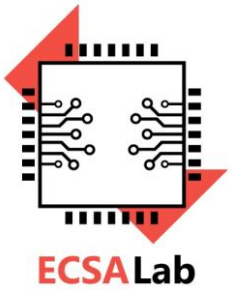
Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Πανεπιστημίου Πελοποννήσου

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



Ασφάλεια Υπολογιστικών Συστημάτων

Διδάσκων: Δρ. Παρασκευάς Κίτσος (Καθηγητής)

Επαναληπτικές Ασκήσεις

1) Έστω οι πρώτοι αριθμοί p=5 και q=7. Να κρυπτογραφήσετε το μήνυμα ECE με τη βοήθεια του αλγορίθμου RSA θεωρώντας ότι το γράμμα Α αντιστοιχεί στον αριθμό 0, το γράμμα Β αντιστοιχεί στον αριθμό 1, το γράμμα C αντιστοιχεί στον αριθμό 2 κ.ο.κ

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 ≡ 1 mod 24.

[Υπολογισμός του d έτσι ώστε να ισχύει ed ≡ 1 (mod φ(n)) ή $d=5^{-1}$(mod 24) ή υπολογισμός του d έτσι ώστε η φ(n)=24 να διαιρεί τη παράσταση ed=5d και να έχει υπόλοιπο 1 (ed ≡ 1 (mod φ(n)) ή ed (mod φ(n))=1 (mod φ(n))=>ed (mod φ(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 = $(424)^5$ mod 35 = 9.

2) Έστω ότι το δημόσιο κλειδί του Θάνου είναι το n = 218160614895087513807 7 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*;

<u>Λύση</u>

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.

3) Έστω ότι έχετε έναν χρήστη ενός δικτύου (Νίκος) ο οποίος θέλει να επικοινωνήσει με κάποιον άλλον χρήστη του ίδιου δικτύου (Κώστας). Τα βήματα που εκτελούνται στις συσκευές των χρηστών είναι αρχικά η Ανταλλαγή των κλειδιών και Πιστοποίηση μηνύματος με συμμετρική κρυπτογράφηση.

Για την ανταλλαγή των κλειδιών να χρησιμοποιήσετε τον DIFFIE-HELLMAN με πρώτους αριθμούς p = 23 και g = 5. Ο αριθμός 5 είναι πρωτογενής ρίζα του 23. Το μυστικό κλειδί του Νίκου είναι το a=2 και του Κώστα το b=3.

Η συνάρτηση κατακερματισμού έχει εξίσωση H(x)=x^3 mod 100. Το μήνυμα προς πιστοποίηση είναι το M=15.

Για την κρυπτογράφηση/αποκρυπτογράφηση να χρησιμοποιήσετε έναν αλγόριθμο τμήματος που έχει σχεδιαστεί με χρήση Feistel δικτύων. Ο αλγόριθμος έχει δύο γύρους χωρίς αρχική και τελική μετάθεση. Η συνάρτηση που χρησιμοποιείται σε κάθε γύρο είναι η $F_i(x, K) = (2iK)^x \mod 15$ για i=1, 2.

Να εκτελέσετε το σχήμα της επικοινωνίας μόνο για τον Νίκο.

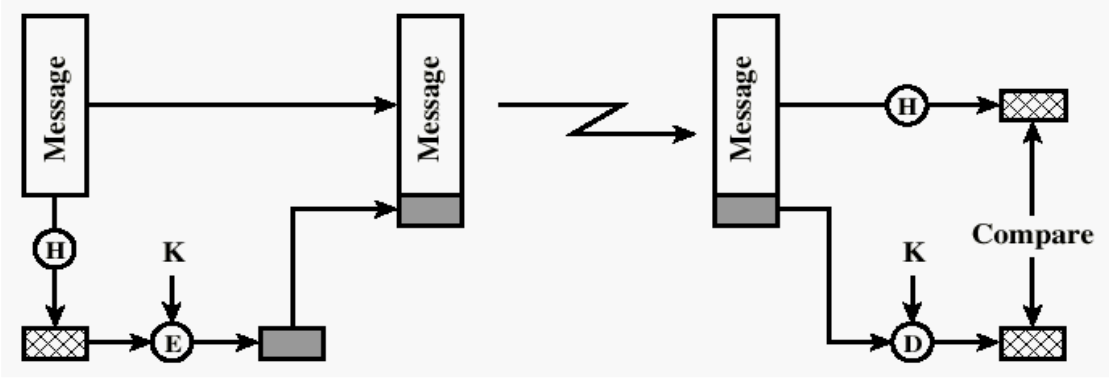
<u>Λύση</u>

Αρχικά θα βρεθεί το μυστικό κλειδί που απαιτείται να μοιραστούν ο Νίκος με τον Κώστα. Άρα

- Ο Νίκος στέλνει στο Κώστα το αποτέλεσμα της παράστασης $g^a \bmod p \rightarrow 5^2 \bmod 23 = 2$
- Ο Κώστας στέλνει στην Νίκο το αποτέλεσμα της παράστασης $g^b \bmod p \rightarrow 5^3 \bmod 23 = 10$
- Ο Νίκος υπολογίζει το κοινό μυστικό κλειδί $(g^b \bmod p)^a \bmod p = 10^2 \bmod 23 = 8$
- Ο Κώστας υπολογίζει το κοινό μυστικό κλειδί $(g^a \bmod p)^b \bmod p = 2^3 \bmod 23 = 8$

Άρα οι δύο χρήστες θα χρησιμοποιήσουν το μυστικό κλειδί K=8 για την κρυπτογράφηση / αποκρυπτογράφηση.

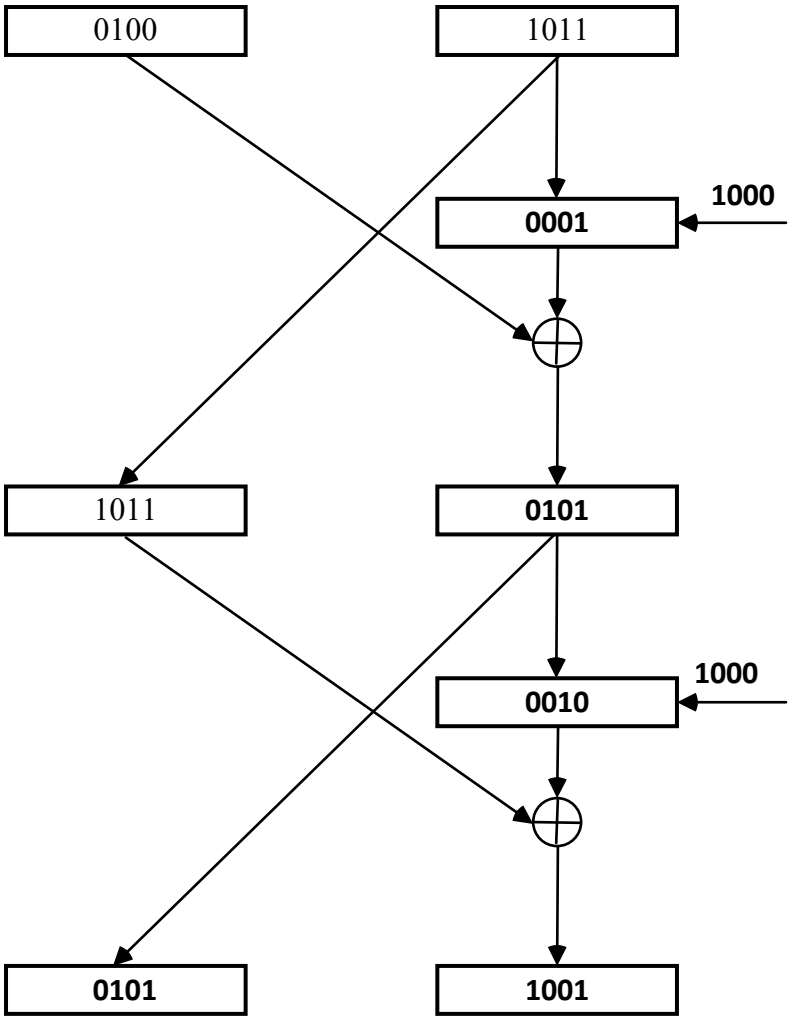
Το σχήμα της πιστοποίησης με συμμετρική κρυπτογράφηση είναι το παρακάτω.



Πρώτα πρέπει να υπολογίσουμε την τιμή της συνάρτησης κατακερματισμού. Έχουμε λοιπόν,

$H(M) = (15)^3 \bmod 100 = 75$ ή 01001011 στο δυαδικό σύστημα είναι η σύνοψη του μηνύματος.

Παρακάτω είναι η κρυπτογράφηση του κειμένου 01001011 με τον αλγόριθμο τμήματος.



F1=$(2K)^x$ mod 15= $(2x8)^{11}$ mod15 = 1

F2=$(4K)^x$ mod 15= $(4x8)^5$ mod 15 = 2

Άρα ο Νίκος Θα στείλει στον Κώστα την συνένωση M || 01011001 ή 15|| 89