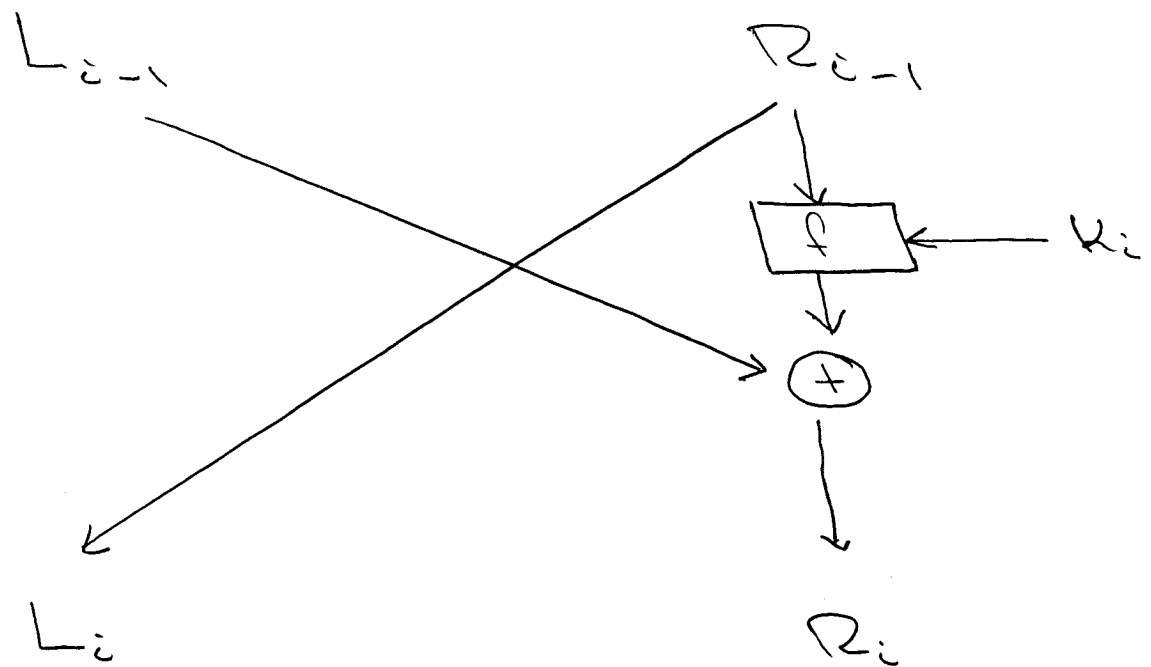


One round of a Feistel System



trapp &
washington

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

9-bit
key

Round $i = 1$

$K = 111010110$

12-bit
message

L_0 | R_0
1 0 1 1 0 1 | 1 1 0 1 0 1

expand to
8 bits

1 1 0 1 0 1
1 1 1 0 1 0 0 0

xor \oplus

1 1 1 0 1 0 1 1

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

S-boxes

1 0 1 1 1 0

xor \oplus

1 0 1 1 0 1

0 0 0 0 1 1

1 1 0 1 0 1

L_1

R_1

take 8 bits
 K_1 1 1 1 0 1 0 1 1
↑
bit #1

Round $i=2$

L_1

R_1

1 1 0 1 0 1 / 0 0 0 0 1 1

0 0 0 0 1 1
0 0 0 0 0 1

\oplus

1 1 0 1 0 1 1 0

1 1 0 1 / 0 1 0 1

column S_1

column S_2

1 1 1

0 0 1

\oplus

1 1 0

1 0 1

0 0 1

1 0 0

L_2

R_2

0 0 0 0 1 1

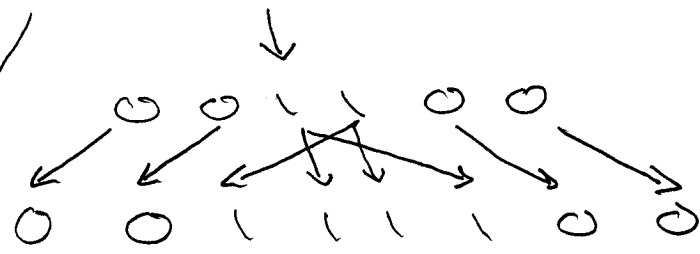
L_2

1 1 0 1 0 1 1 0

bit #2

Round $i=3$

L_2 0 0 0 0 1 1 | R_2 0 0 1 1 0 0



\oplus

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

\oplus

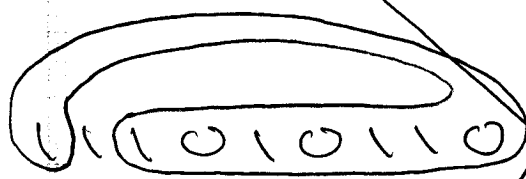
0 0 0 0 1 1 1

1 0 0 0 1 1

L_3

R_3

K_3



↑
bit #3

0 0 1 1 0 0

Round $i = 4$

L_3
0 0 1 1 0 0

R_3
1 0 0 0 1 1

K_A

1 1 1 0 1 0 1 1 0

4th bit

1 0 0 0 1 1

L_4

1 0 0 0 1 1
1 0 0 0 0 0 1 1

(+)

0 1 0 1 1 0 1 1

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

1 1 1 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