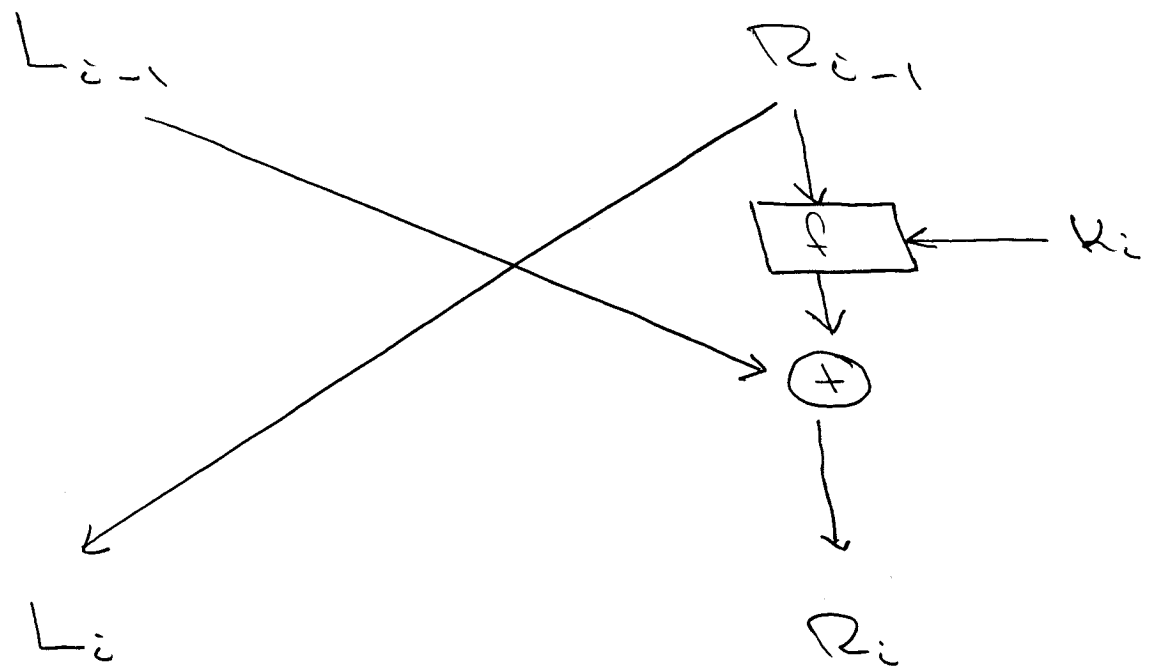


One round of a Feistel System



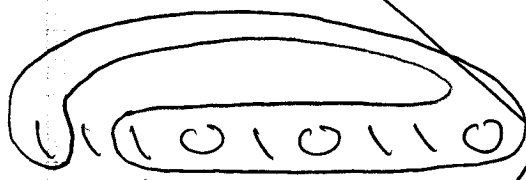
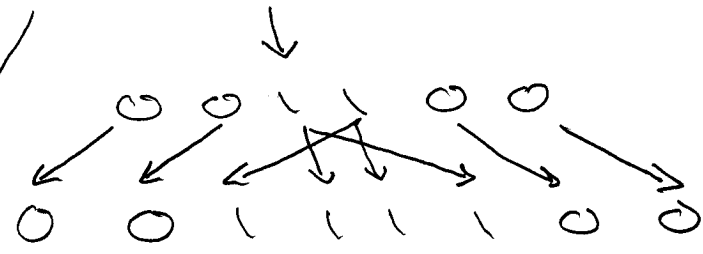
trapp &
washington

Now, ... 4 rounds of
the trapp-washington
Simplified DES-type Algorithm

Round $i=3$

L_2
0 0 0 0 1 1

R_2
0 0 1 1 0 0



K_3

↑
bit#3

1 0 1 0 1 1 0 1

1 0 0 1 | 0 0 0 1
column s_1 | column s_2

1 0 0

0 0 0

0 0 0 | 0 1 1

1 0 0 | 0 1 1

0 0 1 1 0 0

L_3

R_3

Round $i = 4$

L_3
0 0 1 1 0 0

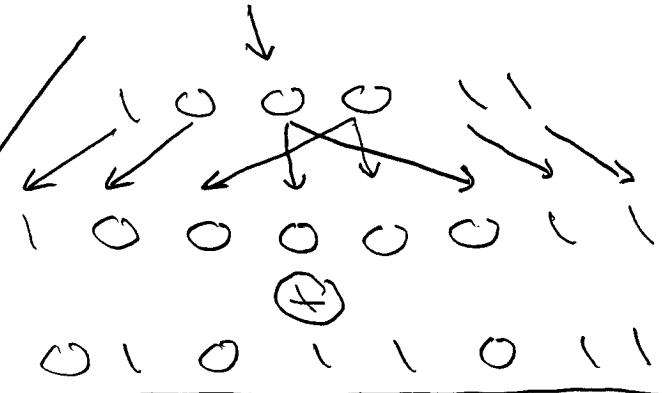
R_3
1 0 0 0 1 1

K_4

1 1 1 0 1 0 1 1 0
↑
4th bit

1 0 0 0 1 1

L_4



0 1 0 1 1 1 0 1 1

column S_1 | column S_2
0 0 0 | 0 0 0
1 0 1

0 0 1 1 0 0

1 1 0 0 0 1

R_4

12-bit
ciphertext

1 0 0 0 1 1 1 0 0 0 1