ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΚΡΥΠΤΟΛΟΓΙΑ
ΦΥΛΛΑΔΙΟ ΑΣΚΗΣΕΩΝ $\#1$

ΘΕΟΔΟΥΛΟΣ ΓΑΡΕΦΑΛΑΚΗΣ

Άσκηση 1

Έστω ότι το μήνυμα

$$OH7F86BB46R3627O266BB9$$

κρυπτογραφήθηκε με χρήση ενός ομοπαραλληλικού συστήματος και του αλφαβήτου $\mathbb{Z}/37\mathbb{Z}$ υπό την αντιστοιχία

$$0 \leftrightarrow 0, 1 \leftrightarrow 1, \ldots 9 \leftrightarrow 9, A \leftrightarrow 10, B \leftrightarrow 11, \ldots, Z \leftrightarrow 35, \text{κενό} \leftrightarrow 36$$

Ας υποθέσουμε επίσης ότι είναι γνωστό ότι τα τρία τελευταία σύμβολα του καθαρού μηνύματος είναι 007. Αποκρυπτογραφήστε το παραπάνω κρυπτογράφημα.

Άσκηση 2

Βρείτε ένα γεννήτορα της ομάδας $(\mathbb{Z}/p\mathbb{Z})^*$ για $p = 29, 61, 73$.

Άσκηση 3

Η Αλίκη και ο Βασίλης θέλουν να κατασκευάσουν ένα κοινό κρυφό κλειδί επικοινωνώντας μέσα από ένα δημόσιο κανάλι. Το κλειδί που θέλουν να κατασκευάσουν θέλουν να έχει μήκος 5 bits. Περιγράψτε ποιά βήματα πρέπει να ακολουθήσουν για να το καταφέρουν.

Άσκηση 4

Κατασκευάστε ένα σύστημα κρυπτογράφησης ElGamal με βάση την ομάδα $(\mathbb{Z}/61\mathbb{Z})^*$. Κατασκευάστε ένα ζευγάρι ιδιωτικού/δημόσιου κλειδιού. Δείξτε πώς ένας τρίτος κρυπτογραφεί το μήνυμα $m = 10$ για να σας το στείλει. Στη συνέχεια αποκρυπτογραφήστε το κρυπτογραφημένο μήνυμα που παραλάβατε.