|  |  |
| --- | --- |
|  | «**Ασφάλεια Υπολογιστικών Συστημάτων**»Δρ. Παρασκευάς Κίτσος, Αναπλ. ΚαθηγητήςΤμήμα 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 :** | Φεβρουάριος 2024 | **ΟΜΑΔΑ ΘΕΜΑΤΩΝ:** | **A** |
| **ΗΜΕΡΟΜΗΝΙΑ :** | 19/02/2024 |

**ΘΕΜΑΤΑ:**

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

P=111001101010011, IV=00010001, για i=1, 2 και συνάρτηση παραγωγής κλειδιών γύρου για j=1, 2 και K= 3.

Να απαντήσετε σύμφωνα με τη μεθοδολογία που έχετε διδαχθεί.



 **4 Μονάδες**

**ΛΥΣΗ**

P=111001101010011 = 01110011 01010011



**Θέμα Β)** Να υπολογίσετε, με χρήση του αλγορίθμου Ευκλείδη, gcd(a, b) = gcd(b, a mod b), και γενικότερα τη μεθοδολογία που έχετε διδαχθεί, τον Μέγιστο Κοινό Διαιρέτη μεταξύ των αριθμών 82 και 57.

 **2 Μονάδες**

**ΛΥΣΗ**

gcd(82, 57) = gcd(57, 82 mod 57) = gcd(57, 25) = gcd(25, 57 mod 25) = gcd(25, 7) gcd(7, 25 mod 7) = gcd(7, 4) = gcd(4, 7 mod 4) = gcd(4, 3) = gcd(3, 4 mod 3) = gcd(3, 1) = gcd(1, 3 mod 1) = gcd(1, 0) = 1.

**Θέμα Γ)** Να συμπληρώσετε τον παρακάτω πίνακα με τα βήματα του αλγορίθμου DIFFIE-HELLMAN σύμφωνα με τη μεθοδολογία που έχετε διδαχθεί. Ο αριθμός 5 είναι πρωτογενής ρίζα του 23.



 **4 Μονάδες**

**ΛΥΣΗ**

