Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Υπολογιστική Κρυπτογραφία
5η Σειρά Ασκήσεων

Προθεσμία παράδοσης: 28/1/2018

30 Δεκεμβρίου 2017

1η Άσκηση

Έστω ένα κρυπτοσύστημα δημοσίου κλειδιού με δημόσιο κλειδί $pk = \langle n, e\rangle$ και ιδιωτικό κλειδί $sk = \langle p, q, d\rangle$ (όπως στο RSA). Η συνάρτηση κρυπτογράφησης $Enc(M) = \langle r^e \mod n, r \oplus M\rangle$ δέχεται ως είσοδο ένα μήνυμα $M \in \mathbb{Z}_n$ και το κρυπτογραφεί χρησιμοποιώντας ένα τυχαίο $r \in \mathbb{Z}_n$.

- Βρείτε τη συνάρτηση αποκρυπτογράφησης.
- Είναι το κρυπτοσύστημα αυτό IND-CPA ασφαλές;

2η Άσκηση

Σταθερό σημείο ενός κρυπτοσυστήματος ονομάζουμε ένα μήνυμα που το κρυπτοκείμενό του είναι το ίδιο το μήνυμα, δηλαδή $enc(m) = m$. Στην περίπτωση του RSA, αν το δημόσιο κλειδί είναι το (N, e), τότε για ένα σταθερό σημείο ισχύει $m^e \equiv m \pmod N$. Αποδείξτε ότι το πλήθος των σταθερών σημείων στο RSA είναι $[gcd(e-1, p-1)+1][gcd(e-1, q-1)+1]$.

3η Άσκηση

Έστω το παρακάτω σχήμα υπογραφών όπου για τις παραμέτρους ισχύει ό,τι στο ElGamal. Κάθε χρήστης έχει ιδιωτικό κλειδί x και δημόσιο $y = g^x \bmod p$. Η υπογραφή λειτουργεί ως εξής:

i. Ο υπογράφων αρχικά επιλέγει $h \in \{0, \cdots, p-1\}$ ώστε: $\mathcal{H}(m) + x + h = 0 \pmod p$, όπου $\mathcal{H}$ κατάλληλη συνάρτηση σύνοψης.

ii. Η υπογραφή είναι η τριάδα: $sign(x, m) = (m, (x+h) \bmod p, g^h \bmod p)$

iii. Για την επαλήθευση ότι μια τριάδα (m, a, b) είναι έγκυρη υπογραφή ελέγχεται ότι:

- $yb = g^a$ και
- $g^{\mathcal{H}(m)} yb = 1$

Να δείξετε ότι το σχήμα αυτό δεν προστατεύει από επίθεση καθολικής πλαστογράφησης.

4η Άσκηση

Έστω το παρακάτω πρωτόκολλο μηδενικής γνώσης. Οι δημόσιες παράμετροι είναι όπως στο πρωτόκολλο του Schnorr $\langle p, q, g, h\rangle$ και ο prover γνωρίζει ένα x τέτοιο ώστε $g^x = h \bmod p$.

- Ο prover επιλέγει τυχαία ένα $t \in \mathbb{Z}_q^*$ και στέλνει στον verifier το $y = g^t \bmod p$.
- Ο verifier επιλέγει τυχαία $c \in \mathbb{Z}_q^*$ και το στέλνει στον prover.
- Ο prover υπολογίζει το $s = t + c + x \bmod q$ και το στέλνει στον verifier.
- Ο verifier αποδέχεται αν και μόνο αν $g^s = yg^c h \pmod p$.

Να εξετάσετε ότι το παραπάνω είναι Σ-πρωτόκολλο. *Για την ιδιότητα HVZK η απόδειξη πρέπει να είναι στο επίπεδο ανάλυσης των διαφανειών, αλλά να φαίνονται αναλυτικά τα transcripts του πρωτοκόλλου και η πιθανότητα εμφάνισής τους.*

5η Άσκηση

Έστω h συνάρτηση κατακερματισμού, η οποία συμπιέζει ακολουθίες μήκους $2n$ σε ακολουθίες μήκους n και έχει την ιδιότητα δυσκολίας εύρεσης συγκρούσεων (collision free). Θέλουμε να φτιάξουμε μία συνάρτηση κατακερματισμού που να συμπιέζει ακολουθίες μήκους $4n$ σε ακολουθίες μήκους n, η οποία να έχει επίσης την ιδιότητα δυσκολίας εύρεσης συγκρούσεων. Έχουμε τις εξής υποψήφιες:

1. $h_1(x) = h((x_1 \oplus x_2)||(x_3 \oplus x_4))$
2. $h_2(x) = h(h(x_1||x_2)||h(x_3||x_4))$
3. $h_3(x) = h(x_1||x_2) \oplus h(x_3||x_4)$
4. $h_4(x) = h(h(h(x_1||x_2)||x_3)||x_4)$

(Με "$\oplus$" συμβολίζουμε το XOR, με "||" την παράθεση και $|x_i| = n$.) Για κάθε i εξετάστε αν η h_i έχει την ιδιότητα δυσκολίας εύρεσης συγκρούσεων ή όχι. *Για να δείξετε ότι την έχει, δείξτε ότι αν μπορούσαμε να βρούμε συγκρούσεις για την h_i , τότε θα μπορούσαμε να βρούμε συγκρούσεις και για την h. Για να δείξετε το αντίθετο βρείτε μία ή περισσότερες συγκρούσεις για την h_i.*