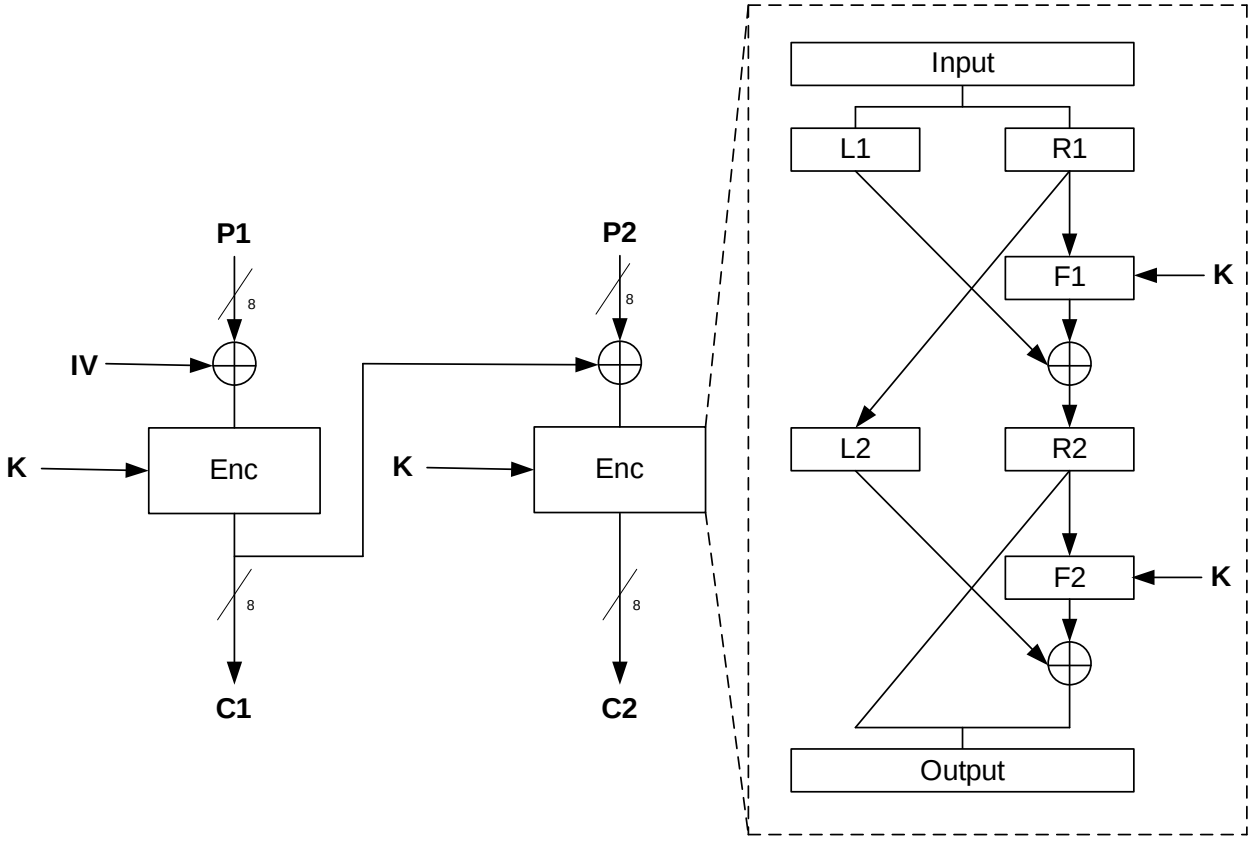
ECSA Lab	**«Ασφάλεια Υπολογιστικών Συστημάτων»** Δρ. Παρασκευάς Κίτσος, Αναπλ. Καθηγητής Εργαστήριο Ηλεκτρονικών Κυκλωμάτων, Συστημάτων και Εφαρμογών (ECSA Lab, https://ecsalab.ece.uop.gr/)

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

ΘΕΜΑΤΑ:

Θέμα 1

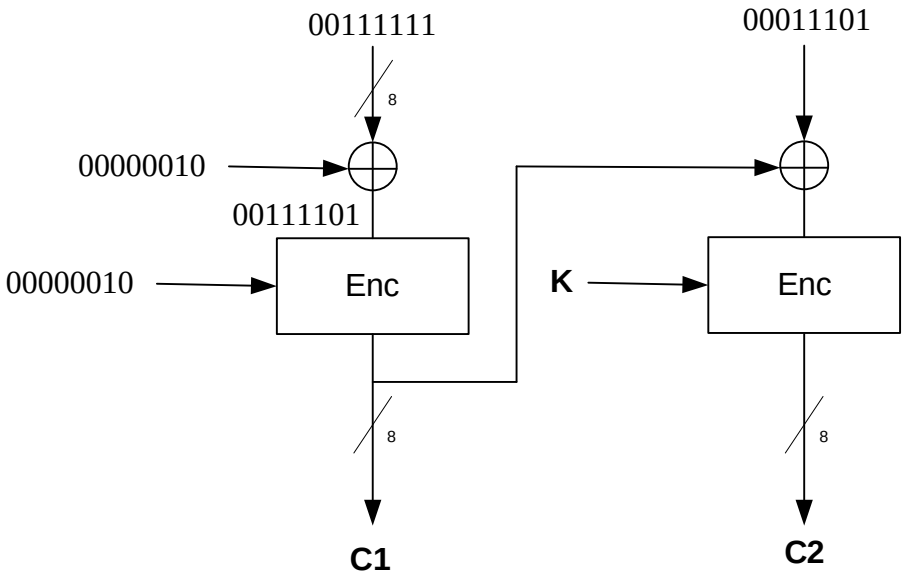
Αν ο τρόπος λειτουργίας ενός αλγορίθμου τμήματος που έχει σχεδιαστεί με χρήση Feistel δικτύων είναι ο Cipher Block Chaining του παρακάτω σχήματος, να εκτελέσετε κρυπτογράφηση με τα παρακάτω δεδομένα.



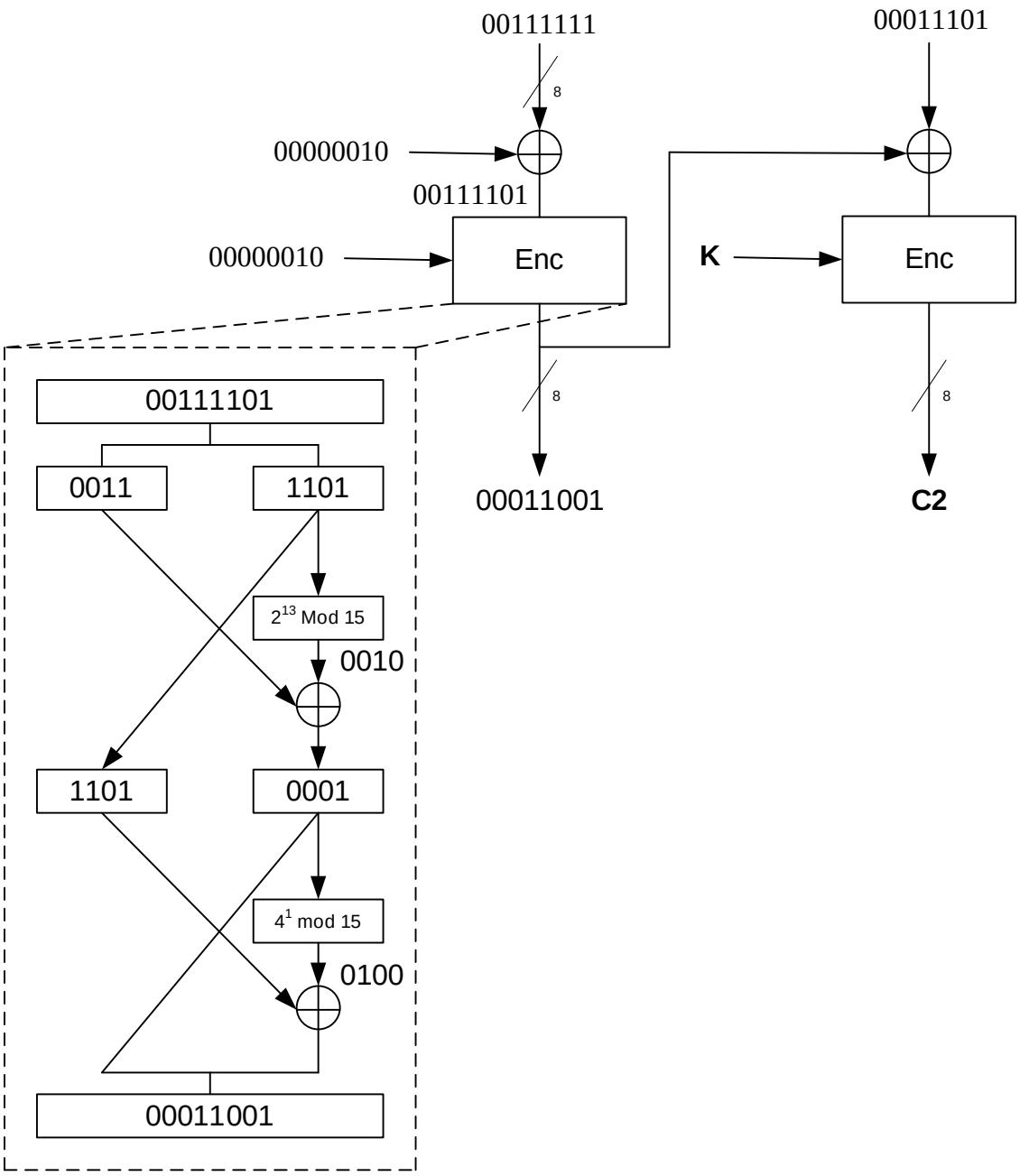
P=011111100011101, IV=00000010, K= 2, $F_i(x,K) = (iK)^x \mod 15$ για i=1, 2.

Λύση

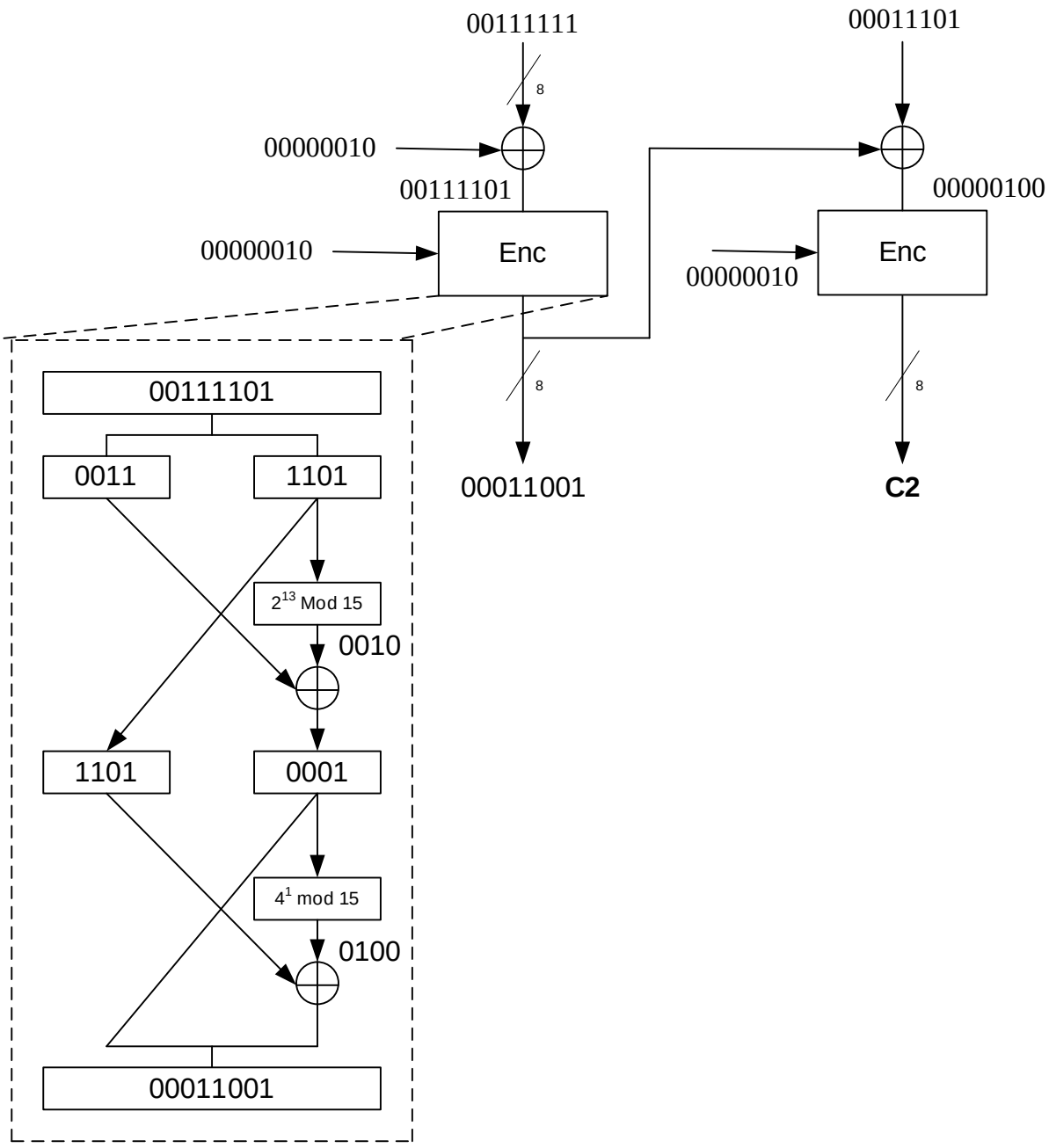
Αρχικά χωρίζουμε το μήνυμα P (P1 = **0**0111111, P2 = 00011101) σε δύο οκτάδες (bytes) και χρησιμοποιούμε μία ανά είσοδο του κάθε αλγορίθμου. Παρατηρούμε ότι το μήνυμα P είναι 15 bits, οπότε πρέπει να προστεθεί ένα 0 αριστερά ώστε να γίνει 16 bits και να μην μεταβληθεί η τιμή του. Χρησιμοποιούμε επίσης τις εισόδους του IV και του κλειδιού και έχουμε το παρακάτω σχήμα.



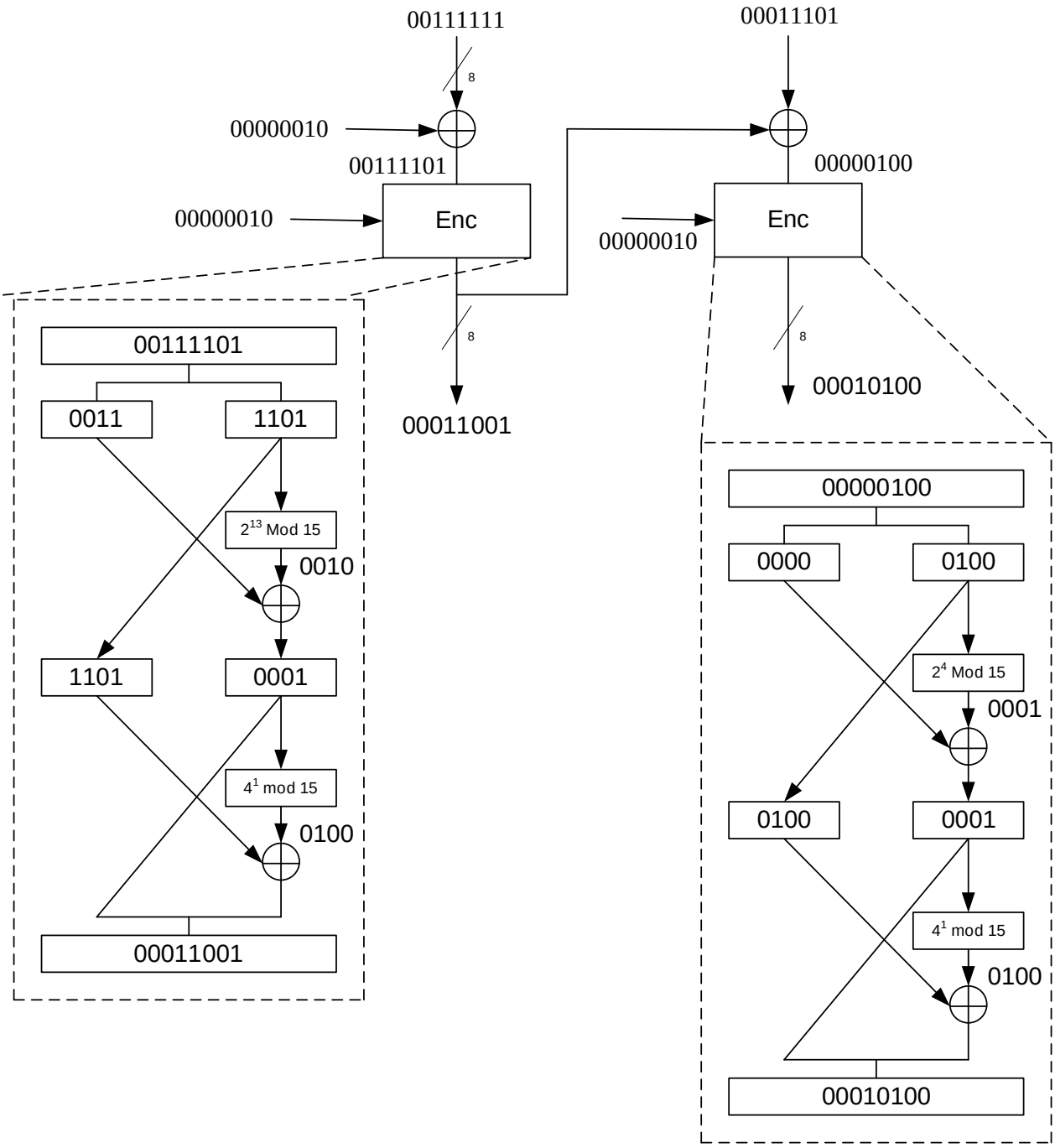
Έπειτα εκτελούμε τις πράξεις στον πρώτο αλγόριθμο και προκύπτει το παρακάτω σχήμα. Προσέχουμε ότι στις συναρτήσεις *Fi* που εκτελούνται ο δείκτης i αναφέρεται στον γύρο του αλγορίθμου, το K είναι το κλειδί που έχει ως είσοδο ο αλγόριθμος, και η είσοδο x (ο εκθέτης στη συγκεκριμένη συνάρτηση) είναι η είσοδος της *Fi* δηλαδή κάθε φορά το τμήμα *Ri*.



Έπειτα εκτελούμε τη λογική πράξη XOR τους αποτελέσματος της πρώτης εκτέλεσης με την είσοδο της δεύτερης εκτέλεσης και έχουμε.



Τέλος εκτελούμε τις πράξεις στον δεύτερο αλγόριθμο χρησιμοποιώντας τις εισόδους και προκύπτει το παρακάτω σχήμα.



Οπότε το τελικά αποτέλεσμα είναι το C=0001100100010100.

Θέμα 2

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

Λύση

Τα βήματα του RSA για τον υπολογισμό των δημοσίου και ιδιωτικού κλειδιού είναι τα παρακάτω.

1) p = 5, q = 13

2) $n = pq = 65$

3) $\varphi(n) = (p - 1)(q - 1) = 48$

4) Επιλογή του ακεραίου e ($1 < e < \varphi(n)$) έτσι ώστε να είναι αμοιβαία πρώτος του $\varphi(n) = 48$. Μια τέτοια επιλογή είναι η $e = 7$

5) Υπολογισμός d έτσι ώστε $de \equiv 1 \bmod 48$ (ή $de \bmod 48 = 1 \bmod 48 \Leftrightarrow 7d \bmod 48 = 1 \Leftrightarrow d=7$)

Άρα

Δημόσιο κλειδί =(7, 65)

Ιδιωτικό κλειδί = (7, 65)

Η κρυπτογράφηση εκτελείται σύμφωνα με τη σχέση

$C=M^7 \bmod 65 = 21^7 \bmod 65 = 31$

$P=31^7 \bmod 65 = 31^7 \bmod 65 = 21.$