Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Υπολογιστική Κρυπτογραφία
4η Σειρά Ασκήσεων

Προθεσμία παράδοσης: 1/12/2017

21 Νοεμβρίου 2017

1η Άσκηση

Έστω ότι υπάρχει ακέραιος n_0 τέτοιος ώστε να ισχύουν $\gcd(p^{ab}, ab) = p$ για κάθε πρώτο $p \leq n_0$ και $\gcd(p^{ab}, ab) = 1$ για κάθε πρώτο $p > n_0$. Δείξτε ότι $\gcd(a, b) = 1$.

2η Άσκηση

(α) Παραγοντοποιήστε τον αριθμό 143 εφαρμόζοντας την μέθοδο ρ και την μέθοδο βάσεων παραγοντοποίησης Dixon. Τι παρατηρείτε;

(β) Υλοποιήστε σε πρόγραμμα τη μέθοδο ρ 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;

3η Άσκηση

Ο διευθυντής μιας εταιρείας χρειάζεται να παίρνει συχνά κρυπτογραφημένα μηνύματα από τους υπαλλήλους του. Για το σκοπό αυτό χρησιμοποιεί RSA, δίνοντας σε όλους το δημόσιο κλειδί του (n, e), όπου $n = pq$ με p, q πρώτους. Φυσικά κρατάει κρυφούς τους πρώτους p, q. Για ευκολία, δίνει επιπλέον στη γραμματέα του μία συσκευή με την οποία θα μπορούν οι υπάλληλοι που δεν διαθέτουν το πρόγραμμα κρυπτογράφησης να κρυπτογραφούν τα μηνύματά τους. Η συσκευή θα λειτουργεί ως εξής για είσοδο m:

- Υπολογίζει $c_p = m^e \bmod p$,
- Υπολογίζει $c_q = m^e \bmod q$,
- Συνδιάζει τις λύσεις με CRT ώστε να δώσει ως έξοδο τη μοναδική τιμή $c \in \mathbb{Z}_n$ τ.ω. $c \equiv m^e \bmod n$.

Λόγω ενός εργοστασιακού λάθους, στο δεύτερο βήμα, η συσκευή υπολογίζει $c'_q = 2m^e \bmod q$ και δίνει έξοδο $c' \in \mathbb{Z}_n$ τ.ω. $c' \equiv c_p \bmod p$, $c' \equiv c'_q \bmod q$. Όπως είναι φυσικό, ο διευθυντής

σύντομα διαπιστώνει ότι κάτι δεν πάει καλά (*με ποιον τρόπο;*) και ζητάει από τη γραμματέα του να στείλει τη συσκευή για επισκευή. Η γραμματέας, όμως, που έχει παρακολουθήσει προσεκτικά το μάθημα της κρυπτογραφίας, κατορθώνει, πριν στείλει τη συσκευή στο service να βρει το ιδιωτικό κλειδί του διευθυντή. Πώς το κατάφερε αυτό;

4η Άσκηση

Έστω $\mathbb{Z}_p^*$ με p πρώτο και g ένας γεννήτορας, p, g γνωστά.

1. Αν d ένας ακέραιος που διαιρεί το $p-1$, βρείτε με αποδοτικό τρόπο ένα στοιχείο b του $\mathbb{Z}_p^*$ τάξης d (δηλαδή d ο μικρότερος ακέραιος με $b^d \equiv 1 \pmod{p}$)
2. Πόσα στοιχεία τάξης d υπάρχουν μέσα στο $\mathbb{Z}_p^*$;
3. Πόσους γεννήτορες έχει η κυκλική υποομάδα που παράγει ένα στοιχείο b τάξης d;
4. Πόσες κυκλικές υποομάδες τάξης d υπάρχουν στο $\mathbb{Z}_p^*$;
5. Αν μας δώσουν ένα στοιχείο h, την τάξη του d και ένα τυχαίο στοιχείο a, πως μπορούμε να δούμε αν το a ανήκει στην υποομάδα που παράγει το h σε πολυωνυμικό χρόνο;