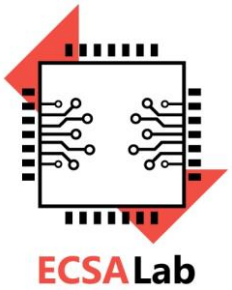
Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Πανεπιστημίου Πελοποννήσου

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.

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).

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.

4) 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