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

ΘΕΟΔΟΥΛΟΣ ΓΑΡΕΦΑΛΑΚΗΣ

Άσκηση 1

Στην άσκηση αυτή θα κατασκευάσουμε ένα αλγόριθμο ο οποίος παραγοντοποιεί αριθμούς της μορφής $n = pq$, όπου p, q πρώτοι και ο $p + 1$ έχει μόνο μικρούς πρώτους παράγοντες, ενώ ο $q + 1$ διαιρείται από ένα τουλάχιστο μεγάλο πρώτο.

Αρχικά επιλέγουμε ένα αριθμό $1 < d < n$, $(d, n) = 1$. Αν $(d, n) > 1$ τότε βρήκαμε ένα πρώτο παράγοντα του n και τελειώσαμε. Ας υποθέσουμε ότι η τάξη του d mod p είναι $p-1$. Αν δεν είναι, τότε ο αλγόριθμος απλά θα αποτύχει. Αυτό συνεπάγεται ότι το πολυώνυμο $X^2 - d$ είναι ανάγωγο πάνω στο $\mathbb{F}_p$.

Επιλέγουμε ακεραίους $a, b \in [1, n - 1]$. Μπορούμε να υποθέσουμε ότι $(a, n) = (b, n) = 1$. Αν $(a, n) > 1$ ή $(b, n) > 1$ παραγοντοποιούμε και τελειώσαμε. Γενικά στις παρακάτω σχέσεις, όπου εμφανίζονται αντίστροφοι mod n μπορούμε να υποθέτουμε ότι υπάρχουν. Αν κάποιος δεν υπάρχει σημαίνει ότι μπορούμε να παραγοντοποιήσουμε. Σχηματίζουμε το πολυώνυμο $f(X) = a+bX$ και ορίζουμε $f^*(X) = a-bX$, όπου $f, f^* \in \mathbb{Z}/n\mathbb{Z}[X]$, δηλαδή κάνουμε στους συντελεστές αριθμητική mod n.

(1) Δείξτε ότι

$$g(X) \equiv \frac{f(X)}{f^*(X)} \equiv \frac{a^2 + b^2d^2}{a^2 - b^2d^2} + \frac{-2ab}{a^2 - b^2d^2}X \pmod{X^2 - d, n}.$$

(2) Αν $s, t \in \mathbb{Z}$ με

$$\begin{aligned} s &\equiv \frac{a^2 + b^2d^2}{a^2 - b^2d^2} \pmod{n}, \\ t &\equiv \frac{-2ab}{a^2 - b^2d^2} \pmod{n} \end{aligned}$$

δείξτε ότι

$$(s + tX)^{p+1} \equiv 1 \pmod{X^2 - d, p}.$$

(3) Έστω $E \in \mathbb{N}$ και ορίζουμε τα $u, v \in \mathbb{Z}$ από τη σχέση

$$u + vX \equiv (s + tX)^E \pmod{X^2 - d, n}.$$

Δείξτε ότι αν $p + 1|E$, τότε

$$u + vX \equiv 1 \pmod{p}.$$

(4) Το πολυώνυμο $u + vX$, όταν το δούμε mod q, τίποτα το αξιοσημείωτο δε συμβαίνει, εφόσον $q + 1 \not| E$. Συγκεκριμένα, περιμένει κανείς να ισχύει για το αντίστοιχο πολυώνυμο

$$u + vX \not\equiv 1 \pmod{q}.$$

Υποδείξτε πώς μπορούμε να παραγοντοποιήσουμε έχοντας υπολογίσει τα u και v.

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 $n \geq 2$ 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.