Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Υπολογιστική Κρυπτογραφία

(ΣΗΜΜΥ-ΣΕΜΦΕ-ΜΠΛΑ)

4η Σειρά Ασκήσεων

Προθεσμία παράδοσης: 16/1/2017

Άσκηση 1. Ο διευθυντής μιας εταιρείας χρειάζεται να παίρνει συχνά κρυπτογραφημένα μηνύματα από τους υπαλλήλους του. Για το σκοπό αυτό χρησιμοποιεί RSA, δίνοντας σε όλους το δημόσιο κλειδί του $\langle n, e\rangle$ όπου $n = pq$ με p, q πρώτους. Φυσικά κρατάει κρυφούς τους πρώτους p, q. Για ευκολία, δίνει επιπλέον στη γραμματέα του μία συσκευή με την οποία θα μπορούν οι υπάλληλοι που δεν διαθέτουν το πρόγραμμα κρυπτογράφησης να κρυπτογραφούν τα μηνύματά τους.
Η συσκευή θα λειτουργεί ως εξής για είσοδο m:

- Υπολογίζει $c_p = m^e \mod p$
- Υπολοίζει $c_q = m^e \mod q$
- Συνδυάζει τις λύσεις με CRT ώστε να δώσει ως έξοδο τη μοναδική τιμή $c \in \mathbb{Z}_n$ τ.ω $c \equiv m^e \mod n$

Λόγω ενός εργοστασιακού λάθους, στο δεύτερο βήμα, η συσκευή υπολογίζει $c'_q = 2m^e \mod q$ και δίνει έξοδο $c' \in \mathbb{Z}_n$ τ.ω $c' \equiv c_p \mod p, c' \equiv c'_q \mod q$ Όπως είναι φυσικό, ο διευθυντής σύντομα διαπιστώνει ότι κάτι δεν πάει καλά (με ποιον τρόπο?) και ζητάει από τη γραμματέα του να στείλει τη συσκευή για επισκευή. Η γραμματέας, όμως, που έχει παρακολουθήσει προσεκτικά το μάθημα της κρυπτογραφίας, κατορθώνει, πριν στείλει τη συσκευή στο service να βρει το ιδιωτικό κλειδί του διευθυντή. Πώς το κατάφερε αυτό?

Άσκηση 2. Έστω ένα κρυπτοσύστημα δημοσίου κλειδιού με δημόσιο κλειδί $pk =< n, e >$ και ιδιωτικό κλειδί $sk =< p, q, d >$ (όπως στο RSA). Η συνάρτηση κρυπτογράφησης $Enc(M) =< r^e \mod n, r \oplus M >$ 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?

Άσκηση 3. Θεωρήστε την παραλλαγή του σχήματος υπογραφής ElGamal όπου η μόνη διαφορά βρίσκεται στον υπολογισμό του s:

$$s = (m - kr)x^{-1} \mod p - 1$$

1. Περιγράψτε τη συνάρτηση επαλήθευσης της υπογραφής για το μήνυμα m
2. Υπάρχει κάποιο υπολογιστικό πλεονέκτημα του τροποποιημένου σχήματος έναντι του αρχικού?
3. Συγκρίνετε την ασφάλεια του αρχικού και του τροποποιημένου σχήματος.

Άσκηση 4. Έστω το παρακάτω σχήμα υπογραφών όπου για τις παραμέτρους ισχύει ό,τι στο ElGamal. Κάθε χρήστης έχει ιδιωτικό κλειδί x και δημόσιο $y = g^x \mod p$. Η υπογραφή λειτουργεί ως εξής:
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.
Η υπογραφή είναι η τριάδα:
$sign(x, m) = (m, (x + h) \mod p, g^h \mod p)$
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 υπαρξιακής πλαστογράφησης.

Άσκηση 5. 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 $y = m^e \mod n$. Επιπλέον θεωρείστε ότι e πρώτος.

- Ο $\mathcal{P}$ επιλέγει τυχαία ένα $t \in \mathbb{Z}_n^*$ και στέλνει στον $\mathcal{V}$ το $h = t^e \mod n$.
- Ο $\mathcal{V}$ επιλέγει ένα τυχαίο $c \in \{0 \cdots e-1\}$ και το στέλνει στον $\mathcal{P}$.
- Ο $\mathcal{P}$ υπολογίζει το $r = tm^c \mod n$ και το στέλνει στον $\mathcal{V}$.
- Ο $\mathcal{V}$ αποδέχεται αν και μόνο αν $r^e = hy^c \pmod n$.

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.

Άσκηση 6. Έστω το παρακάτω πρωτόκολλο μηδενικής γνώσης. Οι δημόσιες παράμετροι είναι όπως στο πρωτόκολλο του Schnorr $< p, q, g, h >$ και ο prover γνωρίζει ένα x τέτοιο ώστε $g^x = h \mod p$.

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

Άσκηση 7. Να δώσετε τις **μη-διαλογικές αποδείξεις** χρησιμοποιώντας την τεχνική Fiat Shamir για τις αποδείξεις:

- Ορθής αποκρυπτογράφησης στο πρωτόκολλο CGS97 (βλ. διαφάνεια 19, διάλεξη 20.12.2016)
- Εγκυρότητας αρνητικής ψήφου στο πρωτόκολλο CGS97 (βλ. διαφάνεια 20, διάλεξη 20.12.2016)
- Ορθού reencryption στο απλό mixnet (βλ. διαφάνεια 30, διάλεξη 20.12.2016)

Συμβουλή: (α) προσπαθήστε μόνοι σας, (β) συζητήστε με συμφοιτητές σας, (γ) αναζητήστε ιδέες στο διαδίκτυο, με αυτή τη σειρά και αφού αφιερώσετε αρκετό χρόνο σε κάθε στάδιο! Σε κάθε περίπτωση οι απαντήσεις πρέπει να είναι *αυστηρά ατομικές*.