ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΚΡΥΠΤΟΛΟΓΙΑ
ΦΥΛΛΑΔΙΟ ΑΣΚΗΣΕΩΝ $\#2$

ΘΕΟΔΟΥΛΟΣ ΓΑΡΕΦΑΛΑΚΗΣ

Άσκηση 1

Σε ένα σύστημα κρυπτογράφησης ElGamal στην ομάδα $(\mathbb{Z}/29\mathbb{Z})^*$, με βάση $g = 2$, η Αλίκη έχει δημόσιο κλειδί $y = 5$. Έστω $(r_1, c_1) = (21, 3)$ το κρυπτογράφημα ενός μηνύματος m_1 και το (r_2, c_2) είναι το κρυπτογράφημα ενός μηνύματος m_2. Γνωρίζετε τα δύο κρυπτογραφήματα, αλλά όχι τα μηνύματα. Υπολογίστε ένα κρυπτογράφημα του μηνύματος $m_1 m_2$.

Άσκηση 2

Ο αριθμός $p = 2 \cdot 3^4 + 1 = 163$ είναι πρώτος και η κλάση του 2 γεννά την ομάδα $(\mathbb{Z}/p\mathbb{Z})^*$. Υπολογίστε το διακριτό λογάριθμο του $y = 3$ ως πρός τη βάση $g = 2$.

Άσκηση 3

Κατασκευάστε ένα σύστημα κρυπτογράφησης RSA. Το n θα πρέπει να είναι τριψήφιος αριθμός. Δώστε ένα παράδειγμα κρυπτογράφησης και απόκρυπτογράφησης.

Άσκηση 4

Δώστε ένα μάρτυρα Fermat της συνθετότητας του 15. Δώστε ένα μάρτυρα Rabin-Miller της συνθετότητας του 15.

Άσκηση 5

Σε ένα σύστημα RSA με $n = 35$ γνωρίζετε ένα ζευγάρι κλειδιών κρυπτογράφησης/αποκρυπρογράφησης, το $(e, d) = (7, 7)$. Υπολογίστε τους πρώτους παράγοντες του n.