Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Υπολογιστική Κρυπτογραφία

(ΣΗΜΜΥ, ΣΕΜΦΕ, ΑΛΜΑ, ΕΜΕ)
2019-20
5η σειρά ασκήσεων

Προθεσμία: 27/7/2020

Ονοματεπώνυμο:

Α.Μ.:

Θέμα 1.
Δίνεται μια κυκλική ομάδα $\mathbb{G}$ τάξης πρώτου q. Να περιγράψετε πώς μπορούν 3 οντότητες με ζεύγη κλειδιών $(x_a, y_a = g^{x_a}), (x_b, y_b = g^{x_b}), (x_c, y_c = g^{x_c})$ να δημιουργήσουν ένα κοινό κλειδί:

- Χωρίς pairings
- Με pairings

Θέμα 2.
Υπολογίστε τις τετραγωνικές ρίζες του 119 modulo 209. Χρησιμοποιήστε μεθόδους της θεωρίας αριθμών αλλά και εμπειρικές παρατηρήσεις. Δείξτε αναλυτικά τις πράξεις που κάνατε.

Θέμα 3.
Έστω g, h στοιχεία της πολλαπλασιαστικής ομάδας Z_p^* έτσι ώστε $\langle g \rangle = \langle h \rangle$ και το μέγεθος της $\langle g \rangle$ είναι q όπου q γνωστός πρώτος αριθμός. Έστω η οικογένεια συναρτήσεων $H_{g,h} : \{0, 1, ..., q-1\} \times \{0, 1, ..., q-1\} \to \{0, ..., p-1\}$ που ορίζεται ως εξής: $H_{g,h}(x, y) = g^x \cdot h^y \bmod p$.

1. Δείξτε ότι η συνάρτηση $H_{g,g}$ είναι μια συνάρτηση σύνοψης με αντίσταση πρώτου ορίσματος αλλά χωρίς αντίσταση δεύτερου ορίσματος.
2. Δείξτε ότι ένας αλγόριθμος που βρίσκει συγκρούσεις για οποιαδήποτε συνάρτηση της οικογένειας $H_{g,h}$ μπορεί να χρησιμοποιηθεί για να λύσει το πρόβλημα του διακριτού λογαρίθμου στην υποομάδα $\langle g \rangle$.
3. Σχεδιάστε έναν αλγόριθμο για την εύρεση του διακριτού λογαρίθμου στην υποομάδα $\langle g \rangle$ που να είναι πιο αποδοτικός από τον brute-force αλγόριθμο.

Θέμα 4.
Έστω ότι οι χρήστες Α και Β θέλουν να 'στρίψουν' ένα νόμισμα με δίκαιο τρόπο και χρησιμοποιούν το παρακάτω πρωτόκολλο όπου T είναι μία έμπιστη αρχή.

- Η T δημοσιοποιεί το δημόσιο κλειδί pk.
- Η A διαλέγει ένα τυχαίο bit b_A, το κρυπτογραφεί με βάση το pk και δημοσιοποιεί το κρυπτογράφημα c_A.
- Ο B κάνει το ίδιο και δημοσιοποιεί το c_B.
- Η T αποκρυπτογραφεί τα c_A και c_B και δημοσιοποιεί τα αποτελέσματα.
- Οι A και B υπολογίζουν τα $b_A \oplus b_B$. Αν το αποτέλεσμα είναι 1 κερδίζει η A, αλλιώς ο B.

(α) Να εξετάσετε αν ένας κακόβουλος παίκτης B μπορεί να κλίνει το τυχαίο νόμισμα, δηλαδή το $b_A \oplus b_B$, στην τιμή 0.
(β) Μπορεί ο B, αν θέλει, να κλίνει το νόμισμα και στην τιμή 1;
Διευκρίνιση: Οι A και T θεωρούνται τίμιες. Για την κρυπτογράφηση χρησιμοποιούμε το εκθετικό ElGamal, όπου αντί για το b κρυπτογραφείται το g^b.

Θέμα 5.
Έστω $n = pq$, p, q πρώτοι, και $p \equiv q \equiv 3 \pmod 4$. Έστω η συνάρτηση:

$$SQ(x) = min\{x^2 \bmod n, n - x^2 \bmod n\}$$

όπου $0 < x < n/2$.

1. Δείξτε ότι η SQ είναι δύο-προς-ένα στο $\{1, ..., (n-1)/2\}$.
   Γιατί χρειαζόμαστε το $p \equiv q \equiv 3 \pmod 4$;
2. Δείξτε ότι η SQ, ως συνάρτηση σύνοψης, είναι ελεύθερη συγκρούσεων, υποθέτοντας ότι είναι υπολογιστικά ανέφικτο να βρεθούν τα p και q.
3. Για n με μήκος 1024 bits, εξηγήστε πως μπορούμε από την SQ να φτιάξουμε μια συνάρτηση σύνοψης που να είναι ελεύθερη συγκρούσεων $SQ' : \{0,1\}^* \mapsto \{0,1\}^{1024}$, κάτω από την παραπάνω υπόθεση.

Θέμα 6.
Έστω το κρυπτοσύστημα RSA με $n = pq$, e δημόσιο κλειδί και d ιδιωτικό κλειδί. Έστω ένα κρυπτοκείμενο $c = enc(m) = m^e \bmod n$. Ένας RSA-βρόχος για το c είναι μια σειρά από τιμές

$$c, enc(c), enc^2(c), \ldots, enc^t(c) = c$$

όπου $enc^i(c) = enc(enc^{i-1}(c))$ και $enc^1(c) = enc(c)$. Το $t > 0$ λέγεται μήκος του RSA-βρόχου.

1. Δείξτε ότι αν βρεθεί ένας RSA-βρόχος για το c τότε μπορεί να βρεθεί το m.

2. Υπάρχει RSA-βρόχος για κάθε $c \in \mathbb{Z}_n$; Επιχειρηματολογήστε.

3. Δείξτε ότι για όλα τα c για τα οποία υπάρχει RSA-βρόχος το μήκος του RSA-βρόχου επιδέχεται ένα άνω φράγμα που εκφράζεται σα συναρτηση του n (ανεξάρτητα από το c). Βρείτε όσο το δυνατόν μικρότερο άνω φράγμα. Είναι το αποτέλεσμά σας 'tight';

4. Τι σημαίνουν τα παραπάνω για την ασφάλεια ενός συστήματος RSA;

Θέμα 7. Δίνεται το παρακάτω σχήμα δέσμευσης το οποίο βασίζεται στο *εκθετικό* κρυπτοσύστημα ElGamal. Έστω p, q πρώτοι με $q \mid (p-1)$ και g ένας γεννήτορας της υποομάδας $\mathbb{G} \subseteq \mathbb{Z}_p^*$ (τάξης q). Για να δεσμευτεί σε κάποιο μήνυμα $m \in \mathbb{Z}_q$ ο αποστολέας υπολογίζει το ζεύγος:
$c = commit(m, r) = (g^r, g^m h^r)$ όπου r τυχαίο στοιχείο της $\mathbb{Z}_q$ και $h = g^x \bmod p$, x το ιδιωτικό κλειδί. Για την επαλήθευση της δέσμευσης ο αποστολέας αποκαλύπτει τα m, r και ο παραλήπτης επαληθεύει αν αντιστοιχούν στη δέσμευση που έλαβε.
Να μελετήσετε το σχήμα ως προς τις ιδιότητες της απόκρυψης (hiding) και δέσμευσης (binding) αιτιολογώντας πλήρως τις απαντήσεις σας.

Θέμα 8. Δίνεται ένα oracle AES_k που μπορεί να δέχεται δυαδικά bitstrings m και να παράγει κρυπτογραφήσεις με βάση το κρυπτοσύστημα AES χρησιμοποιώντας το μυστικό κλειδί k.

1. Να περιγράψετε αλγόριθμο με τον οποίο μπορείτε να βρείτε το μέγεθος block που χρησιμοποιεί το oracle.

2. Να περιγράψετε αλγόριθμο με τον οποίο μπορείτε να δείτε αν το oracle χρησιμοποιεί ECB mode.

3. Να περιγράψετε αλγόριθμο με τον οποίο μπορείτε να αποκρυπτογραφήσετε οποιοδήποτε μήνυμα έχει παραχθεί από το AES_k σε ECB mode. Για τον σκοπό αυτό μπορείτε να χρησιμοποιήσετε το AES_k και να παράγετε κρυπτογραφήσεις μηνυμάτων της επιλογής σας. (Υπόδειξη εκμεταλλευτείτε το ότι μπορείτε να μάθετε το μέγεθος του block).

Θέμα 9. Δίνονται 3 κυκλικές ομαδες $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_3$ με τάξεις πρώτους q_1, q_2, q_3 με ίδιο πλήθος bits, όπου ισχύει η υπόθεση DDH. Σε αυτές ορίζουμε το κρυπτοσύστημα 3-ElGamal το οποίο κρυπτογραφεί ένα μήνυμα $m \in \mathbb{G}_1$ ως εξής:

1. $(a_1, b_1) = Enc_{g_1, pk_1}(m)$

2. $(a_2, b_2) = Enc_{g_2, pk_2}(f_2(a_1))$

3. $(a_3, b_3) = Enc_{g_3, pk_3}(f_3(a_2))$

4. return (b_1, b_2, a_3, b_3)

όπου: g_i γεννήτορας $\mathbb{G}_i$, Enc_{g_i, pk_i} η γνωστή κρυπτογράφηση ElGamal στην $\mathbb{G}_i$ με ζεύγος κλειδιών (pk_i, sk_i) και $f_i : \mathbb{G}_i \rightarrow \mathbb{G}_{i+1}$ είναι αποδοτικά υπολογίσιμη συναρτηση μεταφοράς στοιχείων από την $\mathbb{G}_i$ στην $\mathbb{G}_{i+1}$ η αντιστροφή της οποίας είναι και αυτή αποδοτικά υπολογίσιμη.

1. Να σχεδιάσετε την διαδικασία αποκρυπτογράφησης.
2. Να εξετάσετε αν το 3-ElGamal έχει την ιδιότητα IND-CPA.
3. Είναι το 3-ElGamal πιο ασφαλές από το απλό ElGamal; Να τεκμηριώσετε την απαντησή σας.

Θέμα 10.

Έστω $\mathbb{G}$ μια κυκλική ομάδα με τάξη πρώτο q και οι παρακάτω παραλλαγές του Σ-πρωτοκόλλου του Schnorr για την απόδειξη της σχέσης: $\{(h; x) : h = g^x\}$:

Παραλλαγή 1

- Prover (με ιδιωτικό input $\left(x = \log_g h\right)$):
  - Επιλογή $t \in_R \mathbb{Z}_q$
  - Αποστολή t στον verifier
- Verifier:
  - Επιλογή $c \in_R \mathbb{Z}_q$
  - Αποστολή c στον prover
- Prover:
  - Υπολογισμός $s := t + cx$
  - Αποστολή s στον verifier
- Verifier:
  - Αποδοχή ανν: $g^s = g^t h^c$

Παραλλαγή 2

- Prover (με ιδιωτικό input $\left(x = \log_g h\right)$):
  - Επιλογή $t \in_R \mathbb{Z}_q$
  - Αποστολή t στον verifier
- Verifier:
  - Επιλογή $c \in_R \mathbb{Z}_q$
  - Αποστολή c στον prover
- Prover:
  - Υπολογισμός $\sigma := g^{t-cx}$
  - Αποστολή σ στον verifier
- Verifier:
  - Αποδοχή ανν: $g^t = \sigma h^c$

Να εξετάσετε αν οι παραλλαγές αυτές αποτελούν Σ-πρωτόκολλα.

Καλή Επιτυχία!