

Key Exchange, ElGamal

1. Δίνεται το παρακάτω σχήμα ανταλλαγής κλειδιού¹:

(α') Η Αλίκη επιλέγει τυχαία $k, r \leftarrow \{0, 1\}^n$ και στέλνει στο Βασίλη την τιμή $s := k \oplus r$.

(β') Ο Βασίλης επιλέγει τυχαίο $t \leftarrow \{0, 1\}^n$ και στέλνει στην Αλίκη $u := s \oplus t$.

(γ') Η Αλίκη υπολογίζει την τιμή $w := u \oplus r$ και τη στέλνει στο Βασίλη.

(δ') Η Αλίκη χρησιμοποιεί την τιμή k και ο Βασίλης την τιμή $w \oplus t$.

Να εξετάσετε το παραπάνω σχήμα ως προς την ορθότητα και την ασφάλεια.

2. **[Λύθηκε στην τάξη]** Εξετάστε τι συμβαίνει αν πολλαπλασιάσουμε κατά συντεταγμένη δύο κρυπτοκείμενα ElGamal ως προς το ίδιο δημόσιο κλειδί.
3. Δίνεται ένα κρυπτομήνυμα ElGamal $c = (U, V) \in \mathbb{G}^2$, οι παράμετροι (\mathbb{G}, g, q) της αντίστοιχης ομάδας, και ένα δημόσιο κλειδί $h := g^x$ (το x καθαυτό δεν δίνεται). Περιγράψτε πως μπορούμε να κατακευάσουμε ένα κρυπτομήνυμα $c' \neq c$ με την ιδιότητα $\text{Dec}_x c' = \text{Dec}_x c$.
4. Δίνονται οι παράμετροι: $g \equiv 2 \pmod{23}$, $\mathbb{G} = \mathbb{Z}_{23}^* \cap \langle g \rangle$, $q = 11$. Ακολουθήστε τη διαδικασία κατασκευής ζευγους κλειδιών και κατασκευάστε ένα ζεύγος x, h . Κρυπτογραφήστε το μήνυμα $m \equiv 6 \pmod{23}$ με randomness της επιλογής² σας, και κατόπιν αποκρυπτογραφήστε το.
5. Τι συμβαίνει αν στο κρυπτοσύστημα ElGamal επιλέξουμε ως \mathbb{G} ομάδα σύνθετης τάξης, συγκεκριμένα το \mathbb{Z}_p^* . Δώστε παράδειγμα με βάση το \mathbb{Z}_{23}^* , $g \equiv 5$, $q = 22$.
6. Έστω ένα σχήμα κρυπτογράφησης (Kgen, Enc, Dec), με χώρο μηνυμάτων \mathcal{M} , ασφαλές ως προς IND-CPA. Κατασκευάστε ένα σχήμα κρυπτογράφησης με χώρο μηνυμάτων $\mathcal{M}' := \mathcal{M}^2$. Μπορείτε να είστε σύντομοι στην κατασκευή και την ορθότητα, περιγράψτε όμως αναλυτικά την απόδειξη της ασφαλείας του.

¹Άσκηση 9.3 (1η έκδοση)/ 10.4 (2η έκδοση) από το Katz & Lindell

²Τετριμμένες επιλογές αναιρούν το νόημα της άσκησης.