Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Πανεπιστημίου Πελοποννήσου

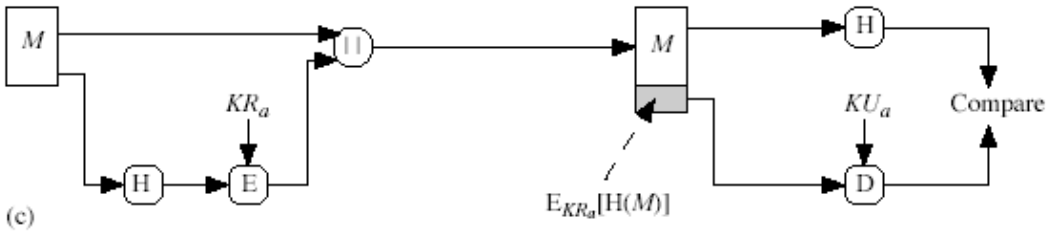
Εργαστήριο Ηλεκτρονικών Κυκλωμάτων, Συστημάτων και Εφαρμογών (ECSA Lab.)

Ασφάλεια Υπολογιστικών Συστημάτων

Διδάσκων: Δρ. Παρασκευάς Κίτσος (Καθηγητής)

Ασκήσεις στη θεματική ενότητα των Ψηφιακών Υπογραφών

1) Έστω ότι έχουμε το παρακάτω σχήμα ψηφιακής υπογραφής



Αν το μήνυμα είναι ίσο με M=32 και το ιδιωτικό κλειδί του χρήστη Α είναι ίσο με K_{Ra} = (d=5, n=323) το δημόσιο κλειδί του είναι ίσο με K_{Ua}=(e=173, n=323) και η συνάρτηση κατακερματισμού έχει εξίσωση H(x)=x^2 mod 10^3, να βρείτε αν το 237 είναι η σωστή ψηφιακή υπογραφή του μηνύματος M (E_{KRA}[H(M)]);

<u>ΛΥΣΗ</u>

Από το σχήμα της ψηφιακής υπογραφής καταλαβαίνουμε ότι πρώτα πρέπει να υπολογίσουμε την τιμή της συνάρτησης κατακερματισμού. Έχουμε λοιπόν,

$H(M) = (32)^2=(2^5)^2 = 2^{10}= 1024 \bmod 1000 = 24$

Επίσης θα υπολογίσουμε την τιμή που μας δίνει ο ασύμμετρος αλγόριθμος κρυπτογραφίας. Έχουμε για αυτόν,

$E_{KRA}[H(M)] = (H(M))^{KRA} \bmod n =(24)^5 \bmod 323 = 28$

Δηλαδή η σωστή ψηφιακή υπογραφή είναι η 28 και όχι η 237.