ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΜΑΘΗΜΑ: ΚΡΥΠΤΟΓΡΑΦΙΑ ΚΑΙ ΕΦΑΡΜΟΓΕΣ, 2013-2014
ΔΙΔΑΣΚΩΝ: Ε. Μαρκάκης

2η Σειρά Ασκήσεων
Προθεσμία Παράδοσης: 19/1/2014

Πρόβλημα 1 (5 μονάδες)

Υπολογίστε τον gcd(995, 220) και τον gcd(332, 111) χρησιμοποιώντας τον αλγόριθμο του Ευκλείδη.

Πρόβλημα 2 (15 μονάδες)

Εφαρμόστε το Κινέζικο θεώρημα υπολοίπων για να βρείτε τη λύση του συστήματος $x \equiv 3 \bmod 4$, $x \equiv 1 \bmod 9$, $x \equiv 3 \bmod 7$. Να χρησιμοποιήσετε τον εκτεταμένο αλγόριθμο του Ευκλείδη για τους υπολογισμούς των πολλαπλασιαστικών αντιστρόφων που θα χρειαστείτε. Σε ποιο modulus έχει μοναδική λύση το σύστημα αυτό;

Πρόβλημα 3 (10 μονάδες)

1) Η εξίσωση $7x \equiv 1 \bmod 128$ έχει λύση στο Z_{128}? Αν ναι βρείτε την. Απαντήστε την ίδια ερώτηση για την $6x \equiv 1 \bmod 128$ στο Z_{128}.
2) Χωρίς να χρησιμοποιήσετε κομπιουτεράκι ή οποιοδήποτε άλλο μέσο (ούτε τον αλγόριθμο του επαναλαμβανόμενου τετραγωνισμού), υπολογίστε τις ποσότητες: $2 \cdot 7^{32} \bmod 31$, και $3 \cdot 7^{17} + 11^{33} + 3 \cdot 13^{49} \bmod 60$.

Πρόβλημα 4 (15 μονάδες)

Έστω ένα S-box S: $\{0, 1\}^3 \rightarrow \{0, 1\}^3$ που ορίζεται από τον παρακάτω πίνακα. Θεωρούμε τον δείκτη *a,* ο οποίος ορίζει τις δυαδικές μεταβλητές της εισόδου και τον δείκτη *b,* ο οποίος ορίζει τις δυαδικές μεταβλητές της εξόδου. Οι δείκτες a και b παίρνουν τιμές από 0 έως 7. Η δυαδική απεικόνιση των δεικτών φανερώνει τα επιλεγμένα bits. Για παράδειγμα, αν $a = (6)_{10} = (110)_2$, ο δείκτης αντιστοιχεί στο P_1 XOR P_2. Βρείτε τις τιμές NS(a, b) για (a, b) = (3,1), (5, 7), και (7, 5).

P1	P2	P3	C1	C2	C3
0	0	0	1	1	0
0	0	1	1	1	1
0	1	0	0	1	1
0	1	1	1	0	1
1	0	0	0	0	0
1	0	1	1	1	0
1	1	0	1	0	1
1	1	1	1	1	1

Πίνακας 1. Πίνακας αληθείας του S

Πρόβλημα 5 (8 μονάδες)

Υπολογίστε την πόλωση της τυχαίας μεταβλητής $P_1 \oplus P_2 \oplus C_1 \oplus C_2 \oplus C_3$ για το 3ο S-box του DES, το S_3. Ο πίνακας αληθείας του S_3 βρίσκεται στο βιβλίο και στις διαφάνειες.

Πρόβλημα 6 (15 μονάδες)

Έστω σχήμα RSA με p = 5 και q = 11. Βρείτε το δημόσιο και ιδιωτικό κλειδί. Έστω ότι η Alice θέλει να στείλει στον Bob το μήνυμα 39. Περιγράψτε τη διαδικασία κρυπτογράφησης/αποκρυπτογράφησης του μηνύματος και τους υπολογισμούς που χρειάζεται να κάνουν η Alice και ο Bob.

Πρόβλημα 7 (10 μονάδες)

Έστω σχήμα RSA με (e, n) και (d, p, q) το δημόσιο και το ιδιωτικό κλειδί του Bob αντίστοιχα. Υποθέτουμε ότι n = pq, όπου p, q διακριτοί πρώτοι αριθμοί. Έστω ότι η Alice έχει στείλει ένα μήνυμα x, και ο Bob έχει λάβει το ciphertext $y = x^e \bmod n$. Ένας αλγόριθμος που χρησιμοποιείται για να επιταχύνουμε τη διαδικασία αποκρυπτογράφησης για τον Bob είναι ο εξής:

$s := d \bmod (p-1)$, $M_p := q^{-1} \bmod p$
$t := d \bmod (q-1)$, $M_q := p^{-1} \bmod q$
//οι παραπάνω τιμές υπολογίζονται 1 φορά και
//χρησιμοποιούνται σε κάθε αποκρυπτογράφηση
$Z := y^s \bmod p$
$W := y^t \bmod q$
Return $(M_p \cdot q \cdot Z + M_q \cdot p \cdot W) \bmod n$

Δείξτε ότι αυτός ο αλγόριθμος όντως επιστρέφει το αρχικό μήνυμα x, στον Bob (Hint: χρησιμοποιήστε το θεώρημα Fermat). Γιατί θεωρείται πιο γρήγορος αυτός ο αλγόριθμος?

Πρόβλημα 8 (10 μονάδες)

Κατασκευάστε τα μερίδια σε ένα Shamir σχήμα κατωφλίου με 6 συμμετέχοντες, έτσι ώστε 3 από τα 6 μερίδια να μπορούν να ανακατασκευάσουν το μυστικό M=14.

Πρόβλημα 9 (12 μονάδες)

1) Εξηγήστε πώς μπορούμε να αναπαραστήσουμε ένα byte στο AES με ένα πολυώνυμο.
2) Έστω τα bytes 10110111 και 00000101. Υπολογίστε τον πολλαπλασιασμό των 2 αντίστοιχων πολυωνύμων, και ανάγετε το αποτέλεσμα mod m(x), όπως δηλαδή υπολογίζεται το γινόμενο στο AES (όπου m(x) είναι το ανάγωγο πολυώνυμο που χρησιμοποιείται στο AES).