# Κρυπτογράφηση ElGamal – Πρωτόκολλα Μηδενικής Γνώσης

1. Εξετάστε τι συμβαίνει αν πολλαπλασιάσουμε κατά συντεταγμένη δύο κρυπτοκείμενα ElGamal ως προς το ίδιο δημόσιο κλειδί.

2. Δίνονται οι παράμετροι: $g \equiv 2 \mod 23, \mathbb{G} = \mathbb{Z}_{23}^* \cap \langle g \rangle, q = 11$. Ακολουθήστε τη διαδικασία κατασκευής ζευγους κλειδιών και κατασκευάστε ένα ζεύγος $x, h$. Κρυπτογραφήστε το μήνυμα $m \equiv 6 \mod 23$ με randomness της επιλογής[1] σας, και κατόπιν αποκρυπτογραφήστε το.

3. Τι συμβαίνει αν στο κρυπτοσύστημα ElGamal επιλέξουμε ως $\mathbb{G}$ ομάδα σύνθετης τάξης, συγκεκριμμένα το $\mathbb{Z}_p^*$. Δώστε παράδειγμα με βάση το $\mathbb{Z}_{23}^*$, $g \equiv 5, q = 22$.

4. Η Μάρτζερι και η Εύα εκτελούν ένα Σ-πρωτόκολλο (δηλ. ένα πρωτόκολλο 3 κινήσεων (έστω $a, c, s$) με πληρότητα, ειδική εγκυρότητα και HVZK). Η Εύα είναι ο Verifier. Κατά το τέλος τη εκτέλεσης η Εύα ισχυρίζεται ότι ο υπολογιστής της λόγω διακοπής ρεύματος έσβυσε, χάνοντας τα μηνύματα $c, s$, οπότε ζητάει από την Μάρτζερι να συνεχίσουν την εκτέλεση από αυτό το σημείο. Έχοντας χάσει την τιμή του $c$, θα στείλει νέα τιμή $c'$. Η Μάρτζερι προτείνει, για οικονομία, να στείλει εκείνη στην Εύα την χαμένη τιμή του $c$ μαζί με την απάντηση $s$. Ποιά από τις αντισυμβαλλόμενες έχει δίκιο;

5. Βασιζόμενοι στο πρωτόκολλο του Schnorr, διατυπώστε ένα Σ-πρωτόκολλο που αποδεικνύει την ισότητα δύο διακριτών λογαρίθμων (δηλ. ο λογάριθμός του $h_1$ ως προς το $g_1$ είναι ίδιος με το λογάριθμο του $h_2$ ως προς το $g_2$). Επιβεβαιώστε ότι είναι πλήρες, ειδικά έγκυρο και HVZK.

6. Αξιολογήστε την εγκυρότητα (όχι την ειδική εγκυρότητα) του παραπάνω πρωτοκόλου σε σχέση με αυτό του Schnorr.

7. Εξηγήστε πως μπορούμε να δείξουμε ότι ένα κρυπτογραφημένο μήνυμα $c = \langle u, v \rangle$ με ElGamal περιέχει ως μήνυμα είτε την τιμή $m_1$ είτε την τιμή $m_2$, χωρίς να δώσουμε άλλη πληροφορία για αυτό.

[1] Τετριμμένες επιλογές αναιρούν το νόημα της άσκησης.