«**Ασφάλεια Υπολογιστικών Συστημάτων**»
Δρ. Παρασκευάς Κίτσος, Καθηγητής
Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών
του Πανεπιστήμιου Πελοποννήσου.
Εργαστήριο Ηλεκτρονικών Κυκλωμάτων, Συστημάτων και Εφαρμογών
(ECSA Lab, https://ecsalab.ece.uop.gr/)

ΕΠΩΝΥΜΟ & ΟΝΟΜΑ : **ΑΜ :**
ΟΝΟΜΑ ΠΑΤΡΟΣ : **ΕΞΑΜΗΝΟ ΦΟΙΤΗΣΗΣ:**
ΠΕΡΙΟΔΟΣ : Ιούνιος 2023 **ΟΜΑΔΑ ΘΕΜΑΤΩΝ:** **Α**
ΗΜΕΡΟΜΗΝΙΑ : 28/06/2023

ΘΕΜΑΤΑ:

Θέμα Α) Να επιλέξετε τις σωστές απαντήσεις στις παρακάτω ερωτήσεις.
1) Ο Αλγόριθμος Triple-DES μπορεί να χρησιμοποιήσει δύο κλειδιά των 64 bits:

Α. Σωστό

Β. Λάθος,

Γ. Χρησιμοποιεί τρία ίδια κλειδιά των 128 bits

2) Ο AES έχει την παρακάτω συνάρτηση στον τελευταίο γύρο του.

Α. Συνάρτηση SubBytes

Β. Συνάρτηση ShiftRows

Γ. Συνάρτηση AddroundKey

Δ. Κανέναν από τους παραπάνω

3) Οι επιθέσεις παράπλευρου καναλιού στο υλικό ανιχνεύουν τις παρακάτω πληροφορίες από τη διακίνηση δεδομένων?

Α. Χρόνος εκτέλεσης διεργασιών

Β. Κατανάλωση ενέργειας

Γ. Ηλεκτρομαγνητική ακτινοβολία

Δ. Όλα τα παραπάνω

Ε. Κανένα από τα παραπάνω.

4) Η πρόταση «Όσο μεγαλύτερο είναι το κλειδί σε έναν αλγόριθμο κρυπτογράφησης τόσο μεγαλύτερα είναι τα επίπεδα ασφάλεια που προσφέρει», είναι:

Α. Σωστή

Β. Λάθος

ΛΥΣΗ

1 → Α

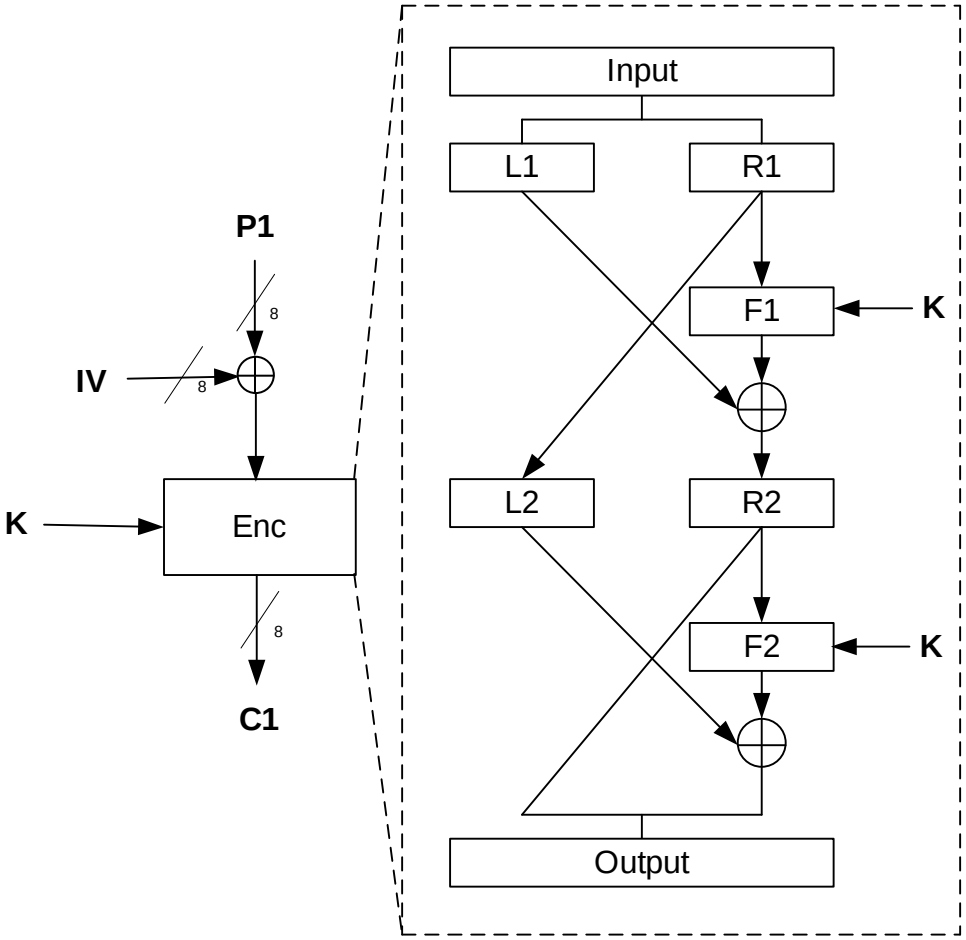
2 → Α, Β, Γ

3 → Δ

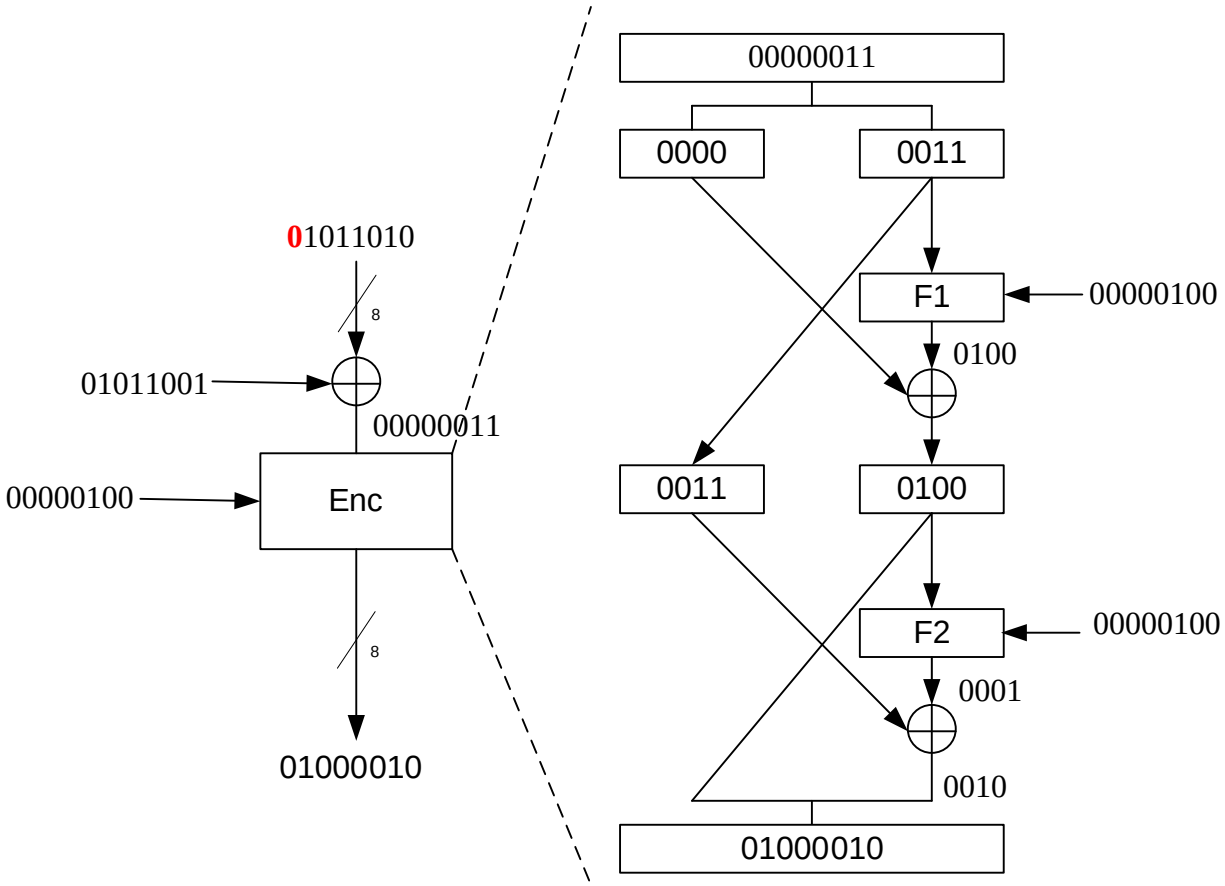
4 → Α

Θέμα Β) Αν ο τρόπος λειτουργίας κατά την κρυπτογράφηση ενός αλγορίθμου τμήματος που έχει σχεδιαστεί με χρήση Feistel δικτύων είναι ο Cipher Block Chaining (CBC) του παρακάτω σχήματος, να εκτελέσετε την κρυπτογράφηση με τα παρακάτω δεδομένα.

P1=1011010, IV=01011001, K= 4, $F_i(x, K) = (iK)^x \ \ mod\ 15$ για i=1, 2.



ΛΥΣΗ



Θέμα Γ) 1. Να υπολογίσετε τον Μέγιστο Κοινό Διαιρέτη μεταξύ των αριθμών 66 και 71.

2. Χρησιμοποιώντας την ανεπτυγμένη μορφή του αλγορίθμου Ευκλείδη να βρείτε τους ακεραίους x και y για τους οποίους ισχύει 71x+66y=1.

ΛΥΣΗ

1. Για οποιονδήποτε μη αρνητικό ακέραιο a και οποιονδήποτε θετικό ακέραιο b, ισχύει: gcd(a, b) =gcd(b, a mod b).

Επίσης ισχύει a mod n= $\begin{cases} a, & \text{αν } n = 0 \\ a - \lfloor a/n \rfloor n, & \text{διαφορετικά} \end{cases}$

Οπότε έχουμε **gcd(66, 71)** = gcd(66, 71mod 66) = **gcd(66, 5)** = gcd(5, 66 mod 5) = **gcd(5, 1)** = gcd(1, 5 mod1) = **gcd(1, 0)**= 1

2. Άρα έχουμε το ζεύγος (a, b) = (1, 0) και ξεκινώντας από αυτό εκτελούμε, «προς τα πίσω», τον αλγόριθμο του Ευκλείδη στην ανεπτυγμένη μορφή του. Άρα για (a, b) = (1, 0) έχουμε d ← 1, x ← 1, y ← 0. Για (a, b) = (5, 1) έχουμε $y \leftarrow x' - \left\lfloor \frac{a}{b} \right\rfloor y' = 1 - \left\lfloor \frac{5}{1} \right\rfloor 0 = 1$ και $x \leftarrow y' = 0$. Όμοια για (a, b) = (66, 5) έχουμε $y \leftarrow x' - \left\lfloor \frac{a}{b} \right\rfloor y' = 0 - \left\lfloor \frac{66}{5} \right\rfloor 1 = -13$ και $x \leftarrow y' = 1$.

Τελικά για το αρχικό ζεύγος (a, b) = (71, 66) έχουμε $y \leftarrow x' - \left\lfloor \frac{a}{b} \right\rfloor y' = 1 - \left\lfloor \frac{71}{66} \right\rfloor (-13) = 1 - (1)(-13) = 14$ και $x \leftarrow y' = -13$.

Άρα οι ζητούμενοι ακέραιοι x και y για τους οποίους ισχύει 71x + 66y = 1 είναι οι $x = -13$ και $y = 14$, δηλαδή ισχύει gcd (66, 71) = 71(-13) +66(14) = -923+924=1.

Θέμα Δ) Έστω ότι ο Κώστας και η Εύα έχουν επιλέξει τους αριθμούς p=13 (πρώτος) και g=6 για δημόσιο κλειδί. Ο αριθμός 6 είναι πρωτογενής ρίζα του 13. Αν ο Κώστας επιλέξει για ιδιωτικό κλειδί το a=5 και η Εύα επιλέξει για ιδιωτικό κλειδί το b=8 να υπολογίσετε το κοινό μυστικό κλειδί που θα υπολογίσουν και οι δύο σύμφωνα με τον αλγόριθμο DIFFIE-HELLMAN.

ΛΥΣΗ

Ο Κώστας υπολογίζει και στέλνει στην Έυα τη παράσταση $g^a \bmod p = 6^5 \bmod 13 = 2$.

Ταυτόχρονα, η Έυα υπολογίζει και στέλνει στον Κώστα τη παράσταση $g^b \bmod p = 6^8 \bmod 13 = 3$.

Έπειτα, ο Κώστας υπολογίζει τη παράσταση $3^a \bmod p = 3^5 \bmod 13 = 9$

Ταυτόχρονα, η Εύα υπολογίζει τη παράσταση $2^b \bmod p = 2^8 \bmod 13 = 9$.

Οπότε, οι δύο μοιράστηκαν το μυστικό κλειδί τον αριθμό 9.