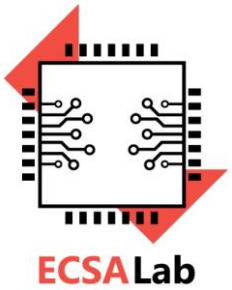
Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Πανεπιστημίου Πελοποννήσου

Εργαστήριο Ηλεκτρονικών Κυκλωμάτων, Συστημάτων και Εφαρμογών (ECSA Lab.)



Ασφάλεια Υπολογιστικών Συστημάτων

Διδάσκων: Δρ. Παρασκευάς Κίτσος (Καθηγητής)

Επαναληπτικές Ασκήσεις

1) Κρυπτογραφήστε και αποκρυπτογραφήστε με το αλγόριθμο RSA το μήνυμα με τις παρακάτω παραμέτρους: p = 3, q = 11, Ke = 7 για M = 5

Λύση

Για να κατασκευάσουμε τις παραμέτρους του αλγορίθμου RSA επιλέγουμε αρχικά δύο πρώτους αριθμούς p, q με τέτοιους ώστε $n = pq$ και έναν ακέραιο K_e. Έπειτα υπολογίζουμε τον αριθμό $K_d \equiv K_e^{-1}(mod\, \varphi\,(n))$. Τότε το δημόσιο κλειδί αποτελείται από το ζεύγος (K_e, n) ενώ το ιδιωτικό κλειδί από το ζεύγος (K_d, n). Για να κρυπτογραφήσουμε το μήνυμα M υπολογίζουμε τον όρο $y = M^{K_e}(mod\, n)$ ενώ για να αποκρυπτογραφήσουμε τον y υπολογίζουμε τον όρο $M = y^{K_d}(mod\, n)$.

Άρα n = 3 x 11 = 33, $\varphi(n)$ = 20 και $K_d = 7^{-1}\, mod\, 2\, 0 = 3$. Οπότε η κρυπτογράφηση του μηνύματος M = 5 δίνει $5^7\, mod\, 3\, 3 = 14$ και η αποκρυπτογράφηση του 14 δίνει $14^3\, mod\, 3\, 3 = 5$.

2) Έστω δύο πρώτοι αριθμοί p, q τέτοιοι ώστε να ισχύει n = pq. Έστω επίσης δύο ακέραιοι αριθμοί d, e τέτοιοι ώστε $de \equiv 1(mod(p-1)(q-1))$.

Να δείξετε ότι εάν $gcd(x, n) = 1$ και $c \equiv x^e(mod\, n)$ τότε ισχύει $x \equiv c^d(mod\, n)$.

Λύση

Έχουμε $de \equiv 1(mod(p-1)(q-1)) => de = 1 + (p-1)(q-1)k$ όπου k ακέραιος. Τότε ισχύει $c^d \equiv x^{de} \equiv x(x^{(p-1)(q-1)})^k \equiv x1^k(mod\, n)$

Γιατί?

$\varphi(n) = \varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1)$

$a^{\varphi(n)} \equiv 1(mod\, n)$

με βάση το θεώρημα Euler.

Άρα: $x \equiv c^d(mod\, n)$.

3) Έστω ότι το δημόσιο κλειδί του Θάνου είναι το n = 2181606148950875138077 και ο εκθέτης στην κρυπτογράφηση του είναι ίσος με 7. Ο Κώστας κρυπτογραφεί το μήνυμα hi eve = 080900052205 = m. Κατά τύχη το μήνυμα, m, ικανοποιεί την σχέση $m^3 \equiv 1(mod\, n)$. Εάν η Αλίκη αναχαιτίσει το κρυπτοκείμενο πως μπορεί να το αποκρυπτογραφήσει (διαβάσει) χωρίς να παραγοντοποιήσει τον *n*;

Λύση

Αφού ισχύει $m^3 \equiv 1(mod\, n)$ το κρυπτοκείμενο θα είναι $c \equiv m^7 \equiv m(m^3)^2 \equiv m1^2 \equiv m(mod\, n)$.

Άρα το κρυπτοκείμενο είναι ίδιο με το απλό κείμενο. Αυτό σημαίνει ότι η Αλίκη μπορεί να το διαβάσει χωρίς αποκρυπτογράφηση.