«**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:** **Β**
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 56 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. Κατανάλωση ενέργειας

Β. Χρόνος εκτέλεσης διεργασιών

Γ. Ηλεκτρομαγνητική ακτινοβολία

Δ. Κανένα από τα παραπάνω

Ε. Όλα τα παραπάνω.

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

Α. Σωστή

Β. Λάθος

<u>ΛΥΣΗ</u>

1→ Β

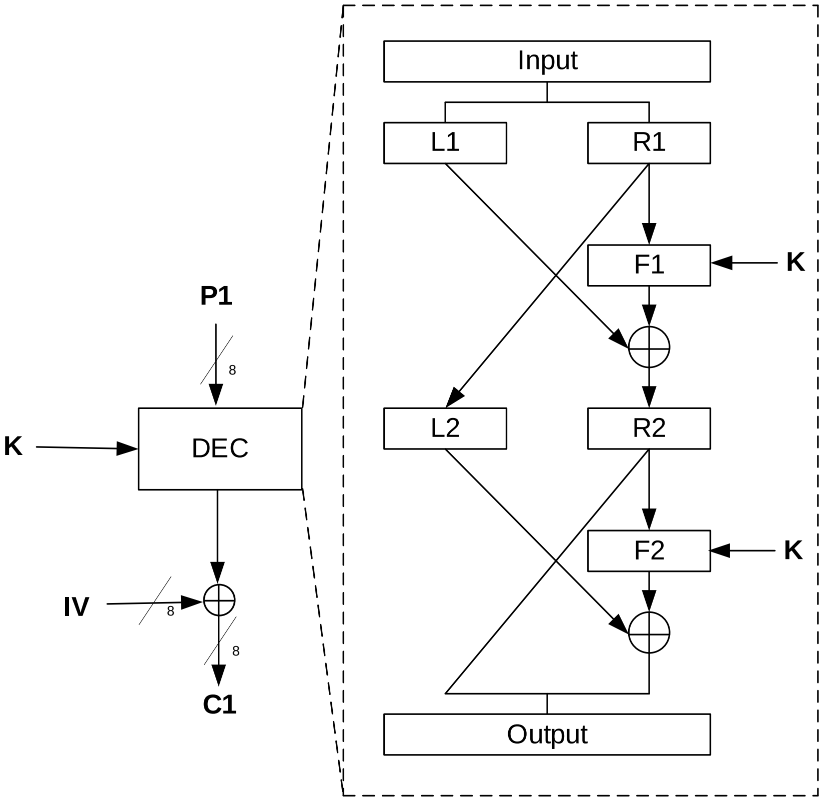
2→ Α, Β, Γ

3→ Ε

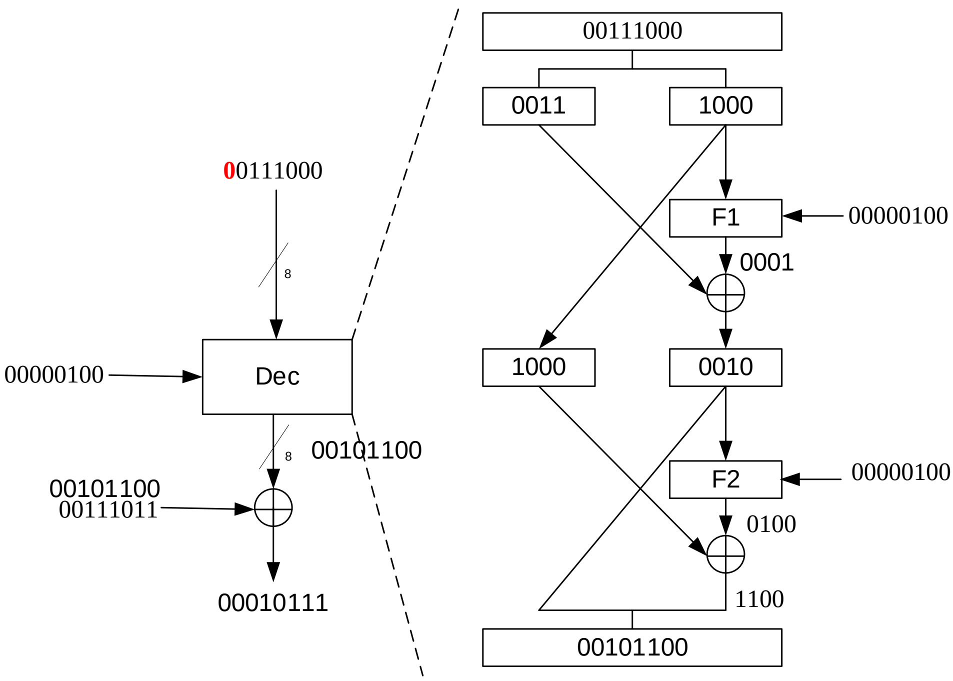
4→ Β

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

P1=0111000, IV=00111011, 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 67 και 72.

2. Χρησιμοποιώντας την ανεπτυγμένη μορφή του αλγορίθμου Ευκλείδη να βρείτε τους ακεραίους x και y για τους οποίους ισχύει 72x+67y=1.

<u>ΛΥΣΗ</u>

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= $\begin{cases} a, & \alpha\nu\ n=0 \\ a-\lfloor a/n \rfloor n, & \delta\iota\alpha\varphi o\rho\varepsilon\tau\iota\kappa\acute{\alpha} \end{cases}$

Οπότε έχουμε **gcd(67, 72)** = gcd(67, 72 mod 67) = **gcd(67, 5)** = gcd(5, 67 mod 5) = **gcd(5, 2)** = gcd(2, 5 mod 2) = **gcd (2, 1)** = gcd(1, 2 mod 1) = **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) = (2, 1) έχουμε $y \leftarrow x' - \left\lfloor \frac{a}{b} \right\rfloor y' = 1 - \left\lfloor \frac{2}{1} \right\rfloor 0 = 1$ και $x \leftarrow y' = 0$. Όμοια για (a, b) = (5, 2) έχουμε $y \leftarrow x' - \left\lfloor \frac{a}{b} \right\rfloor y' = 0 - \left\lfloor \frac{5}{2} \right\rfloor (1) = -2$ και $x \leftarrow y' = 1$.

Επίσης, για (a, b) = (67, 5) έχουμε $y \leftarrow x' - \left\lfloor \frac{a}{b} \right\rfloor y' = 1 - \left\lfloor \frac{67}{5} \right\rfloor (-2) = 27$ και $x \leftarrow y' = -2$.

Τελικά για το αρχικό ζεύγος (a, b) = (72, 67) έχουμε $y \leftarrow x' - \left\lfloor \frac{a}{b} \right\rfloor y' = -2 - \left\lfloor \frac{72}{67} \right\rfloor 27 = -2 - (1)27 = -29$ και $x \leftarrow y' = 27$.

Άρα οι ζητούμενοι ακέραιοι x και y για τους οποίους ισχύει 67x + 72y = 1 είναι οι $x = -29$ και $y = 27$, δηλαδή ισχύει gcd (66, 71) = 72(27) + 67(-29) = 1944-1943=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=6 και η Εύα επιλέξει για ιδιωτικό κλειδί το b=7 να υπολογίσετε το κοινό μυστικό κλειδί που θα υπολογίσουν και οι δύο σύμφωνα με τον αλγόριθμο DIFFIE-HELLMAN.

<u>ΛΥΣΗ</u>

Ο Κώστας υπολογίζει και στέλνει στην Έυα τη παράσταση g^a mod p = 6^6 mod 13 = 12.
Ταυτόχρονα, η Έυα υπολογίζει και στέλνει στον Κώστα τη παράσταση g^b mod p = 6^7 mod 13 = 7.

Έπειτα, ο Κώστας υπολογίζει τη παράσταση 7^a mod p = 7^6 mod 13 = 12.
Ταυτόχρονα, η Εύα υπολογίζει τη παράσταση 12^b mod p = 12^7 mod 13 = 12.

Οπότε, οι δύο μοιράστηκαν το μυστικό κλειδί τον αριθμό 12.