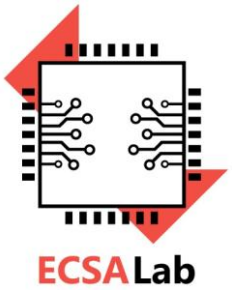
Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Πανεπιστημίου Πελοποννήσου

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

2) 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;

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 $H(x)=x^3 \bmod 100$. Το μήνυμα προς πιστοποίηση είναι το S=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 $F_i(x,K) = (2iK)^x \bmod 15$ για i=1, 2.

Να εκτελέσετε το σχήμα της επικοινωνίας μόνο για τον Νίκο.