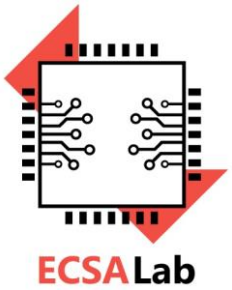
Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Πανεπιστημίου Πελοποννήσου

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



Ασφάλεια Υπολογιστικών Συστημάτων

Διδάσκων: Δρ. Παρασκευάς Κίτσος (Καθηγητής)

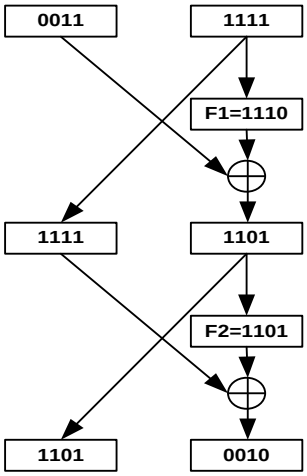
Λύσεις των ασκήσεων στη θεματική ενότητα των Συμμετρικών Αλγορίθμων

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.

Λύση

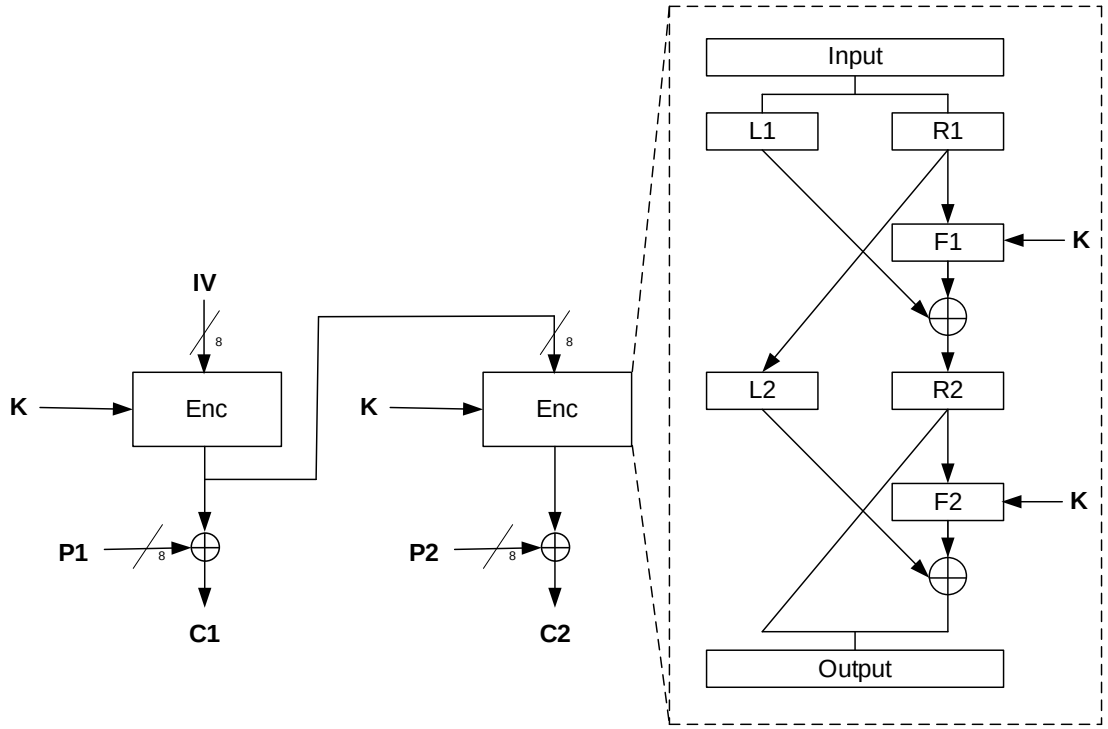


F1=$(2K)^x$ mod 15= 1110

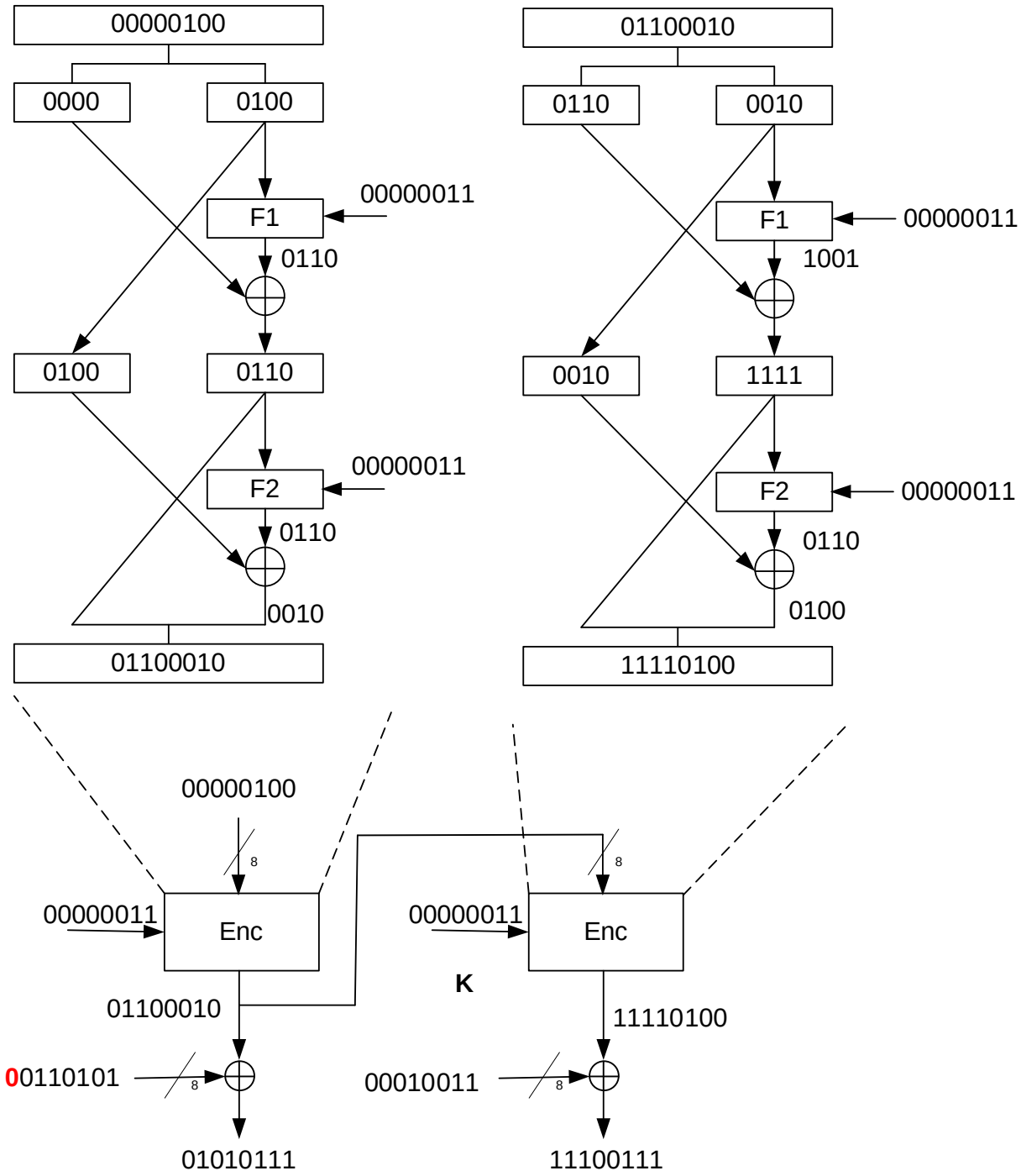
F2=$(4K)^x$ mod 15= 1101

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.



Λύση



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 $(y_1, y_2, y_3, y_4) \mapsto (y_2, y_1, y_4, y_3) \oplus (0,1,1,0)$.

Λύση

Οι έξοδοι του κουτιού για τις δοθείσες εισόδους μπορούν να υπολογιστούν από τον παρακάτω πίνακα.

Είσοδος	Γραμμή	Στήλη	Έξοδος
000000_2	$00_2 = 0_{10}$	$0000_2 = 0_{10}$	$7_{10} = 0111_2$
010011_2	$01_2 = 1_{10}$	$1001_2 = 9_{10}$	$7_{10} = 0111_2$
101100_2	$10_2 = 2_{10}$	$0110_2 = 6_{10}$	$7_{10} = 0111_2$
111011_2	$11_2 = 3_{10}$	$1101_2 = 13_{10}$	$7_{10} = 0111_2$

ii) Η σχέση $(y_1, y_2, y_3, y_4) \mapsto (y_2, y_1, y_4, y_3) \oplus (0,1,1,0)$ επιδρά με τον ακόλουθο τρόπο στην πρώτη γραμμή του κουτιού.

$7_{10} = 0111_2 \mapsto 1011_2 \oplus 0110_2 = 1101_2 = 13_{10}$

$13_{10} = 1101_2 \mapsto 1110_2 \oplus 0110_2 = 1000_2 = 8_{10}$

$14_{10} = 1110_2 \mapsto 1101_2 \oplus 0110_2 = 1011_2 = 11_{10}$

$3_{10} = 0011_2 \mapsto 0011_2 \oplus 0110_2 = 0101_2 = 5_{10}$

$0_{10} = 0000_2 \mapsto 0000_2 \oplus 0110_2 = 0110_2 = 6_{10}$

$6_{10} = 0110_2 \mapsto 1001_2 \oplus 0110_2 = 1111_2 = 15_{10}$

$9_{10} = 1001_2 \mapsto 0110_2 \oplus 0110_2 = 0000_2 = 0_{10}$

$10_{10} = 1010_2 \mapsto 0101_2 \oplus 0110_2 = 0011_2 = 3_{10}$

$1_{10} = 0001_2 \mapsto 0010_2 \oplus 0110_2 = 0100_2 = 4_{10}$

$2_{10} = 0010_2 \mapsto 0001_2 \oplus 0110_2 = 0111_2 = 7_{10}$

$8_{10} = 1000_2 \mapsto 0100_2 \oplus 0110_2 = 0010_2 = 2_{10}$

$5_{10} = 0101_2 \mapsto 1010_2 \oplus 0110_2 = 1100_2 = 12_{10}$

$11_{10} = 1011_2 \mapsto 0111_2 \oplus 0110_2 = 0001_2 = 1_{10}$

$12_{10} = 1100_2 \mapsto 1100_2 \oplus 0110_2 = 1010_2 = 10_{10}$

$4_{10} = 0100_2 \mapsto 1000_2 \oplus 0110_2 = 1110_2 = 14_{10}$

$15_{10} = 1111_2 \mapsto 1111_2 \oplus 0110_2 = 1001_2 = 9_{10}$

Όπου είναι ξεκάθαρο ότι δίνει την δεύτερη γραμμή του κουτιού αντικατάστασης.