Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Υπολογιστική Κρυπτογραφία

(ΣΗΜΜΥ, ΣΕΜΦΕ, ΑΛΜΑ, ΕΜΕ)

Τελική Εξέταση
(125 μονάδες, αρκούν 90)

Μέρος Α (1.5 ώρα, κλειστές σημειώσεις)

Ονοματεπώνυμο:

Α.Μ.:

Θέμα 1. Μονάδες 10 (5+5)

1. Να διατυπώσετε και να αποδείξετε το Κινέζικο Θέωρημα Υπολοίπων.
2. Να υπολογίσετε το $102^{4.800.000.023} \bmod 35$ με όσο το δυνατόν λιγότερες πράξεις.

Θέμα 2. Μονάδες 15 (7+8)

1. Να περιγράφετε τη λειτουργία κρυπτογράφησης και αποκρυπτογράφησης ενός μηνύματος από ένα δίκτυο Feistel.
2. Να ορίσετε τους τρόπους λειτουργίας (modes of operation) ECB, CBC, CFB, OFB, CTR ενός κρυπτοσυστήματος block.

Θέμα 3. Μονάδες 15 (2+3+3+8)

1. Να ορίσετε το πρόβλημα απόφασης Diffie - Hellman σε μια ομάδα $\mathbb{G}$
2. Να ορίσετε την ιδιότητα ασφάλειας IND-CPA για ένα κρυπτοσύστημα δημοσίου κλειδιού χρησιμοποιώντας ένα παίγνιο.
3. Ορίστε το σχήμα κρυπτογράφησης-αποκρυπτογράφησης El Gamal.
4. Να αποδείξετε ότι αν το πρόβλημα απόφασης Diffie - Hellman είναι δύσκολο σε μια ομάδα $\mathbb{G}$, τότε το κρυπτοσύστημα El Gamal που έχει οριστεί στην $\mathbb{G}$ διαθέτει ασφάλεια IND-CPA.

Θέμα 4. Μονάδες 15 (8+7)

Δίνεται μια κυκλική ομάδα $\mathbb{G}$ τάξης q με δύσκολο πρόβλημα απόφασης Diffie - Hellman και στοιχεία $g, y_1 = g^{x_1}, y_2 = g^{x_2}$.

1. Να σχεδιάσετε Σ-πρωτόκολλο το οποίο θα επιτρέπει σε κάποιον prover P να αποδείξει σε κάποιον verifier V ότι γνωρίζει ένα εκ των x_1, x_2 χωρίς να διαρρέει ποιο από τα δύο γνωρίζει.

2. Να αποδείξετε τις ιδιότητες του πρωτοκόλλου.

Θέμα 5. Μονάδες 15 (5+5+5)

Να απαντήσετε στις παρακάτω ερωτήσεις σχετικά με το bitcoin. Να δικαιολογήσετε τις απαντήσεις σας.

1. Ποιες οντότητες είναι σε θέση να λογοκρίνουν συναλλαγές στο δίκτυο του bitcoin και πώς μπορούν να το επιτύχουν; Ποιες υποθέσεις ασφαλείας αποτρέπουν τέτοιες επιθέσεις;

2. Να περιγράψετε τι επίδραση έχουν στην ανωνυμία ενός χρήστη του bitcoin τα παρακάτω σενάρια:

   - Πολλά UTXO αποτελούν είσοδο σε μια συναλλαγή.
   - Μια διεύθυνση χρησιμοποιείται σε περισσότερες από μία συναλλαγές.

3. Να περιγράψετε δύο τρόπους με τους οποίους θα μπορούσατε να υποθέσετε ότι μία διεύθυνση εξόδου κάποιας συναλλαγής αποτελεί διεύθυνση για ρέστα. (*Διευκρίνηση:* Μπορεί κάποιος από τους τρόπους να μην μας δίνει 100% βεβαιότητα).

Μέρος Β (1.5 ώρα, ανοιχτές σημειώσεις)

Ονοματεπώνυμο:

Α.Μ.:

Θέμα 6. Μονάδες 7 (4+3)
Έστω $p > 2$ πρώτος και $M_p = 2^p - 1$.

1. Να δείξετε ότι αν q είναι πρώτος παράγοντας του M_p ισχύει $q = 1 \pmod{p}$.
2. Να δείξετε ότι $p|\varphi(M_p)$.

Θέμα 7. Μονάδες 6
Δίνεται μια συνάρτηση σύνοψης $\mathsf{H} : \{0,1\}^* \to \{0,1\}^n$ η οποία έχει δυσκολία εύρεσης συγκρούσεων. Ορίζουμε τη συνάρτηση $\mathsf{G} : \{0,1\}^* \to \{0,1\}^{2n}$ ως εξής:

$$\mathsf{G}(x) = \mathsf{H}(x)||\mathsf{H}(x)$$

όπου με $||$ συμβολίζουμε τη λειτουργία της συνένωσης.
Να εξετάσετε αν η G έχει δυσκολία εύρεσης συγκρούσεων.

Θέμα 8. μονάδες 12
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, $c \in \{0, \ldots, e-1\}$, 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.

Θέμα 9. Μονάδες 15 (4+4+5+2)
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;

Θέμα 10. Μονάδες 15 $(5 + 4 + 6)$

Θεωρήστε ένα $(3, n)$ σχήμα Shamir secret sharing στο $\mathbb{Z}_{17}$, όπου ο παίκτης i λαμβάνει μερίδιο $y_i = P(i)$ (όπου $P(x)$ το πολυώνυμο που επέλεξε ο διαμοιραστής - dealer). Οι παίκτες $2, 5, 10$ έλαβαν μερίδια $1, 1, 2$ αντίστοιχα.

1. Υπολογίστε το μυστικό. Δείξτε αναλυτικά τους υπολογισμούς σας.

2. Είναι δυνατό να ενταχθούν στο σχήμα παίκτες με δείκτη 0 ή -1; Εξετάστε τις περιπτώσεις ξεχωριστά και εξηγήστε τις απαντήσεις σας;

3. Έστω ότι ένας νέος παίκτης (με δείκτη το 16) θέλει να ενταχθεί στο σχήμα. Ο διαμοιραστής (dealer) δεν είναι διαθέσιμος. Με δεδομένο ότι οι παίκτες είναι τίμιοι, εξηγήστε πως οι παίκτες $2, 5, 10$ μπορούν να στείλουν στον νέο παίκτη αρκετές πληροφορίες ώστε να υπολογίσει το μεριδιό του. Στη λύση σας δεν επιτρέπεται κάποιος παίκτης να είναι σε θέση να παράξει το μυστικό. Θεωρήστε ότι είναι εφικτό οι παίκτες να στέλνουν προσωπικά μηνύματα ο ένας στον άλλο.