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.

gcd(995, 220) = gcd(220, 115) = gcd(115, 105) = gcd(105, 10) = gcd(10, 5) = gcd(5, 0) = 5

gcd(332, 111) = gcd(111, 110) = gcd(110, 1) = gcd(1, 0) = 1

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;

Εφαρμόζουμε τον αλγόριθμο που είδαμε και στην τάξη. Σύμφωνα με τον συμβολισμό που χρησιμοποιήσαμε έχουμε:

$n_1 = 4$, $c_1 = 63$

$n_2 = 9$, $c_2 = 28$

$n_3 = 7$, $c_3 = 36$

$n = 252$

Υπολογίζουμε τους πολλαπλασιαστικούς αντιστρόφους του κάθε $c_i \bmod n_i$ και παίρνουμε

$d_1 = 3 \pmod 4$

$d_2 = 1 \pmod 9$

$d_3 = 1 \pmod 7$

Επομένως η τελική λύση είναι

$SOL = 3 \cdot 63 \cdot 3 + 1 \cdot 28 \cdot 1 + 3 \cdot 36 \cdot 1 \bmod 252 = 199$

Το σύστημα έχει μοναδική λύση στο Z_{252}. Όλες οι λύσεις είναι της μορφής $199 + 252 \cdot t$ για οποιοδήποτε ακέραιο t.

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 $3 \cdot 7^{17} + 11^{33} + 3 \cdot 13^{49} \bmod 60$.

1) Αφού gcd(128, 7) = 1, η εξίσωση έχει λύση, και χρησιμοποιώντας τον εκτεταμένο αλγόριθμο Ευκλείδη, βρίσκουμε ότι είναι η x = 55.

Επειδή gcd(128, 6) >1, η $6x \equiv 1 \bmod 128$ δεν έχει λύση στο Z_{128}.

2) Με χρήση των θεωρημάτων Fermat και Euler. Από Θεώρημα Fermat, ξέρουμε ότι $7^{30} \equiv 1 \bmod 31$. Απλοποιούμε με βάση αυτό και βρίσκουμε τελικά ότι η έκφραση αυτή είναι ίση με 5. Για την 2^{η} έκφραση χρησιμοποιούμε το γεγονός ότι φ(60) = 16. Και επίσης ότι οι αριθμοί 7, 11, 13 είναι σχετικά πρώτοι με το 60, άρα π.χ. $7^{16} \equiv 1 \bmod 60$. Κάνοντας τις απλοποιήσεις παίρνουμε ότι η 2^{η} εκφραση είναι ίση με 11.

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

(a, b) = (3,1): Αυτό αντιστοιχεί στη γραμμική σχέση P_2 XOR $P_3 = C_3$. Ελέγχουμε απλώς σε ποιες από τις 8 πιθανές εισόδους ικανοποιείται αυτή η σχέση. Και καταλήγουμε ότι NS(3, 1) = 5.

Ομοίως για (a, b) = (5, 7), έχουμε τη σχέση P_1 XOR $P_3 = C_1$ XOR C_2 XOR C_3. Ελέγχοντας τον πίνακα παίρνουμε ότι NS(5, 7) = 4.

για (a, b) = (7, 5), έχουμε τη σχέση P_1 XOR P_2 XOR $P_3 = C_1$ XOR C_3. Ελέγχοντας τον πίνακα παίρνουμε ότι NS(7, 5) = 3.

Σημείωση: Θα μπορούσαμε να είχαμε πάρει τα bits με την ανάποδη σειρά. Π.χ. το α = 3 να αντιστοιχούσε στο P_1 XOR P_2. Αυτό είναι απλά θέμα σύμβασης, κάποια βιβλία το κάνουν με τον ένα τρόπο και κάποια με τον άλλο. Δεν επηρεάζεται η κρυπτανάλυση από αυτό. Όποιον από τους 2 τρόπους και αν επιλέξει ο Όσκαρ, αν υπάρχει κάποια γραμμική σχέση που δίνει καλή πόλωση θα τη βρει αφού ο Όσκαρ τις ψάχνει όλες τις σχέσεις (θα ψάξει όλα τα ζεύγη a, b). Το αν η σχέση αυτή είναι η P_2 XOR P_3 = C_3 με τη σύμβαση που ακολουθήσαμε ή η P_1 XOR P_2 = C_1 αν ακολουθούσαμε την άλλη σύμβαση, δεν έχει σημασία για αυτόν.

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.

Θα πρέπει να δούμε τις 64 πιθανές εισόδους για το S_3 και να δούμε πόσες φορές από τις 64 επαληθεύεται η σχέση μας. Μπορείτε να το δείτε απευθείας από τον πίνακα που υπάρχει στο βιβλίο σας (σε πιο συμπαγή μορφή με τις γραμές και τις στήλες να κωδικοποιούν την είσοδο) για το S_3, ή μπορείτε να μετατρέψετε τον πίνακα του βιβλίου σε έναν κλασικό πίνακα αληθείας με 64 γραμμές εισόδου και να μετρήσετε εκεί. Κάνοντας τον υπολογισμό αυτό θα δείτε ότι τελικά η πόλωση είναι -1/32.

Σημείωση: Το νόημα της άσκησης ήταν να δείτε ότι οι γραμμικές σχέσεις δεν έχουν καλή πόλωση στο DES (είναι κοντά στο 0), το οποίο είναι επιθυμητό χαρακτηριστικό σε ένα κρυπτοσύστημα, καθώς δεν είναι τελείως προφανές το πώς θα φτιάξει κανείς μονοπάτια γραμμικών σχέσεων για να κάνει γραμμική κρυπτανάλυση.

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.

Έχουμε n=55. Άρα φ(n) = 40. Πρέπει να διαλέξουμε το δημόσιο κλειδί e, έτσι ώστε gcd(e, φ(n)) = 1. Μας κάνει οποιοσδήποτε πρώτος αριθμός που είναι μεγαλύτερος από το 11. Άρα μπορούμε να επιλέξουμε το 13 (θα μπορούσαμε να επιλέξουμε και μικρότερο αριθμό, π.χ. το 7, αφού είναι σχετικά πρώτος με το 40). Στη συνέχεια βρίσκουμε το d, που είναι ο πολλαπλασιαστικός αντίστροφος του 13 mod φ(n). Προκυπτει ότι d = 37. Επομένως, η κρυπτογράφηση γίνεται με ύψωση στο 13, και η αποκρυπτογράφηση με ύψωση στο 37.

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 mod (p-1), Mp := q^-1 mod p
t := d mod (q-1), Mq := p^-1 mod q
//οι παραπάνω τιμές υπολογίζονται 1 φορά και
//χρησιμοποιούνται σε κάθε αποκρυπτογράφηση
Z := y^s mod p
W := y^t mod q
Return  (Mp·q·Z + Mq·p·W) mod 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?

Έστω $C = M_p \cdot q \cdot Z + M_q \cdot p \cdot W$

Αυτό που έπρεπε να κάνετε είναι να δείξετε πρώτα χρησιμοποιώντας το θεώρημα Fermat ότι $C \equiv x \bmod p$, και μετά ομοίως ότι $C \equiv x \bmod q$.

Στη συνέχεια, από Κινέζικο θεώρημα ξέρουμε ότι για n = pq, ένας αριθμός είναι ισοδύναμος με x mod n αν και μόνο αν είναι ισοδύναμος με x mod p ΚΑΙ ισοδύναμος με x mod q. Άρα τελικά προκύπτει ότι $C \equiv x \bmod n$, που σημαίνει ότι ο Bob όντως αποκρυπτογραφεί σωστά και πάιρνει το αρχικό μήνυμα.

Ο αλγόριθμος αυτός είναι πιο γρήγορος γιατί κάνουμε πράξεις με μικρότερους αριθμούς (mod p και mod q) αντί για την κλασική υλοποίηση που οι πράξεις γίνονται mod n.

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.

Διαλέγουμε αρχικά ένα πεπερασμένο πεδίο, έστω το $(Z_{17}, +, *)$. Αυτό είναι οκ, καθώς 17 > 14. Στη συνέχεια πρέπει να διαλέξουμε ένα πολυώνυμο με βαθμό 3-1 = 2. Ο σταθερός όρος πρέπει να είναι το M. Έστω το $f(x) = 3x^2 + 8x + 14$. Μετά διαλέγουμε 6 σημεία, έστω τα 1, 2,...,6, και υπολογίζουμε τις τιμές f(1),…,f(6) mod 17. Δίνουμε σε κάθε παίκτη i, το ζεύγος (i, f(i) mod 17).

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).

1) Ένα byte αντιστοιχεί σε ένα πολυώνυμο με μέγιστο βαθμό 7. Κάθε bit μας υποδηλώνει αν η αντίστοιχη δύναμη του πολυωνύμου έχει συντελεστή 0 ή 1. Το MSB μας δηλώνει τον συντελεστή του x^7, το επόμενο bit τον συντελεστή του x^6, κ.ο.κ. μέχρι το LSB, το οποίο μας δείχνει τον σταθερό όρο.
2) Έχουμε να κάνουμε τον πολλαπλασιασμό:

$(x^7 + x^5 + x^4 + x^2 + x + 1)(x^2 + 1) = x^9 + x^6 + x^5 + x^3 + x + 1$ (οι όροι που εμφανίζονται 2 φορές ακυρώνονται αφού είμαστε στο $GF(2^8)$)

Στη συνέχεια πρέπει να διαιρέσουμε το πολυώνυμο αυτό με το αμείωτο πολυώνυμο που χρησιμοποιείται στο AES, το $m(x) = x^8 + x^4 + x^3 + x + 1$. Η διαίρεση μας δίνει ως υπόλοιπο το $x^6 + x^4 + x^3 + x^2 + 1$, το οποίο αντιστοιχεί στο 01011101.