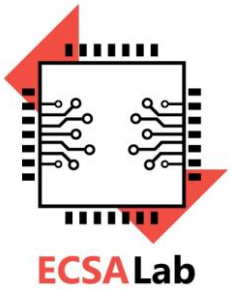
Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Πανεπιστημίου Πελοποννήσου

Εργαστήριο Ηλεκτρονικών Κυκλωμάτων, Συστημάτων και Εφαρμογών (ECSA Lab.)



Ασφάλεια Υπολογιστικών Συστημάτων

Διδάσκων: Δρ. Παρασκευάς Κίτσος (Καθηγητής)

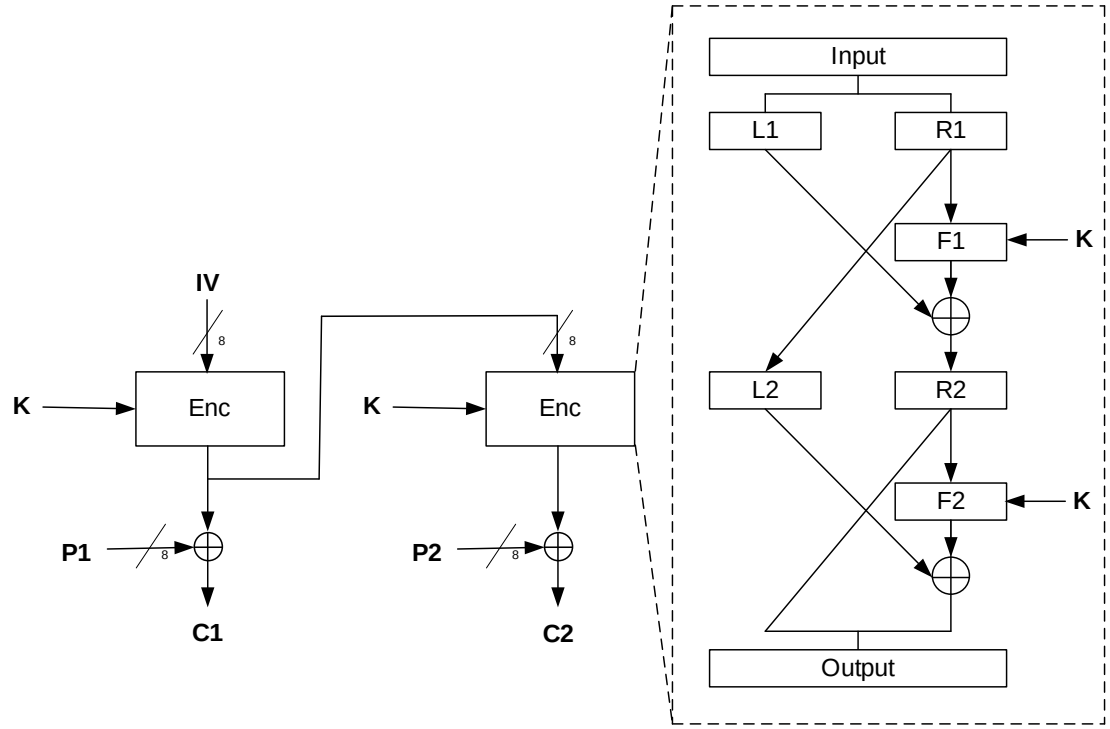
1) Έστω ο αλγόριθμος τμήματος που έχει σχεδιαστεί με χρήση Feistel δικτύων. Ο αλγόριθμος έχει δύο γύρους χωρίς αρχική και τελική μετάθεση. Η συνάρτηση που χρησιμοποιείται σε κάθε γύρο είναι η παρακάτω

$F_i(x,K) = (2iK)^x \bmod 15$ για i=1, 2.

Αν K=7 κρυπτογραφείστε το απλό κείμενο 00111111.

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

P=011010100010011, IV=00000100, K= 3, $F_i(x,K) = (iK)^x \ \ mod\ 15$ για i=1, 2.



3) Έστω ότι έχουμε το παρακάτω κουτί αντικατάστασης (S-Box).

Κουτί Αντικατάστασης															
7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

Θεωρείται ότι το κουτί αντικατάστασης έχει σαν είσοδο μια ακολουθία από 6-bit και σαν έξοδο μια ακολουθία από 4-bit. Για την ακολουθία εισόδου $y_1y_2y_3y_4y_5y_6$ η δυαδική αναπαράσταση y_1y_6 ορίζει την γραμμή του κουτιού ενώ η δυαδική αναπαράσταση $y_2y_3y_4y_5$ δίνει την στήλη του πίνακα. Η έξοδος είναι το στοιχείο που βρίσκεται στην θέση σύμφωνα με την μεθοδολογία που αναφέρθηκε παραπάνω. Τόσο οι γραμμές όσο και οι στήλες του κουτιού αρχίζουν να μετρούνται από το μηδέν.

i) Για τις επόμενες εισόδους, 000000, 010011, 101100, 111011, υπολογίστε την αντίστοιχη έξοδο.

ii) Να δείξετε ότι η δεύτερη γραμμή του κουτιού μπορεί να υπολογιστεί από την πρώτη γραμμή σύμφωνα με την σχέση $(y_1, y_2, y_3, y_4) \mapsto (y_2, y_1, y_4, y_3) \oplus (0,1,1,0)$.