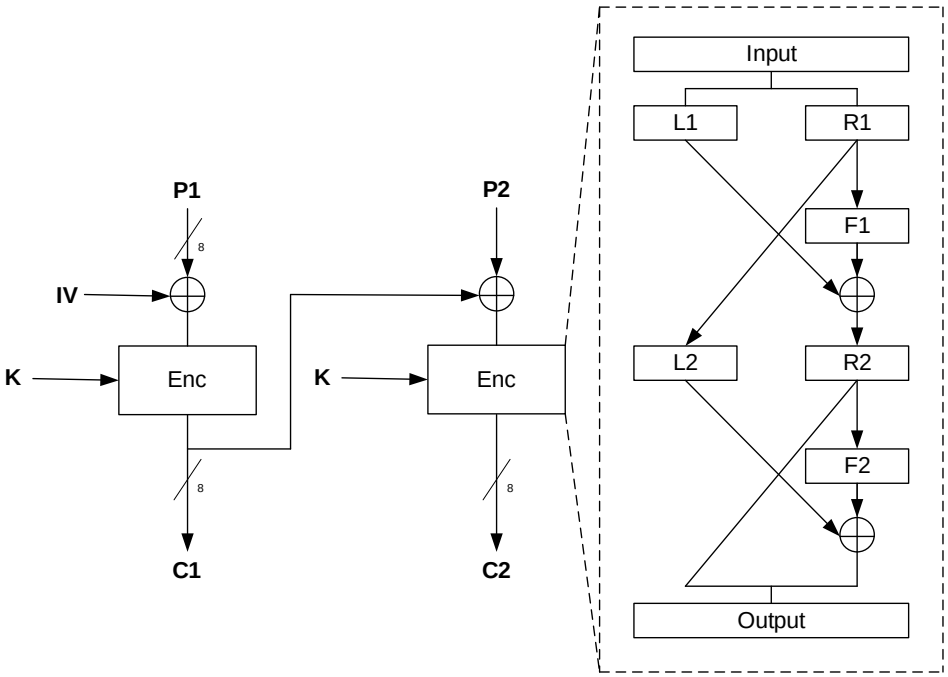
ECSA Lab	**«Ασφάλεια Υπολογιστικών Συστημάτων»** Δρ. Παρασκευάς Κίτσος, Αναπλ. Καθηγητής Εργαστήριο Ηλεκτρονικών Κυκλωμάτων, Συστημάτων και Εφαρμογών (ECSA Lab, https://ecsalab.ece.uop.gr/)

ΕΠΩΝΥΜΟ & ΟΝΟΜΑ :		**ΑΜ :**	
ΟΝΟΜΑ ΠΑΤΡΟΣ :		**ΕΞΑΜΗΝΟ ΦΟΙΤΗΣΗΣ:**	
ΠΕΡΙΟΔΟΣ :	Ιανουάριος 2022	**ΟΜΑΔΑ ΘΕΜΑΤΩΝ:**	-
ΗΜΕΡΟΜΗΝΙΑ :	12/01/2022		

ΘΕΜΑΤΑ:

Θέμα 1

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



P=011111100011101, IV=00000010, K= 2, $F_i(x,K) = (iK)^x \mod 15$ για i=1, 2.

Θέμα 2

Κρυπτογραφήστε και αποκρυπτογραφήστε με το αλγόριθμο RSA το μήνυμα με τις παρακάτω παραμέτρους: p = 5, q = 13, και M = 21.

Καλή Επιτυχία !

Παρατηρήσεις:

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