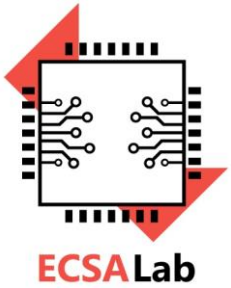
Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του
Πανεπιστημίου Πελοποννήσου

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



Ασφάλεια Υπολογιστικών Συστημάτων

Διδάσκων: Δρ. Παρασκευάς Κίτσος (Καθηγητής)

Λύσεις των ασκήσεων 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.

Λύση:

- p = 17 q = 11 → επιλογή.
- n = pq=187 → υπολογισμός.
- φ(n) = (p - 1)(q - 1) = 160 → υπολογισμός.
- Επιλογή του e έτσι ώστε να είναι αμοιβαία πρώτος του φ(n) = 160 , e = 7 → επιλογή.
- Υπολογισμός d έτσι ώστε $de \equiv 1 \bmod 160$, $d < 160$, d = 23, αφού $23 \times 7 = 161$ και $161 \equiv 1 \bmod 160$ → υπολογισμός.

Άρα

Δημόσιο κλειδί =(7, 187)

Ιδιωτικό κλειδί = (23, 187)

Οπότε η αποκρυπτογράφηση του μηνύματος M = 88:

- $M = 11^{23} \bmod 187 = \{(11^8 \bmod 187)(11^8 \bmod 187)(11^4 \bmod 187)\ (11^2 \bmod 187)\ (11 \bmod 187)\} \bmod 187$.

- $11 \bmod 187 = 11$.
- $11^2 \bmod 187 = 121 \bmod 187 = 121$.
- $11^4 \bmod 187 = 121 \times 121 \bmod 187 = 14641 \bmod 187 = 55$.
- $11^8 \bmod 187 = 55 \times 55 \bmod 187 = 3025 \bmod 187 = 33$.

- Άρα $11^{23} \bmod 187 = (11 \times 121 \times 55 \times 33 \times 33) \bmod 187 = 79720245 \bmod 187 = 88$

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.

Λύση:

Αλίκη		**Βύρωνας**		**Τάκης**	
Γνωρίζει	Δε γνωρίζει	Γνωρίζει	Δε γνωρίζει	Γνωρίζει	Δε γνωρίζει
$p = 23$	$b = 15$	$p = 23$	$a = 6$	$p = 23$	$a = 6$
$g = 5$		$g = 5$		$g = 5$	$b = 15$
$a = 6$		$b = 15$			$S = 2$
$5^6 \bmod 23 = 8$		$5^{15} \bmod 23 = 19$		$5^a \bmod 23 = 8$	
$5^b \bmod 23 = 19$		$5^a \bmod 23 = 8$		$5^b \bmod 23 = 19$	
$19^6 \bmod 23 = 2$		$8^{15} \bmod 23 = 2$		$19^a \bmod 23 = S$	
$19^6 \bmod 23 = 8^b \bmod 23$		$19^a \bmod 23 = 8^{15} \bmod 23$		$8^b \bmod 23 = S$	
$S = 2$		$S = 2$			