβόλων ως εξής:

ΕΠΙΘΕΣ Η⊔ΣΤΙΣ ⊔ΔΕΚΑ⊔

Εφαρμόζοντας σε κάθε μία εξάδα την μετάθεση σ προκύπτει το κείμενο:

ΙΕΕΣΘΠΣΙΗΣΤ⊔ΕΑ⊔⊔ΚΔ

Η αποκρυπτογράφηση γίνεται ομοίως χρησιμοποιώντας την μετάθεση σ^{-1}.

Το κρυπτοσύστημα μετάθεσης είναι ευάλωτο σε επίθεση γνωστού απλού κειμένου. Πράγματι, στη περίπτωση όπου είναι γνωστό ένα τμήμα απλού κειμένου $(x_1,\ldots,x_m)$ και το αντίστοιχο κρυπτογραφημένο $(x_{\sigma(1)},\ldots, x_{\sigma(m)})$, είναι πολύ εύκολα να προσδιοριστεί η μετάθεση σ. Από την άλλη πλευρά, αν το σύνολο A είναι το αλφάβητο μίας φυσικής γλώσσας, τότε οι στατιστικές ιδιότητές της δεν είναι δυνατόν να χρησιμοποιηθούν για την κρυπτανάλυση ενός κρυπτογραφημένου κειμένου, καθώς η κρυπτογράφηση δεν έχει αλλάξει τα γράμματα παρά μόνο τη θέσης τους στο κείμενο. Έτσι, κάθε γράμμα του

κρυπτοκειμένου εμφανίζεται τόσες φορές όσες και στο καθαρό. Αν το κρυπτογραφημένο κείμενο είναι γραμμένο με γράμματα ενός φυσικού αλφαβήτου το οποίο χρησιμοποιείται από πολλές γλώσσες, όπως για παράδειγμα το λατινικό, τότε η μόνη διαπίστωση η οποία μπορεί να γίνει από την στατιστική ανάλυσή του είναι η αποκάλυψη της γλώσσας στην οποία είναι γραμμένο.

Για την κρυπτανάλυση ενός κειμένου κρυπτογραφημένο με ένα κρυπτοσύστημα μετάθεσης πρέπει πρώτα να βρεθεί το μήκος m της μετάθεσης και κατόπιν ποια ακριβώς μετάθεση χρησιμοποιήθηκε από τις m! μεταθέσεις του S_m. Αν το πλήθος των στοιχείων του κειμένου είναι N, τότε ο ακέραιος m είναι ένας από τους θετικούς διαιρέτες του N. Επίσης, η γνώση των δυάδων, τριάδων κ.λπ. γραμμάτων οι οποίες έχουν την μεγαλύτερη συχνότητα εμφάνισης σε μία φυσική γλώσσα είναι δυνατόν να βοηθήσει στη εύρεση της μετάθεσης η οποία χρησιμοποιήθηκε. Θα εφαρμόσουμε αυτές τις παρατηρήσεις στο παρακάτω παράδειγμα.

Παράδειγμα 3.6. Ας υποθέσουμε ότι το παρακάτω κείμενο είναι η κρυπτογράφηση με ένα κρυπτοσύστημα μετάθεσης ενός κειμένου γραμμένου με το αγγλικό αλφάβητο:

RIBNTHGEEAWPNSOTTHOEIVRESIRDRLEH

Το πλήθος των γραμμάτων του κρυπτογραφημένου κειμένου είναι 32. Άρα, το μήκος της μετάθεσης m είναι διαιρέτης του 32. Ας πάρουμε την περίπτωση όπου m = 4. Χωρίζουμε το κείμενο σε ομάδες των τεσσάρων γραμμάτων:

RIBN THGE EAWP NSOT THOE IVRE SIRD RLEH

Το πλήθος των μεταθέσεων του S_4 είναι 4! = 24. Καθώς ο αριθμός αυτός δεν είναι μεγάλος, μπορούμε να δοκιμάσουμε όλες τις περιπτώσεις και να διαπιστώσουμε έτσι αν πράγματι η μετάθεση κλειδί είναι στοιχείο του S_4.

Από την άλλη πλευρά, παρατηρούμε ότι δύο από τις τετράδες του κρυπτοκειμένου είναι της μορφής TH-E. Καθώς η τριάδα THE έχει την μεγαλύτερη συχνότητα εμφάνισης, υποθέτουμε ότι η τετράδα TH-E έχει προκύψει από την κρυπτογράφηση μίας τετράδας της μορφής THE- ή -THE. Τότε, η μετάθεση αποκρυπτογράφησης είναι μία από τις παρακάτω:

$$\begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 2 & 4 & 3\end{pmatrix} \quad \text{και} \quad \begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 1 & 2 & 4\end{pmatrix}.$$

Η εφαρμογή της πρώτης μετάθεσης στο κρυπτογραφημένο κείμενο δίνει μία σειρά γραμμάτων χωρίς νόημα. Η εφαρμογή της δεύτερης δίνει το εξής:

BRING THE WEAPONS TO THE RIVER SIDE RLH

Παρατηρούμε ότι στο τέλος του κειμένου έχουν προστεθεί τρία γράμματα ώστε το πλήθος των γραμμάτων του κείμενου να είναι 32 και έτσι να είναι δυνατόν να εφαρμοστεί για την κρυπτογράφησή του μία μετάθεση του S_4.

3.4 Το σημειωματάριο της μίας χρήσης

Το *σημειωματάριο της μίας χρήσης* προτάθηκε για πρώτη φορά το 1882 από τον Frank Miller για την διαφύλαξη της εμπιστευτικότητας των τηλεγραφικών μηνυμάτων (Bellovin, 2011). Το 1917, μία εκδοχή αυτού του σχήματος προτάθηκε από τον Gilbert Vernam για χρήση στον τηλέτυπο και κατοχυρώθηκε νομικά στις ΗΠΑ για ευρεσιτεχνία το 1919. Χρησιμοποιήθηκε ευρέως μέχρι το πρόσφατο παρελθόν για σημαντικές στρατιωτικές και διπλωματικές εφαρμογές. Το σχήμα αυτό είναι επίσης γνωστό και ως *κρυπτοσύστημα του Vernam.* Το σημειωματάριο της μίας χρήσης είναι ένα κρυπτοσύστημα του Vigenère με κλειδί το οποίο είναι μία τυχαία ακολουθία γραμμάτων με μήκος όσο και το κείμενο.

Παράδειγμα 3.7. Θα χρησιμοποιήσουμε το σημειωματάριο της μίας χρήσης για να κρυπτογραφήσουμε το κείμενο:

THE KEY IS VICTORY

Επιλέγουμε ως κλειδί την ακολουθία των 15 παρακάτω γραμμάτων:

ABGHYUREFPINMKG

Κρυπτογραφούμε το κείμενο χρησιμοποιώντας τον πίνακα του Vigenère και παίρνουμε το κείμενο:

TIKRCSZWAXKGABE

Η αποκρυπτογράφηση γίνεται ως γνωστό με την αντίστροφη διαδικασία.

Το σημειωματάριο της μίας χρήσης μπορεί να διατυπωθεί και πιο γενικά ως ένα κρυπτοσύστημα του Vigenère για ένα πεπερασμένο σύνολο A και για κλειδί ένα τυχαίο σύνολο μετατοπίσεων που έχει το ίδιο πλήθος στοιχείων με το κείμενο που θέλουμε να κρυπτογραφήσουμε. Η πλέον συνηθισμένη σύγχρονη εκδοχή του χρησιμοποιεί το σύνολο $B = \{0,1\}$ εφοδιασμένο με την πράξη XOR. Ας σημειωθεί ότι η απεικόνιση που ορίζεται από την αντιστοιχία $x \mapsto x \oplus 0$ δίνει την ταυτοτική μετατόπιση του B και η αντιστοιχία $x \mapsto x \oplus 1$ την μετατόπιση κατά μία θέση. Έτσι, για να κρυπτογραφήσουμε ένα απλό κείμενο $p \in B^m$, επιλέγουμε ένα τυχαίο στοιχείο $k \in B^m$, ως κλειδί, και υπολογίζουμε το κρυπτοκείμενο $c = p \oplus k$. Η αποκρυπτογράφηση του c γίνεται με τον ίδιο τρόπο. Δηλαδή, υπολογίζουμε:

$$c \oplus k = (p \oplus k) \oplus k = p \oplus (k \oplus k) = p \oplus 0 = p$$

Το σημειωματάριο της μίας χρήσης είναι εξαιρετικά ευάλωτο στη προσβολή γνωστού απλού κειμένου. Πράγματι, αν γνωρίζουμε $p,c \in B^m$ με $p \oplus k = c$, τότε $k = p \oplus c$. Έτσι, αν το ίδιο κλειδί χρησιμοποιηθεί για δεύτερη φορά ο κρυπταναλυτής θα είναι σε θέση ν' αποκρυπτογραφήσει το καινούργιο μήνυμα. Επίσης, αν δύο μηνύματα έχουν κρυπτογραφηθεί με το ίδιο κλειδί k, τότε έχουμε $p_1 \oplus k = c_1$ και $p_2 \oplus k = c_2$, απ' όπου, προσθέτοντας κατά μέλη τις δύο ισότητες, παίρνουμε $c_1 \oplus c_2 = p_1 \oplus p_2$. Οπότε, ο κρυπταναλυτής γνωρίζει το άθροισμα των καθαρών κειμένων p_1 και p_2 τα οποία θέλει ν' αποκρυπτογραφήσει.

Έτσι, για να διατηρηθεί η ασφάλεια του σχήματος θα πρέπει μετά από κάθε κρυπτογράφηση να επιλέγεται ένα καινούργιο κλειδί. Από αυτή την πρακτική, το κρυπτοσύστημα πήρε την ονομασία *σημειωματάριο της μίας χρήσης*. Στο παρελθόν έχει χρησιμοποιηθεί για στρατιωτικές και διπλωματικές εφαρμογές, όπου η εμπιστευτικότητα είναι υψίστης σημασίας.

4. ΣΥΜΜΕΤΡΙΚΑ ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΑ

Οι ηλεκτρονικοί υπολογιστές, ως γνωστόν, διαχειρίζονται μόνο δύο καταστάσεις οι οποίες απεικονίζονται συμβολικά από τους αριθμούς 0 και 1. Επομένως, κάθε πληροφορία η οποία τους δίνεται αντιπροσωπεύεται από μία πεπερασμένη ακολουθία στοιχείων από το σύνολο $B = \{0, 1\}$. Έτσι, αναπτύχθηκαν αρκετά συστήματα παράστασης της πληροφορίας με 0 και 1. Ένα από τα πρώτα συστήματα το οποίο έχει ευρέως χρησιμοποιηθεί στο παρελθόν είναι ο κώδικας ASCII (American Standard Code for Information Interchange). Ο κώδικας αυτός αντιστοιχεί τα γράμματα του λατινικού αλφαβήτου (κεφαλαία και μικρά), τους αριθμούς, τα σημεία στίξης και άλλα σύμβολα στα στοιχεία του B^7, ώστε να δημιουργείται μία αμφίεση μεταξύ των δύο συνόλων. Η πλέον συνηθισμένη κωδικοποίηση χαρακτήρων στο διαδίκτυο μέχρι το τέλος του 2007 ήταν η US-ASCII, η οποία παρουσιάζεται στον παρακάτω Πίνακα (Εικόνα 5). Σ' αυτόν τον Πίνακα, η επτάδα b7…b1 η οποία αντιστοιχεί σ' ένα σύμβολο X αποτελείται από την τριάδα b7b6b5 η οποία βρίσκεται στην ίδια στήλη με το X και την τετράδα b4b3b2b1 η οποία βρίσκεται στην ίδια γραμμή. Έτσι, το γράμμα A αντιστοιχεί στην επτάδα 1000001. Σήμερα , η κωδικοποίηση US-ASCII έχει αντικατασταθεί από άλλα σχήματα, όπως για παράδειγμα η κωδικοποίηση UTF-8 (βλ. https://el.wikipedia.org/wiki/UTF-8).

USASCII code chart

b_7 b_6 b_5 → / b_4 b_3 b_2 b_1 ↓	0 0 0	0 0 1	0 1 0	0 1 1	1 0 0	1 0 1	1 1 0	1 1 1
Row ↓ Column →	0	1	2	3	4	5	6	7
0 0 0 0	0	NUL	DLE	SP	0	@	P	`	p
0 0 0 1	1	SOH	DC1	!	1	A	Q	a	q
0 0 1 0	2	STX	DC2	"	2	B	R	b	r
0 0 1 1	3	ETX	DC3	#	3	C	S	c	s
0 1 0 0	4	EOT	DC4	$	4	D	T	d	t
0 1 0 1	5	ENQ	NAK	%	5	E	U	e	u
0 1 1 0	6	ACK	SYN	&	6	F	V	f	v
0 1 1 1	7	BEL	ETB	'	7	G	W	g	w
1 0 0 0	8	BS	CAN	(	8	H	X	h	x
1 0 0 1	9	HT	EM	)	9	I	Y	i	y
1 0 1 0	10	LF	SUB	*	:	J	Z	j	z
1 0 1 1	11	VT	ESC	+	;	K	[	k	{
1 1 0 0	12	FF	FS	,	<	L	\	l	|
1 1 0 1	13	CR	GS	-	=	M	]	m	}
1 1 1 0	14	SO	RS	.	>	N	^	n	~
1 1 1 1	15	SI	US	/	?	O	_	o	DEL

Εικόνα 5. Ο κώδικας ASCII (Πηγή: Wikipedia[6]).

Συχνά, σε κάθε επτάδα $x_1 \ldots x_7$ του ASCII προστίθεται στο τέλος και ένα ακόμη στοιχείο $x_8 \in B$, ώστε το πλήθος των 1 στην οκτάδα $x_1 \ldots x_8$ να είναι άρτιος αριθμός. Αυτό γίνεται για την ανίχνευση εισδοχής ενός σφάλματος στην οκτάδα κατά την διαχείρισή της από τον ηλεκτρονικό υπολογιστή. Έτσι, η σχεδίαση των σχημάτων κρυπτογράφησης από τα μέσα του εικοστού αιώνα περιλαμβάνει συναρτήσεις κρυπτογράφησης με πεδία ορισμού σύνολα από συμβολοσειρές στοιχείων του B.

Στα 1949, ο C. Shannon δημοσίευσε την περίφημη εργασία του "Communication Theory of Secrecy Systems," η οποία εισήγαγε την έννοια της *τέλειας μυστικότητας* (ή *τέλειας ασφάλειας*) στα σχήματα κρυπτογράφησης και έδωσε ένα θεώρημα για τον χαρακτηρισμό των κρυπτοσυστημάτων τα οποία την έχουν (Πουλάκης, 2004· Shannon, 1949). Ένα τέτοιο σχήμα είναι το σημειωματάριο της μίας χρήσης υπό την προϋπόθεση ότι σε κάθε κρυπτογράφηση χρησιμοποιείται ένα καινούργιο τυχαίο κλειδί. Επιπλέον, στην εργασία του Shannon αναπτύσσονται δύο βασικές αρχές για την ασφάλεια ενός κρυπτοσυστήματος: *η σύγχυση και η διάχυση*. Η σύγχυση έχει ως σκοπό την κάλυψη των αλγεβρικών και στατιστικών ιδιοτήτων του κρυπτοσυστήματος, ενώ η διάχυση επιτρέπει σε

[6] https://en.wikipedia.org/wiki/ASCII#/media/File:USASCII_code_chart.svg

κάθε δυαδικό ψηφίο του απλού κειμένου να επηρεάζει μεγάλο μέρος του κρυπτογραφημένου κειμένου. Στη σχεδίαση των σύγχρονων κρυπτοσυστημάτων τμήματος λαμβάνεται μέριμνα ώστε να εξασφαλίζονται οι παραπάνω ιδιότητες σε ικανοποιητικό βαθμό.

Στις επόμενες δύο ενότητες θα περιγράψουμε τις δύο μεγάλες κατηγορίες των σύγχρονων συμμετρικών κρυπτοσυστημάτων: τα κρυπτοσυστήματα ροής και τα κρυπτοσυστήματα τμήματος.

4.1 Τα κρυπτοσυστήματα ροής

Όπως αναφέραμε παραπάνω, για να διατηρήσει το σημειωματάριο της μίας χρήσης την ιδιότητα της τέλειας μυστικότητας απαιτείται η αλλαγή του κλειδιού σε κάθε κρυπτογράφηση. Ένας τρόπος αντιμετώπισης αυτού του προβλήματος είναι η χρησιμοποίηση κλειδιών τα οποία προέρχονται από ακολουθίες στοιχείων του B οι οποίες ορίζονται από λίγες παραμέτρους. Έτσι, η ανταλλαγή του κλειδιού δεν είναι αναγκαία παρά μόνο η ανταλλαγή των παραμέτρων. Τότε, όμως, το κρυπτοσύστημα δεν έχει πλέον την ιδιότητα της τέλειας μυστικότητας γιατί η επιλογή κλειδιού δεν είναι τυχαία. Αυτή η ιδέα οδήγησε στην ανάπτυξη μίας ολόκληρης οικογένειας κρυπτοσυστημάτων: τα κρυπτοσυστήματα ροής.

Θέτουμε $\Sigma = B^m$, όπου m θετικός ακέραιος, και θεωρούμε το σύνολο

$$\Sigma^* = \{(z_1,\ldots,z_s)\in\Sigma^s/\ s = 1,2,\ldots\}$$

Ένα *κρυπτοσύστημα ροής* είναι ένα συμμετρικό σχήμα κρυπτογράφησης του οποίου ο χώρος των απλών και κρυπτογραφημένων κειμένων είναι το σύνολο Σ^* και ο χώρος των κλειδιών το σύνολο Σ^n, όπου n θετικός ακέραιος. Το σύστημα είναι εφοδιασμένο με μία διαδικασία η οποία από ένα κλειδί $K\in\Sigma^n$ παράγεται μία ακολουθία $k_1,k_2,\ldots$ στοιχείων του Σ η οποία δεν είναι προσδιορίσιμη χωρίς τη γνώση του K. Η συνάρτηση κρυπτογράφησης η οποία αντιστοιχεί στο K είναι η συνάρτηση

$$E_K : \Sigma^* \rightarrow \Sigma^*,\ (z_1,\ldots,z_s) \mapsto (z_1\oplus k_1,\ldots,z_s\oplus k_s)$$

Παρατηρούμε ότι η αντίστροφη απεικόνιση της E_K, η οποία είναι η συνάρτηση αποκρυπτογράφησης D_K, συμπίπτει με την E_k.

Στη συνέχεια, θα περιγράψουμε μία διαδικασία κατασκευής τέτοιων ακολουθιών με την χρήση των *γραμμικών συστημάτων καταγραφής μετατόπισης με ανάδραση*. Ένα τέτοιο σύστημα S αποτελείται από n κατάγραφείς $R_0,\ldots,R_{n-1}$, όπως φαίνεται στην Εικόνα 6, ο καθένας από τους

οποίους σε κάθε χρονική στιγμή t περιέχει το ψηφίο 0 ή 1. Συμβολίζουμε με $X_i(t)$ το περιεχόμενο του καταγραφέα R_i και με

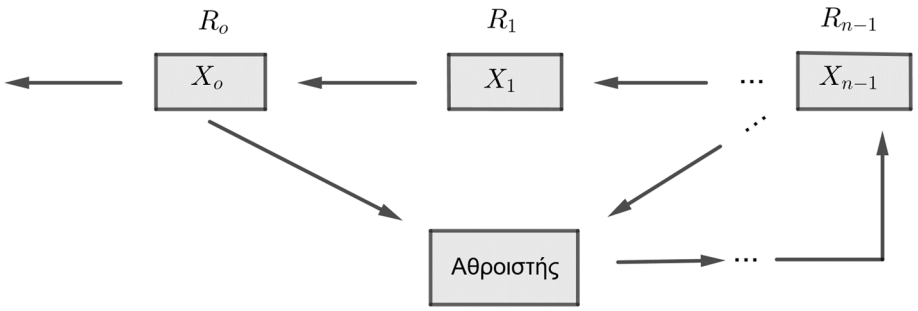
$$x(t) = (X_0(t),\ldots,X_{n-1}(t))$$

την κατάσταση του συστήματος την χρονική στιγμή t. Η ακολουθία x(t) ορίζεται από τις τιμές $X_0(0),\ldots,X_{n-1}(0)$, οι οποίες δίνονται αρχικά και δεν είναι όλες 0, και από τις σχέσεις:

$$X_i(t+1) = X_{i+1}(t) \quad (i = 0,1,\ldots,n-2)$$

$$X_{n-1}(t+1) = c_0X_0(t) \oplus\cdots\oplus c_{n-1}X_{n-1}(t)$$

όπου $c_0,\ldots,c_{n-1}\in B$ με $c_0 = 1$. Έτσι, για κάθε t, έχουμε $x(t) \neq (0,\ldots,0)$.



Εικόνα 6. Γραμμικό σύστημα καταγραφής μετατόπισης με ανάδραση (προσαρμογή από Πουλάκης, 2004).

Ο τρόπος λειτουργίας του συστήματος είναι ο εξής: Κάθε χρονική στιγμή ο καταγραφέας R_0 στέλνει το περιεχόμενό του στην έξοδο και ο R_i στέλνει το περιεχόμενό του στον R_{i-1} (i=1,…,n–1). Αν $c_i = 1$, τότε ο R_i στέλνει το περιεχόμενό του στον αθροιστή. Αυτός προσθέτει τα ψηφία τα οποία δέχεται και στέλνει το αποτέλεσμά στον R_{n-1}. Έτσι, προκύπτει η ακολουθία $s_i = X_0(i)$ (i = 0,1,…) η οποία καλείται *ακολουθία καταγραφής μετατόπισης* του S και ικανοποιεί την σχέση

$$s_{i+n} = c_0s_i\oplus\cdots\oplus c_{n-1}s_{n-1+i}$$

Τα γραμμικά συστήματα καταγραφής μετατόπισης έχουν ευρεία εφαρμογή από την δεκαετία του 1950 όπου αναπτύχθηκαν λόγω της εύκολης υλοποίησής τους από τους ηλεκτρονικούς υπολογιστές και την κατανόηση της μαθηματικής τους θεωρίας σε σημαντικό βαθμό.

Μία ακολουθία $a_0, a_1,\ldots$ στοιχείων ενός συνόλου Α καλείται *περιοδική,* αν υπάρχει δείκτης p τέτοιος, ώστε να ισχύει:

$$a_{i+p} = a_i \quad (i = 0,1,\ldots)$$

Ο μικρότερος δείκτης p με αυτή την ιδιότητα καλείται *περίοδος* της ακολουθίας. Τότε, η ακολουθία έχει την παρακάτω μορφή:

$$a_0,a_1,\ldots,a_{p-1}, a_0,a_1,\ldots,a_{p-1},\ldots$$

Πρόταση 4.1. Η ακολουθία καταγραφής μετατόπισης s_i $(i = 0,1,\ldots)$ είναι περιοδική με περίοδο $\le 2^n-1$.

Απόδειξη. Το πλήθος των στοιχείων του B^n τα οποία είναι διαφορετικά του $(0,\ldots,0)$ είναι 2^n-1. Άρα, υπάρχουν t_1, t_2 με $t_1 < t_2$ και $t_2 - t_1 \le 2^n-1$ έτσι, ώστε να ισχύει $x(t_1) = x(t_2)$. Συνεπώς, η ακολουθία s_i $(i = 0,1,\ldots)$ είναι περιοδική με περίοδο $\le 2^n-1$.

Στην επόμενη πρόταση δίνεται μία χαρακτηριστική ιδιότητα των ακολουθιών καταγραφής μετατόπισης (βλ. σχετικά στο Πουλάκης, 2004).

Πρόταση 4.2. Ας υποθέσουμε ότι η ακολουθία s_i $(i = 0, 1, \ldots)$ έχει περίοδο $m = 2^n-1$. Τότε, η ακολουθία περιέχει $2^{n-1}-1$ φορές το 0 και 2^{n-1} φορές το 1.

Απόδειξη. Ας είναι s_{i+k} $(i = 0,1,\ldots,2^n-2)$ ένα τμήμα της ακολουθίας s_i με m ψηφία. Θεωρούμε τα σύνολα

$$S = \{x(i+k)/\ i = 0,1,\ldots,2^n-2\}, \qquad A = \{x\in\mathbb{Z}/\ 1 \le x \le 2^n-1\}$$

και τη συνάρτηση $f : S_n \to A_n$ με

$$f(x(i+k)) = X_0(i+k)+X_1(i+k)\,2+\cdots+X_{n-1}(i+k)\,2^{n-1}$$

για κάθε $i = 0,1,\ldots,2^n-2$. Θα δείξουμε ότι η συνάρτηση f είναι ένεση. Ας είναι $f(x(i+k)) = f(x(j+k))$. Αν $X_{n-1}(i+k) = 1$ και $X_{n-1}(j+k) = 0$, τότε έχουμε:

$$f(x(j+k)) \le 1+2+\cdots+2^{n-2} \le 2^{n-1}-1 < 2^{n-1} \le f(x(i+k))$$

το οποίο δεν ισχύει. Αν $X_{n-1}(i+k) = 0$ και $X_{n-1}(j+k) = 1$, τότε ομοίως καταλήγουμε σε άτοπο. Άρα, ισχύει $X_{n-1}(i+k) = X_{n-1}(j+k)$. Έτσι, έχουμε:

$$f(x(i+k))-X_{n-1}(i+k) = f(x(j+k))-X_{n-1}(j+k)$$

Ομοίως προκύπτει ότι $X_{n-2}(i+k) = X_{n-2}(j+k)$ και συνεχίζοντας με αυτόν τον τρόπο παίρνουμε ότι $x(i+k) = x(j+k)$. Άρα, η f είναι ένεση. Καθώς η περίοδος της ακολουθίας s_i είναι m, οι n-άδες $x(i+k)$ $(i = 0,1,\ldots,2^n-2)$ είναι όλες διαφορετικές. Έτσι, τα σύνολα S και A έχουν το ίδιο πλήθος στοιχείων και επομένως, η συνάρτηση f είναι αμφίεση. Καθώς υπάρχουν $2^{n-1}-1$ άρτιοι και

2^{n-1} περιττοί μέσα στο Α, το τμήμα s_{i+k} $(i = 0,1,\ldots,2^n–2)$ περιέχει $2^{n-1}–1$ φορές το 0 και 2^{n-1} φορές το 1.

Παράδειγμα 4.1. Ας υποθέσουμε ότι ένας χρήστης Α επιθυμεί να χρησιμοποιήσει ένα κρυπτοσύστημα ροής το οποίο βασίζεται στο σύστημα καταγραφής μετατόπισης με αρχική κατάσταση x(0) = (0,0,0,1) και σχέσεις:

$$X_i(t+1) = X_{i+1}(t) \quad (i = 0,1,2)$$

$$X_3(t+1) = X_0(t) \oplus X_3(t)$$

Η ακολουθία s_i η οποία παράγεται από το σύστημα έχει ως πρώτους όρους τους $s_0 = 0$, $s_1 = 0$, $s_2 = 0$, $s_3 = 1$ και οι επόμενοι ορίζονται από την σχέση

$$s_{i+4} = s_i \oplus s_{3+i} \quad (i = 0,1,\ldots)$$

Πιο αναλυτικά, η ακολουθία s_i είναι:

$$000111101011001000111101011001\ldots$$

Παρατηρούμε ότι η περίοδός της ακολουθίας ισούται με 15.

Ο Α επιθυμεί να κρυπτογραφήσει με αυτό το σύστημα το μήνυμα «Νο». Πρώτα χρησιμοποιεί τον κώδικα ASCII και το μετατρέπει σε ακολουθία στοιχείων του Β. Τα γράμματα «Ν» και «ο» αντιστοιχούν στις ακολουθίες 1001110 και 1101111. Έτσι, το μήνυμα «Νο» γίνεται:

$$M = 10011101101111$$

Ο Α επιλέγει ως κλειδί Κ τους 14 πρώτους όρους της ακολουθίας καταγραφής μετατόπισης, δηλαδή Κ = 00011110101100. Άρα, η κρυπτογράφηση του κειμένου Μ είναι το κείμενο

$$C = K \oplus M = 10000011000011$$

Στη συνέχεια θα δείξουμε ότι ένα κρυπτοσύστημα ροής το οποίο βασίζεται σε ένα σύστημα καταγραφής μετατόπισης με ανάδραση είναι ευάλωτο στην κρυπτανάλυση γνωστού απλού κειμένου. Ας είναι λοιπόν s_i μία ακολουθία καταγραφής μετατόπισης η οποία παράγεται από ένα σύστημα με n καταγραφείς και σταθερές $c_0,\ldots,c_{n-1}$ η οποία χρησιμοποιείται για την κρυπτογράφηση ενός απλού κειμένου $x = x_0\ldots x_{k-1}$. Τότε παίρνουμε το κρυπτοκείμενο $y = y_0\ldots y_{k-1}$, όπου $y_i = x_i \oplus s_i$ $(i = 0,\ldots,k–1)$.

Ας υποθέσουμε στη συνέχεια ότι τα κείμενα x και y είναι γνωστά και ότι $k \geq 2n$. Τότε, μπορούμε να βρούμε τους k πρώτους όρους της ακολουθίας s_i από τις προηγούμενες ισότητες υπολογίζοντας ως εξής:

$$x_i \oplus y_i = x_i \oplus (x_i \oplus s_i) = (x_i \oplus x_i) \oplus s_i = s_i \quad (i = 0,\ldots,k–1)$$

Έτσι, οι σταθερές $c_0,\ldots,c_{n-1}$ είναι λύση του συστήματος:

$$s_n = s_0c_0 \oplus \cdots \oplus s_{n-1}c_{n-1}$$

$$s_{n+1} = s_1c_0 \oplus \cdots \oplus s_nc_{n-1}$$

$$\ldots \qquad \ldots \qquad \ldots$$

$$s_{2n-1} = s_{n-1}c_0 \oplus \cdots \oplus s_{2n-2}c_{n-1}$$

Αν τα n, x, y είναι γνωστά και $k \geq 2n$, αυτό το σύστημα μας δίνει τις τιμές των $c_0,\ldots,c_{n-1}$. Επιπλέον, στην περίπτωση όπου η περίοδος της ακολουθίας s_i είναι $2^n–1$, το σύστημα αυτό έχει μοναδική λύση (βλ. Πουλάκης, 2004).

Παράδειγμα 4.2. Ας υποθέσουμε ότι ο αριθμός 9, του οποίου η γραφή στο κώδικα ASCII αντιστοιχεί στη συμβολοσειρά 0101001, κρυπτογραφείται με κλειδί την συμβολοσειρά η οποία προκύπτει από τους επτά πρώτους όρους μίας ακολουθία καταγραφής μετατόπισης s_i η οποία παράγεται από ένα σύστημα με τρεις καταγραφείς. Έτσι, προκύπτει το κρυπτοκείμενο 1011101. Θα προσδιορίσουμε την ακολουθία s_i. Προσθέτουμε τις δύο συμβολοσειρές και παίρνουμε την 1110100. Η ακολουθία s_i ορίζεται από τις τιμές $s_0 = s_1 = s_2 = 1$ και την σχέση

$$s_{i+3} = s_i \oplus c_1s_{i+1} \oplus c_2s_{i+2} \quad (i = 0,1,\ldots)$$

Για να προσδιορίσουμε τις σταθερές c_1, c_2 θέτουμε στην παραπάνω σχέση

$$(s_i,s_{i+1},s_{i+2},s_{i+3}) = (1,1,1,0),(1,1,0,1),(1,0,1,0),(0,1,0,0)$$

και παίρνουμε:

$$c_1 \oplus c_2 = 0, \quad c_1 = 0, \quad c_2 = 1, \quad c_1 = 0$$

Άρα, έχουμε $c_1 = 0$, $c_2 = 1$ και επομένως η s_i είναι πλήρως προσδιορισμένη.

4.2 Τα κρυπτοσυστήματα τμήματος

Ένα συμμετρικό σχήμα κρυπτογράφησης $(\boldsymbol{\mathcal{P}},\boldsymbol{\mathcal{C}},\boldsymbol{\mathcal{K}},\boldsymbol{\mathcal{E}},\boldsymbol{\mathcal{D}})$ καλείται *Κρυπτοσύστημα Τμήματος*, αν $\boldsymbol{\mathcal{P}} = \boldsymbol{\mathcal{C}} = F^n$, όπου F είναι ένα πεπερασμένο σύνολο. Σ' αυτή την περίπτωση παρατηρούμε ότι οι συναρτήσεις κρυπτογράφησης είναι αμφιέσεις. Παραδείγματα τέτοιων σχημάτων είναι τα κρυπτοσυστήματα αντικατάστασης, μετάθεσης και του Vigenère.

Στα κρυπτοσυστήματα τμήματος η υλοποίηση των ιδιοτήτων της σύγχυσης και διάχυσης τις οποίες αναφέραμε παραπάνω υλοποιούνται από ένα δίκτυο *αντικατάστασης – μετάθεσης* και μία μέθοδο παραγωγής υποκλειδιών $k_1,k_2,\ldots,k_r$ από κάθε κλειδί $K \in \boldsymbol{\mathcal{K}}$. Κάθε δίκτυο αντικατάστασης - μετάθεσης

αποτελείται τουλάχιστον από δέκα γύρους και καθένας από αυτούς χρησιμοποιεί ένα κλειδί k_i. Ο πρώτος γύρος δέχεται ως είσοδο τμήμα του απλού κειμένου και οι υπόλοιποι την έξοδο του προηγούμενου γύρου. Κάθε γύρος διαμερίζει το τμήμα σε μικρότερα τμήματα και σε καθένα από αυτά εφαρμόζει μία απεικόνιση η οποία καλείται S-κιβώτιο. Συχνά προστίθεται η εφαρμογή μίας μετάθεσης στο τμήμα του απλού κειμένου και στην έξοδο του τελευταίου γύρου.

Δύο από τα πλέον γνωστά κρυπτοσυστήματα τμήματος είναι το DES (Data Encryption Standard) (Menezes κ.ά., 1997) και το AES (Advanced Encryption Standard) (Daemen & Rijmen, 2002). Το DES απετέλεσε από 1977 το επίσημο σχήμα κρυπτογράφησης κυβερνητικών δεδομένων των ΗΠΑ. Αντικαταστάθηκε το 2001 από το AES. Απλοποιημένες εκδοχές τους έχουν δημοσιευτεί για διδακτικούς σκοπούς (Musa κ.ά., 2003· Schaefer, 1996).

Στη συνέχεια θα σκιαγραφήσουμε τη λειτουργία ενός κρυπτοσυστήματος τμήματος περιγράφοντας ένα πολύ απλό κρυπτοσύστημα, το *Baby Block,* το οποίο χρησιμοποιεί ένα μόνο S-κιβώτιο. Ο χώρος των απλών και κρυπτογραφημένων κειμένων, καθώς και ο χώρος κλειδιών, είναι το σύνολο B^4. Το σύστημα αυτό χρησιμοποιεί το S-κιβώτιο το οποίο δίνεται στην Εικόνα 7.

Η πρώτη στήλη από αριστερά περιλαμβάνει όλες τις τετράδες του B^4. Κάθε $k \in B^4$ ορίζει μία γραμμή του πίνακα επί της οποίας βρίσκονται τα ζεύγη δυαδικών ψηφίων τα οποία αντιστοιχούν στα ζεύγη 00, 01, 10, 11 της πρώτης γραμμής και κατά συνέπεια ορίζει μία συνάρτηση $f_k : B^2 \rightarrow B^2$. Για παράδειγμα, η τετράδα 0001 η οποία βρίσκεται στη δεύτερη γραμμή του πίνακα ορίζει την συνάρτηση $f_{0001} : B^2 \rightarrow B^2$ με f(00) = 00, f(01) = 11, f(10) = 10, f(11) = 00.

	00	01	10	11
0000	10	10	00	11
0001	00	11	10	00
0010	00	10	01	00
0011	01	00	11	11
0100	11	00	10	01
0101	10	11	01	10
0110	11	01	11	10
0111	10	01	00	01
1000	00	01	11	10
1001	01	00	01	11
1010	11	11	00	00
1011	11	10	01	01
1100	01	11	10	10
1101	00	01	11	00
1110	10	00	00	01
1111	01	10	10	11

Εικόνα 7. Το S – κιβώτιο του Baby Block.

Ας υποθέσουμε ότι το κρυπτοσύστημα χρησιμοποιεί το κλειδί $K = (k_1,k_2,k_3,k_4)$. Θέτουμε $K' = (k_2,k_3,k_4,k_1)$ και $K'' = (k_3,k_4,k_1,k_2)$. Για την κρυπτογράφηση ενός απλού κειμένου $M = m_1m_2m_3m_4$ κάνουμε τα εξής:

1. Υπολογίζουμε $m_1m_2 \oplus f_K(m_3m_4) = n_3n_4$ και σχηματίζουμε την τετράδα $n_1n_2n_3n_4$, όπου $n_1n_2 = m_3m_4$.
2. Υπολογίζουμε $n_1n_2 \oplus f_{K'}(n_3n_4) = r_3r$ και σχηματίζουμε την τετράδα $r_1r_2r_3r_4$, όπου $r_1r_2 = n_3n_4$.
3. Υπολογίζουμε $r_1r_2 \oplus f_{K''}(r_3r_4) = s_1s_2$.
4. Η κρυπτογράφηση του M είναι η τετράδα $C = s_1s_2r_3r_4$.

Η αποκρυπτογράφηση του C γίνεται με τον ίδιο τρόπο χρησιμοποιώντας τα κλειδιά K'', K', K με αυτή την σειρά. Πράγματι, για την ανάκτηση του απλού μηνύματος κάνουμε τα εξής:

1. Υπολογίζουμε
$$s_1s_2 \oplus f_{K''}(r_3r_4) = (r_1r_2 \oplus f_{K''}(r_3r_4)) \oplus f_{K''}(r_3r_4) = r_1r_2$$
και σχηματίζουμε την τετράδα $r_3r_4r_1r_2$.
2. Υπολογίζουμε
$$r_3r_4 \oplus f_{K'}(r_1r_2) = (n_1n_2 \oplus f_{K'}(n_3n_4)) \oplus f_{K'}(n_3n_4) = n_1n_2$$
και σχηματίζουμε την τετράδα $r_1r_2n_1n_2 = n_3n_4n_1n_2$.
3. Υπολογίζουμε
$$n_3n_4 \oplus f_K(n_1n_2) = (m_1m_2 \oplus f_K(m_3m_4)) \oplus f_K(m_3m_4) = m_1m_2$$
4. Η αποκρυπτογράφηση του C είναι η τετράδα
$$m_1m_2n_1n_2 = m_1m_2m_3m_4 = M$$

Παράδειγμα 4.3. Ας υποθέσουμε ότι θέλουμε να κρυπτογραφήσουμε τον αριθμό 8 με το κρυπτοσύστημα Baby Block. Βλέπουμε στον Πίνακα της Εικόνας 5 ότι το αντίστοιχο στοιχείο του κώδικα ASCII είναι το 0111000. Προσθέτουμε και το 1 στο τέλος ώστε να έχει άρτιο πλήθος 1 (όπως συμβαίνει συχνά στη πράξη ώστε να ανιχνευτεί πιθανό λάθος στη μετάδοση) και παίρνουμε το στοιχείο 01110001. Για να το κρυπτογραφήσουμε, το χωρίζουμε σε δύο τμήματα από τέσσερα σύμβολα το καθένα, 0111 και 0001. Θα χρησιμοποιήσουμε το κλειδί 0100. Για την κρυπτογράφηση του 0111 κάνουμε τα εξής:

1. Υπολογίζουμε $01 \oplus f_{0100}(11) = 01 \oplus 01 = 00$ και σχηματίζουμε την τετράδα 1100.
2. Υπολογίζουμε $11 \oplus f_{1000}(00) = 11 \oplus 00 = 11$ και σχηματίζουμε την τετράδα 0011.
3. Υπολογίζουμε $00 \oplus f_{0001}(11) = 00 \oplus 00 = 00$ και σχηματίζουμε την τετράδα 0011.

Άρα, η κρυπτογράφηση της τετράδας 0111 είναι η 0011. Ομοίως υπολογίζουμε ότι η κρυπτογράφηση του 0001 είναι η τετράδα 0100. Έτσι, παίρνουμε το κρυπτοκείμενο 00110100.

Το Baby Block, όπως είδαμε, έχει ένα χώρο κλειδιών ο οποίος αποτελείται από 16 στοιχεία. Μία ιδέα για την ισχυροποίηση της κρυπτογράφησης με αυτό θα ήταν η κρυπτογράφηση ενός κειμένου M δύο φορές με δύο διαφορετικά κλειδιά K και L. Δηλαδή, αν E_K, E_L είναι οι συναρτήσεις κρυπτογράφησης οι οποίες αντιστοιχούν στα κλειδιά K και L, τότε υπολογίζουμε το κείμενο $E_L(E_K(M))$. Τότε, ο χώρος κλειδιών είναι το σύνολο $B^4 \times B^4$ το οποίο έχει 256 στοιχεία**.** Η μέθοδος της διπλής κρυπτογράφησης, αν και αυξάνει αρκετά τον χώρο κλειδιών, είναι ευάλωτη στη επίθεση *συνάντηση στο ενδιάμεσο.* Αυτή πραγματοποιείται όταν είναι γνωστό ένα απλό κείμενο M και το αντίστοιχο κρυπτογραφημένο, $C = E_L(E_K(M))$. Τότε, σχηματίζουμε ένα πίνακα με τα ζεύγη $(M,E_r(M))$, για κάθε κλειδί r. Κατόπιν, για κάθε κλειδί s υπολογίζουμε το $E_s^{-1}(C)$ και θεωρούμε το σύνολο

$$Z = \{(r,s)/\ E_r(M) = E_s^{-1}(C)\}$$

Το σύνολο Z είναι μη κενό καθώς περιέχει το ζεύγος (K,L). Αν διαθέτουμε αρκετά τέτοια ζεύγη γνωστού απλού κειμένου και του αντιστοίχου κρυπτογραφημένου, τότε μπορούμε εύκολα να προσδιορίσουμε τέτοια σύνολα ζευγών και κατά συνέπεια να βρούμε το σωστό ζεύγος κλειδιών (K,L). Η επίθεση αυτή εφαρμόζεται γενικότερα στη διπλή κρυπτογράφηση με οποιοδήποτε κρυπτοσύστημα τμήματος.

5. ΣΤΟΙΧΕΙΑ ΘΕΩΡΙΑΣ ΑΡΙΘΜΩΝ

Σ' αυτή την ενότητα θα δώσουμε μερικές βασικές γνώσεις από την Θεωρία Αριθμών τις οποίες θα χρειαστούμε για την περιγραφή των κρυπτοσυστημάτων δημοσίου κλειδιού τα οποία θα παρουσιάσουμε στην επόμενη ενότητα (βλ. σχετικά και στο Πουλάκης, 1997).

5.1 Διαιρετότητα ακεραίων

Ας είναι a και b ακέραιοι. Λέμε ότι ο a *διαιρεί* τον b και γράφουμε a | b, αν υπάρχει ακέραιος c, ώστε να ισχύει b = ac. Π.χ. 3 | 12, 4 | 20, 7 | 28. Αν ο a δεν διαιρεί τον b, τότε γράφουμε a ∤ b. Μερικές βασικές ιδιότητες της διαίρεσης δίνονται στην παρακάτω πρόταση. Η απόδειξή τους είναι εύκολη και αφήνεται ως άσκηση.

Πρόταση 5.1. Ας είναι $a,b,c\in\mathbb{Z}$. Τότε, ισχύουν τα εξής:

1. Αν a | b και b | c, τότε a | c.
2. Αν a | b και c | d, τότε ac | bd.
3. Αν a | b και a | c, τότε a | bx+cy, $\forall x,y\in\mathbb{Z}$.
4. Αν a | b και b ≠ 0, τότε |a| ≤ |b|.
5. Αν a | b και b | a, τότε |a| = |b|.
6. Αν 0 | b, τότε b = 0.
7. Για κάθε $a\in\mathbb{Z}$, ισχύει a | a και a | 0.
8. Για κάθε $a,b\in\mathbb{Z}$, ισχύει a | b αν και μόνον αν |a| | |b|.

Ας είναι $x\in\mathbb{R}$. Καλούμε *ακέραιο μέρος* του x και το συμβολίζουμε με ⌊x⌋ τον μεγαλύτερο ακέραιο που είναι μικρότερος ή ίσος του x. Άρα x = ⌊x⌋+ε, όπου $\varepsilon\in\mathbb{R}$ με $0 \le \varepsilon < 1$. Π.χ. ⌊5/2⌋ = 2, ⌊–1/2⌋ = –1, ⌊π⌋ = 3. Θα χρησιμοποιήσουμε αυτή την έννοια στην απόδειξη του επόμενου βασικού θεωρήματος.

Θεώρημα 5.1. *Ας είναι* $a,b,c\in\mathbb{Z}$ με b ≠ 0. *Τότε, υπάρχει μοναδικό ζεύγος* $(q,r)\in\mathbb{Z}^2$ *τέτοιο, ώστε να ισχύει:*

$$a = bq+r \quad \textit{και} \quad 0 \le r < |b|$$

Απόδειξη. Ας είναι b > 0. Θέτουμε q = ⌊a/b⌋. Τότε, έχουμε $0 \le a/b–q < 1$ και επομένως για τον ακέραιο r = a–bq ισχύει $0 \le r < b$. Επομένως, το ζεύγος (q,r) έχει τις επιθυμητές ιδιότητες. Ας υποθέσουμε ότι το ζεύγος $(u,v)\in\mathbb{Z}^2$ έχει τις ίδιες ιδιότητες. Τότε, ισχύει $0 \le v/b < 1$ και επομένως u = ⌊a/b⌋ = q. Έτσι, παίρνουμε:

$$r = a–bq = a–bu = v$$

Συνεπώς, το ζεύγος (q,r) είναι μοναδικό. Τέλος, αν $b < 0$, τότε εφαρμόζοντας τα παραπάνω για τους ακέραιους a και |b| παίρνουμε το αποτέλεσμα.

Ο ακέραιος q καλείται *πηλίκο* της διαίρεσης του a δια b και ο r *υπόλοιπο*. Οι σχέσεις του θεωρήματος καλούνται *Ευκλείδεια διαίρεση*. Σύμφωνα με το Θεώρημα 5.1, για κάθε ακέραιο a ισχύει $a = 2q$ ή $a = 2q+1$, με $q \in \mathbb{Z}$. Στην πρώτη περίπτωση ο ακέραιος a καλείται *άρτιος* ενώ στη δεύτερη *περιττός*.

Παράδειγμα 5.1. Θα δείξουμε ότι το γινόμενο n διαδοχικών ακεραίων διαιρείται με n. Θεωρούμε λοιπόν το γινόμενο $A = a(a+1)\cdots(a+n-1)$, όπου a είναι ένας μη μηδενικός ακέραιος. Θα δείξουμε ότι ο A διαιρείται με n. Αν $n \mid a$, τότε $n \mid A$. Στη συνέχεια, ας είναι $n \nmid a$. Από το Θεώρημα 5.1, έχουμε $a = qn+r$, όπου $q,r \in \mathbb{Z}$ με $1 < r < n$. Τότε, ένας από τους όρους του γινομένου A είναι ο $a+n-r = n(q+1)$ ο οποίος διαιρείται από τον n. Άρα $n \mid A$.

Ας είναι a, b ακέραιοι με $a \neq 0$. Ένας ακέραιος d καλείται *κοινός διαιρέτης* των a και b, αν $d \mid a$ και $d \mid b$. Τότε $d \mid a$ και επομένως $|d| \mid |a|$, απ' όπου έπεται ότι το σύνολο των κοινών διαιρετών των a και b είναι πεπερασμένο. Ο μεγαλύτερος θετικός κοινός διαιρέτης των a και b καλείται *μέγιστος κοινός διαιρέτης* των a και b και συμβολίζεται με μκδ(a,b). Παρατηρούμε ότι κάθε ακέραιος a έχει το ίδιο σύνολο θετικών διαιρετών με τον –a και επομένως μκδ(a,b) = μκδ(|a|,|b|). Επίσης, καθώς κάθε ακέραιος διαιρεί το μηδέν, ισχύει μκδ(0,a) = |a|.

Παράδειγμα 5.2. Οι κοινοί διαιρέτες των ακεραίων 30 και 42 είναι οι ακέραιοι 1, 2, 3, 6 και κατά συνέπεια έχουμε: μκδ(30,42) = 6.

Αν μκδ(a,b) = 1, τότε οι ακέραιοι a, b καλούνται *πρώτοι μεταξύ τους*. Π.χ οι ακέραιοι 27 και 44 είναι πρώτοι μεταξύ τους, καθώς ισχύει μκδ(27,44) = 1. Στην επόμενη πρόταση δίνουμε μία βασική ιδιότητα του μέγιστου κοινού διαιρέτη.

Πρόταση 5.2. *Ας είναι* a, b *μη μηδενικοί ακέραιοι και* d = μκδ(a,b). *Τότε, για κάθε ακέραιο* k, *ισχύει:*

$$d = \text{μκδ}(a+kb,b)$$

Απόδειξη. Ας είναι $\delta = \text{μκδ}(a+kb,b)$. Καθώς $d \mid a$ και $d \mid b$, παίρνουμε $d \mid a+kb$. Άρα, ο d είναι ένας θετικός κοινός διαιρέτης των a+kb και b. Έτσι, έχουμε $d \leq \delta$. Αντιστρόφως, έχουμε $\delta \mid a+kb$, $\delta \mid b$, απ' όπου $\delta \mid kb$ και επομένως $\delta \mid a+kb-kb$, απ' όπου $\delta \mid a$. Άρα, ο δ είναι ένας θετικός κοινός διαιρέτης των a και b. Επομένως $\delta \leq d$. Έτσι, καθώς οι ακέραιοι δ και d είναι θετικοί, παίρνουμε $\delta = d$.

Στη συνέχεια θα παρουσιάσουμε μία μέθοδο για την εύρεση του μέγιστου κοινού διαιρέτη δύο ακεραίων η οποία οφείλεται στον Ευκλείδη. Ας είναι a και b ακέραιοι με $a > b > 0$ και $d = \mu\kappa\delta(a,b)$. Θέτουμε $r_0 = a$ και $r_1 = b$. Από το Θεώρημα 5.1 έπεται ότι υπάρχουν ζεύγη ακεραίων (q_i,r_{i+1}) $(i = 1,\ldots,n)$ τέτοια, ώστε να ισχύει: $r_0 = r_1q_1+r_2, \quad 0 \le r_2 < r_1$

$$\begin{aligned}
r_1 &= r_2q_2+r_3, & 0 \le r_3 < r_2\\
r_2 &= r_3q_3+r_4, & 0 \le r_4 < r_3\\
\ldots &\quad \ldots & \ldots \quad \ldots\\
r_{n-3} &= r_{n-2}q_{n-2}+r_{n-1}, & 0 \le r_{n-1} < r_{n-2}\\
r_{n-2} &= r_{n-1}q_{n-1}+r_n, & 0 \le r_n < r_{n-1}\\
r_{n-1} &= r_nq_n+r_{n+1}, & 0 \le r_{n+1} < r_n
\end{aligned}$$

Από τα παραπάνω έχουμε:

$$0 \le r_{n+1} < r_n < r_{n-1} < \ldots < r_2 < r_1$$

Αν για κάθε $n \ge 1$ το υπόλοιπο r_{n+1} είναι $\neq 0$, τότε μεταξύ του 0 και του r_1 θα υπήρχε άπειρο πλήθος διαφορετικών ακεραίων το οποίο είναι αδύνατο. Επομένως, υπάρχει δείκτης n, ώστε να ισχύει $r_j \neq 0$ $(j = 2,\ldots,n)$ και $r_{n+1} = 0$. Από την Πρόταση 5.2, έχουμε:

$$\mu\kappa\delta(r_1,r_2) = \mu\kappa\delta(r_2q_2+r_3,r_2) = \mu\kappa\delta(r_3,r_2) = \ldots = \mu\kappa\delta(r_{n-1},r_n) = \mu\kappa\delta(r_nq_n,r_n) = r_n$$

Άρα $d = r_n$. Η κατάστρωση του παραπάνω συστήματος Ευκλειδείων διαιρέσεων για τον προσδιορισμό του μεγίστου κοινού διαιρέτη των a και b καλείται *Ευκλείδειος αλγόριθμος* για τους ακέραιους a και b.

Παράδειγμα 5.3. Θα χρησιμοποιήσουμε τον Ευκλείδειο αλγόριθμο για τον υπολογισμό του μέγιστου κοινού διαιρέτη των ακεραίων 678 και 118. Έχουμε:

$$\begin{aligned}
678 &= 118\cdot 5+88\\
118 &= 88\cdot 1+30\\
88 &= 30\cdot 2+28\\
30 &= 28\cdot 1+2\\
28 &= 2\cdot 14
\end{aligned}$$

Άρα, ισχύει $\mu\kappa\delta(678,118) = 2$.

Από το σύστημα το οποίο καταστρώσαμε παραπάνω, παίρνουμε:

$$r_{n-2}-r_{n-1}q_{n-1} = r_n \quad \text{και} \quad r_{n-3}-r_{n-2}q_{n-2} = r_{n-1}$$

απ' όπου

$$d = r_n = (1+q_{n-1}q_{n-2})r_{n-2}+(-q_{n-1})r_{n-3}$$

Έτσι, εκφράσαμε τον μέγιστο κοινό διαιρέτη d ως γραμμικό συνδυασμό των r_{n-2} και r_{n-3} με ακέραιους συντελεστές. Συνεχίζοντας με αυτόν τον τρόπο, η τελευταία αντικατάσταση του υπολοίπου $r_2 = a_0-a_1q_1$ θα δώσει την γραφή του d ως γραμμικό συνδυασμό των r_0 και r_1 με ακέραιους συντελεστές. Έχουμε λοιπόν την εξής πρόταση:

Πρόταση 5.3. Ας είναι a, b μη μηδενικοί ακέραιοι και d = μκδ(a,b). Τότε, υπάρχουν ακέραιοι u, v έτσι, ώστε να ισχύει d = au+bv.

Πόρισμα 5.1. Ας είναι $a,b\in\mathbb{Z}$ και d ένας θετικός κοινός διαιρέτης τους. Τότε, ισχύει d = μκδ(a, b), αν και μόνον αν, για κάθε θετικό ακέραιο δ με δ | a και δ | b έχουμε δ | d.

Απόδειξη. Ας υποθέσουμε ότι d = μκδ(a,b). Από την Πρόταση 5.3, έχουμε d = ua+vb, όπου $u,v\in\mathbb{Z}$. Έτσι, αν δ είναι θετικός ακέραιος με δ | a και δ | b, τότε δ | d. Αντιστρόφως, ας υποθέσουμε ότι για κάθε θετικό ακέραιο δ με δ | a και δ | b έχουμε δ | d. Τότε, ισχύει $\delta \le d$ και επομένως d = μκδ(a,b).

Πόρισμα 5.2. Ας είναι a, b μη μηδενικοί ακέραιοι. Οι ακέραιοι a και b είναι πρώτοι μεταξύ τους αν και μόνον αν υπάρχουν ακέραιοι u και v τέτοιοι, ώστε

$$au+bv = 1$$

Πόρισμα 5.3. *Ας είναι* a, b, c *μη μηδενικοί ακέραιοι τέτοιοι, ώστε* a | bc *και* μκδ(a,b) = 1. *Τότε, ισχύει* a | c.

Απόδειξη. Καθώς μκδ(a,b) = 1, το Πόρισμα 5.2 συνεπάγεται ότι υπάρχουν ακέραιοι u, v, ώστε να ισχύει 1 = au + bv. Έτσι, έχουμε c = cax + cby και χρησιμοποιώντας την σχέση a | bc παίρνουμε a | c.

Πόρισμα 5.4. *Ας είναι* a, b, c *μη μηδενικοί ακέραιοι τέτοιοι, ώστε* a | c, b | c *και* μκδ(a,b) = 1. *Τότε, ισχύει* ab | c.

Απόδειξη. Από την σχέση a | c, έχουμε c = ak, όπου $k\in\mathbb{Z}$. Τότε b | ak και μκδ(a,b) = 1. Έτσι, από το Πόρισμα 5.3 έπεται b | k και επομένως k = be, όπου $e\in\mathbb{Z}$. Άρα c = abe και επομένως ab | c.

Παράδειγμα 5.4. Στο Παράδειγμα 5.3 εφαρμόσαμε τον Ευκλείδειο αλγόριθμο και βρήκαμε ότι ισχύει μκδ(678,118) = 2. Στη συνέχεια θα χρησιμοποιήσουμε τα βήματα του Ευκλειδείου αλγορίθμου για να υπολογίσουμε ακεραίους u, v με 678u+118v = 2.

Έχουμε:

$$2 = 30–28 = 30–(88–30\cdot 2) = –88+3\cdot 30 = –88+3\cdot(118–88) =$$
$$3\cdot 118–4\cdot 88 = 3\cdot 118–4(678–5\cdot 118) = 4\cdot 678+23\cdot 118$$

Άρα, ισχύει $4\cdot 678+23\cdot 118 = 2$.

Καλούμε *κοινό πολλαπλάσιο* των ακεραίων a και b κάθε ακέραιο c με $a \mid c$ και $b \mid c$. Αν κάποιος από τους a και b είναι 0, τότε το μοναδικό κοινό τους πολλαπλάσιο είναι το 0. Έτσι, υποθέτουμε ότι $a \neq 0$ και $b \neq 0$. Το γινόμενο |ab| είναι ένα θετικό κοινό πολλαπλάσιο των a και b. Έτσι, το σύνολο των θετικών κοινών πολλαπλασίων των a και b είναι μη κενό και κατά συνέπεια περιέχει ένα στοιχείο το οποίο είναι μικρότερο από όλα τα άλλα. Αυτό το μικρότερο θετικό κοινό πολλαπλάσιο των a και b καλείται *ελάχιστο κοινό πολλαπλάσιο* των a και b και συμβολίζεται με εκπ(a,b). Παρατηρούμε ότι το σύνολο των θετικών κοινών πολλαπλασίων των ακεραίων a και b είναι το ίδιο μ' αυτό των |a| και |b| και επομένως ισχύει εκπ(a, b) = εκπ(|a|,|b|).

Παράδειγμα 5.5. Θα υπολογίσουμε το ελάχιστο κοινό πολλαπλάσιο των ακεραίων 6 και 15. Τα θετικά πολλαπλάσια του 6 είναι 6, 12, 18, 24, 30,… και τα θετικά πολλαπλάσια του 15 είναι 15, 30, 45,… . Άρα εκπ(6,15) = 30.

Πρόταση 5.4. *Ας είναι* m *ένα θετικό κοινό πολλαπλάσιο των ακεραίων* a *και* b. *Τότε* m = εκπ(a,b) *αν και μόνον αν για κάθε θετικό ακέραιο* μ *με* $a \mid \mu$ *και* $b \mid \mu$ ισχύει $m \mid \mu$.

Απόδειξη. Ας υποθέσουμε ότι m = εκπ(a,b). Αν μ είναι θετικός ακέραιος με $a \mid \mu$ και $b \mid \mu$, τότε υπάρχουν $q,r \in \mathbb{Z}$ έτσι, ώστε $\mu = mq + r$ και $0 \leq r < m$. Οι σχέσεις $a \mid m$ και $a \mid \mu$ δίνουν $a \mid \mu – mq$, απ' όπου $a \mid r$. Ομοίως, έχουμε $b \mid r$. Έτσι, αν $r \neq 0$, τότε ισχύει $r \geq m$ το οποίο είναι άτοπο. Άρα $r = 0$ και επομένως $m \mid \mu$. Αντιστρόφως, ας υποθέσουμε ότι για κάθε θετικό κοινό πολλαπλάσιο μ των a και b ισχύει $m \mid \mu$. Άρα $m \leq \mu$. Επομένως, ο m είναι το μικρότερο από όλα τα θετικά κοινά πολλαπλάσια των a, b και κατά συνέπεια ισχύει m = εκπ(a,b).

5.2 Πρώτοι αριθμοί

Ένας θετικός ακέραιος $p > 1$ καλείται *πρώτος*, αν διαιρείται μόνον από τους ακέραιους ± 1, $\pm p$. Ένας πρώτος αριθμός ο οποίος είναι διαιρέτης ενός ακεραίου n καλείται *πρώτος διαιρέτης* ή *πρώτος παράγοντας* του n. Ένας θετικός ακέραιος $n > 1$ καλείται σύνθετος, αν δεν είναι πρώτος. Δηλαδή, ο n

είναι σύνθετος, αν και μόνον αν, υπάρχουν ακέραιοι a, b, ώστε να ισχύει $n = ab$ και $1 < a \le b < n$.

Παράδειγμα 5.6. Οι ακέραιοι 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31 είναι πρώτοι, ενώ οι 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20 σύνθετοι.

Πρόταση 5.5. *Κάθε ακέραιος* $a > 1$ *έχει ένα πρώτο διαιρέτη.*

Απόδειξη. Ας είναι D το σύνολο των διαιρετών d του a με $d > 1$. Καθώς $a \in D$, το σύνολο D είναι μη κενό. Θεωρούμε τον μικρότερο ακέραιο p του D. Αν ο p είναι σύνθετος, τότε υπάρχουν ακέραιοι b, c, ώστε να ισχύει $p = bc$ και $1 < b \le c < p$. Έτσι, έχουμε $b \mid p$ και $p \mid a$. Άρα $b \mid a$ και $b < p$ το οποίο είναι άτοπο. Άρα, ο ακέραιος p είναι ένας πρώτος διαιρέτης του a.

Στη συνέχεια έχουμε το παρακάτω βασικό θεώρημα.

Θεώρημα 5.2. (Ευκλείδης) *Το πλήθος των πρώτων αριθμών είναι άπειρο.*

Απόδειξη. Ας υποθέσουμε ότι $p_1,\ldots,p_k$ είναι όλοι οι πρώτοι. Θέτουμε $P = p_1 \cdots p_k + 1$. Από την Πρόταση 5.5 έπεται ότι υπάρχει δείκτης j με $p_j \mid P$. Οι σχέσεις $p_j \mid P$ και $p_j \mid p_1 \cdots p_k$ δίνουν $p_j \mid 1$ το οποίο είναι άτοπο.

Μία άλλη ενδιαφέρουσα εφαρμογή της Πρότασης 5.5 είναι η παρακάτω πρόταση η οποία μας δίνει μία μέθοδο για να εξετάζουμε αν ένας ακέραιος είναι πρώτος.

Πρόταση 5.6. *Κάθε σύνθετος ακέραιος* $a > 1$ *έχει ένα πρώτο διαιρέτη* p *με* $p \le \sqrt{a}$.

Απόδειξη. Ο ακέραιος a είναι σύνθετος και κατά συνέπεια υπάρχουν ακέραιοι b, c ώστε να ισχύει $a = bc$ και $1 < b \le c < a$. Από την Πρόταση 5.4 έπεται ότι υπάρχει ένας πρώτος p ο οποίος διαιρεί τον b και επομένως διαιρεί και τον a. Από την σχέση $b^2 \le bc = a$ παίρνουμε $p \le b \le \sqrt{a}$.

Πόρισμα 5.5. *Αν ένας ακέραιος* $a > 1$ *δεν έχει κανένα πρώτο διαιρέτη* p, *με* $p \le \sqrt{a}$, *τότε ο* a *είναι πρώτος.*

Έτσι, για να διαπιστώσουμε αν ένας ακέραιος a είναι πρώτος, αρκεί να εξετάσουμε αν διαιρείται από όλους τους πρώτους $\le \sqrt{a}$. Η μέθοδος όμως αυτή δεν είναι πρακτική στην περίπτωση, όπου ο a είναι ένας πολύ μεγάλος πρώτος.

Παράδειγμα 5.7. Θα ελέγξουμε αν ο αριθμός 1151 είναι πρώτος. Έχουμε $\lfloor \sqrt{1151} \rfloor = 33$. Καθώς διαπιστώνουμε εύκολα κανένας πρώτος ≤ 31 δεν διαιρεί τον 1151. Επομένως, ο ακέραιος 1151 είναι πρώτος.

Στη συνέχεια θα δώσουμε την απόδειξη του επομένου θεωρήματος το οποίο είναι γνωστό ως το *Θεμελιώδες Θεώρημα της Αριθμητικής.*

Θεώρημα 5.3. *Κάθε ακέραιος* $a > 1$ *γράφεται με μοναδικό τρόπο ως γινόμενο πρώτων αριθμών.*

Για την απόδειξη του θεωρήματος θα χρειαστούμε το εξής λήμμα:

Λήμμα 5.1. *Ας είναι* $a_1,\ldots,a_n$ *ακέραιοι* $\neq 0,1$ *και* p *ένας πρώτος.* Αν $p \mid a_1\cdots a_n$, *τότε* $p \mid a_i$ *για κάποιο δείκτη* i *με* $1 \le i \le n$.

Απόδειξη. Ας υποθέσουμε ότι $p \nmid a_i$ $(i = 1,\ldots,n)$. Τότε $\mu\kappa\delta(p,a_i) = 1$ $(i = 1,\ldots,n)$. Καθώς $p \mid a_1\cdots a_n$ και $\mu\kappa\delta(p,a_n) = 1$, το Πόρισμα 5.3 συνεπάγεται ότι $p \mid a_1\cdots a_{n-1}$. Ομοίως, επειδή $\mu\kappa\delta(p,a_{n-1}) = 1$, έχουμε $p \mid a_1\cdots a_{n-2}$. Συνεχίζοντας με αυτό τον τρόπο προκύπτει $p \mid a_1$ που είναι άτοπο. Άρα, έχουμε $p \mid a_i$ για κάποιο δείκτη i.

Απόδειξη του Θεωρήματος 5.3. Ας είναι a ένας ακέραιος > 1. Τότε, από την Πρόταση 5.4 έπεται ότι υπάρχει πρώτος διαιρέτης p_1 του a και επομένως έχουμε $a = p_1a_1$, όπου a_1 θετικός ακέραιος. Αν $a_1 > 1$, τότε υπάρχει πρώτος διαιρέτης p_2 του a_1 και επομένως έχουμε $a = p_1p_2a_2$, όπου a_2 θετικός ακέραιος. Συνεχίζοντας με αυτό τον τρόπο παίρνουμε $a = p_1\cdots p_ka_k$, όπου $p_1,\ldots,p_k$ είναι πρώτοι και ο a_k θετικός ακέραιος. Αν για κάθε k ισχύει $a_k > 1$, τότε υπάρχει μία άπειρη ακολοθία ακεραίων μεταξύ του 1 και του a, πράγμα αδύνατο. Άρα, για κάποιο k έχουμε $a_k = 1$ και κατά συνέπεια $a = p_1\cdots p_k$, δηλαδή ο ακέραιος a γράφεται ως γινόμενο πρώτων.

Ας υποθέσουμε στη συνέχεια ότι

$$p_1\cdots p_k = a = q_1\cdots q_l, \quad \text{με} \quad k \le l$$

είναι δύο γραφές του a ως γινόμενο πρώτων. Τότε $p_1 \mid q_1\cdots q_l$. Από το Λήμμα 5.1 έπεται ότι $p_1 \mid q_j$, για κάποιο δείκτη j. Καθώς οι ακέραιοι p_1 και q_j είναι πρώτοι, έπεται $p_1 = q_j$. Έτσι, έχουμε:

$$p_2\cdots p_k = a/p_1 = q_2\cdots q_{j-1}q_{j+1}\cdots q_l$$

Ομοίως βρίσκουμε ότι ο πρώτος p_2 ισούται με κάποιον από τους $q_2,\ldots,q_{j-1},q_{j+1},\ldots,q_l$. Συνεχίζοντας με αυτό τρόπο βλέπουμε ότι οι πρώτοι $p_1,\ldots,p_{k-1}$ είναι κάποιοι από τους πρώτους $q_1,\ldots,q_l$ και $p_k = r_1\cdots r_{l-k+1}$, όπου $r_1, \ldots, r_{l-k+1}$ είναι κάποιοι από τους $q_1, \ldots, q_l$. Ο p_k είναι πρώτος και επομένως έχουμε $k = l$ και $p_k = r_1$. Άρα, η γραφή του a σε γινόμενο πρώτων είναι μοναδική.

Ας είναι a ακέραιος > 1. Τότε, σύμφωνα με το Θεώρημα 5.3, υπάρχουν πρώτοι $p_1,\ldots,p_k$ και θετικοί ακέραιοι $a(1),\ldots,a(k)$ έτσι, ώστε να ισχύει:

$$a = p_1^{a(1)} \cdots p_k^{a(k)}$$

Η παραπάνω γραφή του a καλείται *πρωτογενής ανάλυση* του a. Αν ο a είναι αρκετά μικρός, τότε μπορούμε να εφαρμόσουμε το Πόρισμα 5.5 και να πάρουμε την πρωτογενή του ανάλυση. Ας σημειωθεί ότι η μέθοδος αυτή δεν είναι πρακτική για αρκετά μεγάλους ακεραίους.

Παράδειγμα 5.8. Θα υπολογίσουμε την πρωτογενή ανάλυση του 1073. Έχουμε $\lfloor\sqrt{1073}\rfloor = 32$. Οι πρώτοι που είναι ≤ 32 είναι οι 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31. Ο πρώτος από αυτούς που διαιρεί τον 1073 είναι ο 29. Τότε:

$$1073 = 29 \cdot 37$$

Καθώς ο ακέραιος 37 είναι πρώτος, η παραπάνω γραφή είναι η πρωτογενής ανάλυση του 1073.

Πρόταση 5.7. *Ας είναι* a *ακέραιος* > 1 *με πρωτογενή ανάλυση*

$$a = p_1^{a(1)} \cdots p_k^{a(k)}$$

Τότε, ο θετικός ακέραιος d *διαιρεί τον* a, *αν και μόνον αν, ισχύει:*

$$d = p_1^{b(1)} \cdots p_k^{b(k)}, \quad \text{με} \quad 0 \le b(i) \le a(i) \quad (i = 1,\ldots,k)$$

Απόδειξη. Ας είναι $d = p_1^{b(1)} \cdots p_k^{b(k)}$, με $0 \le b(i) \le a(i)$ $(i = 1,\ldots,k)$. Θεωρούμε τον ακέραιο $c = p_1^{c(1)} \cdots p_k^{c(k)}$, όπου $c(i) = a(i) - b(i)$ $(i = 1,\ldots,k)$. Έτσι, έχουμε $a = dc$ και επομένως $d \mid a$.

Αντιστρόφως, ας είναι $d \mid a$. Τότε, υπάρχει $c \in \mathbb{Z}$, ώστε να ισχύει:

$$dc = p_1^{a(1)} \cdots p_k^{a(k)}$$

Από την μοναδικότητα της πρωτογενούς ανάλυσης παίρνουμε:

$$d = p_1^{b(1)} \cdots p_k^{b(k)} \quad \text{και} \quad c = p_1^{c(1)} \cdots p_k^{c(k)}$$

όπου $0 \le b(i) \le a(i)$, $0 \le c(i) \le a(i)$ και $a(i) = b(i) + c(i)$ $(i = 1,\ldots,k)$.

Πρόταση 5.8. *Ας είναι* a *και* b *ακέραιοι* > 1 *με*

$$a = p_1^{a(1)} \cdots p_k^{a(k)} \quad \text{και} \quad b = p_1^{b(1)} \cdots p_k^{b(k)}$$

όπου $p_1,\ldots,p_k$ *διαφορετικοί πρώτοι και* $a(1),\ldots,a(k),b(1),\ldots,b(k) \in \mathbb{N}$. *Τότε:*

$$\text{μκδ}(a, b) = p_1^{\min\{a(1),b(1)\}} \cdots p_k^{\min\{a(k),b(k)\}}$$

και

$$\text{εκπ}(a, b) = p_1^{\max\{a(1),b(1)\}} \cdots p_k^{\max\{a(k),b(k)\}}$$

Απόδειξη. Θέτουμε $d = p_1^{\min\{a(1),b(1)\}} \cdots p_k^{\min\{a(k),b(k)\}}$. Καθώς έχουμε

$$\min\{a_i,b_i\} \le a_i \quad \text{και} \quad \min\{a_i,b_i\} \le b_i \quad (i = 1,\ldots,k)$$

από την Πρόταση 5.7 παίρνουμε ότι $d \mid a$ και $d \mid b$. Ας είναι δ ένας θετικός διαιρέτης των a και b. Τότε $\delta = p_1^{\delta(1)} \cdots p_k^{\delta(k)}$, με $0 \le \delta(i) \le a(i)$ και $0 \le \delta(i) \le b(i)$ $(i = 1,\ldots,k)$. Άρα, $0 \le \delta(i) \le \min\{a_i,b_i\}$ $(i = 1,\ldots,k)$. Έτσι, από την Πρόταση 5.7, έπεται ότι $\delta \mid d$. Επίσης, το Πόρισμα 5.1 δίνει $d = \mu\kappa\delta(a, b)$. Η απόδειξη της δεύτερης ισότητας είναι όμοια και αφήνεται ως άσκηση.

Άμεση εφαρμογή της Πρότασης 5.8 είναι το εξής πόρισμα του οποίου η απόδειξη αφήνεται ως άσκηση.

Πόρισμα 5.6. *Ας είναι* a *και* b *ακέραιοι* $\neq 0, 1$. *Τότε ισχύει:*

$$\mu\kappa\delta(a,b)\ \varepsilon\kappa\pi(a,b) = |ab|$$

Ένα από τα σημαντικότερα προβλήματα της Υπολογιστικής Θεωρίας Αριθμών είναι το παρακάτω:

Πρόβλημα Παραγοντοποίησης Ακεραίων: Εύρεση ενός ταχύ και αποδοτικού αλγορίθμου για τον υπολογισμό της πρωτογενούς ανάλυσης φυσικών αριθμών.

Η έλλειψη ενός τέτοιου αλγόριθμου αποτελεί τη βάση για την ασφάλεια πολλών σύγχρονων κρυπτογραφικών εφαρμογών. Ας σημειωθεί ότι αν και έχουν αναπτυχθεί μέχρι σήμερα αρκετοί αλγόριθμοι για την παραγοντοποίηση ακεραίων, κανένας από αυτούς δεν είναι αρκετά αποδοτικός ώστε να απειλήσει την ασφάλεια των σύγχρονων κρυπτοσυστημάτων. Ο μόνος αλγόριθμος ο οποίος μπορεί να το καταφέρει είναι ο αλγόριθμος του P. Shor ο οποίος προτάθηκε το 1994 (Shor, 1994). Η υλοποίηση όμως αυτού του αλγορίθμου απαιτεί κβαντικό υπολογιστή με δυνατότητες πολύ μεγαλύτερες από αυτές που προσφέρει η σύγχρονη κβαντική τεχνολογία.

5.3 Το σύνολο $\mathbb{Z}_n$

Ας είναι n ακέραιος > 1. Για κάθε $a \in \mathbb{Z}$ συμβολίζουμε με $a \bmod n$ το υπόλοιπο της διαίρεσης του a με τον n. Π.χ. $15 \bmod 11 = 4$, $35 \bmod 8 = 3$. Θεωρούμε το σύνολο

$$\mathbb{Z}_n = \{0,1,\ldots,n-1\}$$

και για κάθε ζεύγος ακεραίων a και b θέτουμε

$$a \oplus b = a+b \bmod n \quad \text{και} \quad a \odot b = ab \bmod n$$

Έτσι, ορίζουμε δύο πράξεις μέσα στο $\mathbb{Z}_n$, τις οποίες καλούμε *πρόσθεση* και *πολλαπλασιασμό,* αντίστοιχα.

Παράδειγμα 5.9. Θεωρούμε το σύνολο $\mathbb{Z}_{16}$. Θα προσθέσουμε και θα πολλαπλασιάσουμε τα στοιχεία 11 και 7 του $\mathbb{Z}_{16}$. Έχουμε:

$$11 \oplus 7 = 11+7 \bmod 16 = 18 \bmod 16 = 2$$

$$11 \odot 7 = 11 \cdot 7 \bmod 16 = 77 \bmod 16 = 13$$

Πρόταση 5.9. *Ας είναι* $a,b,c \in \mathbb{Z}_n$. *Τότε, ισχύουν τα εξής:*

1. $(a \oplus b) \oplus c = a \oplus (b \oplus c)$, $(a \odot b) \odot c = a \odot (b \odot c)$
2. $a \oplus b = b \oplus a$, $a \odot b = b \odot a$
3. $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$, $(a \oplus b)c = (a \odot c) \oplus (b \odot c)$
4. $a \oplus 0 = a$, $a \odot 1 = a$
5. $a \oplus (n-a) = 0$

Απόδειξη.

1. Έχουμε $a \oplus b = a+b-kn$, όπου $k \in \mathbb{Z}$, και $(a \oplus b) \oplus c = a \oplus b+c-ln$, όπου $l \in \mathbb{Z}$ (k και l είναι αντίστοιχα τα πηλίκα των διαιρέσεων των $a+b$ και $a \oplus b+c$ με n). Έτσι, παίρνουμε:

$$(a \oplus b) \oplus c = a+b+c-(k+l)n = a+b+c \bmod n$$

Επίσης, έχουμε $b \oplus c = b+c-qn$, όπου $q \in \mathbb{Z}$, και $a \oplus (b \oplus c) = a+b \oplus c-rn$, όπου $r \in \mathbb{Z}$. Οπότε, προκύπτει:

$$a \oplus (b \oplus c) = a+b+c-(q+r)n = a+b+c \bmod n$$

Άρα, ισχύει $(a \oplus b) \oplus c = a \oplus (b \oplus c)$. Ομοίως αποδεικνύεται και η δεύτερη ισότητα.

2. Αν $a \oplus b = r$, τότε $a+b = qn+r$, όπου $q \in \mathbb{Z}$, και επομένως $b \oplus a = r$, απ' όπου $a \oplus b = b \oplus a$. Ομοίως προκύπτει και η δεύτερη ισότητα.

3. Ας είναι $b \oplus c = r$ και $a \odot r = s$. Τότε, έχουμε $b+c = qn+r$ και $ar = un+s$, όπου $q,u \in \mathbb{Z}$, και επομένως

$$a(b+c) = a(qn+r) = aqn+ar = aqn+un+s = (aq+u)n+s$$

Δηλαδή, ισχύει $a(b+c) \bmod n = s$. Επίσης, θέτουμε $a \odot b = v$, $a \odot c = z$ και $v \oplus z = p$. Έτσι, έχουμε $ab = xn+v$, $ac = yn+z$ και $v+z = wn+p$, όπου $x,y,w \in \mathbb{Z}$, και επομένως

$$ab+ac = xn+v+yn+z = (x+y)n+wn+p = (x+y+w)n+p$$

απ' όπου $(ab+ac) \bmod n = p$. Οπότε, έχουμε:

$$a\odot(b\oplus c) = s = a(b+c) \bmod n = (ab+ac) \bmod n = p = (a\odot b)\oplus(a\odot c)$$

Η δεύτερη ισότητα αποδεικνύεται με όμοιο τρόπο.

4. Έχουμε $a+0 \bmod n = a \bmod n$ και $a\cdot 1 \bmod n = a \bmod n$. Επομένως, έχουμε $a\oplus 0 = a$ και $a\odot 1 = a$.

5. Έχουμε:

$$a\oplus(n-a) = a+(n-a) \bmod n = n \bmod n = 0$$

Αν $a\in\mathbb{Z}_n$, τότε ο ακέραιος $n-a$ καλείται *αντίθετο στοιχείο* του a και συμβολίζεται με $\ominus a$. Ισχύει $\ominus a = n-a = -a \bmod n$. Επίσης, γράφουμε:

$$a\ominus b = a\oplus(\ominus b) = a+(n-b) \bmod n = (a-b) \bmod n$$

Π.χ. Στο $\mathbb{Z}_{14}$ έχουμε $\ominus 5 = 14-5 = 9$, $5\ominus 13 = 5-13 \bmod 14 = -8 \bmod 14 = 6$.

Πρόταση 5.10. *Ας είναι* $a_1,\ldots,a_k\in\mathbb{Z}_n$ $(k \geq 3)$. *Τότε, με οποιοδήποτε τρόπο εφαρμόσουμε τις πράξεις* $\oplus$ *και* $\odot$ *στους* $a_1,\ldots,a_k$ *θα πάρουμε τους ακεραίους* $a_1+\cdots+a_k \bmod n$ *και* $a_1\cdots a_k \bmod n$, *αντίστοιχα.*

Απόδειξη. Στην απόδειξη της Πρότασης 5.9(1), είδαμε ότι καθένα από τα δύο αθροίσματα $(a\oplus b)\oplus c$ και $a\oplus(b\oplus c)$ ισούται με $a+b+c \bmod n$, γράφοντας $x\oplus y = x+y-qn$, όπου q είναι το πηλίκο της διαίρεσης του $x+y$ με τον n. Την ίδια μέθοδο μπορούμε να χρησιμοποιήσουμε για $k \geq 4$. Για παράδειγμα, ας θεωρήσουμε το άθροισμα $(a_1\oplus a_2)\oplus(a_3\oplus a_4)$. Γράφουμε:

$$a_1\oplus a_2 = a_1+a_2-qn, \qquad a_3\oplus a_4 = a_3+a_4-rn$$

και

$$(a_1\oplus a_2)\oplus(a_3\oplus a_4) = (a_1\oplus a_2)+(a_3\oplus a_4)-sn$$

όπου $q,r,s\in\mathbb{Z}$. Τότε, έχουμε:

$$(a_1\oplus a_2)\oplus(a_3\oplus a_4) = (a_1+a_2-qn)+(a_3+a_4-rn)-sn = a_1+a_2+a_3+a_4 \bmod n$$

Το ίδιο αποτέλεσμα παίρνουμε αν προσθέσουμε τους a_1, a_2, a_3, a_4 με οποιονδήποτε άλλο τρόπο. Ομοίως εργαζόμαστε και στην περίπτωση του πολλαπλασιασμού.

Ας είναι $a_1,\ldots,a_k\in\mathbb{Z}_n$ $(k \geq 3)$. Σύμφωνα με την Πρόταση 5.10, με οποιοδήποτε τρόπο εφαρμόσουμε τις πράξεις $\oplus$ και $\odot$ στους $a_1,\ldots,a_k$ θα έχουμε τα ίδια αποτελέσματα, τα οποία θα συμβολίζουμε αντίστοιχα με $a_1\oplus\cdots\oplus a_k$ και $a_1\odot\cdots\odot a_k$. Έτσι, έχουμε:

$$a_1\oplus\cdots\oplus a_k = a_1+\cdots+a_k \bmod n \quad \text{και} \quad a_1\odot\cdots\odot a_k = a_1\cdots a_k \bmod n$$

Επίσης, αν $a\in\mathbb{Z}_n$ και k είναι θετικός ακέραιος θα γράφουμε:

$$(\oplus k)a = a\oplus\cdots\oplus a, \quad (\ominus k)a = (n-a)\oplus\cdots\oplus(n-a), \quad a^{\odot k} = a\odot\cdots\odot a$$

όπου το πλήθος των a στα αθροίσματα και το γινόμενο είναι k. Από την Πρόταση 5.10 έχουμε:

$$(\oplus k)a = ka \bmod n \quad \text{και} \quad a^{\odot k} = a^k \bmod n$$

Ένα στοιχείο $a\in\mathbb{Z}_n$ καλείται *αντιστρέψιμο,* αν υπάρχει $b\in\mathbb{Z}_n$ έτσι, ώστε $a\odot b = 1$. Αν υπάρχει και άλλο στοιχείο $c\in\mathbb{Z}_n$ με $a\odot c = 1$, τότε έχουμε:

$$b = b\odot 1 = b\odot(a\odot c) = (b\odot a)\odot c = 1\odot c = c$$

Άρα, το στοιχείο b (αν υπάρχει) είναι μοναδικό. Το στοιχείο b καλείται *αντίστροφο* του a και συμβολίζεται με $a^{-1} \bmod n$. Το σύνολο των αντιστρέψιμων στοιχείων του $\mathbb{Z}_n$ συμβολίζεται με $\mathbb{Z}_n^*$.

Πρόταση 5.11. *Ας είναι* $a\in\mathbb{Z}_n$. *Τότε* $a\in\mathbb{Z}_n^*$ *αν και μόνον αν* $\text{μκδ}(a,n) = 1$. Επίσης, αν $a,b\in\mathbb{Z}_n^*$, τότε $a\odot b\in\mathbb{Z}_n^*$.

Απόδειξη. Ας είναι $a\in\mathbb{Z}_n^*$. Τότε υπάρχει $b\in\mathbb{Z}_n$ έτσι, ώστε $a\odot b = 1$. Άρα, ισχύει $ab \bmod n = 1$, απ' όπου έχουμε $ab+kn = 1$, με $k\in\mathbb{Z}_n$. Έτσι, από το Πόρισμα 5.2, έπεται ότι $\text{μκδ}(a,n) = 1$. Αντιστρόφως, αν $\text{μκδ}(a,n) = 1$, τότε, από την Πρόταση 5.2 έχουμε ότι υπάρχουν $u,v\in\mathbb{Z}$ τέτοιοι, ώστε $au+nv = 1$. Επομένως, προκύπτει $a\odot u = au \bmod n = 1$ και κατά συνέπεια $a\in\mathbb{Z}_n^*$.

Ας είναι $a\odot b = r$. Επομένως, υπάρχει $k\in\mathbb{Z}$ με $ab = kn+r$. Αν υπάρχει πρώτος p με $p \mid n$ και $p \mid r$, τότε $p \mid ab$. Έτσι, από το Λήμμα 5.1 έχουμε ότι $p \mid a$ ή $p \mid b$. Επομένως $\text{μκδ}(a,n) > 1$ ή $\text{μκδ}(b,n) > 1$ το οποίο δεν συμβαίνει γιατί $a,b\in\mathbb{Z}_n^*$. Άρα, $\text{μκδ}(r,n) = 1$ και κατά συνέπεια $a\odot b\in\mathbb{Z}_n^*$.

Πόρισμα 5.7. *Ο ακέραιος* n *είναι πρώτος αν και μόνον αν κάθε μη μηδενικό στοιχείο του* $\mathbb{Z}_n$ *είναι αντιστρέψιμο.*

Απόδειξη. Ο ακέραιος n είναι πρώτος αν και μόνον αν ισχύει:

$$\text{μκδ}(1,n) = \text{μκδ}(2,n) = \ldots = \text{μκδ}(n-1,n) = 1$$

Έτσι, από την Πρόταση 5.11 έπεται ότι ο n είναι πρώτος αν και μόνον έχουμε $1,\ldots,n-1\in\mathbb{Z}_n^*$.

Παράδειγμα 5.10. Έχουμε $\mathbb{Z}_{24}^* = \{1,5,7,11,13,17,19,23\}$.

Ας $a\in\mathbb{Z}_n^*$. Για να κατασκευάσουμε το στοιχείο $a^{-1} \bmod n$ εργαζόμαστε ως εξής: Χρησιμοποιούμε τον Ευκλείδειο αλγόριθμο για τους ακεραίους a, n και, καθώς ισχύει $\text{μκδ}(a,n) = 1$, υπολογίζουμε ακεραίους u και v με $au+nv = 1$.

Έτσι, έχουμε $au \bmod n = 1$ και επομένως $a^{-1} \bmod n = u \bmod n$. Στη συνέχεια δίνουμε ένα παράδειγμα τέτοιου υπολογισμού.

Παράδειγμα 5.11. Θεωρούμε το σύνολο $\mathbb{Z}_{53}^*$. Θα ελέγξουμε αν ο ακέραιος 8 ανήκει σ' αυτό. Εφαρμόζουμε τον Ευκλείδειο αλγόριθμο για τους ακεραίους 53 και 8. Έχουμε:

$$53 = 8\cdot 6+5$$
$$8 = 5\cdot 1+3$$
$$5 = 3\cdot 1+2$$
$$3 = 2\cdot 1+1$$
$$2 = 2\cdot 1$$

Άρα, ισχύει μκδ(53, 8) = 1 και κατά συνέπεια $8\in\mathbb{Z}_{53}^*$. Στη συνέχεια, θα υπολογίσουμε τον ακέραιο $8^{-1} \bmod 53$. Έχουμε :

$$1 = 3–2 = 3–(5–3) = 2\cdot 3–5 = 2(8–5)–5 = 2\cdot 8–3\cdot 5 =$$
$$2\cdot 8–3\cdot(53–8\cdot 6) = –3\cdot 53+20\cdot 8$$

Επομένως, ισχύει $–3\cdot 53+20\cdot 8 = 1$ και κατά συνέπεια $8^{-1} \bmod 53 = 20$.

Εφαρμογή: *Το ομοπαραλληλικό κρυπτοσύστημα.*

Το κρυπτοσύστημα αυτό είναι μία ειδική περίπτωση του κρυπτοσυστήματος αντικατάστασης. Ο χώρος των απλών και κρυπτογραφημένων κειμένων είναι το σύνολο $\mathbb{Z}_n$ και ο χώρος των κλειδιών το σύνολο $K = \mathbb{Z}_n^*\times\mathbb{Z}_n$. Για κάθε $(a,b)\in K$, η συνάρτηση κρυπτογράφησης είναι η συνάρτηση

$$E_{(a,b)} : \mathbb{Z}_n \to \mathbb{Z}_n,\ x \mapsto (a\odot x)\oplus b$$

και η συνάρτηση αποκρυπτογράφησης, η

$$D_{(a,b)} : \mathbb{Z}_n \to \mathbb{Z}_n,\ x \mapsto (a^{-1} \bmod n)\odot(x\ominus b).$$

Για κάθε $x\in\mathbb{Z}_n$ έχουμε:

$$(D_{(a,b)}\circ E_{(a,b)})(x) = D_{(a,b)}((a\odot x)\oplus b) = x$$

Επομένως, το παραπάνω σχήμα είναι ένα κρυπτοσύστημα.

Παράδειγμα 5.12. Αντιστοιχούμε τα γράμματα του Ελληνικού αλφαβήτου με τους ακεραίους 0,1,…,23, το κενό διάστημα με τον ακέραιο 24 και το ερωτηματικό ";" με τον 25. Έτσι, έχουμε $n = 26$. Τότε το μήνυμα

ΘΑ ΕΡΘΕΙΣ;

αντιστοιχεί στην ακολουθία ακεραίων:

7 0 24 4 16 7 4 8 17 25

Επιλέγουμε ως κλειδί κρυπτογράφησης το ζεύγος k = (7,4). Έτσι, η συνάρτηση κρυπτογράφησης είναι:

$$E_{(7,4)} : \mathbb{Z}_{26} \to \mathbb{Z}_{26},\ x \mapsto (7 \odot x) \oplus 4$$

Υπολογίζουμε:

$$E_{(7,4)}(7) = 1,\quad E_{(7,4)}(0) = 4,\quad E_{(7,4)}(24) = 16,\quad E_{(7,4)}(4) = 6,$$

$$E_{(7,4)}(16) = 12,\quad E_{(7,4)}(8) = 8,\quad E_{(7,4)}(17) = 19,\quad E_{(7,4)}(25) = 23$$

Επομένως, το κρυπτογραφημένο μήνυμα είναι:

ΒΕΡΘΝΕΙΥΩ

Καθώς $7^{-1} \bmod 26 = 15$, η συνάρτηση αποκρυπτογράφησης είναι:

$$D_{(7,4)} : \mathbb{Z}_{26} \to \mathbb{Z}_{26},\ x \mapsto x \mapsto 15 \odot (x \ominus 4)$$

Χρησιμοποιώντας την $D_{(7,4)}$, ο παραλήπτης παίρνει την αρχική ακολουθία ακεραίων και στη συνέχεια το μήνυμα.

Στην περίπτωση όπου ο ακέραιος n είναι αρκετά μικρός η κρυπτανάλυση είναι δυνατόν να γίνει με δοκιμή όλων των κλειδιών. Για παράδειγμα, αν n = 26, τότε το πλήθος των κλειδιών είναι:

$$|\mathbb{Z}_{26}^*||\mathbb{Z}_{26}| = 12 \cdot 26 = 312$$

Παρατηρούμε ότι για a = 1 έχουμε το κρυπτοσύστημα μετατόπισης το οποίο μετατοπίζει κυκλικά τα στοιχεία του $\mathbb{Z}_n$ κατά b θέσεις. Έτσι, είναι δυνατόν το κρυπτοσύστημα του Vigenère να περιγραφεί ως εξής: Ο χώρος των απλών κειμένων, ο χώρος των κρυπτογραφημένων κειμένων και ο χώρος των κλειδιών είναι το σύνολο $\mathbb{Z}_n^m$, όπου m θετικός ακέραιος. Για κάθε κλειδί $k = (k_1,\ldots,k_m)$ η συνάρτηση κρυπτογράφησης είναι

$$E_k: \mathbb{Z}_n^m \to \mathbb{Z}_n^m,\ (x_1,\ldots,x_m) \mapsto (x_1 \oplus k_1,\ldots,x_m \oplus k_m)$$

και η συνάρτηση αποκρυπτογράφησης

$$D_k: \mathbb{Z}_n^m \to \mathbb{Z}_n^m,\ (x_1,\ldots,x_m) \mapsto (x_1 \ominus k_1,\ldots,x_m \ominus k_m)$$

5.4 Η συνάρτηση φ του Euler

Η συνάρτηση $\varphi : \mathbb{N}\setminus\{0\} \to \mathbb{N}$, με $\varphi(n) = |\mathbb{Z}_n^*|$, για κάθε $n \in \mathbb{N}\setminus\{0\}$, καλείται *συνάρτηση του Euler.* Από την Πρόταση 5.11 έπεται ότι η τιμή φ(n) είναι το πλήθος των ακεραίων k με $1 \le k \le n$ και μκδ(k,n) = 1. Αν p είναι πρώτος, τότε από το Πόρισμα 5.7 έχουμε ότι για κάθε μη μηδενικό στοιχείο $a \in \mathbb{Z}_p$ ισχύει μκδ(a,p) = 1 και κατά συνέπεια έχουμε φ(p) = p–1.

Πρόταση 5.12. *Ας είναι* m, n *θετικοί ακέραιοι με* μκδ(m,n) = 1. *Τότε ισχύει:*

$$\varphi(mn) = \varphi(m)\varphi(n)$$

Απόδειξη. Θεωρούμε την συνάρτηση

$$f : \mathbb{Z}_{mn}^* \longrightarrow \mathbb{Z}_m^* \times \mathbb{Z}_n^* : a \mapsto (a \bmod m, a \bmod n)$$

Αν $f(a) = f(b)$, τότε $a \bmod m = b \bmod m$ και $a \bmod n = b \bmod n$, απ' όπου έπεται $m \mid a–b$ και $n \mid a–b$. Κατόπιν, το Πόρισμα 5.4 δίνει $mn \mid a–b$. Καθώς $a,b \in \mathbb{Z}_{mn}^*$, έχουμε $|a–b| < mn$ και επομένως η σχέση $mn \mid a–b$ δίνει $a = b$. Συνεπώς, η συνάρτηση f είναι ένεση. Ας είναι $(a, b) \in \mathbb{Z}_m^* \times \mathbb{Z}_n^*$. Καθώς ισχύει μκδ(m, n) = 1, υπάρχουν ακέραιοι u, v με $mu+nv = 1$. Άρα, έχουμε $mu \bmod n = 1$ και $nv \bmod m = 1$. Έτσι, για $c = (bmu+anv) \bmod mn$, ισχύει:

$$f(c) = (c \bmod m, c \bmod n) = (a,b)$$

Άρα, η συνάρτηση f είναι και έφεση. Συνεπώς, η f είναι αμφίεση και επομένως παίρνουμε $|\mathbb{Z}_{mn}^*| = |\mathbb{Z}_m^*||\mathbb{Z}_n^*|$, απ' όπου έπεται $\varphi(mn) = \varphi(m)\varphi(n)$.

Πόρισμα 5.8. *Ας είναι* n *ακέραιος* > 1 *και* $n = p_1^{e(1)} \cdots p_k^{e(k)}$ *η πρωτογενής ανάλυσή του. Τότε, ισχύει:*

$$\varphi(n) = n(1–1/p_1)\cdots(1–1/p_k)$$

Απόδειξη. Καθώς μκδ$(p_1^{e(1)} \cdots p_i^{e(i)}, p_{i+1}^{e(i+1)}) = 1$ (i = 1,…,k–1), από την Πρόταση 5.12 έχουμε:

$$\varphi(n) = \varphi(p_1^{e(1)} \cdots p^{e(k-1)})\varphi(p_k^{e(k)}) = \cdots = \varphi(p_1^{e(1)}) \cdots \varphi(p_k^{e(k)})$$

Θα υπολογίσουμε την τιμή $\varphi(p_i^{e(i)})$. Για έναν ακέραιο $a > 1$, ισχύει μκδ$(a,p_i^{e(i)}) = 1$ αν και μόνον αν $p_i \nmid a$. Οι θετικοί ακέραιοι $\leq p_i^{e(i)}$ οι οποίοι διαιρούνται από τον p_i είναι: $p_i, 2p_i, \ldots, p_i^{e(i)-1} p_i$. Το πλήθος αυτών των ακεραίων είναι $p_i^{e(i)-1}$ και επομένως έχουμε $\varphi(p_i^{e(i)}) = p_i^{e(i)} – p_i^{e(i)-1}$. Τότε:

$$\varphi(n) = (p_1^{e(1)} – p_1^{e(1)-1}) \cdots (p_k^{e(k)} – p_k^{e(k)-1}) = n(1–1/p_1)\cdots(1–1/p_k)$$

Παράδειγμα 5.13. Ας είναι $n = 100793$. Θα υπολογίσουμε την τιμή φ(n). Πρώτα υπολογίζουμε την πρωτογενή ανάλυση του n: $n = 7^2 \cdot 11^2 \cdot 17$. Κατόπιν εφαρμόζουμε το Πόρισμα 5.8 και παίρνουμε:

$$\varphi(n) = 100793\ (1–1/7)(1–1/11)(1–1/17) = 73920$$

Θεώρημα 5.4. *(Fermat-Euler) Ας είναι* $a \in \mathbb{Z}_n^*$. *Τότε ισχύει:* $a^{\varphi(n)} \bmod n = 1$.

Απόδειξη. Ας είναι $\mathbb{Z}_n^* = \{x_1, \ldots, x_{\varphi(n)}\}$. Αν $a \odot x_i = a \odot x_j$ με $i \neq j$, τότε πολλαπλασιάζοντας από αριστερά την ισότητα με $a^{-1} \bmod n$, παίρνουμε $x_i = x_j$ που είναι άτοπο. Άρα, οι ακέραιοι $r_i = a \odot x_i$ (i = 1,…,φ(n)) είναι

διαφορετικοί ανά δύο. Επιπλέον, η Πρόταση 5.11 μας δίνει ότι οι ακέραιοι r_i ($i = 1,\ldots,\varphi(n)$) είναι στοιχεία του $\mathbb{Z}_n^*$. Συνεπώς, έχουμε:

$$\{x_1,\ldots,x_{\varphi(n)}\} = \mathbb{Z}_n^* = \{r_1,\ldots,r_{\varphi(n)}\}$$

Έτσι, παίρνουμε:

$$x_1 \odot \cdots \odot x_{\varphi(n)} = a^{\odot\varphi(n)} \odot x_1 \odot \cdots \odot x_{\varphi(n)}$$

Πολλαπλασιάζοντας διαδοχικά αυτή την ισότητα με $x_i^{-1} \bmod n$ ($i = 1,\ldots,\varphi(n)$) προκύπτει $a^{\odot\varphi(n)} = 1$ και κατά συνέπεια έχουμε $a^{\varphi(n)} \bmod n = 1$.

Πόρισμα 5.9. *(Fermat) Ας είναι* p πρώτος και $a \in \mathbb{Z}_p^*$. *Τότε ισχύει:*

$$a^{p-1} \bmod p = 1$$

Πόρισμα 5.10. *Ας είναι* p πρώτος και $a \in \mathbb{Z}_p$. *Τότε ισχύει:*

$$a^p \bmod p = a$$

Παράδειγμα 5.14. Θα δείξουμε ότι για κάθε ακέραιο n ισχύει $246 \mid n^{41}-n$. Καθώς $246 = 6\cdot 41$ και μκδ(6,41) = 1, από το Πόρισμα 5.4 έπεται ότι αρκεί να δείξουμε ότι $6 \mid n^{41}-n$ και $41 \mid n^{41}-n$. Αν n = 0, αυτό ισχύει. Ας υποθέσουμε ότι $n \neq 0$. Έχουμε:

$$n^{41}-n = n(n^{40}-1) = n(n^2-1)((n^2)^{19}+\cdots+n^2+1) = n(n-1)(n+1)((n^2)^{19}+\cdots+1)$$

Ο ακέραιος n(n–1)(n+1) είναι γινόμενο τριών διαδοχικών ακεραίων. Έτσι, σύμφωνα με το Παράδειγμα 5.1, διαιρείται από τους 2 και 3. Από το Πόρισμα 5.4 έχουμε $6 \mid n(n-1)(n+1)$ και επομένως $6 \mid n^{41}-n$. Ας είναι $r = n \bmod 41$. Τότε $n = 41q+r$ και από το Πόρισμα 4.9 έχουμε $41 \mid r^{41}-r$, απ' όπου έπεται $41 \mid (n-41q)^{41}-(n-41q)$. Συνεπώς $41 \mid n^{41}-n$.

Ας σημειωθεί ότι υπάρχουν περιπτώσεις όπου $a \in \mathbb{Z}_n^*$ και k θετικός ακέραιος $< \varphi(n)$ με $a^k \bmod n = 1$. Π.χ. ισχύει $3^4 \bmod 20 = 1$ και $\varphi(20) = 8$. Ο μικρότερος θετικός ακέραιος r για τον οποίο ισχύει $a^r \bmod n = 1$ καλείται *τάξη* του a mod n και συμβολίζεται με $\mathrm{ord}_n(a)$. Αν $\mathrm{ord}_n(a) = \varphi(n)$, τότε ο ακέραιος a καλείται *αρχική ρίζα κατά μέτρο* n. Αποδεικνύεται ότι μόνον αν $n = 2, 4, p^m, 2p^m$, όπου p πρώτος και m θετικός ακέραιος, υπάρχουν αρχικές ρίζες κατά μέτρο n (βλ. Πουλάκης, 1997).

Πρόταση 5.13. *Ας είναι* $a \in \mathbb{Z}_n^*$ *με* $\mathrm{ord}_n(a) = r$. *Τότε ισχύει:*

$$a^k \bmod n = a^l \bmod n \Leftrightarrow r \mid k-l$$

Απόδειξη. Μπορούμε να υποθέσουμε ότι $k \geq l$. Τότε, υπάρχουν ακέραιοι r, s με $k-l = qr+s$ και $0 \leq s < r$. Έχουμε:

$$a^k \bmod n = a^l \bmod n \Leftrightarrow a^{k-l} \bmod n = 1 \Leftrightarrow a^{qr+s} \bmod n = 1$$

Καθώς $a^q \bmod n = 1$, η τελευταία ισότητα είναι ισοδύναμη με την $a^s \bmod n = 1$. Από την ανισότητα $0 \le s < r$ έπεται ότι η προηγουμένη ισοτιμία ισχύει αν και μόνον αν $s = 0$ το οποίο ισοδυναμεί με $r \mid k$–l.

Πόρισμα 5.10. *Ας είναι* n *ακέραιος* > 1 *και* $a \in \mathbb{Z}_n^*$. *Αν* $r = \mathrm{ord}_n(a)$, *τότε* οι *ακέραιοι* 1, a, $a^2 \bmod n$,…, $a^{r-1} \bmod n$ *είναι διαφορετικοί. Ειδικότερα, αν* a *είναι αρχική ρίζα κατά μέτρο* n, *τότε*

$$\mathbb{Z}_n^* = \{1, a, a^2 \bmod n, \ldots, a^{r-1} \bmod n\}$$

Πόρισμα 5.11. *Ας είναι* n *ακέραιος* > 1 *και* $a \in \mathbb{Z}_n^*$. *Αν* $r = \mathrm{ord}_n(a)$, *τότε:* $a^k \bmod n = 1 \Leftrightarrow r \mid k$.

Πόρισμα 5.12. *Ας είναι* n *ακέραιος* > 1 *και* $a \in \mathbb{Z}_n^*$. *Αν* $r = \mathrm{ord}_n(a)$, *τότε* $r \mid \varphi(n)$.

Παράδειγμα 5.15. Θα υπολογίσουμε την ποσότητα $r = \mathrm{ord}_{31}(2)$. Από το Πόρισμα 5.12 έχουμε $r \mid \varphi(31)$. Καθώς ο 31 είναι πρώτος, έχουμε $\varphi(31) = 30$ και επομένως $r \mid 30$, απ' όπου $r \in \{1,2,3,5,6,10,15,30\}$. Υπολογίζουμε: $2^2 = 4$, $2^3 = 8$, $2^5 \bmod 31 = 1$. Επομένως, ισχύει $r = 5$.

Ας είναι $a \in \mathbb{Z}_n^*$. Θεωρούμε το σύνολο

$$\langle a \rangle = \{1, a, a^2 \bmod n, \ldots, a^{r-1} \bmod n\}, \text{ όπου } r = \mathrm{ord}_n(a)$$

Αν $b \in \langle a \rangle$, τότε υπάρχει $k \in \{0,\ldots,r-1\}$, ώστε να ισχύει $b = a^k \bmod n$. Ο ακέραιος k καλείται *διακριτός λογάριθμος* του b ως προς βάση a κατά μέτρο n. Τότε, γράφουμε: $k = \log_a b$.

Παράδειγμα 5.16. Θα δείξουμε πρώτα ότι ο ακέραιος 3 είναι μία αρχική ρίζα κατά μέτρο 17. Σύμφωνα με το Πόρισμα 5.11 έχουμε $\mathrm{ord}_{17}3 \mid \varphi(17)$. Καθώς $\varphi(17) = 16$, έπεται ότι $\mathrm{ord}_{17}3 \in \{1,2,4,8,16\}$. Υπολογίζουμε:

$$3^2 = 9, \quad 3^4 \bmod 17 = 13, \quad 38 \bmod 17 = 16$$

Άρα, ισχύει $\mathrm{ord}_{17}3 = 16$ και επομένως ο 3 είναι μία αρχική ρίζα κατά μέτρο 17. Έτσι, προκύπτει $\mathbb{Z}_{17}^* = \langle 3 \rangle$. Θα υπολογίσουμε τους διακριτούς λογαρίθμους ως προς βάση 3 όλων των στοιχείων του $\mathbb{Z}_{17}^*$. Έχουμε:

$$3^1 = 3, \quad 3^2 = 9, \quad 3^3 \bmod 17 = 10, \quad 3^4 \bmod 17 = 13, \quad 3^5 \bmod 17 = 5$$

$$3^6 \bmod 17 = 15, \quad 3^7 \bmod 17 = 11, \quad 3^8 \bmod 17 = 16, \quad 3^9 \bmod 17 = 14$$

$$3^{10} \bmod 17 = 8, \quad 3^{11} \bmod 17 = 7, \quad 3^{12} \bmod 17 = 4, \quad 3^{13} \bmod 17 = 12$$

$$3^{14} \bmod 17 = 2, \quad 3^{15} \bmod 17 = 6$$

Έτσι, παίρνουμε:

$$\log_3 1 = 0, \quad \log_3 2 = 14, \quad \log_3 3 = 1, \quad \log_3 4 = 12, \quad \log_3 5 = 5,$$

$$\log_3 6 = 15,\ \log_3 7 = 11,\ \log_3 8 = 10,\ \log_3 9 = 2,\ \log_3 10 = 3,$$
$$\log_3 11 = 7,\ \log_3 12 = 13,\ \log_3 13 = 4,\ \log_3 14 = 9,\ \log_3 15 = 6,\ \log_3 16 = 8$$

Το παρακάτω πρόβλημα συνδέεται πολύ στενά με την κρυπτογραφία:

Πρόβλημα του διακριτού λογαρίθμου. Δίνονται οι ακέραιοι $n > 1$, $a \in \mathbb{Z}_n^*$ και $b \in \langle a \rangle$. Να υπολογιστεί ο διακριτός λογάριθμος του b ως προς βάση a, $\log_a b$.

Καθώς δεν έχει βρεθεί μέχρι σήμερα ταχύς πρακτικός αλγόριθμος για την επίλυσή αυτού του προβλήματος, η ασφάλεια πολλών κρυπτοσυστημάτων βασίζεται σε αυτό. Ο μόνος αλγόριθμος ο οποίος μπορεί να το επιλύσει αποτελεσματικά είναι ο αλγόριθμος του P. Shor ο οποίος προτάθηκε το 1994 (Shor, 1994), αλλά καθώς επισημάναμε προηγουμένως η υλοποίησή του απαιτεί κβαντικό υπολογιστή με πολύ μεγαλύτερες δυνατότητες από αυτές οι οποίες υπάρχουν σήμερα.

Εφαρμογή. *Το εκθετικό κρυπτοσύστημα.*

Το κρυπτοσύστημα αυτό προτάθηκε το 1978, από τους Pohlig και Hellman [Pohlig, S.C., and Hellman, M. 1978]. Ο χώρος των απλών και κρυπτογραφημένων κειμένων αυτού του σχήματος είναι το σύνολο $\mathbb{Z}_p$, όπου p είναι πρώτος και ο χώρος των κλειδιών το $\mathbb{Z}_{p-1}^*$. Για κάθε κλειδί $k \in \mathbb{Z}_{p-1}^*$ υπάρχει κλειδί $l \in \mathbb{Z}_{p-1}^*$ με $kl \bmod (p-1) = 1$. Η συνάρτηση κρυπτογράφησης η οποία ορίζεται από το k είναι η συνάρτηση

$$E_k: \mathbb{Z}_p \to \mathbb{Z}_p,\ x \mapsto x^k \bmod p$$

και η αντίστοιχη συνάρτηση αποκρυπτογράφησης είναι η συνάρτηση

$$D_l: \mathbb{Z}_p \to \mathbb{Z}_p,\ x \mapsto x^l \bmod p$$

Καθώς $kl \bmod (p-1) = 1$, ισχύει $kl - 1 = a(p-1)$, όπου a θετικός ακέραιος. Οπότε, σύμφωνα με το Πόρισμα 5.9, για κάθε $x \in \mathbb{Z}_p^*$, έχουμε:

$$x^{\odot kl} = x^{kl} \bmod p = x^{1+a(p-1)} \bmod p = x \odot x^{a(p-1)} \bmod p = x$$

Άρα, για κάθε $x \in \mathbb{Z}_p$ ισχύει:

$$D_l(E_k(x)) = D_l(x^{\odot k}) = x^{\odot kl} = x$$

Συνεπώς, όλα τα παραπάνω συνθέτουν ένα σχήμα κρυπτογράφησης.

Για να κρυπτογραφήσουμε ένα μήνυμα $\mathcal{M}$ γραμμένο στην αγγλική γλώσσα, αντιστοιχούμε τα γράμματα A, B, C,... στα ζεύγη αριθμών 01, 02, …, 09, 10, …, 26, το κενό διαστήματος στο 00, και μετά χωρίζουμε την ακολουθία των αριθμών $\mathcal{A}$, η οποία προκύπτει μετά από αυτή την αντιστοίχιση, σε τμήματα $A_1, \ldots, A_n$, με $0 < A_i < p$, τα οποία αποτελούνται από το ίδιο πλήθος αριθμών

το οποίο είναι συνήθως όσο το δυνατόν μεγαλύτερο. Στη συνέχεια κρυπτογραφούμε κάθε αριθμό A_i και παίρνουμε τον αριθμό $C_i = E_k(A_i)$. Το κρυπτογραφημένο κείμενο είναι το $\mathcal{C} = C_1 \ldots C_n$. Βέβαια, με ανάλογο τρόπο αντιστοιχούμε οποιοδήποτε αλφάβητο σε αριθμούς και χρησιμοποιούμε το κρυπτοσύστημα.

Παράδειγμα 5.17. Θεωρούμε το εκθετικό κρυπτοσύστημα το οποίο ορίζεται από τον πρώτο αριθμό $p = 5237$ για να κρυπτογραφήσουμε το μήνυμα:

THERE ARE TREES

Έχουμε $p-1 = 5236 = 2^2 \cdot 7 \cdot 11 \cdot 17$. Έτσι, επιλέγουμε ως κλειδί κρυπτογράφησης τον ακέραιο $k = 67$ με μκδ(5236,67) = 1. Κατόπιν, μετατρέπουμε τα γράμματα του μηνύματος σε αντίστοιχα ζεύγη αριθμών και παίρνουμε την εξής ακολουθία ζευγών:

20 08 05 18 05 00 01 18 05 00 20 18 05 05 19

Ενώνουμε τα ζεύγη ώστε να προκύψουν ακέραιοι οι οποίοι να είναι στοιχεία του $\mathbb{Z}_p$. Στην προκειμένη περίπτωση μπορούμε να ενώνουμε μόνο δύο ζεύγη κάθε φορά. Έτσι, προκύπτουν οι εξής τετραψήφιοι ακέραιοι:

2008 0518 0500 0118 0500 2018 0505 1900

(Στο τέλος έχουμε προσθέσει το ζεύγος 00, ώστε όλοι οι ακέραιοι να είναι τετραψήφιοι). Κρυπτογραφούμε αυτούς τους αριθμούς και παίρνουμε:

$$E67(2008) = 200867 \bmod 5237 = 2542$$

$$E67\ (0518) = 51867 \bmod 5237 = 1230$$

$$E67\ (0500) = 50067 \bmod 5237 = 0045$$

$$E67\ (0118) = 11867 \bmod 5237 = 2742$$

$$E67\ (0500) = 50067 \bmod 5237 = 0045$$

$$E67\ (2018) = 201867 \bmod 5237 = 4864$$

$$E67\ (0505) = 50567 \bmod 5237 = 4213$$

$$E67\ (1900) = 190067 \bmod 5237 = 3209$$

Επομένως, η κρυπτογράφηση του μηνύματος είναι η ακολουθία τετράδων:

2542 1230 0045 2742 0045 4864 4213 3209

Χρησιμοποιώντας τον Ευκλείδειο αλγόριθμο υπολογίζουμε:

$$67^{-1} \bmod 5237 = 469$$

Η συνάρτηση αποκρυπτογράφησης D_{469} εφαρμόζεται στην παραπάνω ακολουθία τετράδων και δίνει την ακολουθία τετράδων η οποία κρυπτογραφήθηκε, απ' όπου προκύπτει το μήνυμα.

6. ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΑ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ

Όπως αναφέραμε στην Ενότητα 2, ένα βασικό πρόβλημα των συμμετρικών κρυπτοσυστημάτων είναι η ασφαλής διανομή κλειδιού για συμμετρικά κρυπτοσυστήματα. Το 1976 οι Diffie και Hellman δημοσιεύουν ένα πρωτόκολλο κατασκευής κοινού κλειδιών μεταξύ δύο οντοτήτων το οποίο αποτελεί μία λύση σε αυτό το πρόβλημα και σηματοδοτεί την δημιουργία της Κρυπτογραφίας Δημοσίου Κλειδιού (Diffie & Hellman, 1976]. Η ασφάλεια αυτού του σχήματος βασίζεται στη δυσκολία επίλυσης του προβλήματος του διακριτού λογαρίθμου. Κατόπιν, το 1978, οι Rivest, Shamir και Adleman δημοσιεύουν το πρώτο κρυπτοσύστημα δημοσίου κλειδιού, το γνωστό RSA (ονομασία η οποία δόθηκε από τα αρχικά των ονομάτων τους), το οποίο χρησιμοποιείται μέχρι σήμερα και η ασφάλειά του βασίζεται στη δυσκολία παραγοντοποίησης μεγάλων ακεραίων (Rivest κ.ά., 1978).

Αξίζει να σημειωθεί, ότι το 1970, ο J. H. Ellis, μέλος της Βρετανικής κρατικής υπηρεσίας Government Communications Headquarters, ανέπτυξε την ιδέα της κρυπτογραφίας του δημοσίου κλειδιού, χωρίς όμως να μπορέσει να την υλοποίηση (Ellis, 1970). Το 1973, ο C. Cocks προσελήφθη σ' αυτή την υπηρεσία και λαμβάνοντας γνώση αυτής της εργασίας κατασκεύασε το πρώτο κρυπτοσύστημα δημοσίου κλειδιού (Cocks, 1973). Η ασφάλεια αυτού του σχήματος βασίζεται στη δυσκολία παραγοντοποίησης μεγάλων ακεραίων. Το κρυπτοσύστημα αυτό δημοσιοποιήθηκε το 1997, καθώς η ύπαρξή του κρατήθηκε μυστική από την παραπάνω υπηρεσία. Επίσης, το 1974, ο M. J. Williamson, μέλος της ίδιας υπηρεσίας, κατασκεύασε το ίδιο πρωτόκολλο δημιουργίας κοινού κλειδιού με αυτό των Diffie και Hellman. Η δημοσιοποίηση της εργασίας του Williamson επιτράπηκε το 1997.

Από την δημοσίευση του κρυπτοσυστήματος RSA έως σήμερα έχει προταθεί μεγάλο πλήθος κρυπτοσυστημάτων δημοσίου κλειδιού. Ας σημειωθεί και το κρυπτοσύστημα του ElGamal το οποίο προτάθηκε το 1985 και αποτέλεσε πρότυπο για την ανάπτυξη και άλλων σχημάτων κρυπτογράφησης (ElGamal, 1985). Η ασφάλεια αυτού του σχήματος κρυπτογράφησης βασίζεται επίσης στο πρόβλημα του διακριτού λογαρίθμου.

Σε αυτή την ενότητα θα περιγράψουμε το πρωτόκολλο των Diffie και Hellman, το κρυπτοσύστημα RSA, καθώς και το κρυπτοσύστημα του

ElGamal. Στα τρία αυτά σχήματα, όπως και στο Εκθετικό Κρυπτοσύστημα, το οποίο περιγράψαμε παραπάνω, απαιτείται ο υπολογισμών ποσοτήτων της μορφής $a^k \bmod n$. Θα δείξουμε μία ταχεία μέθοδος υπολογισμού τέτοιων ποσοτήτων στην επόμενη παράγραφο.

6.1 Ταχύς υπολογισμός δύναμης μέσα στο $\mathbb{Z}_n$

Ας είναι g ακέραιος > 1. Θα δείξουμε πρώτα ότι για κάθε ακέραιο $x \geq 0$ υπάρχουν ακέραιοι $a_1,\ldots,a_k \in \{0,1,\ldots,g-1\}$ τέτοιοι, ώστε να ισχύει:

$$x = a_{k-1}g^{k-1}+\cdots+a_1g+a_0$$

Για να το δείξουμε εργαζόμαστε ως εξής:

1. Βρίσκουμε θετικό ακέραιο k τέτοιον, ώστε να έχουμε:
$$g^{k-1} \leq x < g^k$$
2. Διαιρούμε τον x με g^{k-1} και έχουμε $x = a_{k-1}g^{k-1}+x_{k-1}$, όπου
$$0 \leq x_{k-1} < g^{k-1}$$
3. Διαιρούμε τον x_{k-1} με g^{k-2} και έχουμε $x_{k-1} = a_{k-2}g^{k-2}+x_{k-2}$, όπου
$$0 \leq x_{k-2} < g^{k-2}$$
4. Διαιρούμε τον x_2 με τον g^{k-3} και συνεχίζουμε όπως προηγουμένως.
5. Στο (k–1)-οστή διαίρεση παίρνουμε $x_2 = a_1g+x_1$, όπου $0 \leq x_1 < g$.

Επομένως, θέτοντας $a_0 = x_1$, έχουμε

$$x = a_{k-1}g^{k-1}+\cdots+a_1g+a_0, \text{ με } a_0,\ldots,a_{\kappa-1} \in \{0,1,\ldots,g-1\}$$

Η γραφή αυτή του x καλείται *παράσταση του* x *στην κλίμακα του* g ή g-*αδική παράσταση* του x και συμβολίζεται συνήθως με $x = (a_1\ldots a_k)_g$. Ο ακέραιος g καλείται *βάση* της κλίμακας και οι $a_1,\ldots,a_k$ g-*αδικά ψηφία* του x. Αν είναι σαφές ποια βάση χρησιμοποιείται, τότε συμβολίζουμε πιο απλά με $a_1\ldots a_k$ την g-αδική παράσταση του a. Η συνηθισμένη γραφή των ακεραίων χρησιμοποιεί την παράστασή τους στην κλίμακα του 10. Π.χ. $512 = 5\cdot10^2+1\cdot10+2$. Ας σημειωθεί ότι η παράσταση των ακεραίων στις κλίμακες g = 2, 8, 16 χρησιμοποιείται στους ηλεκτρονικούς υπολογιστές για αναπαράσταση δεδομένων. Αν g > 10, τότε συνήθως χρησιμοποιούνται γράμματα για να αναπαραστήσουν τα ψηφία τα οποία είναι > 9. Για παράδειγμα, στην 16-αδική παράσταση των ακεραίων αντί των ψηφίων 10, 11, 12, 13, 14, 15 χρησιμοποιούνται τα γράμματα A, B, C, D, E, F. Έτσι, D2F είναι η 16-αδική παράσταση του $3375 = 13\cdot16^2+2\cdot16+15$.

Καλούμε *μήκος* ενός φυσικού αριθμού a το πλήθος των ψηφίων στη δυαδική γραφή του και το συμβολίζουμε με $\ell(a)$.

Παράδειγμα 6.1. Θα υπολογίσουμε την δυαδική γραφή του 323. Πρώτα βρίσκουμε:

$$256 = 2^8 < 323 < 2^9 = 512$$

Κατόπιν διαιρούμε τον 323 με 256 και έχουμε:

$$323 = 256+67$$

Ο αριθμός 67 διαιρούμενος από τον $2^7 = 256$ δίνει ως πηλίκο το 0 και υπόλοιπο τον ίδιο. Στη συνέχεια διαιρούμε τον 67 με τον $2^6 = 64$ και έχουμε:

$$67 = 64+3$$

Συνεπώς, η δυαδική παράσταση του 323 είναι:

$$323 = 2^8+2^6+2+1$$

Άρα, ισχύει $323 = (101000011)_2$ και επομένως $\ell(323) = 9$.

Σε πολλά κρυπτοσυστήματα δημοσίου κλειδιού τα οποία χρησιμοποιούν το σύνολο $\mathbb{Z}_n$ απαιτείται ο υπολογισμός δυνάμεων στοιχείων του $\mathbb{Z}_n$. Για παράδειγμα, σήμερα το RSA, το οποίο θα περιγράψουμε παρακάτω, χρησιμοποιεί ακεραίους n με $2^{2047} < n < 2^{2048}$, και για τις λειτουργίες κρυπτογράφησης και αποκρυπτογράφησης απαιτεί τον υπολογισμό δυνάμεων $a^k \bmod n$, με k αρκετά μεγάλο (συχνά $k > n/10$). Έτσι, αν $k = 2^{2010}$ και θελήσουμε να κάνουμε τον υπολογισμό πολλαπλασιάζοντας το a με τον εαυτό του (μέσα στο $\mathbb{Z}_n$), κατόπιν το αποτέλεσμα $a \odot a$ πάλι με τον a κ.ο.κ., τότε θα χρειαστεί να εκτελέσουμε 2^{2010} πολλαπλασιασμούς μέσα στο $\mathbb{Z}_n$ πράγμα το οποίο είναι εξαιρετικά χρονοβόρο και καθιστά το σύστημα αναποτελεσματικό. Στη συνέχεια θα δείξουμε μία μέθοδος γρήγορου υπολογισμού τέτοιων ποσοτήτων η οποία χρησιμοποιεί την δυαδική παράσταση ενός ακεραίου.

Ας είναι $a \in \mathbb{Z}_n$ και k ακέραιος > 0. Για να υπολογίσουμε την ποσότητα $a^k \bmod n$ κάνουμε τα εξής:

1. Υπολογίζουμε την δυαδική παράσταση του k: $k = k_m 2^m + \cdots + k_0$.
2. Θέτουμε $A_0 = a$, $P_0 = a^{k_0}$ και για $i = 1,\ldots,m$ υπολογίζουμε:
$$A_i = A_{i-1} \odot 2, \quad P_i = \mathbf{A_i}^{\mathbf{k_i}} \odot P_{i-1}$$
3. Έχουμε $P_m = a^k \bmod n$.

Πράγματι, ισχύει:

$$P_m = A_m^{k_m} \odot P_{m-1} = A_m^{k_m} \odot A_{m-1}^{k_m-1} \odot P_{m-2} = \ldots =$$

$$A_m^{k_m} \odot A_{m-1}^{k_m-1} \odot \ldots \odot A_0^{k_0} = a^{k_m 2^m + k_{m-1} 2^{m-1} + \cdots + k_0} = a^k \bmod n$$

Η μέθοδος αυτή απαιτεί το πολύ $2\ell(k)$ πολλαπλασιασμούς μέσα στο $\mathbb{Z}_n$. Έτσι, αν ο ακέραιος k είναι πολύ μεγάλος, τότε μπορούμε να υπολογίσουμε γρήγορα την ποσότητα $a^k \bmod n$. Π.χ. αν $k = 2^{2010}$, τότε απαιτούνται το πολύ 4020 πολλαπλασιασμοί μέσα στο $\mathbb{Z}_n$ και όχι 2^{2010} όπως με την κλασική μέθοδο.

Παράδειγμα 6.2. Θα υπολογίσουμε τον ακέραιο $11^{71} \bmod 53$. Η δυαδική γραφή του 167 είναι: $71 = 2^6+2^2+2+1$. Έτσι, έχουμε:

$$k_0 = k_1 = k_2 = 1,\ k_3 = k_4 = k_5 = 0,\ k_6 = 1$$

Θέτουμε $A_0 = 11$, $P_0 = 11$ και υπολογίζουμε:

$$A_1 = A_0^2 \bmod 53 = 15, \quad P_1 = A_1^{k_1} P_0 \bmod 53 = 6$$

$$A_2 = A_1^2 \bmod 53 = 13, \quad P_2 = A_2^{k_2} P_1 \bmod 53 = 25$$

$$A_3 = A_2^2 \bmod 53 = 10, \quad P_3 = A_3^{k_3} P_2 \bmod 53 = 25$$

$$A_4 = A_3^2 \bmod 53 = 47, \quad P_4 = A_4^{k_4} P_3 \bmod 53 = 25$$

$$A_5 = A_4^2 \bmod 53 = 36, \quad P_5 = A_5^{k_5} P_3 \bmod 53 = 25$$

$$A_6 = A_5^2 \bmod 53 = 24, \quad P_6 = A_6^{k_6} P_3 \bmod 53 = 17$$

Έτσι, παίρνουμε $11^{71} \bmod 53 = 17$.

6.2 Το πρωτόκολλο των Diffie-Hellman

Το πρωτόκολλο αυτό επιτρέπει σε δύο χρήστες, Α και Β, να κατασκευάσουν ένα κοινό κλειδί το οποίο θα χρησιμοποιήσουν για να επικοινωνήσουν δια μέσου ενός συμμετρικού κρυπτοσυστήματος. Για τον σκοπό αυτό, οι Α και Β επιλέγουν έναν ακέραιο $n > 1$ και έναν ακέραιο $g \in \mathbb{Z}_n^*$. Θέτουμε $r = \mathrm{ord}_n(g)$. Στη συνέχεια, οι Α και Β κάνουν τα εξής:

1. Ο Α επιλέγει $z \in \{1,\ldots,r-1\}$ και υπολογίζει $a = g^z \bmod n$.
2. Ο Α κρατά μυστικό τον z και στέλνει τον a στον Β.
3. Ο Β επιλέγει $w \in \{1,\ldots,r-1\}$ και υπολογίζει $b = g^w \bmod n$.
4. Ο Β κρατά μυστικό τον w και στέλνει τον b στον Α.
5. Ο Α υπολογίζει $b^z \bmod n$.
6. Ο Β υπολογίζει $a^w \bmod n$.

Με την παραπάνω διαδικασία, οι Α και Β υπολόγισαν ταυτόχρονα:

$$b^z \bmod n = g^{zw} \bmod n \quad \text{και} \quad a^w \bmod n = g^{zw} \bmod n$$

Συνεπώς, το κοινό κλειδί το οποίο κατασκευάστηκε με αυτή την διαδικασία είναι το $K = g^{zw} \bmod n$.

Η πιο συνηθισμένη εκδοχή του πρωτοκόλλου είναι η περίπτωση όπου ο n είναι πρώτος και ο g αρχική ρίζα κατά μέτρο n. Ας σημειωθεί ότι η ταχεία μέθοδος υπολογισμού της ποσότητας $g^x \bmod n$ καθιστά την εφαρμογή του πρωτοκόλλου πρακτικά εφικτή.

Ένας επιτιθέμενος στο σύστημα, ο οποίος έχει ως σκοπό την εύρεση του κοινού κλειδιού K, έχει την δυνατότητα να δεσμεύσει τις ποσότητες n, g, a, b και επομένως έχει να επιλύσει το εξής πρόβλημα:

Πρόβλημα των Diffie – Hellman. Δίνονται οι ακέραιοι $n > 1$, $g \in \mathbb{Z}_n$, $a = g^z \bmod n$ και $b = g^w \bmod n$ (χωρίς να είναι οι γνωστοί οι ακέραιοι z και w). Να υπολογιστεί η ποσότητα $K = g^{zw} \bmod n$.

Ο μόνος γνωστός τρόπος επίλυσής αυτού του προβλήματος είναι ο υπολογισμός του z (αντίστοιχα του w) και κατόπιν του $b^z \bmod n$ (αντίστοιχα, του $a^w \bmod n$). Έτσι, ο επιτιθέμενος οδηγείται στο πρόβλημα του διακριτού λογαρίθμου το οποίο είδαμε στη προηγούμενη ενότητα. Συνεπώς, οι ακέραιοι οι οποίοι θα χρησιμοποιηθούν θα πρέπει να είναι αρκετά μεγάλοι και τέτοιοι, ώστε τα στιγμιότυπα του προβλήματος του διακριτού λογάριθμου τα οποία θα δημιουργηθούν να είναι δισεπίλυτα.

Τέλος, ας σημειωθεί ότι το πρωτόκολλο των Diffie – Hellman είναι ευάλωτο στην επίθεση *συνάντηση στο ενδιάμεσο*, κατά την οποία ο επιτιθέμενος παρεμβαίνει στην επικοινωνία των Α και Β προφασιζόμενος στον Α (αντίστοιχα στον Β) ότι είναι ο Β (αντίστοιχα ο Α) και έτσι δημιουργεί, ακολουθώντας το πρωτόκολλο, ένα κοινό κλειδί με τον Α και ένα κοινό κλειδί με τον Β. Η επίθεση αυτή αποτυγχάνει αν η χρήση του πρωτοκόλλου συνδυαστεί με ένα πρωτόκολλο ταυτοποίησης ή με ψηφιακή υπογραφή.

Παράδειγμα 6.3. Ας υποθέσουμε ότι οι Α και Β επιθυμούν να κατασκευάσουν ένα κοινό κλειδί χρησιμοποιώντας το πρωτόκολλο των Diffie - Hellman. Επιλέγουν τον πρώτο $p = 109$ και τον ακέραιο $g = 2$. Έχουμε $\mathrm{ord}_{109}(2) = 108$ και επομένως ο ακέραιος 2 είναι αρχική ρίζα κατά μέτρο 109, απ' όπου έπεται $\mathbb{Z}_n^* = \langle a \rangle$. Οι Α και Β κάνουν τα εξής:

1. Ο Α επιλέγει $z = 35$ και υπολογίζει $a = g^z \bmod p = 2^{35} \bmod 109 = 55$.
2. Ο Α κρατά μυστικό τον z και στέλνει τον a στον Β.

3. Ο Β επιλέγει $w = 27$ και υπολογίζει $b = g^w \bmod p = 2^{27} \bmod 109 = 33$.
4. Ο Β κρατά μυστικό τον w και στέλνει τον b στον Α.
5. Ο Α υπολογίζει $b^z \bmod p = 33^{35} \bmod 109 = 76$.
6. Ο Β υπολογίζει $a^w \bmod p = 55^{27} \bmod 109 = 76$.

Άρα, το κοινό κλειδί το οποίο κατασκεύασαν οι Α και Β είναι το $K = 76$.

6.3 Το κρυπτοσύστημα RSA

Ας υποθέσουμε ότι ο Α επιθυμεί να κατασκευάσει ένα κρυπτοσύστημα RSA. Επιλέγει δύο πρώτους p, q και υπολογίζει $n = pq$ και $\varphi(n) = (p-1)(q-1)$. Ο χώρος των απλών κειμένων $\boldsymbol{\mathcal{P}}$, ο χώρος των κρυπτογραφημένων κειμένων $\boldsymbol{\mathcal{C}}$ είναι το σύνολο $\mathbb{Z}_n$ και ο χώρος κλειδιών το σύνολο $\boldsymbol{\mathcal{K}} = \mathbb{Z}_{\varphi(n)}^*$. Το σύνολο των συναρτήσεων κρυπτογράφησης $\boldsymbol{\mathcal{E}}$ αποτελείται από τις συναρτήσεις

$$E_k : \boldsymbol{\mathcal{P}} \longrightarrow \boldsymbol{\mathcal{C}},\ x \mapsto x^k \bmod n, \quad k \in \boldsymbol{\mathcal{K}}$$

Το σύνολο των συναρτήσεων αποκρυπτογράφησης $\boldsymbol{\mathcal{D}}$ συμπίπτει με το $\boldsymbol{\mathcal{E}}$. Ο Α επιλέγει $e \in \mathbb{Z}_{\varphi(n)}^*$ και υπολογίζει $d = e^{-1} \bmod \varphi(n)$. Θα δείξουμε ότι ισχύει

$$D_d(E_e(m)) = m, \quad \forall\ m \in \mathbb{Z}_n$$

ή ισοδύναμα,

$$m^{ed} \bmod n = m, \quad \forall\ m \in \mathbb{Z}_n$$

Καθώς $d = e^{-1} \bmod \varphi(n)$, έχουμε $ed \bmod \varphi(n) = 1$, και επομένως υπάρχει $k \in \mathbb{Z}$ με $ed = k(p-1)(q-1)+1$. Ας είναι $p \nmid m$. Τότε, το Πόρισμα 5.9 δίνει $m^{p-1} \bmod p = 1$. Συνδυάζοντας τα παραπάνω, παίρνουμε:

$$m^{ed} \bmod p = (m^{(p-1)(q-1)k} \bmod p)\ m \bmod p = m$$

Αν $p \mid m$, τότε $m^p \bmod p = 0 = m \bmod p$. Άρα, σε κάθε περίπτωση ισχύει $m^{ed} \bmod p = m$, ή ισοδύναμα $p \mid m^{ed}-m$. Ομοίως, ισχύει $q \mid m^{ed}-m$. Έτσι, από το Πόρισμα 5.4, παίρνουμε $n \mid m^{ed}-m$ και επομένως $m^{ed} \bmod n = m$.

Το ζεύγος (e,d) καλείται *δημόσιο κλειδί* του Α και δημοσιοποιείται. Το d καλείται *ιδιωτικό κλειδί* του Α και κρατείται μυστικό. Όποιος επιθυμεί να στείλει ένα μήνυμα m στον Α χρησιμοποιεί την συνάρτηση κρυπτογράφησης E_e και υπολογίζει την ποσότητα $E_e(m)$. Κατόπιν στέλνει στον Α το κρυπτογραφημένο μήνυμα $E_e(m)$ ο οποίος υπολογίζει $D_d(E_e(m)) = m$ και ανακτά το μήνυμα m. Ας σημειωθεί ότι η ταχεία μέθοδος υπολογισμού της ποσότητας $m^x \bmod n$ καθιστά την χρήση του κρυπτοσυστήματος πρακτικά εφικτή.

Παράδειγμα 6.4. Για την κατασκευή ενός κρυπτοσυστήματος RSA, ο Α επιλέγει τους πρώτους $p = 31$ και $q = 47$. Κατόπιν, ο Α υπολογίζει:

$$n = pq = 31\cdot 47 = 1457 \quad \text{και} \quad \varphi(n) = (p-1)(q-1) = 1380$$

Στη συνέχεια ο Α επιλέγει τον ακέραιο $e = 11$ και εφαρμόζει τον Ευκλείδειο αλγόριθμο για τον υπολογισμό του μκδ$(e,\varphi(n))$. Έχουμε:

$$1380 = 11\cdot 125+5$$

$$11 = 5\cdot 2+1$$

Άρα, ισχύει μκδ$(1380,11) = 1$ και επομένως $11 \in \mathbb{Z}_{1380}^*$. Για τον προσδιορισμό του $d = 11^{-1} \bmod 1380$, ο Α υπολογίζει:

$$1 = 11-5\cdot 2 = 11-2\,(1380-11\cdot 125) = -2\cdot 1380+251\cdot 11$$

Άρα, έχουμε $-2\cdot 1380+251\cdot 11 = 1$ και επομένως $d = 11^{-1} \bmod 1380 = 251$. Έτσι, το δημόσιο κλειδί του Α είναι το ζεύγος $(n,e) = (1457,11)$ και το ιδιωτικό ο ακέραιος $d = 251$.

Ο Β επιθυμεί να στείλει στον Α το μήνυμα $m = 67$ κρυπτογραφημένο με το δημόσιο κλειδί του. Ο Β υπολογίζει:

$$c = m^{11} \bmod n = 67^{11} \bmod 1457 = 1017$$

Κατόπιν, ο Β στέλνει τον c στον Α και αυτός ανακτά το m υπολογίζοντας

$$m = c^d \bmod n = 1017^{251} \bmod 1457 = 67$$

Αν οι πρώτοι παράγοντες p και q του n είναι γνωστοί, τότε είναι δυνατόν να υπολογιστεί η τιμή $\varphi(n) = (p-1)(q-1)$. Από την άλλη πλευρά ισχύει $n = pq$ και $p+q = n+1-\varphi(n)$. Έτσι, αν η τιμή $\varphi(n)$ είναι γνωστή, τότε οι πρώτοι p και q είναι λύσεις της εξίσωσης

$$T^2-(n+1-\varphi(n))T+n = 0$$

και επομένως προκύπτει

$$p,q = \frac{n+1-\varphi(n)\pm\sqrt{(n+1-\varphi(n))^2-4n}}{2}$$

Συνεπώς, ο υπολογισμός της τιμής $\varphi(n)$ είναι ισοδύναμος με τον προσδιορισμό των πρώτων p και q.

Έτσι, αν ένας επιτιθέμενος στο σύστημα γνωρίζει τους πρώτους παράγοντες p και q του n, τότε μπορεί να υπολογίσει την τιμή $\varphi(n)$ και κατόπιν να υπολογίσει, χρησιμοποιώντας την μέθοδο την οποία είδαμε στην Ενότητα 5.3, το ιδιωτικό κλειδί $d = e^{-1} \bmod \varphi(n)$. Αντιστρόφως, αν είναι γνωστό το

ιδιωτικό κλειδί d, τότε κάτω από ορισμένες υποθέσεις, είναι δυνατόν να υπολογιστούν οι πρώτοι p και q (May, 2004· Πουλάκης, 2004· Rivest κ.ά., 1978). Επομένως, η ασφάλεια του RSA βασίζεται πρωτίστως στη επιλογή των πρώτων p και q ώστε η παραγοντοποίηση του n να μην είναι πρακτικά εφικτή. Έτσι, οι πρώτοι p, q πρέπει να είναι αρκετά μεγάλοι (η συνηθισμένη επιλογή σήμερα είναι $2^{1023} < p, q < 2^{1024}$) και να μην έχουν κάποιες ιδιότητες οι οποίες θα επιτρέψουν τη γρήγορη παραγοντοποίηση του n με την χρήση των γνωστών αλγορίθμων παραγοντοποίησης (Πουλάκης, 2015).

Μέχρι σήμερα έχουν γίνει πολλές κρυπταναλυτικές επιθέσεις στο RSA οι οποίες όμως δεν έχουν περιορίσει την χρήση του. Αρκετές από αυτές περιλαμβάνονται στο σύγγραμμα του Yan (2008). Μερικές από αυτές τις επιθέσεις είναι δυνατόν να αποτραπούν, αν προστεθεί στο μήνυμα ένας αριθμός τυχαίων συμβόλων. Στην πράξη χρησιμοποιείται μία συγκεκριμένη μέθοδος επέκτασης απλού κειμένου, η οποία είναι γνωστή ως OAEP (Optimal Asymmetric Encryption Padding· Moriarty κ.ά., 2016).

6.4 Το κρυπτοσύστημα του El Gamal

Ας υποθέσουμε ότι ο Α επιθυμεί να κατασκευάσει ένα κρυπτοσύστημα του ElGamal. Επιλέγει ένα πρώτο $p > 2$, μία αρχική ρίζα g κατά μέτρο p και $x \in \{0,\ldots,p-2\}$. Κατόπιν, υπολογίζει $y = g^x \bmod p$. Το δημόσιο κλειδί του σχήματος είναι η τριάδα (p,g,y) και το ιδιωτικό κλειδί ο ακέραιος x.

Ένας άλλος χρήστης Β ο οποίος θέλει να στείλει στον Α το μήνυμα $m \in \mathbb{Z}_p$ κρυπτογραφημένο, επιλέγει τυχαία $z \in \{0,\ldots,p-2\}$ και υπολογίζει

$$b = g^z \bmod p \qquad \text{και} \qquad c = y^z m \bmod p$$

Ο Β στέλνει στον Α την κρυπτογράφηση του m η οποία είναι το ζεύγος (b,c). Ο Α υπολογίζει

$$b^{-x} c \bmod p = g^{-zx} y^z m \bmod p = m$$

και έτσι αποκρυπτογραφεί το μήνυμα. Παρατηρούμε ότι οποιοδήποτε z να έχει επιλεγεί για την κρυπτογράφηση, το αποτέλεσμα της αποκρυπτογράφησης θα είναι το m.

Η κρυπτογράφηση απαιτεί τον υπολογισμό των $g^z \bmod p$, $y^z \bmod p$ και $y^z m \bmod p$. Καθώς όμως οι ακέραιοι $g^z \bmod p$ και $yz \bmod p$ είναι ανεξάρτητοι του κειμένου m, είναι δυνατόν να έχουν υπολογιστεί προηγουμένως και επομένως η κρυπτογράφηση απαιτεί μόνον ένα πολλαπλασιασμό μέσα στο $\mathbb{Z}_p$, τον υπολογισμό του $y^z m \bmod p$ από τον $y^z \bmod p$ και τον m. Από την

άλλη πλευρά, η αποκρυπτογράφηση απαιτεί τον υπολογισμό ενός αντιστρόφου, μία ύψωση σε δύναμη και ένα πολλαπλασιασμό μέσα στο $\mathbb{Z}_p$.

Ένα μειονέκτημα του κρυπτοσυστήματος του ElGamal είναι ότι το κρυπτογραφημένο κείμενο είναι δύο φορές μεγαλύτερο από το απλό. Από την άλλη πλευρά, ένα βασικό πλεονέκτημα του είναι ότι το ίδιο απλό κείμενο κρυπτογραφημένο με την χρήση διαφορετικών z αντιστοιχεί σε διαφορετικά κρυπτογραφημένα κείμενα.

Παράδειγμα 6.5. Ας υποθέσουμε ότι ο Α επιλέγει τον πρώτο p = 521 και την αρχική ρίζα g = 3 κατά μέτρο 521. Επίσης, παίρνει x = 94 και υπολογίζει

$$y = 3^{94} \mod 521 = 234.$$

Οπότε, το δημόσιο κλειδί του Α είναι η τριάδα (521,3,234) και το ιδιωτικό του κλειδί ο ακέραιος 94.

Ο Β επιθυμεί να στείλει στον Α το μήνυμα m = 46. Επιλέγει τυχαία τον ακέραιο z = 315 και υπολογίζει:

$$g^z \mod p = 3^{315} \mod 521 = 386 \quad \text{και} \quad y^z m \mod p = \mod 521 = 34.$$

Κατόπιν στέλνει στον Α το ζεύγος (386,34). Για την αποκρυπτογράφηση του κρυπτοκειμένου (386, 34), ο Α υπολογίζει:

$$m = 42^{-94}\ 34 \mod 521 = 46$$

και έτσι προκύπτει το αντίστοιχο απλό κείμενο.

Αν ένας επιτιθέμενος στο σύστημα μπορέσει να υπολογίσει τον διακριτό λογάριθμο x του y ως προς βάση g, τότε είναι δυνατόν ν' αποκρυπτογραφεί κάθε κείμενο που έχει κρυπτογραφηθεί με την χρήση του ιδιωτικού κλειδιού x. Επιπλέον, αν ο επιτιθέμενος μπορέσει να υπολογίσει τον διακριτό λογάριθμο z του b ως προς βάση g, τότε μπορεί να υπολογίσει εύκολα την ποσότητα $y^z \mod p$ και κατόπιν το μήνυμα $m = c(y^z)^{-1} \mod p$. Συνεπώς, η ασφάλεια του σχήματος εξαρτάται από την σωστή επιλογή των παραμέτρων οι οποίες δεν θα επιτρέπουν τον πρακτικό υπολογισμό του διακριτού λογάριθμου με τις μέχρι σήμερα υπάρχουσες μεθόδους. Από την άλλη πλευρά, δεν είναι γνωστό αν η ύπαρξη ενός αποτελεσματικού αλγορίθμου για την αποκρυπτογράφηση του σχήματος του ElGamal δίνει έναν αποτελεσματικό αλγόριθμο για την επίλυση του προβλήματος του διακριτού λογάριθμου. Τέλος, ας σημειωθεί ότι η ύπαρξη ενός αλγόριθμου ο οποίος αποκρυπτογραφεί το κρυπτοσύστημα του ElGamal ισοδυναμεί με την λύση του προβλήματος των Diffie-Hellman (Πουλάκης, 2004).

Ας υποθέσουμε ότι δύο κείμενα m_1 και m_2 κρυπτογραφούνται με το ίδιο z και δίνουν τα ζεύγη (b,c_1), (b,c_2), αντίστοιχα. Τότε, έχουμε:

$$c_1 = y^z m_1 \bmod p \quad \text{και} \quad c_2 = y^z m_2 \bmod p$$

Συνδυάζοντας τις δύο ισότητες, παίρνουμε:

$$m_1 = (c_1 c_2^{-1})\, m_2 \bmod p$$

Οπότε, αν κάποιος γνωρίζει το m_2 μπορεί να βρει εύκολα το m_1 και αντιστρόφως. Συνεπώς, για κάθε κρυπτογράφηση είναι προτιμότερο να χρησιμοποιείται ένας νέος εκθέτης z.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Αλβανός Π., & Δ. Πουλάκης (2022). *Επανάληψη στη Θεωρία Αριθμών, Συνοπτική Θεωρία, Μεθοδολογία, Ασκήσεις*. Κάλλιπος, Ανοικτές Ακαδημαϊκές Εκδόσεις. https://repository.kallipos.gr/handle/11419/8008

Bellovin, S. M. (2011). Frank Miller: Inventor of the One-Time Pad. *Cryptologia, 35*(3), 203–222.

https://doi.org/10.1080/01611194.2011.583711

Bernstein, D.J., Buchmann, J., & Dahmen, E. (Eds) (2009). *Post – Quantum Cryptography*, Springer. https://doi.org/10.1007/978-3-540-88702-7

Cocks, C. C. (1973). A note on non-secret encryption. *CESG Memo*.

Daemen, J., & Rijmen, V. (2002). *The Design of Rijndael*, AES - The Advanced Encryption Standard. Springer.

Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. *IEEE Transactions on Information Theory, 22*(6), 644–654.

https://doi.org/10.1109/TIT.1976.1055638

ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE transactions on information theory, 31*(4), 469-472. https://doi.org/10.1109/TIT.1985.1057074

Ellis, J.H. (1970). *The Possibility of Secure Non-Secret Digital Encryption*, CESG Report.

Kerckhoffs, A. (1883α). La cryptographie militaire, *Journal des sciences militaires. IX*: 5–83.

Kerckhoffs, A. (1883β). La cryptographie militaire, *Journal des sciences militaires IX*: 161–191.

Koblitz, N. (1994). *A course in number theory and cryptography* (Vol. 114). Springer Science & Business Media.

May, A. (2004). *Computing the RSA Secret Key Is Deterministic Polynomial Time Equivalent to Factoring*. In: Franklin, M. (eds) Advances in Cryptology – CRYPTO 2004. (pp. 213–219). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-28628-8_13

Menezes, A., van Oorschot, P., & Vastone, S.A. (1997). *Handbook of Applied Cryptography*. CRC Press.

Moriarty, K. M., Kaliski, B., Jonsson, J., & Rusch, A. (2016). *PKCS #1: RSA cryptography specifications version 2.2* (RFC 8017). https://doi.org/10.17487/RFC8017

Musa, M. A., Schaefer, E. F., & Wedig, S. (2003). A Simplified AES Algorithm and its Linear and Differential Cryptanalysis. Cryptologia, 27(2), 148-177.

Πουλάκης, Δ. (1997). *Θεωρία Αριθμών*. Εκδόσεις Ζήτη.

Πουλάκης, Δ. (2004). *Κρυπτογραφία*. Εκδόσεις Ζήτη.

Πουλάκης, Δ. (2015). *Υπολογιστική Θεωρία Αριθμών*. Κάλλιπος, Ανοικτές Ακαδημαϊκές Εκδόσεις. https://repository.kallipos.gr/handle/11419/1045.

Pohlig, S., C., & Hellman, M. (1978). An Improved Algorithm for Computing Logarithms over GF(p) and its cryptographic significance. IEEE Transactions in Information Theory, 24, 106-110.

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM, 21*(2), 120–126. https://doi.org/10.1145/359340.359342

Schaefer, E. F. (1996). A simplified Data Encryption Standard algorithm. *Cryptologia, 20*(1), 77–84. https://doi.org/10.1080/0161-119691867768

Shannon, C. E. (1949). Communication theory of secrecy systems. *Bell System Technical Journal, 28*(4), 656–715. https://doi.org/10.1002/j.1538-7305.1949.tb00928.x

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium*

on Foundations of Computer Science (pp. 124–134). IEEE. https://doi.org/10.1109/SFCS.1994.365700

Sinkov, A. (2009). *Elementary cryptanalysis: A mathematical approach* (2nd ed.). The Mathematical Association of America

Yan, S. Y. (2008). *Cryptanalytic attacks on RSA*. Springer.

Φ.Ε.Κ. 8-3-2023, τεύχος 2ο, αρ. 1326, Πρόγραμμα Σπουδών του μαθήματος των Μαθηματικών των Α΄, Β΄ και Γ΄ τάξεων Γενικού Λυκείου.

ΠΑΡΑΡΤΗΜΑ Α

Παρακάτω παραθέτουμε μερικά συγγράμματα και ιστότοπους τα οποία θα βοηθήσουν το ενδιαφερόμενο αναγνωστικό κοινό να μελετήσει διεξοδικότερα τα θέματα που αναπτύχθηκαν στο κείμενο.

Burmester, M., Γκρίτζαλης, Σ., Κάτσικας, Σ., & Χρυσικόπουλος, Β. (2011). *Σύγχρονη κρυπτογραφία: Θεωρία και εφαρμογές*. Εκδόσεις Παπασωτηρίου.

Cozzens, M., & Miller, S**.** (2013). *The mathematics of encryption: An elementary introduction* (Mathematical World, Vol. 29). American Mathematical Society.

Δραζιώτης, Κ. (2022). *Εισαγωγή στην κρυπτογραφία*. Κάλλιπος, Ανοικτές Ακαδημαϊκές Εκδόσεις. https://repository.kallipos.gr/handle/11419/8016

Δροσάτος, Γ., Μαυρίδης, Ι., & Ράντος, Κ. (2025). *Θεμελιώσεις και εφαρμογές της σύγχρονης κρυπτογραφίας*. Κάλλιπος, Ανοικτές Ακαδημαϊκές Εκδόσεις. https://repository.kallipos.gr/handle/11419/14387

Κάτος, Β., & Στεφανίδης, Γ. (2003). *Τεχνικές κρυπτογραφίας και κρυπτανάλυσης*. Εκδόσεις Ζυγός.

Νάστου, Π. Ε., Σπυράκης, Π. Γ., & Σταματίου, Γ. Κ. (2003). *Σύγχρονη κρυπτογραφία: Μία ξέγνοιαστη διαδρομή στα μονοπάτια της*. Ελληνικά Γράμματα.

Paar, C., & Pelzl, J. (2010). *Understanding cryptography: A textbook for students and practitioners*. Springer.

Phan, R. C. W. (2002). Mini Advanced Encryption Standard (Mini-AES): A testbed for cryptanalysis students. *Cryptologia, 26*(4), 283–306. https://doi.org/10.1080/0161-11960215507

Pincock, S. (2008). *Κρυπτογραφία*. Εκδόσεις Τραυλός.

Poulakis, D. (2026). Mathematical Cryptology. De Gruyter. (υπό έκδοση).

Φυραρίδης, Α. (1986). *Θεωρία αριθμών*. Πανεπιστήμιο Ιωαννίνων.

International Association for Cryptologic Research, https://iacr.org/

CryptoHack, https://cryptohack.org/

NIST Cryptography, https://www.nist.gov/cryptography

Practical Cryptography, http://practicalcryptography.com/

Cryptotool – Online, https://www.cryptool.org/en/cto/

Elliptic Curve Cryptography (ECC), https://asecuritysite.com/ecc/

ΠΑΡΑΡΤΗΜΑ Β

Προτείνεται μια συλλογή ασκήσεων οι οποίες συμβάλλουν στη βαθύτερη κατανόηση των εννοιών οι οποίες αναπτύχθηκαν σε αυτό το κείμενο (βλ. και Αλβανός και Πουλάκης, 2022).

1. Το μήνυμα VHFUHW κρυπτογραφήθηκε με την χρήση ενός κρυπτοσυστήματος μετατόπισης με χώρο απλών κειμένων το αγγλικό αλφάβητο. Να βρεθεί το κλειδί κρυπτογράφησης και το αντίστοιχο απλό κείμενο.

2. Το παρακάτω κείμενο:

RJJY ZXYT RTWW TBFY KNAJ HTRJ FQTS JYMN WYJJ SNRU TWYF SYIT HZRJ SYXR ZXYG JJCH MFSL JIMJ WHZQ JUTN WTY

έχει προκύψει από την κρυπτογράφηση ενός κειμένου στην αγγλική γλώσσα και την χρήση του κρυπτοσύστημα αντικατάστασης. Να βρεθεί το κλειδί κρυπτογράφησης με την μέθοδο της ανάλυσης συχνότητας εμφάνισης των γραμμάτων.

3. Ένα κρυπτοσύστημα αντικατάστασης το οποίο χρησιμοποιεί το λατινικό

αλφάβητο έχει ως κλειδί την παρακάτω μετάθεση γραμμάτων:

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

Με την χρήση αυτού του κλειδιού κρυπτογραφούμε την λέξη SECRET και προκύπτει η λέξη AJPDJB την οποία πάλι κρυπτογραφούμε και συνεχίζουμε να κρυπτογραφούμε κάθε λέξη που προκύπτει. Πόσες διαφορετικές λέξεις θα προκύψουν;

4. Το κείμενο LOSVW AZBSH DHQID ARSLG EL έχει προκύψει μετά την κρυπτογράφηση ενός απλού κειμένου με το κρυπτοσύστημα του Vigenère και κλειδί την λέξη SHOES. Να βρεθεί το αντίστοιχο απλό κείμενο.

5. Το κείμενο UENZH ZIMPW EPEVZ PETJR NI έχει κρυπτογραφηθεί με το κρυπτοσύστημα του Vigenère. Να βρεθεί το αντίστοιχο απλό κείμενο το οποίο αρχίζει με ANEDOE.

6. Να αποκρυπτογραφηθεί το παρακάτω κείμενο το οποίο είναι η κρυπτογράφηση με ένα κρυπτοσύστημα μετάθεσης ενός κειμένου γραμμένου στην αγγλική γλώσσα:

RIBNTHGEESMSGEATTHOERODPOIPNRLTH

7. Να βρεθούν όλα τα συστήματα καταγραφής μετατόπισης με ανάδραση με τρεις καταγραφείς των οποίων οι ακολουθίες έχουν την μέγιστη περίοδο.

8. Το κείμενο 111000101 κρυπτογραφείται με το σημειωματάριο της μίας χρήσης και κλειδί την ακολουθία $s_0 \ldots s_8$. Το κείμενο που προκύπτει είναι το 111111000. Η ακολουθία $s_0 \ldots s_8$ προέρχεται από ένα σύστημα καταγραφής μετατόπισης. Να προσδιοριστεί αυτό το σύστημα.

9. Να βρεθεί θετικός ακέραιος a ο οποίος διαιρούμενος με τον 53 δίνει πηλίκο ένα πολλαπλάσιο του 7 και υπόλοιπο το τετράγωνο του πηλίκου.

10. Να υπολογιστεί ο μέγιστος κοινός διαιρέτης $d = μκδ(737,191)$ και κατόπιν να προσδιοριστούν ακέραιοι x, y έτσι, ώστε να ισχύει

$$d = 737x+191y$$

11. Ας είναι a, b θετικοί ακέραιοι πρώτοι μεταξύ τους. Να δειχθεί ότι ισχύει

$μκδ(2a+b,a+2b) = 1$ ή 3.

12. Ας είναι n φυσικός τέτοιος, ώστε ο 2^n+1 να είναι πρώτος. Δείξτε ότι ο n είναι δύναμη του 2.

13. Ας είναι n περιττός θετικός ακέραιος. Να δειχθεί ότι ισχύει $24 \mid n(n^2-1)$.

14. Να βρεθεί η πρωτογενής ανάλυση των ακεραίων: 63063, 97768, 582467.

15. Να εξεταστεί αν οι ακέραιοι 14, 23, 30, 41 είναι αντιστρέψιμα στοιχεία μέσα στο $\mathbb{Z}_{105}$ και στην περίπτωση όπου είναι να υπολογιστεί το αντίστροφο στοιχείο τους.

16. Να υπολογιστεί το τελευταίο ψηφίο του αριθμού 3^{145}.

17. Να βρεθούν οι θετικοί ακέραιοι n τέτοιοι, ώστε $\varphi(n) = n/2$.

18. Να βρεθούν όλοι οι φυσικοί n με $\varphi(n) = 16$.

19. Ας είναι ακέραιοι $a > b > 0$ και $\Phi = (1+\sqrt{5})/2$. Να δειχθεί ότι το πλήθος των βημάτων που χρειάζεται ο Ευκλείδειος αλγόριθμος για τον υπολογισμό του μκδ των a και b είναι $n \le (\log b/\log\Phi)+1$.

20. Να υπολογιστούν όλα τα στοιχεία του $\mathbb{Z}_{23}$ τα οποία είναι αρχικές ρίζες.

21. Να αποκρυπτογραφηθεί το παρακάτω κείμενο το οποίο κρυπτογραφήθηκε με τη χρήση του ομοπαραλληλικού κρυπτοσυστήματος με $n = 26$ και την αντιστοίχιση των γραμμάτων του αγγλικού αλφαβήτου με τους ακέραιους 0,1,…,25:

FMXVEDKAPHFERBNDKRXRSREFMORUD

SDKDVSHVUFEDKAPRKDLYEVLRHHRH

22. Να χρησιμοποιηθεί ο ταχύς υπολογισμός δύναμης για να υπολογιστούν οι ποσότητες: $4^{23} \bmod 30$, $5^{32} \bmod 39$, $14^{26} \bmod 28$, $31^{29} \bmod 42$.

23. Να χρησιμοποιηθεί ο πρώτος $p = 53$ και το πρωτόκολλο των Diffie-Hellman για την κατασκευή ενός κοινού κλειδιού μεταξύ δύο οντοτήτων.

24. Ισχύει $2^a \bmod 67 = 55$ και $2^b \bmod 67 = 38$. Να βρεθεί ο ακέραιος $K = 2^{ab} \bmod 67$, να γραφεί στο δυαδικό σύστημα και να χρησιμοποιηθεί ως κλειδί στο σημειωματάριο της μίας χρήσης για την κρυπτογράφηση του κειμένου (1,0,1,0,0,1). Να υπολογιστεί ο ακέραιος του οποίου η δυαδική γραφή είναι το αντίστοιχο κρυπτοκείμενο.

25. Ας είναι p, q πρώτοι μήκους 6 τέτοιοι, ώστε το ζεύγος (pq,15) ν' αποτελεί ένα δημόσιο κλειδί RSA. Η κρυπτογράφηση του κειμένου 2 με αυτό το κλειδί δίνει το 385. Να υπολογιστεί το ιδιωτικό κλειδί του σχήματος.

26. Ας είναι (n,3) ένα δημόσιο κλειδί RSA. Οι κρυπτογραφήσεις των κειμένων m και 2m είναι 112 και 403, αντίστοιχα. Να βρεθεί το κείμενο m.

27. Να δειχθεί ότι αν $(n,e) = (85,33)$ είναι ένα δημόσιο κλειδί RSA, τότε κανένα μήνυμα το οποίο κρυπτογραφείται με αυτό δεν έχει απόκρυψη.

28. Ας είναι $(n,e) = (6887,11)$ ένα δημόσιο κλειδί RSA. Να προσδιοριστεί το ιδιωτικό κλειδί του σχήματος. Κατόπιν, να κωδικοποιηθεί το απλό κείμενο

WE WILL MEET ON MONDAY

με την μέθοδο της Ενότητας 5.4 και να κρυπτογραφηθεί με το παραπάνω δημόσιο κλειδί.

29. Το κείμενο m έχει κρυπτογραφηθεί με την χρήση του RSA και των δημόσιων κλειδιών (187,7) και (187,3). Τα αντίστοιχα κρυπτογραφημένα κείμενα είναι τα 93 και 9. Να βρεθεί το κείμενο m, χωρίς να υπολογιστεί το ιδιωτικό κλειδί κάποιου από τα δύο σχήματα, να γραφεί στο δυαδικό σύστημα και να χρησιμοποιηθεί ως κλειδί στο κρυπτοσύστημα του σημειωματάριου της μίας χρήσης για την κρυπτογράφηση του κειμένου 0101.

30. Ας είναι (53,2,24) ένα δημόσιο κλειδί για το κρυπτοσύστημα του ElGamal. Τα μηνύματα 9 και m κρυπτογραφούνται και προκύπτουν τα κρυπτογραφημένα κείμενα (B,40) και (B,49), αντίστοιχα. Να υπολογιστεί το μήνυμα m χωρίς να υπολογιστεί το ιδιωτικό κλειδί του σχήματος.

*Ο **Δρ. Δημήτριος Πουλάκης** είναι Ομότιμος καθηγητής του Τμήματος Μαθηματικών του Αριστοτελείου Πανεπιστημίου Θεσσαλονίκης. Έλαβε το δίπλωμα Μαθηματικών από το Τμήμα Μαθηματικών του Πανεπιστημίου Ιωαννίνων και το Μεταπτυχιακό καθώς και Διδακτορικό δίπλωμα από το Τμήμα Μαθηματικών του Πανεπιστημίου του Παρισιού XI. Τα Ερευνητικά του Ενδιαφέροντα εστιάζονται στη Θεωρία Αριθμών, Αλγεβρική Γεωμετρία και Κρυπτολογία. Το ερευνητικό του έργο αποτελείται από πλέον των 60 άρθρων σε διεθνή έντυπα με σύστημα κριτών (βλ. https://zbmath.org/?q=ia%3Apoulakis.dimitrios) και το συγγραφικό του έργο από 10 βιβλία στους τομείς της Θεωρίας Αριθμών, Κρυπτολογίας, Άλγεβρας και Γεωμετρίας. Έχει διατελέσει Καθηγητής του Τμήματος Μαθηματικών του ΑΠΘ και επιπλέον έχει διδάξει και σε άλλα Ιδρύματα, όπως το Πανεπιστήμιο Ιωαννίνων, το Ελληνικό Ανοικτό Πανεπιστήμιο, κ.ά.. Επίσης, ήταν επισκέπτης καθηγητής σε Πανεπιστήμια της Αλλοδαπής, όπως το Πανεπιστήμιο του Παρισιού VII, το Πανεπιστήμιο της Μασσαλίας II, κ.ά. (βλ. και https://poulakis.webpages.auth.gr/)*

Introduction to Cryptology

Dimitrios Poulakis

Professor Emeritus, Department of Mathematics,

Aristotle University of Thessaloniki

poulakis@math.auth.gr

Abstract

This paper provides a concise introduction to modern Cryptology along with the necessary Number Theory background for its understanding. It presents fundamental concepts of Cryptography and Cryptanalysis and describes some historical cryptosystems. The two types of symmetric cryptosystems, stream and block ciphers, are introduced, and their operation is described. Next, the basic concepts and results of Number Theory required for the presentation of Public Key Cryptography are given. Finally, the operation of the RSA and ElGamal public key cryptosystems, as well as the Diffie-Hellman protocol, is described.

Keywords: Cryptology, Cryptography, Cryptanalysis, Symmetric ciphers, Public-Key Ciphers.

Dr. Dimitrios Poulakis *is an Emeritus Professor in the Department of Mathematics at Aristotle University of Thessaloniki. He received his degree in Mathematics from the Department of Mathematics at the University of Ioannina, and both his Master's and Doctorate from the Department of Mathematics at the University of Paris XI. His research interests focus on Number Theory, Algebraic Geometry, and Cryptology. His research work consists of more than 60 articles in international peer-reviewed journals (see https://zbmath.org/?q=ia%3Apoulakis.dimitrios), and his authorship includes 10 books in the fields of Number Theory, Cryptology, Algebra, and Geometry. He has served as a Professor in the Department of Mathematics at Aristotle University of Thessaloniki, and has also taught at other institutions, such as the University of Ioannina, the Hellenic Open University, among others. Additionally, he has been a visiting professor at foreign universities, such as the University of Paris VII, the University of Aix-Marseille II, and others (see also https://poulakis.webpages.auth.gr/).*