Α44 – ΚΡΥΠΤΟΓΡΑΦΙΑ
ΦΥΛΛΑΔΙΟ ΑΣΚΗΣΕΩΝ $\#4$

ΘΕΟΔΟΥΛΟΣ ΓΑΡΕΦΑΛΑΚΗΣ

Άσκηση 1

Στην άσκηση αυτή θα δούμε πώς είναι δυνατό να πραγματοποιηθεί μια πλαστογραφία σε ένα σύστημα υπογραφής ElGamal, όταν δεν χρησιμοποιήται συνάρτηση κατακερματισμού. Υποθέστε ότι έχουμε ένα κλασικό σύστημα ElGamal στην ομάδα $\mathbb{F}_p^\times$ με παράμετρο g τάξης q (πρώτου), ένα ιδιωτικό κλειδί x και ένα δημόσιο κλειδί $y = g^x \mod p$. Υποθέτουμε ότι οι υπογραφές δημιουργούνται *χωρίς* τη χρήση συνάρτησης κατακερματισμού. Δεδομένης μίας υπογραφής (r, s) σε ένα μήνυμα m, δείξτε πώς μπορείτε να κατασκευάσετε μία ισχύουσα υπογραφή σε ένα νέο μήνυμα (χωρίς φυσικά τη γνώση του ιδιωτικού κλειδιού).

Υπόδειξη: Δείξτε πώς μπορεί να υπολογιστεί το β έτσι ώστε το $(r^\gamma, \beta s)$ να είναι ισχύουσα υπογραφή στο μήνυμα $\beta\gamma m$.

Άσκηση 2

Έστω οι τρείς παρακάτω παραλλαγές του σχήματος υπογραφής ElGamal. Όπως στο βασικό σχήμα, επιλέγουμε $g \in \mathbb{F}_p^\times$ τάξης πρώτου q, ιδιωτικό κλειδί $0 \leq a \leq q-1$ και δημόσιο κλειδί $y = g^a \mod p$. Για να υπογράψουμε το μήνυμα $m \in \mathbb{Z}$ υπολογίζουμε τα

(1) $r = g^k$ για τυχαίο $0 \leq k \leq q-1$, $s = a^{-1}(h(m) + kr) \mod q$.
(2) $r = g^k$ για τυχαίο $0 \leq k \leq q-1$, $s = ah(m) - kr \mod q$.
(3) $r = g^k$ για τυχαίο $0 \leq k \leq q-1$, $s = k(h(m) + ar) \mod q$.

Εδώ $h : \mathbb{Z} \longrightarrow \mathbb{Z}/q\mathbb{Z}$ είναι μια συνάρτηση κατακερματισμού. Σε όλα τα σχήματα η υπογραφή στο μήνυμα m είναι το (r, s).

(1) Περιγράψτε για τα δύο πρώτα σχήματα πώς γίνεται η πιστοποίηση της υπογραφής.
(2) Εξηγήστε γιατί δεν είναι δυνατό να πιστοποιηθεί η υπογραφή του τρίτου σχήματος.
(3) Περιγράψτε τη δική σας παραλλαγή του σχήματος του ElGamal.