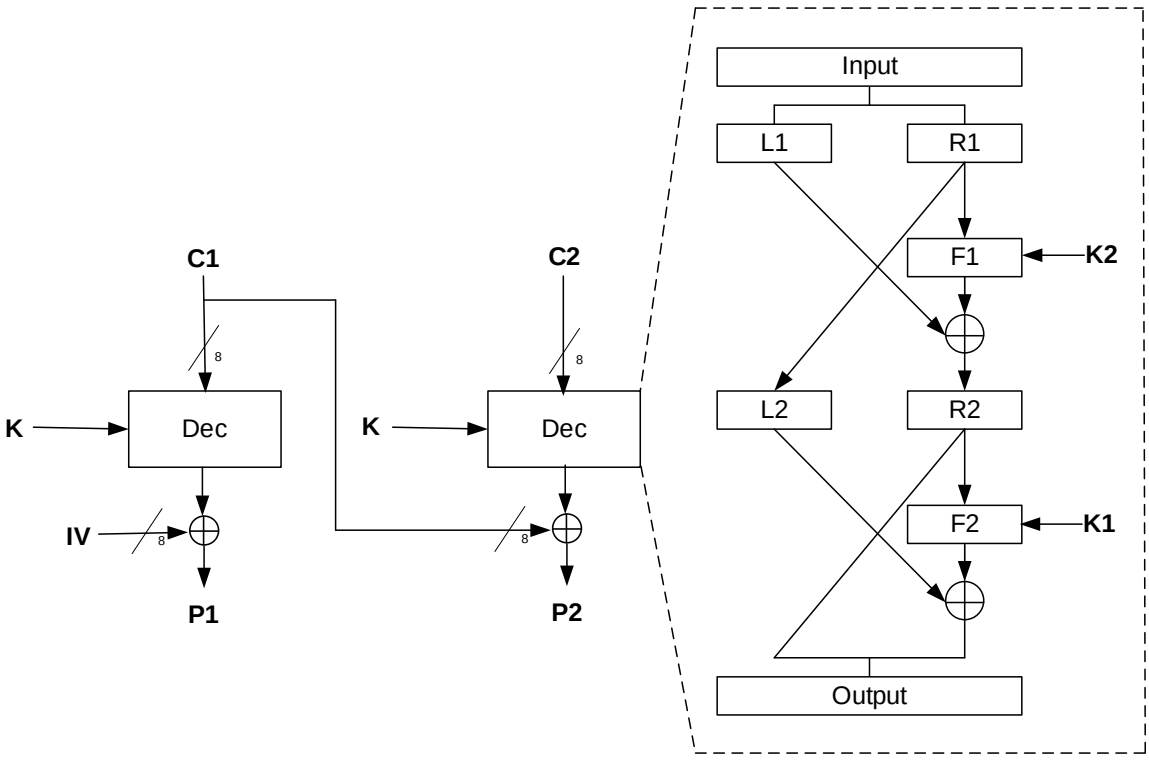
«**Ασφάλεια Υπολογιστικών Συστημάτων**»
Δρ. Παρασκευάς Κίτσος, Αναπλ. Καθηγητής
Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών
του Πανεπιστήμιου Πελοποννήσου.
Εργαστήριο Ηλεκτρονικών Κυκλωμάτων, Συστημάτων και Εφαρμογών
(ECSA Lab, https://ecsalab.ece.uop.gr/)

ΕΠΩΝΥΜΟ & ΟΝΟΜΑ : **ΑΜ :**
ΟΝΟΜΑ ΠΑΤΡΟΣ : **ΕΞΑΜΗΝΟ ΦΟΙΤΗΣΗΣ:**
ΠΕΡΙΟΔΟΣ : Φεβρουάριος 2024 **ΟΜΑΔΑ ΘΕΜΑΤΩΝ:** **Δ**
ΗΜΕΡΟΜΗΝΙΑ : 19/02/2024

ΘΕΜΑΤΑ:

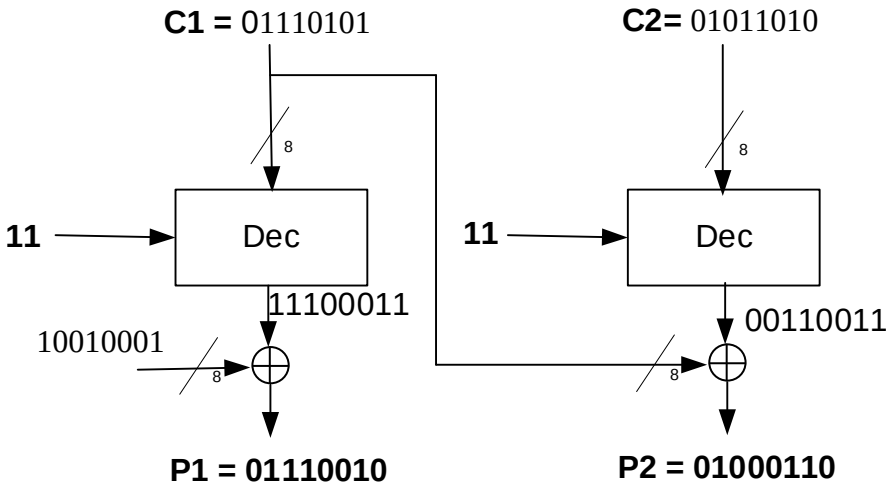
Θέμα Α) Αν ο τρόπος λειτουργίας κατά τη αποκρυπτογράφηση ενός αλγορίθμου τμήματος που έχει σχεδιαστεί με χρήση Feistel δικτύων είναι ο Cipher Block Chaining του παρακάτω σχήματος, να εκτελέσετε την αποκρυπτογράφηση με τα παρακάτω δεδομένα.

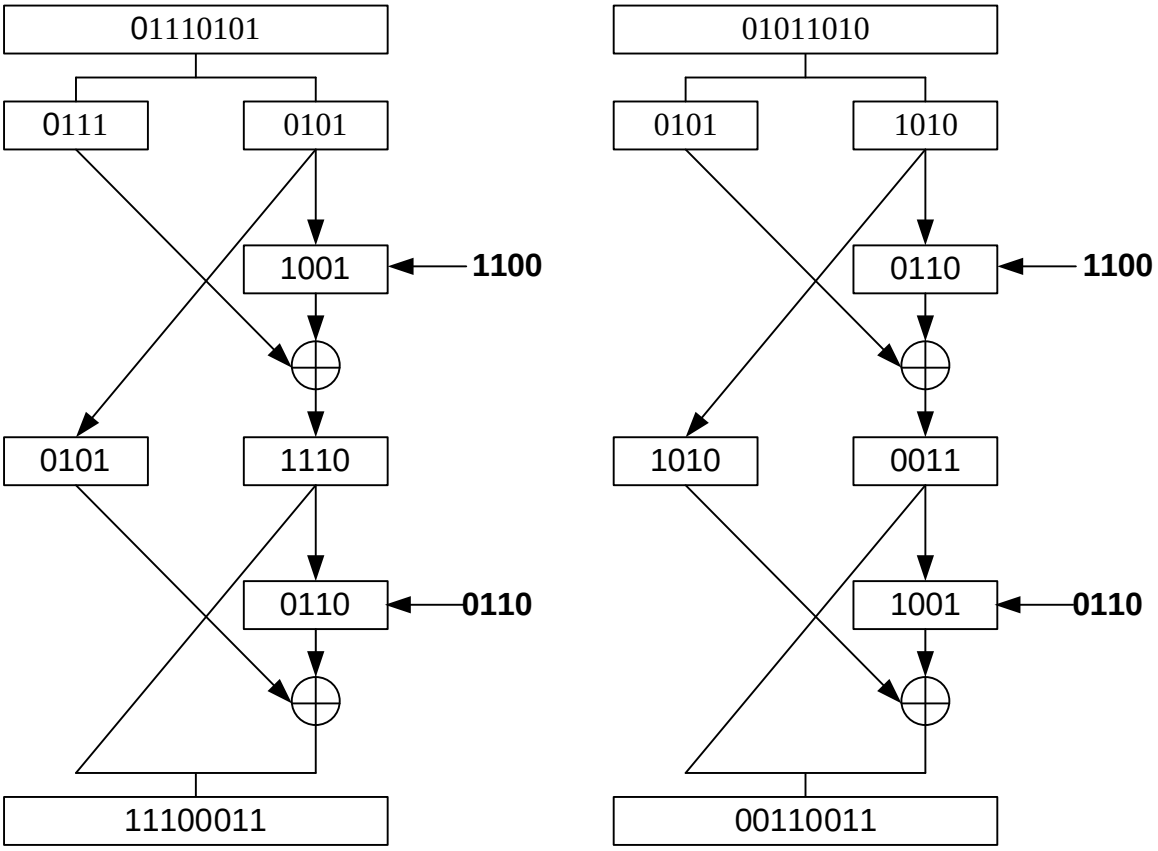
C=111010101011010, IV=10010001, $F_i(x,K) = (2iK)^x \ mod 15$ για i=1, 2 και συνάρτηση παραγωγής κλειδιών γύρου $Kj(K) = (2jK) \ mod 15$ για j=1, 2 και K= 3.
Να απαντήσετε σύμφωνα με τη μεθοδολογία που έχετε διδαχθεί.



4 Μονάδες

ΛΥΣΗ





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 79 και 55.

2 Μονάδες

ΛΥΣΗ

gcd(79, 55) = gcd(55, 79 mod 55) = gcd(55, 24) = gcd(24, 55 mod 24) = gcd(24, 7) gcd(7, 24 mod 7) = gcd(7, 3) = gcd(3, 7 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.

Τάκης		**Μαρία**
k=23 , j=5	**Δημόσιο Κλειδί**	k=23 , j=5
m=8	**Ιδιωτικό Κλειδί**	n=3
	Πράξη και Αποτέλεσμα	
	Πράξη και Αποτέλεσμα	

4 Μονάδες

ΛΥΣΗ