Α44 – ΚΡΥΠΤΟΓΡΑΦΙΑ
ΦΥΛΛΑΔΙΟ ΑΣΚΗΣΕΩΝ $\#3\beta$

ΘΕΟΔΟΥΛΟΣ ΓΑΡΕΦΑΛΑΚΗΣ

Άσκηση 1

Υλοποιήστε το σύστημα κρυπτογράφησης ElGamal σε ομάδες της μορφής $\mathbb{F}_p^\times$. Υλοποιήστε τρεις συνατρήσεις:

- Την gen_params, η οποία ρωτά το χρήστη το μέγεθος του πρώτου και δίνει ως έξοδο τον πρώτο p και ένα ακέραιο $g \in [2, p-1]$. Η επιλογή του πρώτου θα πρέπει να είναι «καλή», δηλαδή το $p-1$ θα πρέπει να διαιρείται από μεγάλο πρώτο q. Επίσεις, η τάξη του g mod p θα πρέπει να είναι τουλάχιστον q.
- Την encrypt, η οποία παίρνει ως είσοδο τα p, g και ένα μήνυμα (το οποίο αν θέλετε μπορείτε να θεωρήσετε ότι είναι ένας αριθμός), και δίνει ως έξοδο το κρυπτογράφημα.
- Την decrypt, η οποία παίρνει ως είσοδο τα p, g και ένα κρυπτογράφημα και δίνει ως έξοδο το καθαρό μήνυμα.

Μία βιβλιοθήκη C++ την οποία μπορείτε (αλλά δεν είστε φυσικά υποχρεωμένοι) να χρησιμοποιήσετε για την άσκηση είναι η NTL του Victor Shoup η οποία διατίθεται ελεύθερα στη διεύθυνση www.shoup.net.

Άσκηση 2

Έστω ότι χρησιμοποιήτε ένα σύστημα κρυπτογράφησης RSA, με δημόσιο κλειδί n, e και ιδιωτικό κλειδί d, όπου φυσικά $ed \equiv 1 \pmod{\phi(n)}$. Για να προστατεύσετε το ιδιωτικό σας κλειδί, το «χωρίζετε» σε δύο κομμάτια, d_1 και d_2, όπου $d_1 + d_2 \equiv d \pmod{\phi(n)}$ και αποθηκεύετε κάθε κομμάτι σε διαφορετικό υπολογιστή, έτσι ώστε αν κάποιος αποκτήσει παράνομα πρόσβαση σε έναν από τους υπολογιστές να μην μάθει τίποτα για το κλειδί σας. Έστω ότι λαμβάνετε ένα κρυπτογράφημα c και το στέλνετε και στους δύο υπολογιστές. Ο κάθε υπολογιστής κάνει κάποιο υπολογισμό με δεδομένα το c και το κομμάτι του κλειδιού που γνωρίζει (π.χ. ο υπολογιστής i έχει δεδομένα τα c, d_i), και σας στέλνει το αποτέλεσμα m_i του υπολογισμού του. Έσεις στη συνέχεια συνδοιάζετε τα m_i για να πάρετε το καθαρό μήνυμα.

(1) Περιγράψτε τον υπολογισμό που πρέπει να κάνει κάθε υπολογιστής.
(2) Περιγράψτε πώς έσεις συνδοιάζετε τα αποτελέσματα για να πάρετε το καθαρό μήνυμα.
(3) Γενικεύστε το σχήμα για περισσότερους υπολογιστές.
(4) Εξηγήστε, χώρις αυστηρή απόδειξη, γιατί αν κάποιος μάθει το πολύ $n-1$ κομμάτια του κλειδιού δεν έχει μάθει ουσιαστικά τίποτα.

Παρατηρήστε ότι με το παραπάνω σχήμα αποκρυπτογραφήτε χώρις ποτέ να ανακατασκευάσετε το κλειδί d. Το κειδί δηλαδή δεν εμφανίζεται σε κανένα υπολογιστή.