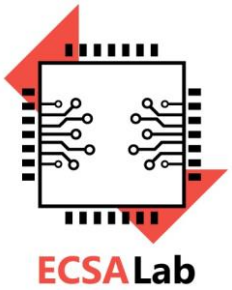
Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Πανεπιστημίου Πελοποννήσου

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



Ασφάλεια Υπολογιστικών Συστημάτων

Διδάσκων: Δρ. Παρασκευάς Κίτσος

Ασκήσεις στη θεματική ενότητα των Ασύμμετρων Αλγορίθμων

1) Θεωρήστε τους πρώτους αριθμούς p=17 και q=11. Με τη βοήθεια του αλγορίθμου RSA να αποκρυπτογραφήσετε το μήνυμα C=11.

2) Έστω ότι ο Τάκης παρακολουθεί παθητικά τη γραμμή επικοινωνίας των Αλίκη και Βύρωνα. Να δοθεί το σχηματικό διάγραμμα της επικοινωνίας Αλίκη - Βύρωνα (με τον αλγόριθμο Diffie-Hellman) με τα εξής στοιχεία: Ιδιωτικό κλειδί της Αλίκης ίσο με 6, ιδιωτικό κλειδί του Βύρωνα ίσο με 15, δημόσιο κλειδί g ίσο με 5 και τέλος δημόσιο κλειδί p ίσο με 23.

3) Έστω η ελλειπτική καμπύλη με εξίσωση $y^2=x^3+73$ και δύο σημεία της το $P_1(2, 9)$ και $P_2(3, 10)$. Να βρείτε τις συντεταγμένες που αντιστοιχούν στα σημεία i) $P_3(x_3, y_3)=P_1+P_2$ και ii) $2P_3$.