Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Υπολογιστική Κρυπτογραφία

(ΣΗΜΜΥ, ΣΕΜΦΕ, ΑΛΜΑ, ΕΜΕ, ΜΠ)

3η Σειρά Ασκήσεων

Προθεσμία παράδοσης: Ημέρα & ώρα εξέτασης μαθήματος

Άσκηση 1. Να δείξετε ότι το πρόβλημα RSA είναι random self-reducible.

Άσκηση 2. Έστω μια κυκλική ομάδα $\mathbb{G}$ με τάξη πρώτο q και γεννήτορα g.

1. Ορίζουμε το Τετραγωνικό πρόβλημα Diffie - Hellman (SDH) ως εξής:
   Δίνονται $g, g^x \in \mathbb{G}$. Να υπολογιστεί το g^{x^2}.
2. Ορίζουμε το πρόβλημα Diffie - Hellman Αντιστρόφου (IDH) ως εξής:
   Δίνονται $g, g^x \in \mathbb{G}$. Να υπολογιστεί το $g^{x^{-1}}$.

Να αποδείξετε ότι τα παραπάνω προβλήματα είναι ισοδύναμα τόσο μεταξύ τους, όσο και με το υπολογιστικό πρόβλημα Diffie - Hellman (CDH).

Άσκηση 3. 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. διαφάνειες RSA).

Συγκεκριμένα πρέπει να υλοποιήσετε 2 τμήματα κώδικα:
(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 ή

εσωτερικά στο πρόγραμμα με κατάλληλη κλήση συνάρτησης. Η παραγωγή των κλειδιών και η αρχική κρυπτογράφηση μπορεί να γίνει από δικό σας κώδικα ή χρησιμοποιώντας ένα έτοιμο εργαλείο όπως το Openssl.

Άσκηση 4. Έστω το κρυπτοσύστημα RSA με $n = pq$, e δημόσιο κλειδί και d, p, q ιδιωτικό κλειδί. Έστω ένας αριθμός $c = m^e \pmod{n}$. Ένας RSA-κύκλος για το c

$$c, c^e, c^{e^2}, \ldots, c^{e^t} = c$$

είναι μια σειρά από τιμές το $t > 0$ είναι το μήκος του RSA κύκλου.

1. Δείξτε ότι αν βρεθεί ένας RSA-κύκλος τότε είναι εύκολο να βρεθεί το m.
2. Υπάρχει RSA-κύκλος για κάθε c; Επιχειρηματολογήστε.
3. Δείξτε ότι για όλα τα c για τα οποία υπάρχει RSA-κύκλος το μήκος του RSA-κύκλου δέχεται ένα άνω φράγμα που εκφράζεται σα συναρτηση του n (ανεξάρτητα από το c).
4. Το γεγονός ότι θεωρούμε την RSA συνάρτηση κρυπτογράφησης δύσκολη να αντιστραφεί σημαίνει κάτι σχετικά με τους RSA-κύκλους;

Άσκηση 5. Στη διάλεξη για τα κρυπτοσυστήματα του Διακριτού Λογαρίθμου (DL) είδαμε ότι η διαρροή του parity του DL μέσω του συμβόλου Legendre μπορεί να επιτρέψει την κατασκευή αποδοτικού διαχωριστή για τριάδες Diffie-Hellman και κατά συνέπεια την επίλυση του προβλήματος DDH στην $\mathbb{Z}_p^*$. Μπορεί η συγκεκριμένη διαρροή να οδηγήσει σε αποκάλυψη ολόκληρου του διακριτού λογαρίθμου στην $\mathbb{Z}_p^*$; Να τεκμηριώσετε την απάντησή σας.

Άσκηση 6. Δίνεται η παρακάτω παραλλαγή του πρωτοκόλλου ElGamal το οποίο λειτουργεί σε μια ομάδα $\mathbb{G}$ με τάξη πρώτο q και γεννήτορες g, h:

- $\mathsf{KGen}(\lambda) \to (\mathsf{sk}, \mathsf{pk}) = (x, g^x)$ όπου $x \leftarrow\$ \mathbb{Z}_q^*$
- $\mathsf{Enc}(\mathsf{pk}, m) \to (\mathsf{pk}^r, g^r h^m)$ όπου $r \leftarrow\$ \mathbb{Z}_q^*$

1. Να ορίσετε την συνάρτηση της αποκρυπτογράφησης $\mathsf{Dec}(\mathsf{sk}, m)$ και να αποδείξετε την ορθότητά της.
2. Να μελετήσετε την ασφάλεια της παραλλαγής ως προς τις ιδιότητες OW-CPA, IND-CPA, IND-CCA.

Να υποθέσετε ότι η διαδικασία παραγωγής των παραμέτρων έχει γίνει έντιμα (δηλαδή ότι g, h είναι ομοιόμορφα επιλεγμένοι γεννήτορες με άγνωστους τους μεταξύ τους διακριτούς λογαρίθμους).

Άσκηση 7. Δίνεται μια ομάδα $\mathbb{G}$ με τάξη q πρώτο όπου το πρόβλημα απόφασης Diffie - Hellman είναι δύσκολο. Έστω g, h γεννήτορες της $\mathbb{G}$ τέτοιοι ώστε να είναι άγνωστοι οι διακριτοί λογάριθμοι $\log_g h$ και $\log_h g$. Σε αυτή την ομάδα ορίζουμε το σχήμα δέσμευσης του Pedersen με αλγόριθμο δέσμευσης $\mathsf{Commit}(m, r) = c = g^m h^r$ με $m, r \in \mathbb{Z}_q^*$.
Θεωρήστε το παρακάτω πρωτόκολλο Π με δημόσια είσοδο $\langle \mathbb{G}, g, h, q, c \rangle$ που αποδεικνύει ότι ο prover γνωρίζει m, r ώστε $c = g^m h^r$:

- Ο prover επιλέγει ομοιόμορφα ένα $t_1, t_2 \in \mathbb{Z}_q^*$ και στέλνει στον verifier το $t = g^{t_1} h^{t_2}$.
- Ο verifier επιλέγει ομοιόμορφα $e \in \mathbb{Z}_q^*$ και το στέλνει στον prover.
- Ο prover υπολογίζει το $s_1 = t_1 + em \bmod q$, $s_2 = t_2 + er \bmod q$ και τα στέλνει στον verifier.
- Ο verifier αποδέχεται αν και μόνο αν $g^{s_1} h^{s_2} = t c^e$.

1. Είναι το Π Σ-πρωτόκολλο, διαθέτει δηλαδή πληρότητα, ειδική ορθότητα, μηδενική γνώση για τίμιους επαληθευτές; Να αιτιολογήσετε τις απαντήσεις σας.
2. Είναι το Π witness indistinguishable; Δηλαδή με δεδομένο έναν τίμιο prover και κοινή δημόσια είσοδο $\langle \mathbb{G}, g, h, q, c \rangle$ τι συμπεράσματα μπορεί να βγάλει ένας κακόβουλος επαληθευτής, από τις συζητήσεις (t, e, s_1, s_2) για witness (m, r) και (t', e', s_1', s_2') για witness (m', r') με $m \neq m'$ και $r \neq r'$.
3. Αλλάζουμε το Π σε Π', έτσι ώστε στο πρώτο βήμα ο prover υπολογίζει και στέλνει αντί για $t = g^{t_1} h^{t_2}$ τις τιμές $a = g^{t_1}$ και $b = h^{t_2}$. Ποια είναι η σχέση που πρέπει να ελέγξει ο verifier για να πειστεί ότι ο prover γνωρίζει τα m, r; Είναι τώρα το Π' Σ-πρωτόκολλο;

Άσκηση 8. Στην non-interactive έκδοση του πρωτοκόλλου του Schnorr (βλ. διάλεξη ZK - διαφάνεια 42) το challenge υπολογίζεται ως $c := \mathsf{H}(h||y)$, όπου y το πρώτο μήνυμα του prover και h το δημόσιο κλειδί του prover. Έστω η παραλλαγή με $c := \mathsf{H}(y)$, χωρίς δηλαδή να συμπεριληφθεί το δημόσιο κλειδί του prover. Να αποδείξετε ότι η έκδοση αυτή δεν διαθέτει την ιδιότητα της ορθότητας.
Υπόδειξη: Να σχεδιάσετε μια επίθεση όπου ένας κακόβουλος prover να μπορεί να φτιάξει έγκυρη απόδειξη γνώσης του διακριτού λογαρίθμου *κάποιου* στοιχείου της ομάδας $\mathbb{G}$ χωρίς όμως να τον γνωρίζει.

Άσκηση 9. Υλοποιήστε ένα από τα σχήματα υπογραφών Schnorr *ή* edDSA σε γλώσσα προγραμματισμού της επιλογής σας. Για τις υπογραφές Schnorr χρησιμοποιήστε υποομάδα πρώτης τάξης q του $\mathbb{Z}_p^*$ ενώ για τις υπογραφές edDSA ομάδα με βάση τις ελλειπτικές καμπύλες Edwards. Η υλοποίηση θα πρέπει και να επαληθεύει την υπογραφή Schnorr ή edDSA σε κατά προτίμηση μεγάλο αρχείο.

Άσκηση 10. Έστω το παρακάτω σχήμα υπογραφών όπου για τις παραμέτρους ισχύει ό,τι και στο σχήμα υπογραφών ElGamal. Κάθε χρήστης έχει ιδιωτικό κλειδί x και δημόσιο $y = g^x \bmod p$. Η υπογραφή λειτουργεί ως εξής:

i. Ο υπογράφων αρχικά επιλέγει $h \in \{0, \ldots, p{-}2\}$ ώστε: $\mathsf{H}(m) + x + h \equiv 0 \pmod{p-1}$, όπου H collision resistant συνάρτηση σύνοψης.
ii. Η υπογραφή είναι η τριάδα: $\mathsf{Sign}(x, m) = (m, (x + h) \bmod p - 1, g^h \bmod p)$.
iii. Για την επαλήθευση ότι μια τριάδα (m, a, b) είναι έγκυρη υπογραφή ελέγχεται εάν:

- $yb \equiv g^a \pmod{p}$ και
- $g^{\mathsf{H}(m)} yb \equiv 1 \pmod{p}$.

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

Άσκηση 11. Για κάθε μία από τις περιπτώσεις α) και β) παρακάτω, περιγράψτε επίθεση του αντιπάλου που επιτυγχάνει με πιθανότητα μεγαλύτερη του $1/2$ fork μήκους 6. Πιο συγκεκριμένα, σε κάποιο γύρο υπάρχουν δύο τίμιοι παίκτες με αλυσίδες C και C^* με $|C| \leq |C^*|$ και κανένα από τα τελευταία 6 blocks της C^* δεν ανήκουν στην C. Εξηγείστε γιατί η πιθανότητα επιτυχίας είναι μεγαλύτερη από $1/2$.

α) Έστω εκτέλεση του bitcoin με συνολικό αριθμό παικτών $n = 2t$, όπου ο αντίπαλος ελέγχει t παίκτες.

β) Έστω εκτέλεση του bitcoin με συνολικό αριθμό παικτών $n = 3t$, όπου ο αντίπαλος ελέγχει t παίκτες και έχει την ικανότητα να διαμερίσει τους τίμιους παίκτες σε δύο σύνολα ώστε να μην είναι δυνατή η επικοινωνία μεταξύ δύο παικτών που δεν ανήκουν στο ίδιο σύνολο.

Σε όλες τις ασκήσεις με "$\oplus$" συμβολίζουμε το XOR και με "$||$" την παράθεση.

Σύντομες οδηγίες: (α) προσπαθήστε μόνοι σας, (β) συζητήστε με συμφοιτητ(ρι)ές 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*. Ενδεχομένως σας ζητηθεί να παρουσιάσετε σύντομα κάποιες από τις λύσεις σας.

Καλή επιτυχία!