

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.

Λύση Η ορθότητα ισχύει με έλεγχο των πράξεων. Δεν είναι όμως ασφαλές. Υπολογίστε το $s \oplus u \oplus w$.

2. [Λύθηκε στην τάξη] Εξετάστε τι συμβαίνει αν πολλαπλασιάσουμε κατά συντεταγμένη δύο κρυπτοκειμένα ElGamal ως προς το ίδιο δημόσιο κλειδί.

Λύση Έστω $c_1 = (g^{r_1}, m_1 h^{r_1})$ και $c_2 = (g^{r_2}, m_2 h^{r_2})$. Το αποτέλεσμα της πράξης $c_1 \odot c_2$ θα είναι $c^* = (g^{r_1+r_2}, m_1 m_2 h^{r_1+r_2})$. Ξαναγράφουμε το $r_1 + r_2$ ως r^* και το $m_1 m_2$ ως m^* . Τελικά έχουμε $c_1 \odot c_2 := c^* = (g^{r^*}, m^* h^{r^*})$, δηλαδή η κρυπτογράφηση του $m^* = m_1 m_2$ με τυχαιότητα $r^* = r_1 + r_2$. Άρα, ο πολλαπλασιασμός κατά συντεταγμένη δύο κρυπτοκειμένων ElGamal είναι ομοιομορφισμός (ως προς την πρόσθεση $\bmod q$ για τις τυχαίες τιμές και ως προς την πράξη της ομάδας για τα μηνύματα).

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: $g \equiv 2 \bmod 23, \mathbb{G} = \mathbb{Z}_{23}^* \cap \langle g \rangle, q = 11$. Ακολουθήστε τη διαδικασία κατασκευής ζευγους κλειδιών και κατασκευάστε ένα ζεύγος x, h . Κρυπτογραφήστε το μήνυμα $m \equiv 6 \bmod 23$ με randomness της επιλογής² σας, και κατόπιν αποκρυπτογραφήστε το.

Παράδειγμα

Δημιουργία κλειδιού. Επιλέγουμε ένα x ως ιδιωτικό κλειδί από το \mathbb{Z}_q , πχ $x = 3$. Υπολογίζουμε το δημόσιο κλειδί ως $h = g^x$, οπότε έχουμε $h \equiv 2^3 \equiv 8 \bmod 23$.

Κρυπτογράφηση. Μας έχει δοθεί το μήνυμα $m = 6 \bmod 23$ το οποίο είναι στοιχείο της ομάδας. Επιλέγουμε ένα r ως τυχαίο παράγοντα από το \mathbb{Z}_q , πχ $r = 7$. Υπολογίζουμε τα U, V ως $U = g^r$ και $V = h^r$.

Για το U έχουμε: $U \equiv 2^7 \equiv 128 \equiv 128 - 115 \equiv 13 \bmod 23$.

Για το V έχουμε $V \equiv 6 \cdot 8^7 \equiv 6 \cdot 64 \cdot 64 \cdot 64 \cdot 8 \bmod 23$. Όμως, $64 \equiv 64 - 69 \equiv -5 \bmod 23$. Οπότε $V \equiv 6 \cdot -5 \cdot -5 \cdot -5 \cdot 8 \equiv 6 \cdot 25 \cdot -40 \equiv 6 \cdot 2 \cdot (46 - 40) \equiv 72 \equiv 72 - 69 \equiv 3 \bmod 23$.

Άρα $c = (U, V) = (13, 3)$.

Αποκρυπτογράφηση. Γνωρίζουμε ότι $x = 3$ και $c = (U, V) = (13, 3)$. Υπολογίζουμε το $\tilde{m} = U^{-x} \cdot V$. Έχουμε: $U^{-x} \cdot V = 13^{-3} \cdot 3 \equiv 13^{-3} \cdot 3 \equiv 13^8 \cdot 3 \bmod 23$. Στον εκθέτη το -3 είναι ισοδύναμο με το 8 αφού η τάξη της ομάδας είναι $q = 11$. Επίσης, παρατηρούμε ότι $13 \equiv -10 \bmod 23$. Έχουμε λοιπόν $\tilde{m} \equiv (-10)^8 \cdot 3 \equiv 100 \cdot 100 \cdot 100 \cdot 100 \cdot 3 \equiv (100 - 92) \cdot (100 - 92) \cdot (100 - 92) \cdot (100 - 92) \cdot 3 \equiv 8 \cdot 8 \cdot 8 \cdot 8 \cdot 3 \equiv 64 \cdot 64 \cdot 3 \equiv (-5) \cdot (-5) \cdot 3 \equiv 25 \cdot 3 \equiv 2 \cdot 3 \equiv 6 \bmod 23$.

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

²Τετριμμένες επιλογές αναιρούν το νόημα της άσκησης.

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

Σκιαγράφηση Έχουμε συναντήσει αντίστοιχα παραδείγματα τόσο στο σύστημα του Pedersen όσο και στο Diffie-Hellman. Επειδή η τάξη της ομάδας είναι σύνθετος αριθμός ($22 = 2 \cdot 11$) μπορούμε να υψώσουμε στοιχεία της ομάδας στην 11η ώστε να προκύψουν στοιχεία τάξης το πολύ 2. Συγκεκριμένα, για οποιοδήποτε $a \in \mathbb{G}$ και $b = a^{11}$ έχουμε $(b)^2 \equiv 1$. Με έλεγχο μπορούμε να δούμε ότι $b \equiv \pm 1$. Οπότε, μπορούμε να ορίσουμε ένα «πρόσημο» για κάθε στοιχείο ανάλογα με το αν υψωμένο στην 11 είναι $+1$ ή -1 . Σαν συνέπεια, αν στο πείραμα της ασφάλειας IND-CPA δώσουμε m_0, m_1 με διαφορετικό «πρόσημο», είμαστε τελικά σε θέση να ξεχωρίσουμε ποιό από τα δύο κρυπτογραφήθηκε.

6. Έστω ένα σχήμα κρυπτογράφησης ($K_{\text{gen}}, \text{Enc}, \text{Dec}$), 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.