# ΚΡΥΠΤΟΓΡΑΦΙΑ ΚΑΙ ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ

**Νικόλαος Α. Φωτιάδης**
Δρ Μαθηματικών
Επιμορφωτής Β΄ επιπέδου κλάδου ΠΕ 03
E-mail: nikos.fotiades@gmail.com
Website: http://users.sch.gr/nfotiades/

**Περίληψη**

Η κρυπτογραφία αποτελεί παράδειγμα εφαρμογής της θεωρίας αριθμών σε πρακτικά προβλήματα της καθημερινής ζωής. Εκτός από το πρόβλημα της μυστικής επικοινωνίας, που ενδιαφέρει κυρίως τις στρατιωτικές και διπλωματικές υπηρεσίες μιας χώρας, η κρυπτογραφία είναι απαραίτητη σε θέματα όπως η ασφάλεια των τραπεζικών συναλλαγών ή το ηλεκτρονικό εμπόριο. Στην παρούσα εργασία παρουσιάζονται παραδείγματα συμμετρικής, αλλά και ασύμμετρης κρυπτογραφίας, καθώς και ο ρόλος της θεωρίας αριθμών σε αυτά.

**Abstract**

Cryptography is an example of applying number theory to practical problems in everyday life. In addition to the problem of secret communication, which is primarily concerned with a country's military and diplomatic services, cryptography is essential in matters such as banking security or e-commerce. This paper presents examples of both symmetric and asymmetric cryptography, as well as the role of number theory in them.

## Εισαγωγή

Η κρυπτογραφία μελετά τρόπους με τους οποίους μπορούμε να μετασχηματίσουμε ένα μήνυμα σε ακατάληπτη μορφή, ώστε μόνο ο παραλήπτης στον οποίο προορίζεται να μπορεί να το διαβάσει. Αυτό είναι γνωστό ως πρόβλημα της μυστικής επικοινωνίας αποστολέα και παραλήπτη παρουσία κάποιου τρίτου, τον οποίο θα αποκαλούμε *αντίπαλο*. Αρχικά η κρυπτογραφία χρησιμοποιήθηκε για την ασφαλή μεταφορά μηνυμάτων με στρατιωτικό ή διπλωματικό περιεχόμενο. Στη σύγχρονη εποχή, με την ανάπτυξη των ηλεκτρονικών υπολογιστών, δημιουργήθηκε η ανάγκη

προστασίας των ευαίσθητων πληροφοριών που διακινούνται μέσω του διαδικτύου. Η κρυπτογραφία σήμερα βρίσκει εφαρμογές σε δραστηριότητες της καθημερινής ζωής όπως οι τραπεζικές συναλλαγές, οι τηλεπικοινωνίες, το ηλεκτρονικό εμπόριο, το ηλεκτρονικό ταχυδρομείο, η ψηφιακή υπογραφή κ.α.

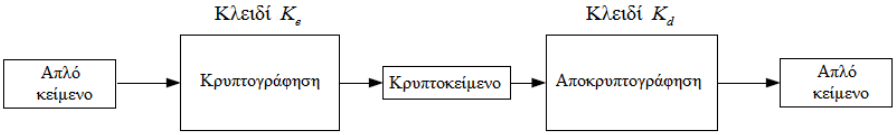
Η κρυπτογραφία έχει ιστορία χιλιάδων ετών. Πρώιμες μορφές κρυπτογραφίας, που βασίζονται κυρίως σε αντικαταστάσεις των συμβόλων, έχουν εντοπιστεί σε κείμενα της Αρχαίας Αιγύπτου και της Μεσοποταμίας [1]. Η Σπαρτιάτικη σκυτάλη ήταν μια μέθοδος κρυπτογραφίας που χρησιμοποιούσαν οι Έφοροι για να επικοινωνούν μυστικά με τον στρατηγό ή τον ναύαρχο που ήταν σε εκστρατεία. Η σκυτάλη είναι ένα ξύλινο ραβδί γύρω από το οποίο τυλίγεται μια μακριά και λεπτή λωρίδα δέρματος. Ο αποστολέας γράφει το μήνυμα κατά μήκος της σκυτάλης και μετά ξετυλίγει τη λωρίδα. Για να μπορέσει ο παραλήπτης να διαβάσει το μήνυμα έπρεπε να τυλίξει τη λωρίδα στη δική του σκυτάλη που είχε ακριβώς την ίδια διάμετρο. Ο Πλούταρχος, στο έργο του «Ο βίος του Λύσανδρου», κεφ. ΙΘ, περιγράφει τη λειτουργία της σκυτάλης.


Εικόνα 1. Η Σπαρτιάτικη σκυτάλη

Το μήνυμα που πρέπει να αποκρύψουμε ονομάζεται *απλό κείμενο*. Μετά τη μετατροπή του σε μυστική μορφή το μήνυμα ονομάζεται *κρυπτοκείμενο*. Η διαδικασία μετατροπής του απλού κειμένου σε κρυπτοκείμενο ονομάζεται *κρυπτογράφηση*, ενώ η αντίστροφη πορεία *αποκρυπτογράφηση*. Οι δύο διαδικασίες απαιτούν μια ιδιαίτερη ποσότητα πληροφορίας που ονομάζεται *κλειδί*. Η προσπάθεια που κάνει ο αντίπαλος να αποκρυπτογραφήσει το κείμενο χωρίς να έχει το κλειδί ονομάζεται *κρυπτανάλυση*. Αν το κλειδί της κρυπτογράφησης $K_e$ είναι ίδιο με το κλειδί της αποκρυπτογράφησης $K_d$ η κρυπτογραφία ονομάζεται *συμμετρική*. Στην περίπτωση αυτή το κοινό κλειδί ονομάζεται *μυστικό κλειδί*. Όταν τα δύο κλειδιά $K_e$ και $K_d$ είναι διαφορετικά η κρυπτογραφία ονομάζεται *ασύμμετρη*. Στην ασύμμετρη κρυπτογραφία το κλειδί της κρυπτογράφησης ονομάζεται *δημόσιο κλειδί*, ενώ της αποκρυπτογράφησης *ιδιωτικό κλειδί*. Όλα τα κρυπτογραφικά συστήματα από την αρχαιότητα μέχρι το 1976 ήταν

συμμετρικά [2]. Μια σημαντική αδυναμία της συμμετρικής κρυπτογραφίας είναι ότι ο αποστολέας και ο παραλήπτης θα πρέπει να έχουν βρει έναν ασφαλή τρόπο να μοιραστούν την πληροφορία του μυστικού κλειδιού, χωρίς αυτή να γίνει αντιληπτή από τον αντίπαλο. Το πρόβλημα γίνεται πιο έντονο στην περίπτωση ενός δικτύου επικοινωνίας με πολλά μέλη. Ας υποθέσουμε ότι σε ένα δίκτυο επικοινωνίας υπάρχουν 100 μέλη. Το κάθε μέλος θα πρέπει να αποθηκεύσει 99 διαφορετικά κλειδιά για να επικοινωνεί μυστικά με οποιοδήποτε από τα άλλα μέλη. Ο συνολικός αριθμός των κλειδιών είναι $\frac{99 \cdot 100}{2} = 4950$. Τα 100 μέλη θα πρέπει να διαθέτουν 4950 ασφαλή κανάλια επικοινωνίας για να ανταλλάξουν την πληροφορία του μυστικού κλειδιού.

Οι δυσκολίες που δημιουργεί η διαχείριση των μυστικών κλειδιών οδήγησαν στην επινόηση της ασύμμετρης κρυπτογραφίας. Το 1976 οι Diffie και Hellman απέδειξαν ότι είναι δυνατόν η κρυπτογράφηση και η αποκρυπτογράφηση να γίνουν με διαφορετικά κλειδιά [3]. Με αυτή την ασύμμετρη κρυπτογραφία ο αποστολέας μπορεί να κρυπτογραφήσει ένα μήνυμα χρησιμοποιώντας ένα δημόσιο κλειδί γνωστό σε όλους. Το μήνυμα αυτό μπορεί να αποκρυπτογραφήσει μόνο ο παραλήπτης χρησιμοποιώντας το ιδιωτικό του κλειδί. Ο αποστολέας και ο παραλήπτης δεν είναι αναγκαίο να έχουν επικοινωνήσει στο παρελθόν για να ανταλλάξουν την πληροφορία του κλειδιού. Οι Diffie και Hellman απέδειξαν θεωρητικά ότι είναι δυνατόν να υπάρξει ασύμμετρη κρυπτογραφία, όμως δεν περιέγραψαν κάποιον πρακτικό τρόπο για να γίνει αυτό. Λίγο αργότερα οι Rivest, Shamir και Adleman περιέγραψαν μια μέθοδο κρυπτογραφίας δημόσιου κλειδιού που έγινε γνωστή ως RSA κρυπτογραφία [4].




Εικόνα 2

Είναι ενδιαφέρον ότι η ασύμμετρη κρυπτογραφία μπορεί να λειτουργήσει και αντίστροφα. Ο κάτοχος του ιδιωτικού κλειδιού μπορεί να κρυπτογραφήσει ένα κείμενο με το ιδιωτικό του κλειδί, ενώ οποιοσδήποτε μπορεί να το αποκρυπτογραφήσει. Αυτή είναι η αρχή λειτουργίας της ψηφιακής υπογραφής.

Στη σύγχρονη κρυπτογραφία οι αλγόριθμοι κρυπτογράφησης και αποκρυπτογράφησης βασίζονται στα μαθηματικά και κυρίως στη θεωρία αριθμών. Αυτό προϋποθέτει μια ένα προς ένα αντιστοιχία των χαρακτήρων που χρησιμοποιούνται για ένα κείμενο (γράμματα, πεζά ή κεφαλαία, σημεία στίξης κ.α.) με αριθμούς. Στα παραδείγματα που θα αναφέρουμε στην παρούσα εργασία θα χρησιμοποιήσουμε 25 χαρακτήρες (τα 24 κεφαλαία γράμματα της ελληνικής αλφαβήτου και το κενό). Κάθε ένας χαρακτήρας έχει ένα αριθμητικό ισοδύναμο σύμφωνα με την παρακάτω αντιστοιχία.

| | Α | Β | Γ | Δ | Ε | Ζ | Η | Θ | Ι | Κ | Λ | Μ | Ν | Ξ | Ο | Π | Ρ | Σ | Τ | Υ | Φ | Χ | Ψ | Ω |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 |

Σε κάθε κεφαλαίο γράμμα αντιστοιχεί ένας διψήφιος αριθμός (το 1 γράφεται 01, το 2 γράφεται 02 κλπ) και στο κενό ανάμεσα σε δύο λέξεις αντιστοιχεί το 00. Η φράση

ΣΕ ΚΑΘΕ

αποτελείται από 7 σύμβολα, τα 6 γράμματα και το κενό ανάμεσα στις δύο λέξεις. Το αριθμητικό ισοδύναμο της φράσης είναι μια σειρά από 14 ψηφία

18 05 00 10 01 08 05.

**Συμμετρική κρυπτογραφία**

Ένα παράδειγμα συμμετρικής κρυπτογραφίας είναι η αντικατάσταση ενός χαρακτήρα με εκείνον που βρίσκεται 3 θέσεις δεξιότερα του στον παραπάνω πίνακα. Έτσι το κενό αντικαθίσταται με το Γ, το Α με το Δ, το Β με το Ε κλπ. Τα τρία τελευταία γράμματα Χ, Ψ και Ω με κυκλικότητα αντικαθίστανται με το κενό, το Α και το Β αντίστοιχα. Αν συμβολίσουμε με $P$ το αριθμητικό ισοδύναμο κάποιου χαρακτήρα του απλού κειμένου και με $C$ το αριθμητικό ισοδύναμο του αντίστοιχου χαρακτήρα του κρυπτοκειμένου, η διαδικασία της κρυπτογράφησης μπορεί να περιγραφεί με την ισότητα

$$C = P + 3 \pmod{25}.$$

Το αριθμητικό ισοδύναμο της φράσης

ΕΥΚΛΕΙΔΕΙΟΣ ΧΩΡΟΣ

είναι

05 20 10 11 05 09 04 05 09 15 18 00 22 24 17 15 18.

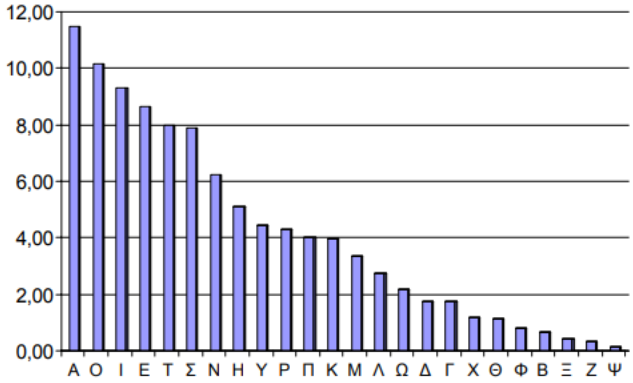
Εφαρμόζοντας την ισότητα $C = P + 3 \pmod{25}$ σε κάθε διψήφιο αριθμό προκύπτει

08 23 13 14 08 12 07 08 12 18 21 03 00 02 20 18 21

που είναι το αριθμητικό ισοδύναμο του κρυπτοκειμένου

ΘΨΝΞΘΜΗΘΜΣΦΓ ΒΥΣΦ.

Σύμφωνα με τον Ρωμαίο ιστορικό Γάιο Σουητώνιο, ο Ιούλιος Καίσαρας χρησιμοποιούσε αυτή τη μέθοδο κρυπτογράφησης για την επικοινωνία του με τον Μάρκο Κικέρωνα. Το συγκεκριμένο σύστημα κρυπτογραφίας είναι μονοαλφαβητικό, δηλαδή κάθε χαρακτήρας αντικαθίσταται με τον ίδιο πάντα χαρακτήρα. Τα μονοαλφαβητικά συστήματα κρυπτογραφίας είναι εξαιρετικά επισφαλή γιατί η κρυπτανάλυσή τους στηρίζεται στη συχνότητα εμφάνισης κάθε χαρακτήρα.




Εικόνα 3. Συχνότητα εμφάνισης γραμμάτων (%)

Ένα δημοφιλές πολυαλφαβητικό σύστημα κρυπτογραφίας προτάθηκε το 1586 από τον Γάλλο κρυπτογράφο Blaise de Vigenère. Ο αποστολέας και ο παραλήπτης χρησιμοποιούν μια λέξη-κλειδί που έχουν από κοινού επιλέξει. Ας η υποθέσουμε ότι έχουν επιλέξει τη λέξη-κλειδί

ΠΡΑΞΗ.

Το αριθμητικό ισοδύναμο της λέξης-κλειδί είναι πέντε διψήφιοι αριθμοί

16 17 01 14 07.

Επαναλαμβάνουμε τους πέντε διψήφιους αριθμούς όσες φορές είναι απαραίτητο κάτω από το αριθμητικό ισοδύναμο του απλού κειμένου, ώστε σε κάθε στήλη να υπάρχουν δύο διψήφιοι αριθμοί. Το κρυπτοκείμενο προκύπτει με την πρόσθεση modulo 25 των αριθμών της κάθε στήλης.

Παρουσιάζουμε τη μέθοδο κρυπτογράφησης Vigenère με την κρυπτογράφηση της φράσης

ΕΥΚΛΕΙΔΕΙΟΣ ΧΩΡΟΣ

| | |
|---|---|
| Απλό κείμενο | 05 20 10 11 05 09 04 05 09 15 18 00 22 24 17 15 18 |
| Λέξη κλειδί | 16 17 01 14 07 16 17 01 14 07 16 17 01 14 07 16 17 |
| Κρυπτοκείμενο | 21 12 11 00 12 00 21 06 23 22 09 17 23 13 24 06 10 |

Η κρυπτογραφημένη φράση είναι

ΦΜΛ Μ ΦΖΨΧΙΡΨΝΩΖΚ

Τα τρία Ε που υπάρχουν στο απλό κείμενο εμφανίζονται το πρώτο ως Φ, το δεύτερο ως Μ και το τρίτο ως Ζ στο κρυπτοκείμενο. Από τα δύο Μ που υπάρχουν στο κρυπτοκείμενο το πρώτο προέρχεται από το Υ και το δεύτερο από το Ε του απλού κειμένου.

Αν συμβολίσουμε με $P_i$ το αριθμητικό ισοδύναμο του χαρακτήρα του απλού κειμένου, με $b_i$ το αριθμητικό ισοδύναμο του χαρακτήρα της λέξης-κλειδί και με $C_i$ το αριθμητικό ισοδύναμο του χαρακτήρα του κρυπτοκειμένου που βρίσκονται στη στήλη $i$, η διαδικασία της κρυπτογράφησης μπορεί να περιγραφεί με την ισότητα

$$C_i = P_i + b_i \pmod{25}.$$

Η κρυπτανάλυση ενός κειμένου που κρυπτογραφήθηκε με τη μέθοδο του Vigenère επικεντρώνεται στην εύρεση του μήκους της λέξης-κλειδί. Στην περίπτωση αυτή το κρυπτογραφημένο κείμενο χωρίζεται σε τόσα μέρη όσο το μήκος της λέξης-κλειδί. Στο παραπάνω παράδειγμα που η λέξη-κλειδί έχει 5 χαρακτήρες συγκεντρώνουμε όλους τους χαρακτήρες του κρυπτοκειμένου που κρυπτογραφήθηκαν με το γράμμα Π, δηλαδή τον 1ο, τον 6ο, τον 11ο κλπ. Στη συνέχεια συγκεντρώνουμε όλους τους χαρακτήρες που κρυπτογραφήθηκαν με το γράμμα Ρ και κάνουμε το ίδιο με τα υπόλοιπα γράμματα. Κάθε ένα από τα 5 μέρη που δημιουργούνται μπορεί να αποκρυπτογραφηθεί με την ανάλυση συχνοτήτων εμφάνισης των χαρακτήρων. Μια μέθοδος για τον υπολογισμού του μήκους του κλειδιού είναι ο έλεγχος Kasiski που αναπτύχθηκε από τον απόστρατο αξιωματικό του Πρωσικού στρατού F. W. Kasiski το 1863 [5].

**Ασύμμετρη κρυπτογραφία**

Η κεντρική ιδέα στην οποία στηρίζεται η κρυπτογραφία RSA, γνωστή ως κρυπτογραφία του δημόσιου κλειδιού, είναι ότι, ενώ είναι εύκολο να βρούμε το γινόμενο δύο φυσικών αριθμών, είναι δύσκολο, και σε αρκετές περιπτώσεις ακατόρθωτο να βρούμε τους πρώτους παράγοντες ενός σύνθετου αριθμού. Οι αριθμοί $p = 48611$ και $q = 59359$ είναι πρώτοι. Το γινόμενό τους μπορούμε να βρούμε εύκολα ότι είναι $n = pq = 2885500349$ ενώ αν δοθεί ο αριθμός $n = 2885500349$, είναι αρκετά δύσκολο και χρονοβόρο να βρούμε τους παράγοντες $p$ και $q$.

Για την κρυπτογραφημένη επικοινωνία ο παραλήπτης επιλέγει δύο πρώτους αριθμούς $p, q$ που ο καθένας έχει τουλάχιστον 200 ψηφία και

υπολογίζει το γινόμενο $n = pq$. Στη συνέχεια επιλέγει έναν φυσικό αριθμό $k$ τέτοιο ώστε

$$\text{ΜΚΔ}(k, \varphi(n)) = 1,$$

όπου $\varphi(n)$ είναι η συνάρτηση $\varphi$ του Euler που εκφράζει το πλήθος των αριθμών του συνόλου $\{1, 2, \ldots, n-1\}$ οι οποίοι είναι σχετικά πρώτοι με τον $n$. Επειδή ο αριθμός $n$ είναι γινόμενο δύο πρώτων αριθμών $p, q$ ισχύει $\varphi(n) = (p-1)(q-1)$. Τέλος, ο παραλήπτης βρίσκει έναν φυσικό αριθμό $m$ για τον οποίο ισχύει

$$km = 1 \pmod{\varphi(n)}.$$

Η ύπαρξη του αριθμού $m$ δικαιολογείται ως εξής: Από την ισότητα $\text{ΜΚΔ}(k, \varphi(n)) = 1$ προκύπτει ότι υπάρχουν ακέραιοι $x, y$ για τους οποίους ισχύει

$$xk + y\varphi(n) = 1.$$

Με τον Ευκλείδειο αλγόριθμο μπορούμε να βρούμε έναν φυσικό αριθμό $m$ από το σύνολο των λύσεων $x$ της παραπάνω διοφαντικής εξίσωσης.

Ο παραλήπτης κοινοποιεί δημόσια το ζεύγος των αριθμών $(n, k)$. Οι αριθμοί αυτοί αποτελούν το δημόσιο κλειδί για τον συγκεκριμένο παραλήπτη. Όποιος θέλει να του στείλει ένα κρυπτογραφημένο κείμενο, χρησιμοποιεί τους αριθμούς $(n, k)$ για την κρυπτογράφηση. Ο αποστολέας δεν είναι απαραίτητο να έχει επικοινωνήσει στο παρελθόν με τον παραλήπτη, για να συμφωνήσουν για κάποιο μυστικό κλειδί, όπως συμβαίνει στη συμμετρική κρυπτογραφία. Το μόνο που χρειάζεται είναι να ψάξει να βρει τους αριθμούς $(n, k)$ του παραλήπτη, οι οποίοι είναι διαθέσιμοι σε καταλόγους ανάλογους με τους τηλεφωνικούς καταλόγους. Η τριάδα των αριθμών $(p, q, m)$ αποτελεί το ιδιωτικό κλειδί. Τους αριθμούς αυτούς τους γνωρίζει μόνο ο παραλήπτης και τους χρησιμοποιεί για την αποκρυπτογράφηση του κειμένου που παραλαμβάνει από οποιονδήποτε αποστολέα.

Ο αποστολέας βρίσκει το αριθμητικό ισοδύναμο του απλού κειμένου και το χωρίζει σε τμήματα των 4 ψηφίων. Έστω $P$ ένας τέτοιος τετραψήφιος. Ο αποστολέας υπολογίζει τη δύναμη $P^k$ και στη συνέχεια βρίσκει το κρυπτοκείμενο $C$ με αναγωγή $(\text{mod}\, n)$, δηλαδή

$$P^k = C \pmod{n}.$$

Για την αποκρυπτογράφηση ο παραλήπτης υπολογίζει τη δύναμη $C^m$ και στη συνέχεια αποκαλύπτει το απλό κείμενο $P$ με αναγωγή $(\text{mod}\, n)$.

Η απόδειξη της ισότητας $C^m = P \pmod n$, με την οποία γίνεται η αποκρυπτογράφηση, στηρίζεται στο θεώρημα του Euler, σύμφωνα με το οποίο αν $\alpha, n$ είναι δύο ακέραιοι αριθμοί με $\text{ΜΚΔ}(\alpha, n) = 1$, τότε

$$\alpha^{\varphi(n)} = 1 \pmod n.$$

Πράγματι,

$$C^m = (P^k)^m = P^{km} = P^{1-r\varphi(n)} = P \cdot (P^{\varphi(n)})^{-r} = P \cdot 1 = P \pmod n$$

όπου $r$ είναι ο ακέραιος για τον οποίο ισχύει $mk + r\varphi(n) = 1$. Η ισότητα $P^{\varphi(n)} = 1 \pmod n$ προκύπτει από το θεώρημα του Euler, αφού $\text{ΜΚΔ}(P, n) = 1$. Ο τετραψήφιος αριθμός $P$ είναι σχετικά πρώτος με τον αριθμό $n$, γιατί είναι μικρότερος από τους αριθμούς $p, q$.

Παρουσιάζουμε, στη συνέχεια, ένα παράδειγμα για να δείξουμε πώς λειτουργεί η κρυπτογραφία RSA. Υποθέτουμε ότι ο παραλήπτης επιλέγει τους πρώτους αριθμούς $p = 43$ και $q = 59$. Στην πραγματικότητα, οι αριθμοί $p, q$ θα πρέπει να έχουν τουλάχιστον 200 ψηφία, όμως για την απλοποίηση των πράξεων στο συγκεκριμένο παράδειγμα επιλέξαμε διψήφιους πρώτους αριθμούς. Το γινόμενο των δύο πρώτων αριθμών είναι

$$n = 43 \cdot 59 = 2537.$$

Η τιμή της συνάρτησης $\varphi$ του Euler είναι

$$\varphi(n) = (p-1)(q-1) = 42 \cdot 58 = 2436.$$

Ένας αριθμός σχετικά πρώτος με τον 2436 είναι ο $k = 11$. Με τον Ευκλείδειο αλγόριθμο βρίσκουμε ότι μια λύση της διοφαντικής εξίσωσης $11x + 2436y = 1$ είναι $(x, y) = (443, -2)$. Η κρυπτογράφηση γίνεται με ύψωση στη δύναμη $k = 11$ και αναγωγή $(\text{mod}\, 2537)$, ενώ η αποκρυπτογράφηση γίνεται με ύψωση στη δύναμη $m = 443$ και αναγωγή $(\text{mod}\, 2537)$.

Υποθέτουμε ότι το απλό κείμενο που θέλει να στείλει ο αποστολέας είναι η λέξη ΚΥΚΛΟΣ. Το αριθμητικό ισοδύναμο είναι 10 20 10 11 15 18, το οποίο χωρίζουμε σε τρία τετραψήφια τμήματα.

$$P_1 = 1020,\ P_2 = 1011 \text{ και } P_3 = 1518.$$

Από τις ισότητες

$$1020^{11} = 2210 \pmod{2537}$$

$$1011^{11} = 1341 \pmod{2537}$$

$$1518^{11} = 23 \pmod{2537}$$

προκύπτει το κρυπτοκείμενο 22 10 13 41 00 23. Για την αποκρυπτογράφηση ο παραλήπτης σχηματίζει τρεις τετραψήφιους

$$C_1 = 2210,\ C_2 = 1341 \text{ και } C_3 = 0023.$$

Από τις ισότητες

$$2210^{443} = 1020 \pmod{2537}$$
$$1341^{443} = 1011 \pmod{2537}$$
$$23^{443} = 1518 \pmod{2537}$$

προκύπτει το απλό κείμενο.

Η ασφάλεια της κρυπτογράφησης RSA εξαρτάται από το χρόνο που χρειάζεται ένας υπολογιστής για να παραγοντοποιήσει ένα φυσικό αριθμό. Για να μπορέσει ο αντίπαλος να αποκρυπτογραφήσει ένα κείμενο, θα πρέπει να βρει την παραγοντοποίηση του $n$. Με τα σύγχρονα[1] δεδομένα της τεχνολογίας ο γρηγορότερος υπολογιστής χρειάζεται 3.800.000 χρόνια για να παραγοντοποιήσει τον αριθμό $n$ στην περίπτωση που οι πρώτοι $p, q$ έχουν 200 ψηφία [6]. Μια ενδεχόμενη εντυπωσιακή αύξηση της ταχύτητας των υπολογιστών θα αντιμετωπιστεί με την επιλογή πρώτων αριθμών με μεγαλύτερο πλήθος ψηφίων.

**Βιβλιογραφία**


1. D. Kahn (1996), *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet,* Scribner.
2. C. Parr, J. Pelzl (2010), *Understanding Cryptography*, Springer.
3. W. Diffie, M. Hellman, New Directions in Cryptography, *IEEE Trans. Inf. theory* IT-22(6), 644–654, 1976.
4. R.L. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM*, 21:120–126, 1978.
5. S. Singh (2000), *The Code Book*, Anchor.
6. D. M. Burton (2011), *Elementary Number Theory*, McGraw-Hill.


[1] Τα στοιχεία αντλήθηκαν από το βιβλίο του D. M. Burton που εκδόθηκε το 2011.