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;

   Λύση Ναι. Αν το μήνυμα πράγματι προέρχεται από τον Λυκούργο, θα πρέπει να σταματήσει να εμπιστεύεται το αντίστοιχο κλειδί. Εάν το μήνυμα προέρχεται από κάποιο τρίτο χρήστη, αυτό σημαίνει ότι είτε το ιδιωτικό κλειδί του Λυκούργου διέρευσε (άρα πρέπει να μην εμπιστευόμαστε το αντίστοιχο δημόσιο) ή ότι υπάρχει μια γενικότερη επίθεση στο σχήμα υπογραφών.

2. Εξετάστε τι συμβαίνει αν πολλαπλασιάσουμε κατά συντεταγμένη δύο κρυπτοκείμενα 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 $\mod q$ για τις τυχαίες τιμές και ως προς την πράξη της ομάδας για τα μηνύματα).

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.

   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 $h \equiv 2^3 \equiv 8 \mod 23$.

   Κρυπτογράφηση. Μας έχει δωθεί το μήνυμα $m = 6 \mod 23$ 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: $U \equiv 2^7 \equiv 128 \equiv 128 - 115 \equiv 13 \mod 23$.

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

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

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

   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. Συγκεκριμμένα, για οποιοδήποτε $a \in \mathbb{G}$ και $b = a^1 1$ 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] Τετριμμένες επιλογές αναιρούν το νόημα της άσκησης.

$+1$ 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.

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

   Δεν το καλύψαμε το 2020.

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

   Λύση Ναι, υπό συνθήκες. Συγκεκριμένα, πρέπει να ενισχύσουμε την ιδιότητα της συμπίεσης. Αρχικά θα υποθέσουμε ότι η συνάρτηση συμπιέζει κατά τουλάχιστον ένα bit, δηλαδή αντιστοιχίζει $2n$ ορίσματα σε (το πολύ) n διαφορετικές εικόνες. Με αυτή την (ισχυρότερη) υπόθεση, μπορούμε να κάνουμε την εξής παρατήρηση: τουλάχιστον n από τα πιθανά ορίσματα της συνάρτησης δεν έχουν μοναδική εικόνα (δηλαδή «μοιράζονται» την εικόνα τους με τουλάχιστον ένα άλλο στοιχείο). Πράγματι, έστω ότι το παραπάνω δεν ισχύει. Αυτό σημαίνει ότι υπάρχουν τουλάχιστον $2n - n = n$ ορίσματα τα οποία έχουν μοναδική εικόνα. Όμως, το σύνολο των διαφορετικών εικόνων έχει μέγεθος το πολύ n στοιχεία, άρα τα υπόλοιπα στοιχεία του πεδίου ορισμού δεν μπορούν να πάρουν εικόνα, άτοπο.

   Μετά την παραπάνω παρατήρηση, μπορούμε πλέον να δείξουμε ότι αν υπάρχει αντίπαλος $\mathcal{A}$ που αντιστρέφει την συνάρτηση με καλή πιθανότητα έστω a, τότε μπορούμε με αντίστοιχα καλή πιθανότητα να παράξουμε σύγκρουση. Για να παράξουμε σύγκρουση εργαζόμαστε ως εξής: επιλέγουμε ένα τυχαίο στοιχείο x από το D και υπολογίζουμε την εικόνα του y. Δίνουμε το y στον αλγόριθμο $\mathcal{A}$ που μας επιστρέφει x'. Η απαντησή μας είναι x, x'.

   Για να ολοκληρώσουμε την απόδειξη πρέπει να υπολογίσουμε την πιθανότητα επιτυχίας της παραπάνω διαδικασίας. Από την παραπάνω παρατήρηση, με πιθανότητα τουλάχιστον $1/2$ το x είναι στοιχείο τέτοιο όπου το y έχει $n_y \geq 1$ αντίστροφες εικόνες. Οπότε εάν ο $\mathcal{A}$ επιτύχει (με πιθανότητα a), τότε με πιθανότητα $\frac{n_y - 1}{n_y} \geq \frac{1}{2}$ το x' θα είναι πράγματι μια αντίστροφη εικόνα του y διαφορετική από το x. Συνολικά η πιθανότητα επιτυχίας είναι τουλάχιστον $\frac{a}{4}$.

   Η ίδια απόδειξη δουλεύει όσο η διαφορά μεγέθους R_i και D_i είναι σημαντική. Σε ακραίες περιπτώσεις, που δεν εμφανίζονται στην πράξη, (πχ από 2^λ στοιχεία σε $2^\lambda - 1$) είναι δυνατό τα στοιχεία που δεν έχουν μοναδική εικόνα να είναι αμελητέο κλάσμα του R_i και άρα η τελική πιθανότητα επιτυχίας να είναι και αυτή αμελητέα.

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;

   Λύση Όχι. Παράδειγμα η ταυτοτική συνάρτηση. Είναι εξ'ορισμού ανθεκτική σε συγκρούσεις αλλά προφανώς όχι μονόδρομη.