Υπογραφές, RSA και ElGamal

1. Η Καρολίνα λαμβάνει το παρακάτω μήνυμα, μαζί με μία σωστή ηλεκτρονικη υπογραφή ως προς το κλειδί του Λυκούργου PK_Λ «Παραβίασαν τον υπολογιστή μου, παρακαλώ μην εμπιστεύεσαι πλέον αυτό το κλειδί, και ειδοποίησε όσους μπορεις». Θα πρέπει να πιστέψει το μήνυμα η Καρολίνα;

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

3. 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.

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

5. Εξηγήστε επιγραμματικά γιατί στο RSA μπορούμε να χρησιμοποιήσουμε (ουσιαστικά) ομάδα σύνθετης τάξης.

6. Εάν μια συνάρτηση κατακερματισμού είναι ανθεκτική σε συγκρούσεις, είναι απαραίτητα και μονόδρομη;

7. Εάν γενικεύσουμε σε συναρτήσεις που είναι εύκολες στον υπολογισμό και τη δειγματοληψία, ισχύει ότι η αντοχή σε συγκρούσεις συνεπάγεται οτι η συνάρτηση είναι μονόδρομη;

[1] Τετριμμένες επιλογές αναιρούν το νόημα της άσκησης.