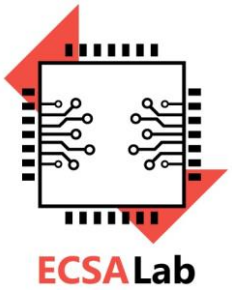
Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Πανεπιστημίου Πελοποννήσου

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



Ασφάλεια Υπολογιστικών Συστημάτων

Διδάσκων: Δρ. Παρασκευάς Κίτσος (Καθηγητής)

Επαναληπτικές Ασκήσεις

1) Να υπολογίσετε τον αντίστροφο του 4 mod (11) με την βοήθεια του θεωρήματος Euler.

Λύση

Το θεώρημα του Euler είναι το παρακάτω:

Εάν gcd(a, n)=1 και n>1 τότε $a^{\varphi(n)} \equiv 1 \pmod n$ για κάθε a

Ο αντίστροφος του a (a^{-1}) είναι ο $x= a^{\varphi(n)-1} \pmod n$

Άρα από τα δεδομένα της άσκησης προκύπτει ότι a=4 και n=11 που ισχύει ότι gcd(4, 11)=1.

Επίσης, ο n=11 είναι πρώτος άρα φ(n)=11-1=10 και ο αντίστροφος είναι ο $x=4^{10-1} \bmod 11 = 3$.

Άρα ο ζητούμενος αντίστροφος είναι ο 3.

2) Να υπολογίσετε τον Μέγιστο Κοινό Διαιρέτη μεταξύ των αριθμών 109 και 71. Υπόδειξη: Να κάνετε χρήση της σχέσης gcd(a, b) =gcd(b, a mod b) που ισχύει για οποιονδήποτε μη αρνητικό ακέραιο a και οποιονδήποτε θετικό ακέραιο b.

Λύση

Θα κάνουμε χρήση της σχέσης: $a \bmod n = \begin{cases} a, & \text{αν } n = 0 \\ a - \lfloor a/n \rfloor n, & \text{διαφορετικά} \end{cases}$

Έχουμε, gcd(109, 71) = gcd(71, 109 mod 71) = gcd(71, 38) = gcd(38, 71 mod 38) = gcd(38, 33) = gcd(33, 38 mod 33) = gcd(33, 5) = gcd (5, 33 mod 5) = gcd(5, 3) = gcd(3, 5 mod 3) = gcd(3,2) = gcd(2, 3 mod 2) = gcd(2, 1)= gcd(1, 2 mod 1) = gcd(1, 0) = 1.

Άρα, gcd(109, 71) = 1.

3) Έστω ότι ο Τάκης και ο Σωτήρης έχουν επιλέξει τους πρώτους αριθμούς p=11 και g=2 για δημόσιο κλειδί. Ο αριθμός 2 είναι πρωτογενής ρίζα του 11. Αν ο Τάκης επιλέξει για ιδιωτικό κλειδί το a=2 και ο Σωτήρης επιλέξει για ιδιωτικό κλειδί το b=3 να υπολογίσετε το κοινό μυστικό κλειδί που θα υπολογίσουν και οι δύο σύμφωνα με τον αλγόριθμο DIFFIE-HELLMAN.

Λύση

Ο Τάκης υπολογίζει τη παράσταση $g^a \bmod p = 2^2 \bmod 11 = 4$ και το αποτέλεσμα το στέλνει στον Σωτήρη.

Ταυτόχρονα, ο Σωτήρης υπολογίζει τη παράσταση $g^b \bmod p = 2^3 \bmod 11 = 8$ και το αποτέλεσμα το στέλνει στον Τάκη.

Ο Τάκης αφού έλαβε τον αριθμό 8 υπολογίζει την παράσταση $8^a \bmod p = 8^2 \bmod 11 = 64 \bmod 11 = 9$.

Ταυτόχρονα ο Σωτήρης αφού έλαβε τον αριθμό 4 υπολογίζει την παράσταση $4^b \bmod p = 4^3 \bmod 11 = 64 \bmod 11 = 9$.

Άρα, οι Τάκης και Σωτήρης υπολόγισαν τον αριθμό 9 ως κοινό μυστικό κλειδί με τον αλγόριθμο DIFFIE-HELLMAN.

4) Έστω οι πρώτοι αριθμοί p=5 και q=7. Να κρυπτογραφήσετε το μήνυμα 424 με τη βοήθεια του αλγορίθμου RSA.

Λύση

Τα βήματα εκτέλεσης του RSA είναι τα παρακάτω:

p = 5, q = 7.

n = pq=35.

φ(n) = (p - 1)(q - 1) = 24.

Επιλογή του e έτσι ώστε να είναι αμοιβαία πρώτος του φ(n) = 24, e = 5.

Υπολογισμός d έτσι ώστε $de \equiv 1 \bmod 24$.

[Υπολογισμός του d έτσι ώστε να ισχύει $ed \equiv 1 \pmod{\varphi(n)}$ ή $d=5^{-1} \pmod{24}$ ή υπολογισμός του d έτσι ώστε η φ(n)=24 να διαιρεί τη παράσταση ed=5d και να έχει υπόλοιπο 1 ($ed \equiv 1 \pmod{\varphi(n)}$ ή $ed \pmod{\varphi(n)} = 1 \pmod{\varphi(n)} \Rightarrow ed \pmod{\varphi(n)} = 1$.

Δοκιμές για d=2,3,4,…

Υπολογίζεται ότι d=5.]

Άρα

Δημόσιο κλειδί =(5, 35)

Ιδιωτικό κλειδί = (5, 35)

Οπότε η κρυπτογράφηση του μηνύματος M = 424:

$C = (424)^5 \bmod 35 = 9.$