

Υπολογιστική Κρυπτογραφία

(ΣΗΜΜΥ, ΣΕΜΦΕ, ΑΛΜΑ, ΕΜΕ, ΜΠ)

3η Σειρά Ασκήσεων

Προθεσμία παράδοσης: Προηγούμενη της εξέτασης του μαθήματος

Άσκηση 1. Ο διευθυντής μιας εταιρείας χρειάζεται να παίρνει συχνά κρυπτογραφημένα μηνύματα από τους υπαλλήλους του. Για τον σκοπο αυτό χρησιμοποιεί RSA, δηλαδή δίνει 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 υποτίθεται ότι λειτουργεί ως εξής για είσοδο m :

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

Λόγω όμως εργοστασιακού λάθους, στο δεύτερο βήμα η συσκευή υπολογίζει $c'_q = m^e + 1 \bmod q$ και δίνει στην έξοδο $c' \in \mathbb{Z}_n$, τ.ω. $c' \equiv c_p \pmod{p}$ και $c' \equiv c'_q \pmod{q}$.

Όπως είναι φυσικό, ο διευθυντής σύντομα διαπιστώνει (με ποιον τρόπο;) ότι κάτι δεν πάει καλά, και ζητάει από την γραμματέα του να στείλει την συσκευή για επισκευή. Η γραμματέας όμως, που έχει παρακολουθήσει μαθήματα κρυπτογραφίας, κατορθώνει πριν στείλει την συσκευή στο service να βρει το ιδιωτικό κλειδί του διευθυντή. Πώς το κατάφερε αυτό;

Άσκηση 2. [KL2, Άσκηση 8.20] Έστω $KGen$ η γεννήτρια κλειδιών RSA (όπως στις σχετικές διαφάνειες, σελ. 10). Κατασκευάζουμε συνάρτηση κατακερματισμού όπως παρακάτω.

- $(N, e, d) \leftarrow KGen(1^n)$, $y \in_R \mathbb{Z}_N^*$, $s = (N, e, y)$.
- Με $f_b^s(x) = y^b x^e \bmod N$ για $b \in \{0, 1\}$, ορίζουμε $H^s(x) : \{0, 1\}^{3n} \rightarrow \mathbb{Z}_N^*$ ως εξής:

$$H^s(x) = f_{x_1}^s(f_{x_2}^s(\dots(1)\dots)) \quad (3n \text{ συναρτήσεις}).$$

Δείξτε ότι αν το πρόβλημα RSA είναι δύσκολο, τότε η H είναι collision-resistant. Συγκεκριμένα, αν με μη-αμελητέα πιθανότητα μπορεί κάποιος να βρει $u, v \in \{0, 1\}^{3n}$ με $u \neq v$ και $H^s(u) = H^s(v)$, τότε το RSA πρόβλημα δεν είναι δύσκολο για την KGen.

Άσκηση 3. 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 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. 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 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 :

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

1. Να ορίσετε την συνάρτηση της αποκρυπτογράφησης $\text{Dec}(\text{sk}, m)$ 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 $\text{Commit}(m, r) = c = g^m h^r$ 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 $g^{s_1} h^{s_2} = tc^e$.

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 8. 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 $c, c \in \{0, \dots, e-1\}$, 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 9. Στην non-interactive έκδοση του πρωτοκόλλου του Schnorr (βλ. διάλεξη ZK) το challenge υπολογίζεται ως $c := H(h||y)$, όπου y το πρώτο μήνυμα του prover και h το δημόσιο κλειδί του prover. Έστω η παραλλαγή με $c := H(y)$, 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 10. Υλοποιήστε ένα από τα σχήματα υπογραφών Schnorr σε γλώσσα προγραμματισμού της επιλογής σας. Για τις υπογραφές Schnorr χρησιμοποιήστε υποομάδα πρώτης τάξης q του \mathbb{Z}_p^* . Η υλοποίηση θα πρέπει και να επαληθεύει την υπογραφή Schnorr σε κάποια δεδομένα της επιλογής σας.

Άσκηση 11. 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:

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

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

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

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!