

T-79.5501

Cryptology

Lecture 5 (Oct 11, 2005):

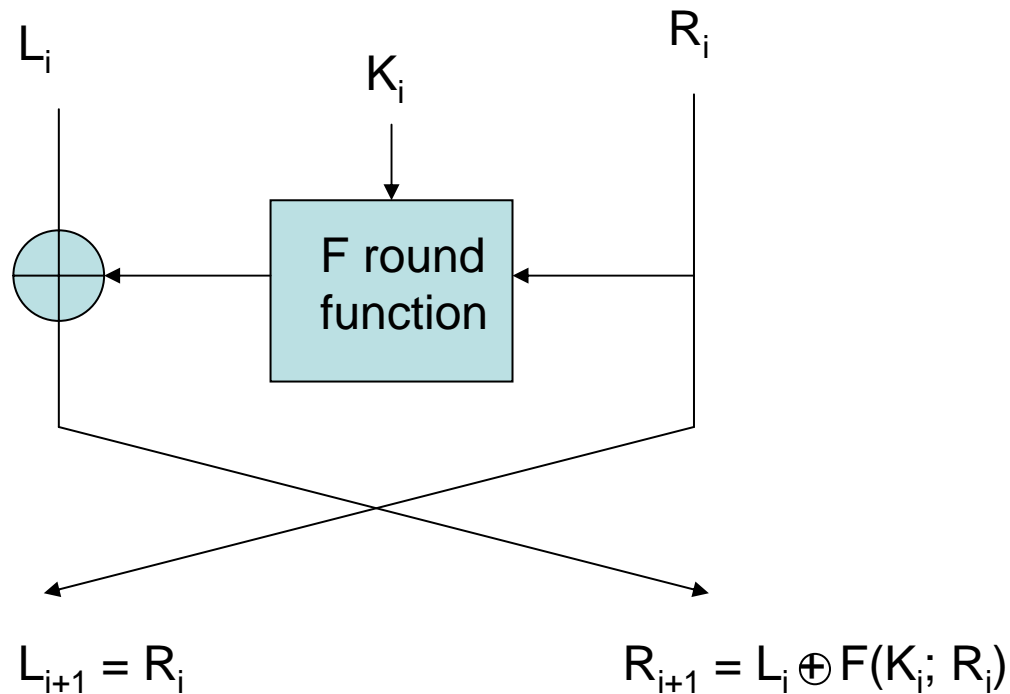
- Substitution-Permutation Networks (SPN)
- Feistel Networks
- Linear cryptanalysis

Substitution-Permutation Networks

- Textbook: Sections 3.1, 3.2

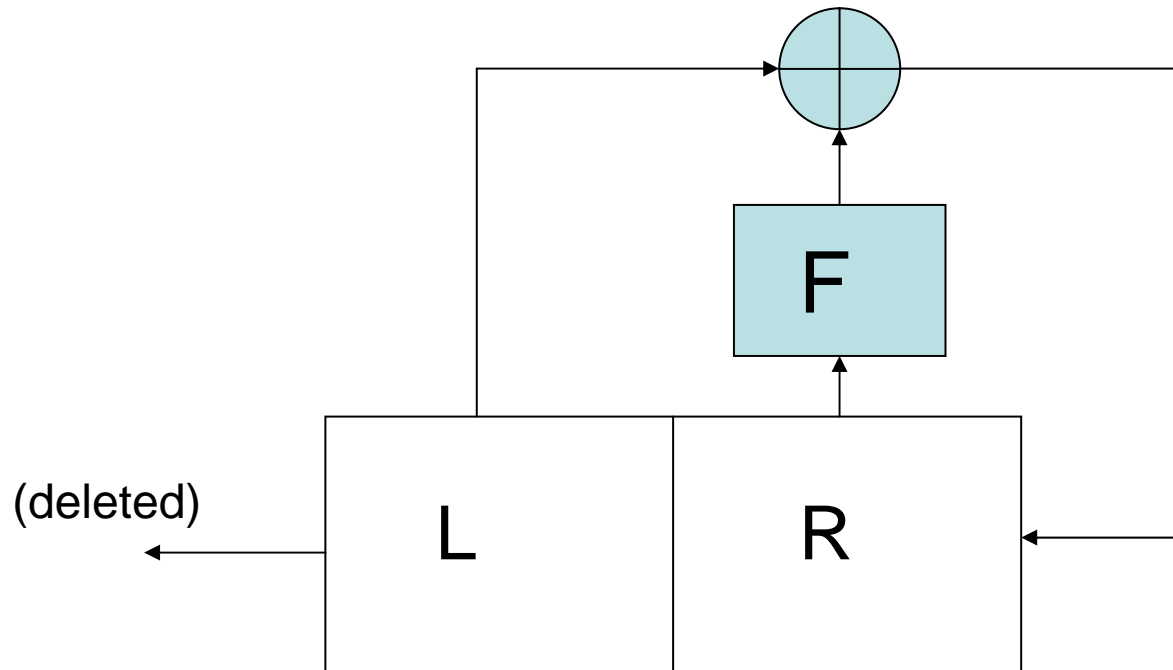
Feistel Ciphers

- Special structure to make it invertible
- S-boxes and round-functions need not be invertible
- Example: DES (Section 3.5)



Feistel cipher

Seen as a nonlinear feedback shift register:



Linear Cryptanalysis

- Text-book section 3.3

Example: A linear approximation of the first line of DES S-box S_3

Y	$X_1X_2X_3X_4$	$Y_1Y_2Y_3Y_4$	Y_3	$X_3 \oplus X_4$	=?
10	0000	1010	1	0	no
0	0001	0000	0	1	no
9	0010	1001	0	1	no
14	0011	1110	1	0	no
6	0100	0110	1	0	no
3	0101	0011	1	1	yes
15	0110	1111	1	1	yes
5	0111	0101	0	0	yes
1	1000	0001	0	0	yes
13	1001	1101	0	1	no
12	1010	1100	0	1	no
7	1011	0111	1	0	no
11	1100	1011	1	0	no
4	1101	0100	0	1	no
2	1110	0010	1	1	yes
8	1111	1000	0	0	yes

a = 0011

b = 0010

bias (a,b) =

$(6-8)/16 = -2^{-3}$