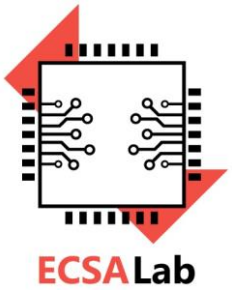
Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Πανεπιστημίου Πελοποννήσου

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

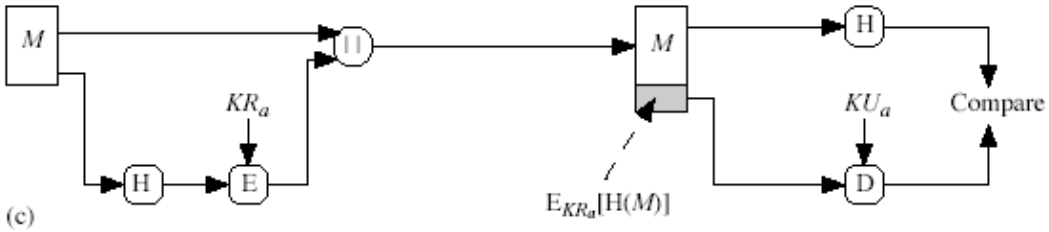


Ασφάλεια Υπολογιστικών Συστημάτων

Διδάσκων: Δρ. Παρασκευάς Κίτσος (Καθηγητής)

Άσκηση 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 $H(x)=x^2 \bmod 10^3$, να βρείτε αν το 237 είναι η σωστή ψηφιακή υπογραφή του μηνύματος M ($E_{KRA}[H(M)]$);