Εργασία Κρυπτογραφίας

1. Vigenère – ανάκτηση κλειδιού (γνωστό μήκος)

Δίνονται το κρυπτογράφημα: `LXFOPVEFRNHR`. Γνωρίζετε ότι το μήκος των κλειδιών είναι 5 και ότι τα κείμενα είναι αγγλικά πεζά χωρίς σημεία στίξης.

Ζητούμενα:

α) Βρείτε τα κλειδιά με ανάλυση ανά στήλη (τύπου Caesar).

β) Αποκρυπτογραφήστε τα μηνύματα.

2. RSA πλήρης κύκλος με ταχείες υψώσεις

Δίνονται οι πρώτοι p=197, q=211.

Ζητούμενα:

α) Υπολογίστε το n και τη φ(n). Πάρτε e=24377 και βρείτε το ιδιωτικό εκθετικό d.

β) Κρυπτογραφήστε το μήνυμα m=1234 και αποκρυπτογραφήστε για να επαληθεύσετε.

γ) Δείξτε ρητά τα βήματα **square-and-multiply** για ένα από τα εκθετικά (e ή d).

3.Τρόποι λειτουργίας μπλοκ CBC & CFB, διάδοση σφάλματος

Έστω block cipher E_k 128-bit και δύο blocks P_1,P_2.

- **CBC:** $C_1=E_k(P1 \oplus IV)$, $C2=E_k(P2 \oplus C1)$.
- **CFB (128-bit):** $C_1=P_1 \oplus E_k(IV)$, $C2=P_2 \oplus E_k(C_1)$.
  Κατά τη μετάδοση αλλοιώνεται **ένα μόνο bit** του C_1.
  Ζητούμενα: Περιέγραψε ακριβώς τι παθαίνουν τα P_1' και P_2' στην αποκρυπτογράφηση για **CBC** και για **CFB** (ποια/πόσα bits επηρεάζονται και γιατί).

4. ElGamal αριθμητικό παράδειγμα αποκρυπτογράφησης

Δίνεται p=23, γεννήτορας g=5. Το ιδιωτικό κλειδί είναι x=6 και άρα το δημόσιο $y=g^x \bmod p$. Ένα κρυπτογράφημα είναι $C=(C_1,C_2)=(20,22)$.

Ζητούμενα:

α) Υπολόγισε το $C_1^x \bmod p$.

β) Βρες το M χρησιμοποιώντας τον πολλαπλασιαστικό αντίστροφο του $C_1^x \bmod p$.

γ) Δείξε τα ενδιάμεσα βήματα (εύρεση αντίστροφου modulo).

ΤΥΠΟΛΟΓΙΟ

Κρυπτοσυστήματα συμμετρικά

- **Vigenère:**
  $Ci=(Pi+Ki)\bmod 26, Pi=(Ci-Ki)\bmod 26$
- **Caesar:**
  $C=(P+k)\bmod 26, P=(C-k)\bmod 26$
- **CBC mode:**
  $C1=Ek(P1\oplus IV), Ci=Ek(Pi\oplus Ci-1)$
  $Pi=Dk(Ci)\oplus Ci-1$
- **CFB mode:**
  $Ci=Pi\oplus Ek(Ci-1), Pi=Ci\oplus Ek(Ci-1)$

Ασύμμετρα κρυπτοσυστήματα

- **RSA:**
  $n=pq$
  $\varphi(n)=(p-1)(q-1)$
  $e\cdot d\equiv 1(\mod \varphi(n))$
  Κρυπτογράφηση: $C=M^e \bmod n$
  Αποκρυπτογράφηση: $M=C^d \bmod n$
- **ElGamal:**
  Δημόσιο: $y=g^x \bmod p$
- Κρυπτογράφηση: $C_1=g^k \bmod p$, $C2=M\cdot y^k \bmod p$
  Αποκρυπτογράφηση: $M=C_2\cdot (C1^x)^{-1} \bmod p$