Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Υπολογιστική Κρυπτογραφία

(ΣΗΜΜΥ, ΣΕΜΦΕ, ΑΛΜΑ, ΕΜΕ, ΜΠ)

3η Σειρά Ασκήσεων

Προθεσμία παράδοσης: Προηγούμενη της εξέτασης του μαθήματος

Άσκηση 1. Να αποδείξετε ότι το πρόβλημα RSA έχει την ιδιότητα Random Self-Reducibility.

Άσκηση 2. Δίνεται μια κυκλική ομάδα $\mathbb{G}$ με τάξη πρώτο q και γεννήτορες $g_1, g_2, \cdots g_n$. Ορίζουμε το εκτεταμένο πρόβλημα του διακριτού λογαρίθμου (XDL) για κάποιο φυσικό $n \geq 2$ ως:
Να βρεθούν στοιχεία $x_1, x_2, \cdots x_n \in \mathbb{Z}_q^*$ ώστε $\prod_{i=1}^{n} g_i^{x_i} = 1$.
Να αποδείξετε ότι η δυσκολία του προβλήματος XDL είναι ισοδύναμη με τη δυσκολία του προβλήματος του διακριτού λογαρίθμου.

Άσκηση 3. Αποδείξτε ότι, αν το πρόβλημα BDDH είναι δύσκολο, τότε το πρωτόκολλο ανταλλαγής κλειδιού του Joux είναι ασφαλές έναντι παθητικού αντιπάλου. Στη συνέχεια εξηγήστε πώς ένας ενεργός αντίπαλος μπορεί να επιτεθεί στο πρωτόκολλο.

Άσκηση 4. 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 5.
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 της μυστικότητας (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 6.

Έστω μια παραλλαγή του πρωτοκόλλου του Schnorr για την απόδειξη γνώσης του διακριτού λογαρίθμου x ενός στοιχείου $h = g^x$ σε μια ομάδα $\mathbb{G}$ με γεννήτορα g και τάξη πρώτο q. Η παραλλαγή λειτουργεί με τον ίδιο τρόπο με τη διαφορά ότι στο τελευταίο μήνυμα (response) ο prover υπολογίζει και στέλνει το $s \leftarrow tc + x \bmod q$ αντί για $s \leftarrow t + cx \bmod q$. Να εξετάσετε αν η παραλλαγή αυτή διαθέτει τις ιδιότητες πληρότητας, ορθότητας και μηδενικής γνώσης (για τίμιους επαληθευτές).

Άσκηση 7.

Στην non-interactive έκδοση του πρωτοκόλλου του Schnorr (βλ. διάλεξη ZK) το challenge υπολογίζεται ως $c \leftarrow \mathsf{H}(g, Y, T)$, όπου T το πρώτο μήνυμα του prover και Y το δημόσιο κλειδί του. Έστω η παραλλαγή με $c \leftarrow \mathsf{H}(T)$, 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 8. 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 $\mathsf{Commit}(m, r) = c \leftarrow g^m h^r$ 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 $t \leftarrow g^{t_1} h^{t_2}$.
- Ο verifier επιλέγει ομοιόμορφα $e \in \mathbb{Z}_q^*$ και το στέλνει στον prover.
- Ο prover υπολογίζει το $s_{11} + em \bmod q,\ s_2 \leftarrow t_2 + er \bmod q$ και τα στέλνει στον verifier.
- Ο verifier αποδέχεται αν και μόνο αν $g^{s_1} h^{s_2} = tc^e$.

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 9.
΄Εστω 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: $\mathcal{H}(m) + x + h = 0 \pmod{p-1}$, όπου $\mathcal{H}$ collision resistant συνάρτηση σύνοψης.

ii. Η υπογραφή $sign(x, m)$ είναι η τριάδα: $(m, (x + h) \bmod p - 1, g^h \bmod p)$.

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

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

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

Άσκηση 10. 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.

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!