Στοιχεία Θεωρίας Αριθμών και Εφαρμογές στην Κρυπτογραφία
(Κρυπτογραφία και Πολυπλοκότητα)
ΣΗΜΜΥ - ΣΕΜΦΕ - ΜΠΛΑ
Διδάσκοντες: Ε. Ζάχος, Α. Παγουρτζής

Ονοματεπώνυμο:

Σχολή:

Σύνολο 115 μονάδες

1. (8 μονάδες)
   Περιγράψτε και εξηγήστε τον τρόπο εύρεσης πολλαπλασιαστικού αντιστρόφου modulo N.

2. (6 μονάδες)
   Περιγράψτε τον τρόπο λειτουργίας του DES με αλυσιδωτή σύνδεση των πακέτων και εξηγήστε την ορθότητα κρυπτογράφησης και αποκρυπτογράφησης. Αναφέρατε πλεονεκτήματα και μειονεκτήματα αυτού του τρόπου λειτουργίας.

3. (12 μονάδες)
   Υπολογίστε τις τετραγωνικές ρίζες του 42 modulo 143. Χρησιμοποιήστε μεθόδους της θεωρίας αριθμών αλλά και εμπειρικές παρατηρήσεις (για διευκόλυνση των πράξεων). Περιγράψτε τα βήματα που ακολουθήσατε.

4. (12 μονάδες: 3,4,5)

   (a) Περιγράψτε τη μέθοδο παραγοντοποίησης ρ.

   (b) Εφαρμόστε την για παραγοντοποίηση του αριθμού 77.

   (c) Ποια είναι η αναμενόμενη πολυπλοκότητά της και γιατί;

5. (6 μονάδες)
   Αποδείξτε, χωρίς χρήση του Θεωρήματος Lagrange, ότι για κάθε θετικό ακέραιο n και κάθε ακέραιο $a \in U(\mathbb{Z}_n)$ ισχύει ότι η τάξη του a στην ομάδα $U(\mathbb{Z}_n)$ διαιρεί το $\phi(n)$.

6. (10 μονάδες)
   Δώστε τον ορισμό της τέλειας μυστικότητας κατά Shannon. Χρησιμοποιήστε την για να δείξετε ότι το παρακάτω κρυπτοσύστημα XOR δεν έχει τέλεια μυστικότητα: το 1ο κλειδί (για τον πρώτο χαρακτήρα) επιλέγεται με ομοιόμορφη πιθανότητα από το σύνολο των κλειδιών, το 2ο κλειδί επιλέγεται ομοιόμορφα από το σύνολο των υπολοίπων κλειδιών, και η διαδικασία επαναλαμβάνεται.

7. (10 μονάδες)
Αποδείξτε ότι N πρώτος αν και μόνο αν $(N-1)! \equiv -1 \pmod{N}$.

Υπόδειξη: για το ευθύ θεωρήστε ζεύγη αντιστρόφων στο $\mathbb{Z}_p^*$, για το αντίστροφο εξετάστε τον $gcd(N,(N-1)!)$ για N σύνθετο.

8. (6 μονάδες)
Σχεδιάστε αλγόριθμο πολυωνυμικού χρόνου για τον υπολογισμό του $x^{y^z} \bmod p$, με είσοδο x, y, z, p, για p πρώτο αριθμό. Εξηγήστε την πολυπλοκότητά του.

9. (12 μονάδες: 4, 8)
Οι χρήστες $A_1, \ldots, A_n$ ενός δικτύου θέλουν να φτιάξουν ένα κοινό κλειδί με τη βοήθεια μιας έμπιστης αρχής T. Όλοι θα πρέπει να είναι σε θέση να υπολογίσουν αυτό το κλειδί, αλλά για κάποιον υποκλοπέα θα πρέπει να είναι δύσκολο να το υπολογίσει.

Για να πετύχουν το στόχο τους χρησιμοποιούν την εξής παραλλαγή του Diffie - Hellman: Έχουν για δημόσιο κλειδί έναν πρώτο αριθμό p και ένα στοιχείο $g \in Z_p$ τάξης q με q πρώτο και $q \mid (p-1)$. Η αρχή T διαλέγει έναν κρυφό τυχαίο αριθμό $t \in [1, \ldots, q-1]$ και υπολογίζει το $K = g^t \pmod{p}$. Κάθε χρήστης A_i διαλέγει έναν κρυφό τυχαίο αριθμό $a_i \in [1, \ldots, q-1]$ και υπολογίζει το $x_i = g^{a_i} \pmod{p}$. Μετά ο A_i στέλνει το x_i στην T, που του απαντάει στέλνοντάς του το $z_i = x_i^t$.

(α) Περιγράψτε τι πρέπει να κάνει ο χρήστης A_i για να υπολογίσει το K.

(β) Δείξτε ότι το πρωτόκολλο είναι ασφαλές κάτω από την υπόθεση Diffie-Hellman. Δηλαδή, δείξτε ότι ένας αλγόριθμος που με είσοδο x_i, z_i μπορεί να υπολογίσει το K, μπορεί να χρησιμοποιηθεί για την επίλυση του Decisional Diffie-Hellman προβλήματος.

10. (10 μονάδες)
Δείξτε πώς μπορεί να επιλυθεί σε πολυωνυμικό χρόνο το πρόβλημα του Διακριτού Λογαρίθμου στην υποομάδα του $\mathbb{Z}_p^*$, με γεννήτορα g τάξης $k = 3^m$ (p, g, k γνωστά).

11. (11 μονάδες: 4,7)

Οι χρήστες ενός δικτύου χρησιμοποιούν το κρυπτοσύστημα RSA. Κάθε χρήστης U_i διαθέτει ένα δημόσιο κλειδί n_i, e_i και ένα ιδιωτικό κλειδί d_i. Οι χρήστες χρησιμοποιούν το σύστημα τόσο για κρυπτογράφηση όσο και για υπογραφή. Δηλαδή, κάθε χρήστης U_i χρησιμοποιεί το ιδιωτικό του κλειδί d_i (και το n_i) για να υπογράψει ένα μήνυμα, και το δημόσιο κλειδί του U_k, δηλ. το (e_k, n_k) για να κρυπτογραφήσει ένα μήνυμα και να το στείλει στον U_k.

(α) Δείξτε ότι αυτό μπορεί να είναι επικίνδυνο στο εξής σενάριο: αν η διευθύντρια U_i υπογράφει ο,τιδήποτε της δίνει ο έμπιστος γραμματέας της, τότε ο γραμματέας μπορεί να αποκρυπτογραφήσει κάθε μήνυμα που στέλνει ο χρήστης U_k στη διευθύντρια.

(β) Έστω ότι η διευθύντρια είναι κάπως καχύποπτη, και αρνείται να δώσει το υπογεγραμμένο μήνυμα στον γραμματέα, αν αυτό μοιάζει πολύ με ένα κανονικό κείμενο. Πώς ο γραμματέας μπορεί να παρακάμψει αυτό το "πρόβλημα";

12. (12 μονάδες: 5,7)
Έστω f μία συνάρτηση μονής κατεύθυνσης. Ορίζουμε την γλώσσα L:

$$L = \{(a, b) \mid \exists x : f(x) = a \quad \wedge \quad b \text{ είναι suffix του } x\}$$

(α) Αποδείξτε ότι $L \in UP$.

(β) Αποδείξτε ότι $L \in UP \setminus P$.

Καλή επιτυχία!