Στοιχεία Θεωρίας Αριθμών και Εφαρμογές στην Κρυπτογραφία (ΣΗΜΜΥ)
Κρυπτογραφία και Πολυπλοκότητα (ΣΕΜΦΕ, ΜΠΛΑ)

Επαναληπτική Εξέταση ακ. έτους 2010-11

Διδάσκοντες: Ε. Ζάχος, Α. Παγουρτζής

Ονοματεπώνυμο:
Σχολή:

Σύνολο 120 πόντοι

1. (8 πόντοι)
   Διατυπώστε και αποδείξτε το Κινέζικο Θεώρημα Υπολοίπων.

2. (5 πόντοι)
   Υπολογίστε το $7^{31} \bmod 13$ με όσο το δυνατόν λιγότερες πράξεις (δείξτε τις πράξεις αναλυτικά).

3. (6 πόντοι)
   Υπολογίστε το $28^{-1} \bmod 75$ (δείξτε τις πράξεις αναλυτικά).

4. (5 πόντοι) Περιγράψτε πώς γίνεται η διανομή κλειδιών κατά το σχήμα Diffie-Hellman. Σε ποιό πρόβλημα βασίζεται η ασφάλεια του συστήματος;

5. (15 πόντοι: 5,10)

   (a) Εφαρμόστε την μέθοδο ρ για να παραγοντοποιήσετε τον αριθμό 91 (χρησιμοποιήστε $x_0 = 1$ και $x_{i+1} = x_i^2 + 1$).

   (b) Συζητήστε την πολυπλοκότητά της. Ποια η σχέση με το παράδοξο των γενεθλίων;

6. (16 πόντοι: 2,4,5,5)

   (a) Ορίστε τι είναι ένα τετραγωνικό υπόλοιπο στην πολλαπλασιαστική ομάδα Z_n^* (γνωστή και ως $U(Z_n)$).

   (b) Δείξτε ότι το σύνολο των τετραγωνικών υπολοίπων της Z_n^* είναι μια υποομάδα.

   (c) Ποιο το μέγεθος της υποομάδας αυτής αν το n είναι πρώτος αριθμός; Επιχειρηματολογήστε.

   (d) Ποιο το μέγεθος της υποομάδας αν το n είναι γινόμενο δύο πρώτων αριθμών και γιατί;

7. (16 πόντοι: 6,10)
   Έστω μια συνάρτηση κρυπτογράφησης $E(k, m)$, όπου k είναι το κλειδί και m το αρχικό κείμενο, τέτοια ώστε k, m, και $E(k, m)$ έχουν όλα τον ίδιο αριθμό bits n. Θέλουμε να την χρησιμοποιήσουμε για να φτιάξουμε συνάρτηση κατακερματισμού που να συμπιέζει ακολουθίες $2n$ bits σε ακολουθία n bits.

(a) Δείξτε ότι η χρήση της E αυτούσιας δεν είναι καλή ιδέα. Συγκεκριμένα, δείξτε ότι η συνάρτηση

$$h_1(x, x') = E(x, x')$$

δεν είναι ελεύθερη συγκρούσεων. (Υπόδειξη: θεωρήστε ότι η συνάρτηση αποκρυπτογράφησης $D(k, c)$ είναι επίσης γνωστή και σκεφτείτε με τι είναι ίσο το $E(k, D(k, c))$.)

(b) Εξετάστε αν η παρακάτω συνάρτηση είναι ελεύθερη συγκρούσεων:

$$h_2(x, x') = E(x', x) \oplus x'$$

8. (16 πόντοι: 4,6,6)
Ο Βαγγέλης χρησιμοποιεί το κρυπτοσύστημα RSA για να λαμβάνει απόρρητους 5-ψήφιους κωδικούς από συνεργάτες του.

(a) Περιγράψτε τη λειτουργία του συστήματος.

(b) Μετά από λίγο καιρό ο Βαγγέλης φοβάται ότι το μυστικό κλειδί του d έχει διαρρεύσει. Επειδή δεν ξέρει πώς να βρει νέους πρώτους αριθμούς p, q σκέφτεται να διαλέξει καινούρια e', d' και να κρατήσει το ίδιο n. Τι ακριβώς πρέπει να κάνει;

(c) Τι πρέπει να προσέξει δεδομένου ότι το n έχει μήκος 512 ψηφίων;

(d) Είναι καλή η ιδέα του; επιχειρηματολογήστε.

9. (18 πόντοι: 3,6,9)
Δίνονται p πρώτος και h ένα στοιχείο της πολλαπλασιαστικής ομάδας Z_p^* με τάξη $k = 2^m$ (το k δίνεται επίσης).

(a) Τι μορφής είναι ο πρώτος p;

(b) Δώστε αποδοτικό αλγόριθμο που να ελέγχει αν ένα στοιχείο $a \in Z_p^*$ ανήκει στην υποομάδα $\langle h \rangle$ που παράγει το h.

(c) Δώστε αποδοτικό αλγόριθμο που να λύνει το πρόβλημα του διακριτού λογαρίθμου στην υποομάδα $\langle h \rangle$.

10. (15 πόντοι: 6,9)

(a) Έστω f μία συνάρτηση μονής κατεύθυνσης και γλώσσα L:

$$L = \{(a, b_1, b_2) \mid \exists x : f(b_1||x||b_2) = a \}$$

Δείξτε ότι $L \in UP$.
(με '||' συμβολίζουμε την παράθεση συμβολοσειρών)

(b) Εξετάστε αν είναι δυνατόν να ισχύει $L \in P$.

Καλή Επιτυχία!