Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Υπολογιστική Κρυπτογραφία

(ΣΗΜΜΥ, ΣΕΜΦΕ, ΑΛΜΑ, ΕΜΕ)

3η Σειρά Ασκήσεων

Προθεσμία παράδοσης 22/12/2018

Άσκηση 1.

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 $[\gcd(e-1, p-1) + 1][\gcd(e-1, q-1) + 1]$.

Άσκηση 2.

΄Εστω 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 $h \in \{0, \ldots, p-1\}$ ώστε: $\mathcal{H}(m)+x+h \equiv 0 \pmod p$, 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 εάν:
• $y^b \equiv g^a \pmod p$ και
• $g^{\mathcal{H}(m)} y^b \equiv 1 \pmod p$.

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

Άσκηση 3.

Δίνεται το παρακάτω πρωτόκολλο μεταξύ ενός prover $\mathcal{P}$ και ενός verifier $\mathcal{V}$ το οποίο έχει στόχο την απόδειξη γνώσης του μηνύματος που αντιστοιχεί σε ένα δεδομένο κρυπτοκείμενο RSA με δημόσιο κλειδί (e, n), δηλαδή $m \in \mathbb{Z}_n^*$ τέτοιο ώστε $y = m^e \bmod n$. Επιπλέον θεωρήστε ότι e πρώτος.

- Ο $\mathcal{P}$ επιλέγει τυχαία ένα $t \in \mathbb{Z}_n^*$ και στέλνει στον $\mathcal{V}$ το $h = t^e \bmod n$.
- Ο $\mathcal{V}$ επιλέγει ένα τυχαίο c, $c \in \{0, \ldots, e-1\}$, και το στέλνει στον $\mathcal{P}$.

- Ο $\mathcal{P}$ υπολογίζει το $r = tm^c \bmod n$ και το στέλνει στον $\mathcal{V}$.
- Ο $\mathcal{V}$ αποδέχεται αν και μόνο αν $r^e \equiv hy^c \pmod{n}$.

Να αποδείξετε ότι το παραπάνω είναι Σ-πρωτόκολλο. Για την ιδιότητα HVZK η απόδειξη πρέπει να είναι στο επίπεδο ανάλυσης που ακολουθήθηκε στις διαφάνειες, αλλά να φαίνονται αναλυτικά τα transcripts του πρωτοκόλλου και η πιθανότητα εμφάνισής τους.

Άσκηση 4.

Να υλοποιήσετε σε γλώσσα προγραμματισμού της επιλογής σας την επίθεση αποκρυπτογράφησης ενός κρυπτοκειμένου c σε RSA που χρησιμοποιεί ένα oracle το οποίο μπορεί να αποφανθεί αν το μήνυμα που αντιστοιχεί στο κρυπτοκείμενο είναι στο 'πάνω' ή στο 'κάτω' μισό του $\mathbb{Z}_n$ (δηλ. συνάρτηση loc - βλ. διάλεξη RSA - διαφάνειες 36, 40).

Συγκεκριμένα πρέπει να υλοποιήσετε 2 προγράμματα:

(1) Το πρώτο θα 'προσομοιώνει' το oracle, αποκρυπτογραφώντας (κανονικά με το ιδιωτικό κλειδί) το c και υπολογίζοντας την loc.

(2) Το δεύτερο θα υλοποιεί την επίθεση ρωτώντας επαναληπτικά το oracle κατάλληλες ερωτήσεις για την loc.

Για την επικοινωνία των προγραμμάτων μπορείτε να χρησιμοποιήσετε οποιαδήποτε μορφή interprocess communication (RPC) γνωρίζετε, ή ακόμα και απλούστερη επικοινωνία μέσω ενός αρχείου. Η παραγωγή των κλειδιών και η αρχική κρυπτογράφηση μπορεί να γίνει από δικό σας κώδικα ή χρησιμοποιώντας ένα έτοιμο εργαλείο όπως το Openssl.

Άσκηση 5.

Έστω το παρακάτω σχήμα MAC για μηνύματα μήκους $2n-2$ με χρήση μιας ψευδοτυχαίας συνάρτησης F: Με είσοδο το μήνυμα $m_0||m_1$ (όπου $|m_0| = |m_1| = n-1$) και κλειδί $k \in \{0,1\}^n$, ο αλγόριθμος MAC δίνει $t = F_k(0||m_0)||F_k(1||m_1)$. (όπου $F : \{0,1\}^n \mapsto \{0,1\}^n$)

(α) Ορίστε τον αλγόριθμο Vrfy.

(β) Είναι αυτό το σχήμα ασφαλές; Επιχειρηματολογήστε για τον ισχυρισμό σας.