

## «Ασφάλεια Υπολογιστικών Συστημάτων»

Δρ. Παρασκευάς Κίτσος, Αναπλ. Καθηγητής

Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

του Πανεπιστημίου Πελοποννήσου.

Εργαστήριο Ηλεκτρονικών Κυκλωμάτων, Συστημάτων και Εφαρμογών

(ECSA Lab, <https://ecsalab.ece.uop.gr/>)

**ΕΠΩΝΥΜΟ & ΟΝΟΜΑ :**

**ΟΝΟΜΑ ΠΑΤΡΟΣ :**

**ΠΕΡΙΟΔΟΣ :** Φεβρουάριος 2023

**ΗΜΕΡΟΜΗΝΙΑ :** 09/02/2023

**ΑΜ :**

**ΕΞΑΜΗΝΟ ΦΟΙΤΗΣΗΣ:**

**ΟΜΑΔΑ ΘΕΜΑΤΩΝ: B**

### ΘΕΜΑΤΑ:

**Θέμα Α)** Να επιλέξετε τις σωστές απαντήσεις στις παρακάτω ερωτήσεις.

**1)** Ο Αλγόριθμος Triple-DES μπορεί να χρησιμοποιήσει δύο κλειδιά των 64 bits:

- A. Σωστό
- B. Λάθος,
- Γ. Χρησιμοποιεί τρία ίδια κλειδιά των 128 bits

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

- A. Συνάρτηση SubBytes
- B. Συνάρτηση ShiftRows
- Γ. Συνάρτηση AddroundKey
- Δ. Κανέναν από τους παραπάνω

**3)** Ποιες από τις παρακάτω πληροφορίες δεν ανιχνεύουν οι επιθέσεις παράπλευρου καναλιού στο υλικό από τη διακίνηση δεδομένων?

- A. Χρόνος εκτέλεσης διεργασιών
- B. Κατανάλωση ενέργειας
- Γ. Ηλεκτρομαγνητική ακτινοβολία
- Δ. Όλα τα παραπάνω
- Ε. Κανένα από τα παραπάνω.

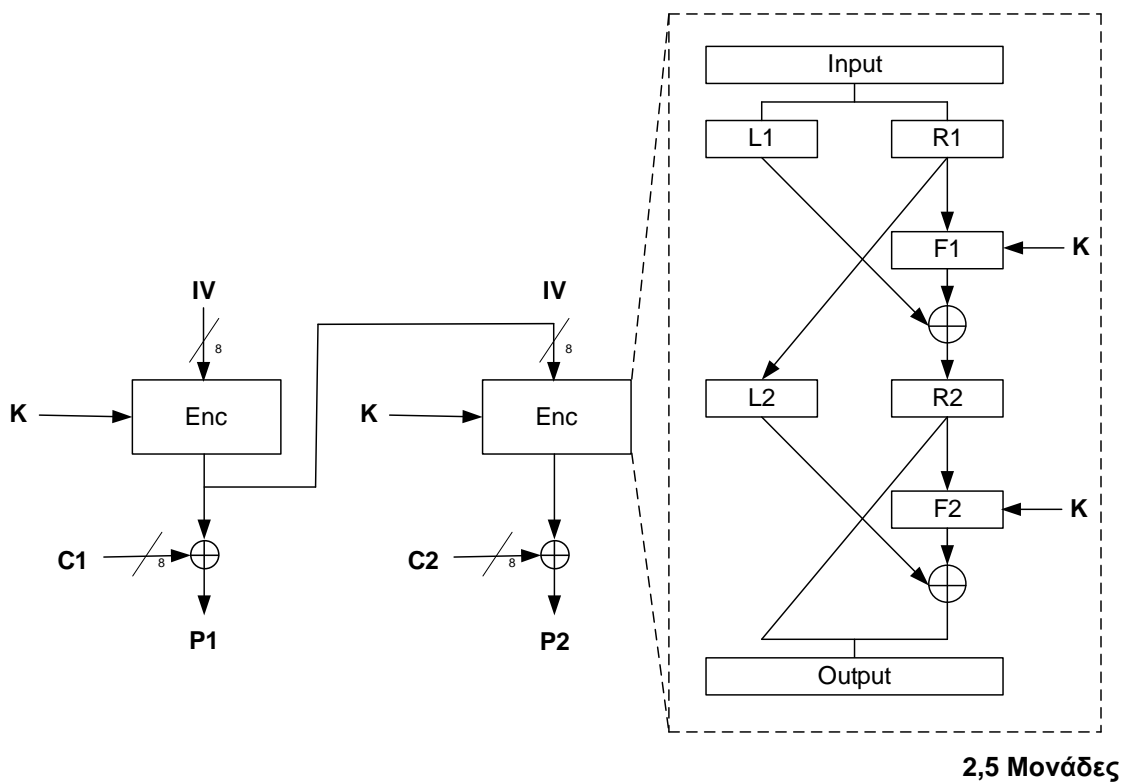
**4)** Η πρόταση «Όσο μικρότερο είναι το κλειδί σε έναν αλγόριθμο κρυπτογράφησης τόσο μικρότερα είναι τα επίπεδα ασφάλειας που προσφέρει», είναι:

- A. Σωστή
- B. Λάθος

**2 Μονάδες**

**Θέμα Β)** Αν ο τρόπος λειτουργίας κατά την αποκρυπτογράφηση ενός αλγορίθμου τμήματος που έχει σχεδιαστεί με χρήση Feistel δικτύων είναι ο Output Feedback του παρακάτω σχήματος, να εκτελέσετε την αποκρυπτογράφηση με τα παρακάτω δεδομένα.

$C=010110100010101$ ,  $IV=00000100$ ,  $K=4$ ,  $F_i(x, K) = (iK)^x \bmod 15$  για  $i=1, 2$ .



**Θέμα Γ)** 1. Να υπολογίσετε τον Μέγιστο Κοινό Διαιρέτη μεταξύ των αριθμών 68 και 73.

**1 Μονάδα**

2. Χρησιμοποιώντας την ανεπτυγμένη μορφή του αλγορίθμου Ευκλείδη να βρείτε τους ακεραίους  $x$  και  $y$  για τους οποίους ισχύει  $68x+73y=1$ .

**2 Μονάδες**

**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  $a=8$  και η Εύα επιλέξει για ιδιωτικό κλειδί το  $b=6$  να υπολογίσετε το κοινό μυστικό κλειδί που θα υπολογίσουν και οι δύο σύμφωνα με τον αλγόριθμο DIFFIE-HELLMAN.

**2,5 Μονάδες**

**Καλή Επιτυχία !**

*Παρατηρήσεις:*

- **Απαγορεύετε** η χρήση κινητού τηλεφώνου
- **Επιτρέπεται** η χρήση υπολογιστή τσέπης
- Η διάρκεια εξέτασης είναι **2 ώρες**