Α 44 – ΚΡΥΠΤΟΓΡΑΦΙΑ
ΦΥΛΛΑΔΙΟ ΑΣΚΗΣΕΩΝ #2

ΘΕΟΔΟΥΛΟΣ ΓΑΡΕΦΑΛΑΚΗΣ

(1) Περιγράψτε παραμέτρους για το πρωτόκολλο Diffie-Hellman με βάση την ομάδα $\mathbb{F}_p^\times$, όπου p είναι πρώτος με 5 δεκαδικά ψηφία. Δικαιολογήστε την επιλογή των παραμέτρων (συμπεριλαμβανομένου και του p). Περιγράψτε μια εφαρμογή του πρωτοκόλλου ανάμεσα στην Αλίκη και το Βασίλη και δώστε το κρυφό κλειδί.

(2) Περιγράψτε πώς ένας τρίτος μπορεί να βρει το κλειδί της άσκησης (1) με τη χρήση του αλγόριθμου Baby-step/Giant-step.

(3) Κατασκευάστε ένα σύστημα ElGamal με βάση την ομάδα $\mathbb{F}_{3^{11}}^\times$. Για την αριθμητική στο $\mathbb{F}_{3^{11}}$ μπορείτε να χρησιμοποιήσετε το πολυώνυμο $f = X^{11} + 2X^2 + 1 \in \mathbb{F}_3[X]$ που είναι ανάγωγο. Περιγράψτε τις δημόσιες παραμέτρους, και ένα ζεύγος ιδιωτικού/δημόσιου κλειδιών. Κρυπτογραφήστε το μήνυμα $m = X^7 + X^5 + 2X + 1$. Αποκρυπτογραφήστε για να πάρετε πίσω το καθαρό μήνυμα m.

(4) Περιγράψτε δύο ζεύγη ιδιωτικού/δημόσιου κειδιών για ένα σύστημα κρυπτογράφησης RSA όπου το modulus και στις δύο περιπτώσεις έχει 10 ψηφία. Κρυπτογραφήστε ένα μήνυμα της επιλογής σας (με το ένα κειδί), και αποκρυπτογραφήστε.