

## Υπολογιστική Κρυπτογραφία

(ΣΗΜΜΥ-ΣΕΜΦΕ-ΜΠΛΑ)

### 3η Σειρά Ασκήσεων

Προθεσμία παράδοσης: 4/12/2016

#### Άσκηση 1.

(α) Παραγοντοποιήστε τον αριθμό 143 εφαρμόζοντας τη μέθοδο  $\rho$  και τη μέθοδο βάσεων παραγοντοποίησης Dixon. Τι παρατηρείτε;

(β) Υλοποιήστε σε πρόγραμμα τη μέθοδο  $\rho$  και χρησιμοποιήστε την για παραγοντοποίηση σύνθετων αριθμών της μορφής  $n = pq$  με  $p, q$  πρώτους αριθμούς στο διάστημα  $[10^3, 10^4]$ . Μετρήστε το πλήθος των βημάτων σε κάθε εκτέλεση και τον συνολικό χρόνο. Τι παρατηρείτε;

#### Άσκηση 2.

Θεωρήστε την παραλλαγή του DES-X, με 2 κλειδιά  $k_1, k_2$ , όπου η κρυπτογράφηση ενός απλού κειμένου  $M$  γίνεται ως εξής :

$$Enc_{k_1, k_2}(M) = E_{k_1}(M \oplus k_2),$$

όπου  $E$  η συνάρτηση κρυπτογράφησης του DES.

Έχουμε περισσότερη ασφάλεια από τον κλασικό DES στο παραπάνω σύστημα; Θεωρήστε ότι ο αντίπαλος έχει δυνατότητα KPA (διαθέτει αρκετά ζεύγη απλού κειμένου - κρυπτοκειμένου).

#### Άσκηση 3.

Εξετάστε τη γεννήτρια ψευδοτυχαιότητας RC4. Αποδείξτε ότι το δεύτερο byte (κλειδί) εξόδου είναι ίσο με 0 με πιθανότητα περίπου ίση με  $2^{-7}$ . Ξεκινήστε δείχνοντας ότι αν μετά τη φάση δημιουργίας κλειδιών (KSA) ισχύει για την μετάθεση  $P$  ότι  $P[2] = 0$  και  $P[1] \neq 2$  τότε το δεύτερο byte εξόδου είναι ίσο 0 με πιθανότητα 1.

#### Άσκηση 4.

Έστω  $h$  συνάρτηση κατακερματισμού, η οποία συμπίεζει ακολουθίες μήκους  $2n$  σε ακολουθίες μήκους  $n$  και έχει την ιδιότητα δυσκολίας εύρεσης συγκρούσεων (collision free). Θέλουμε να φτιάξουμε μία συνάρτηση κατακερματισμού που να συμπίεζει ακολουθίες μήκους  $4n$  σε ακολουθίες μήκους  $n$ , η οποία να έχει επίσης την ιδιότητα δυσκολίας εύρεσης συγκρούσεων. Έχουμε τις εξής υποψήφιες:

1.  $h_1(x) = h((x_1 \oplus x_2) || (x_3 \oplus x_4))$

2.  $h_2(x) = h(h(x_1||x_2)||h(x_3||x_4))$
3.  $h_3(x) = h(x_1||x_2) \oplus h(x_3||x_4)$
4.  $h_4(x) = h(h(h(x_1||x_2)||x_3)||x_4)$

(Με "⊕" συμβολίζουμε το XOR, με "||" την παράθεση και  $|x_i| = n$ .)

Για κάθε  $i$  εξετάστε αν η  $h_i$  έχει την ιδιότητα δυσκολίας εύρεσης συγκρούσεων ή όχι. Για να δείξετε ότι την έχει, δείξτε ότι αν μπορούσαμε να βρούμε συγκρούσεις για την  $h_i$ , τότε θα μπορούσαμε να βρούμε συγκρούσεις και για την  $h$ . Για να δείξετε το αντίθετο βρείτε μία ή περισσότερες συγκρούσεις για την  $h_i$ .

### Άσκηση 5.

Οι χρήστες  $A_1, \dots, A_n$  και  $B$  ενός δικτύου θέλουν να φτιάξουν ένα κοινό κλειδί. Όλοι θα πρέπει να γνωρίζουν αυτό το κλειδί, αλλά για κάποιον υποκλοπέα θα πρέπει να είναι αδύνατο να υπολογίσει το κλειδί. Για αυτό χρησιμοποιούν την εξής παραλλαγή του Diffie - Hellman: Έχουν για δημόσιο κλειδί έναν πρώτο αριθμό  $p$  και ένα στοιχείο  $g \in \mathbb{Z}_p$  τάξης  $q$  με  $q$  πρώτο και  $q|(p-1)$ . Ο  $B$  διαλέγει έναν κρυφό τυχαίο αριθμό  $b \in \mathbb{Z}_q^*$  και υπολογίζει το  $y = g^b \pmod{p}$ . Κάθε χρήστης  $A_i$  διαλέγει έναν κρυφό τυχαίο αριθμό  $a_i \in \mathbb{Z}_q^*$  και υπολογίζει το  $x_i = g^{a_i} \pmod{p}$ . Μετά ο χρήστης  $A_i$  στέλνει το  $x_i$  στον  $B$ , που του απαντάει στέλνοντας του το  $z_i = x_i^b$ .

1. Δείξτε ότι κάθε χρήστης  $A_i$  έχοντας το  $z_i$  (και το  $a_i$ ) μπορεί να υπολογίσει το  $y$ .
2. Δείξτε ότι το παραπάνω πρωτόκολλο είναι ασφαλές αν αποδεχτούμε την υπόθεση Diffie - Hellman. Δηλαδή αν υπάρχει αλγόριθμος που με είσοδο τις δημόσιες τιμές επιτρέπει σε έναν υποκλοπέα να υπολογίσει το  $y$ , τότε μπορούμε να χρησιμοποιήσουμε τον αλγόριθμο αυτό για να καταρρίψουμε την υπόθεση Diffie - Hellman.

Συμβουλή: (α) προσπαθήστε μόνοι σας, (β) συζητήστε με συμφοιτητές 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.