13.10

Berechnen Sie den Ciphertext C.
der Plaintext (in Bits) 10011100

die Rundenschlüssel K_1 = 0101 und K_2 = 1101

durchgänge: 2

1/2

L0: 1001

R0: 1100 -> XOR mit K1: 1100

0101

1001=f

L0 XOR mit f -> 1001

1001

0000=R1

L1=R0,

Neu: 1100 0000

Erster Durchgang beendet

2/2

1100 0000

L1= 1100

R1= 0000 -> XOR mit K2: 0000

1101

1101=f2

L1 Xor mit f2 -> 1100

1101

0001=R2

L2=R1

Neu: 0000 0001

Zweiter Durchgang beendet

Ergebnis C = 0000 0001

Berechnen Sie aus C wieder den Plaintext P.

L2=0000, R2=0001

L2 XOR K2= 0000

1101

1101=f2

R2 XOR f2 = 0001

1101

1100=L1

R1=L2=0000

Zwischenstand: 1100 0000 = c1

L1=1100, R1=0000

L1 XOR K1= 1100

0101

1001=f1

R1 XOR f1= 0000

1001

1001=L0

R0=L1=1100

C= 1001 1100