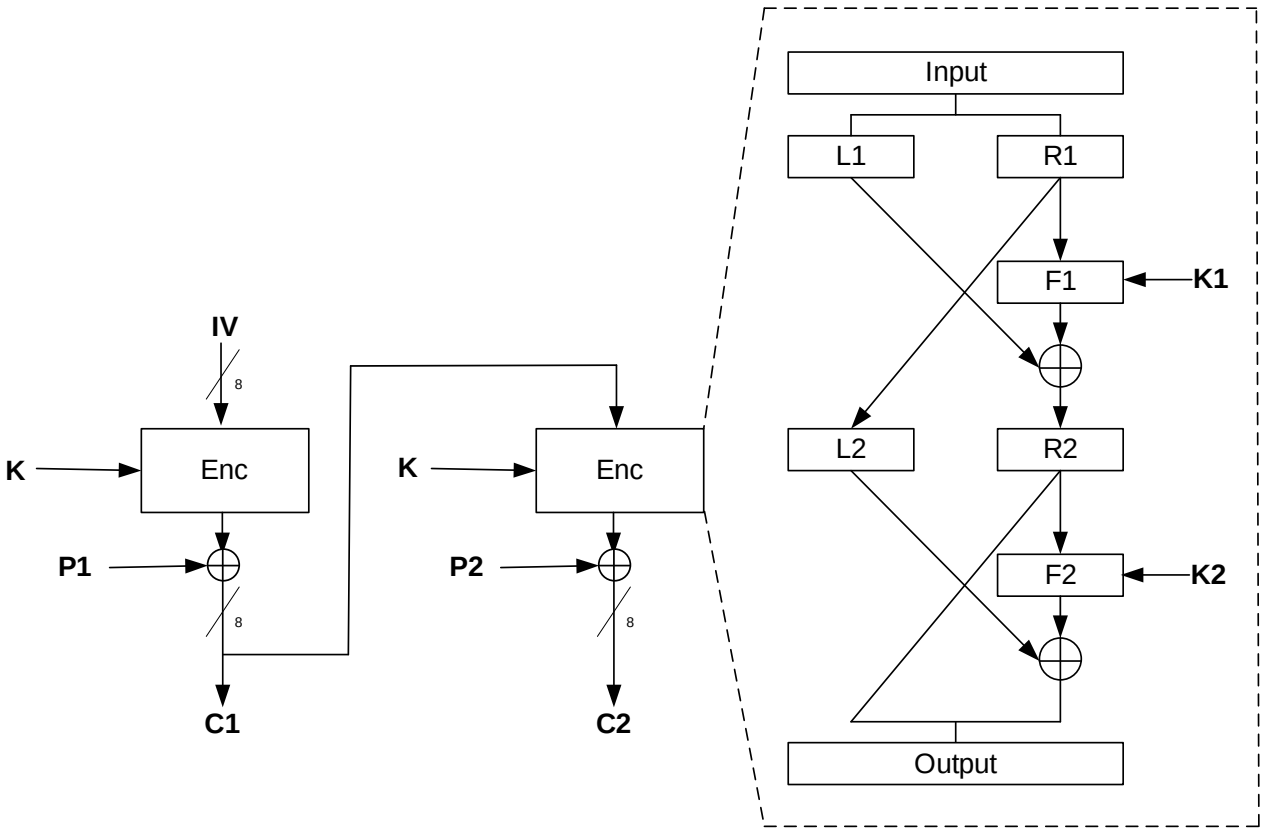
«**Ασφάλεια Υπολογιστικών Συστημάτων**»
Δρ. Παρασκευάς Κίτσος, Αναπλ. Καθηγητής
Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών
του Πανεπιστήμιου Πελοποννήσου.
Εργαστήριο Ηλεκτρονικών Κυκλωμάτων, Συστημάτων και Εφαρμογών
(ECSA Lab, https://ecsalab.ece.uop.gr/)

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

ΘΕΜΑΤΑ:

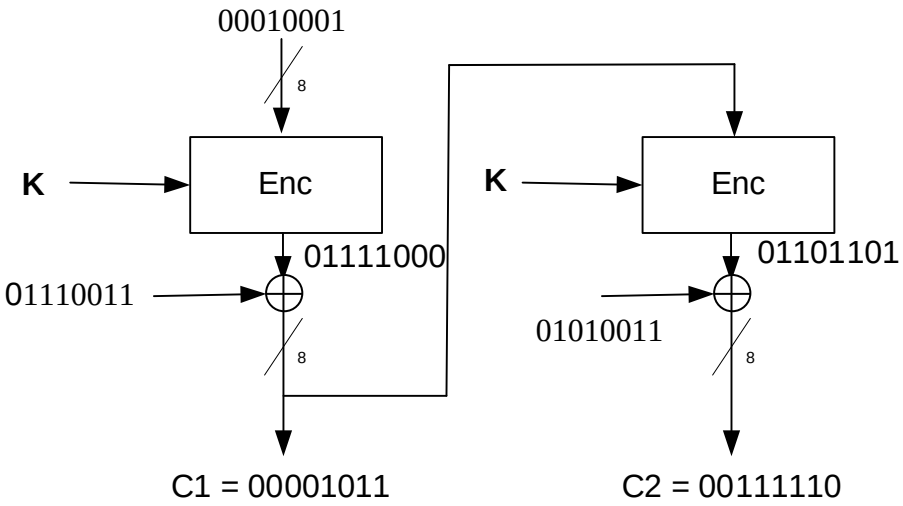
Θέμα Α) Αν ο τρόπος λειτουργίας κατά τη κρυπτογράφηση ενός αλγορίθμου τμήματος που έχει σχεδιαστεί με χρήση Feistel δικτύων είναι ο Cipher Feedback του παρακάτω σχήματος, να εκτελέσετε τη κρυπτογράφηση με τα παρακάτω δεδομένα.

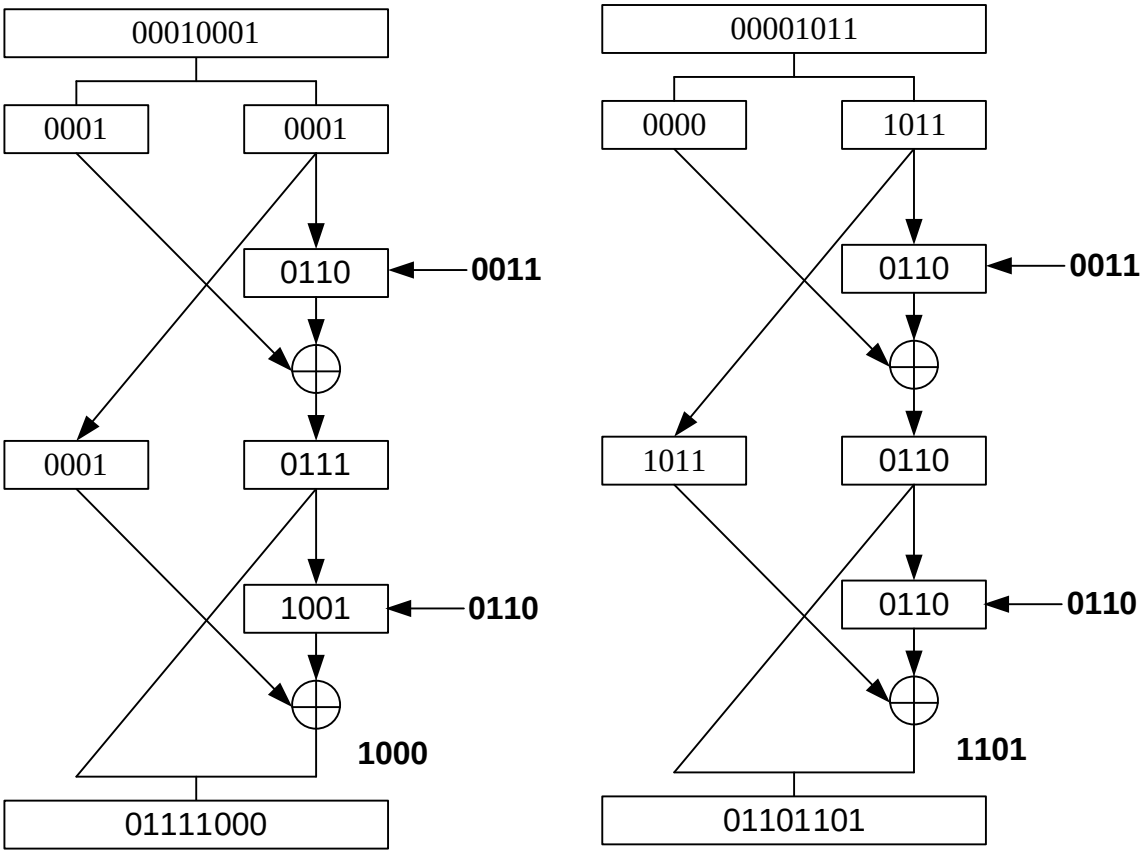
P=111001101010011, IV=00010001, $F_i(x,K) = (2iK)^x \ mod 15$ για i=1, 2 και συνάρτηση παραγωγής κλειδιών γύρου $Kj(K) = (jK) \ mod 15$ για j=1, 2 και K= 3.
Να απαντήσετε σύμφωνα με τη μεθοδολογία που έχετε διδαχθεί.



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 83 και 57.

2 Μονάδες

ΛΥΣΗ

gcd(83, 57) = gcd(57, 83 mod 57) = gcd(57, 26) =gcd(26, 57 mod 26) = gcd(26, 5) = gcd(5, 26 mod 5) = gcd(5, 1) = gcd(1, 5 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
n=7	**Ιδιωτικό Κλειδί**	m=6
	Πράξη και Αποτέλεσμα	
	Πράξη και Αποτέλεσμα	

4 Μονάδες

ΛΥΣΗ

Τάκης		**Μαρία**
k=23 , j=5	**Δημόσιο Κλειδί**	k=23 , j=5
n=7	**Ιδιωτικό Κλειδί**	m=6
5^7 mod 23 = 17	**Πράξη και Αποτέλεσμα**	5^6 mod 23 = 8
8^7 mod 23 = 12	**Πράξη και Αποτέλεσμα**	17^6 mod 23 = 12