Chapter 4

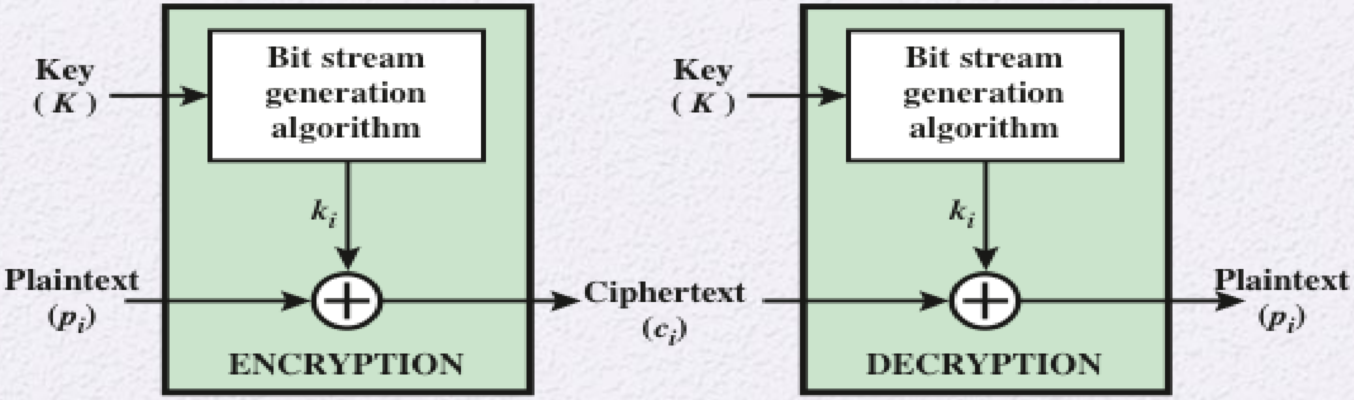
Block Ciphers and the Data Encryption Standard

Stream Cipher

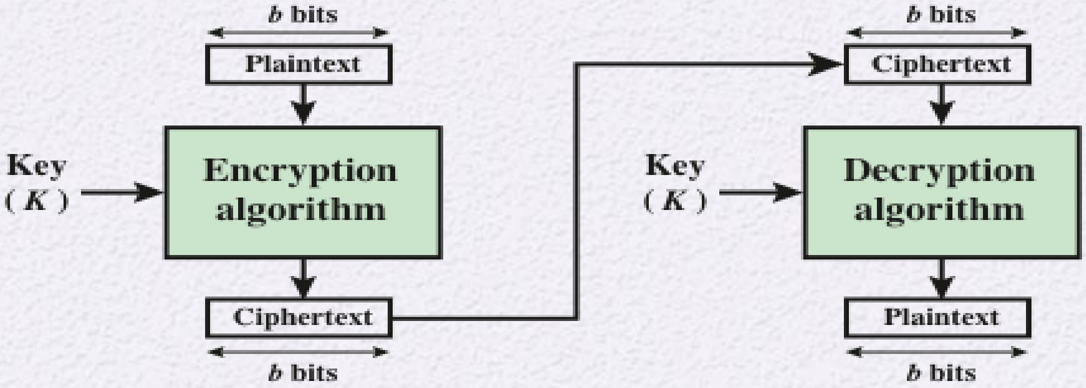
- Encrypt plaintext bit by bit or byte by byte.
- Each unit (bit or byte) is encrypted with a different key.
  - $E(k_i, p_i)=c_i, 1 \leq i \leq m$
- Examples
  - Autokeyed Vigenère cipher
  - Vernam cipher, one-time pad
  - RC4
  - Hardware-based: Linear Feed Shift Register (LFSR)

Block Cipher

- Encrypt plaintext block by block, typically 128 bits
- Each unit is encrypted with the same key
    - $E(k, p_i)=c_i$, $1 \leq i \leq m$
- Examples
    - Playfair cipher
    - Hill cipher
    - DES, AES



(a) Stream Cipher Using Algorithmic Bit Stream Generator



(b) Block Cipher

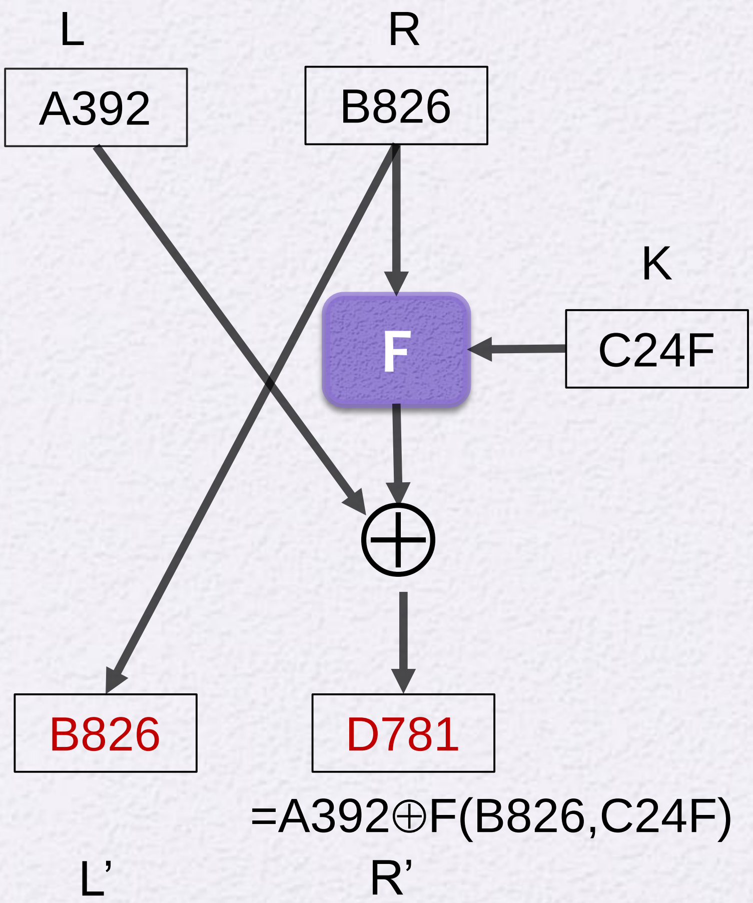
Design principles

- Horst Feistel
  - a cipher should alternate substitutions and permutations
  - Feistel structure
    - Easy decryption no matter what functions are used
    - Focus on substitution and permutation design
- Claude Shannon
  - for practical application, a cipher should be a product of alternate confusion and diffusion functions
  - Accumulate full security from small security of each function

Diffusion and Confusion

- To thwart “statistical analysis”
- Diffusion
  - The statistical structure of the plaintext is dissipated into long-range statistics of the ciphertext
  - Each plaintext digit affects many ciphertext digits
- Confusion
  - Complicate the statistics relationship between of the ciphertext and the encryption key
  - Even if the attacker gets some statistics of the ciphertext, the key is still too complex to deduce

Feistel structure



L R

A392 B826

K

C24F

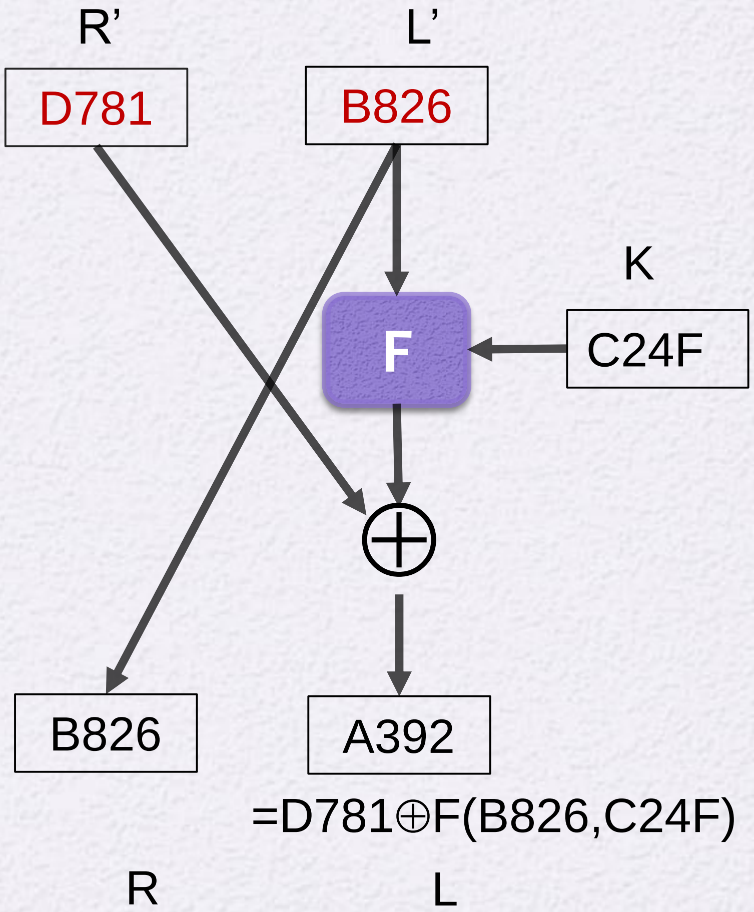
F

B826 D781

=A392⊕F(B826,C24F)

L’ R’

Encryption



R’ L’

D781 B826

K

C24F

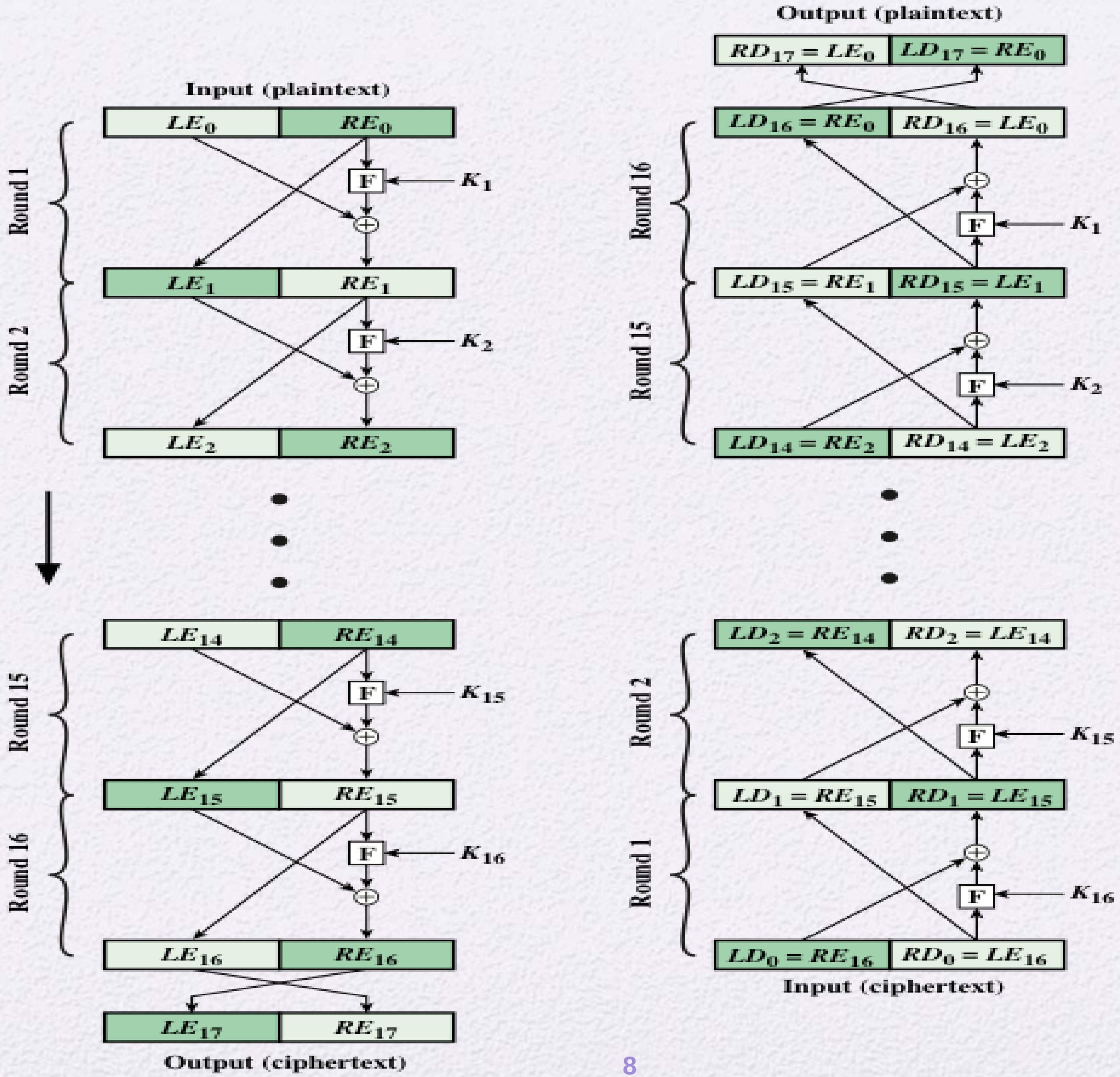
F

B826 A392

=D781⊕F(B826,C24F)

R L

Decryption

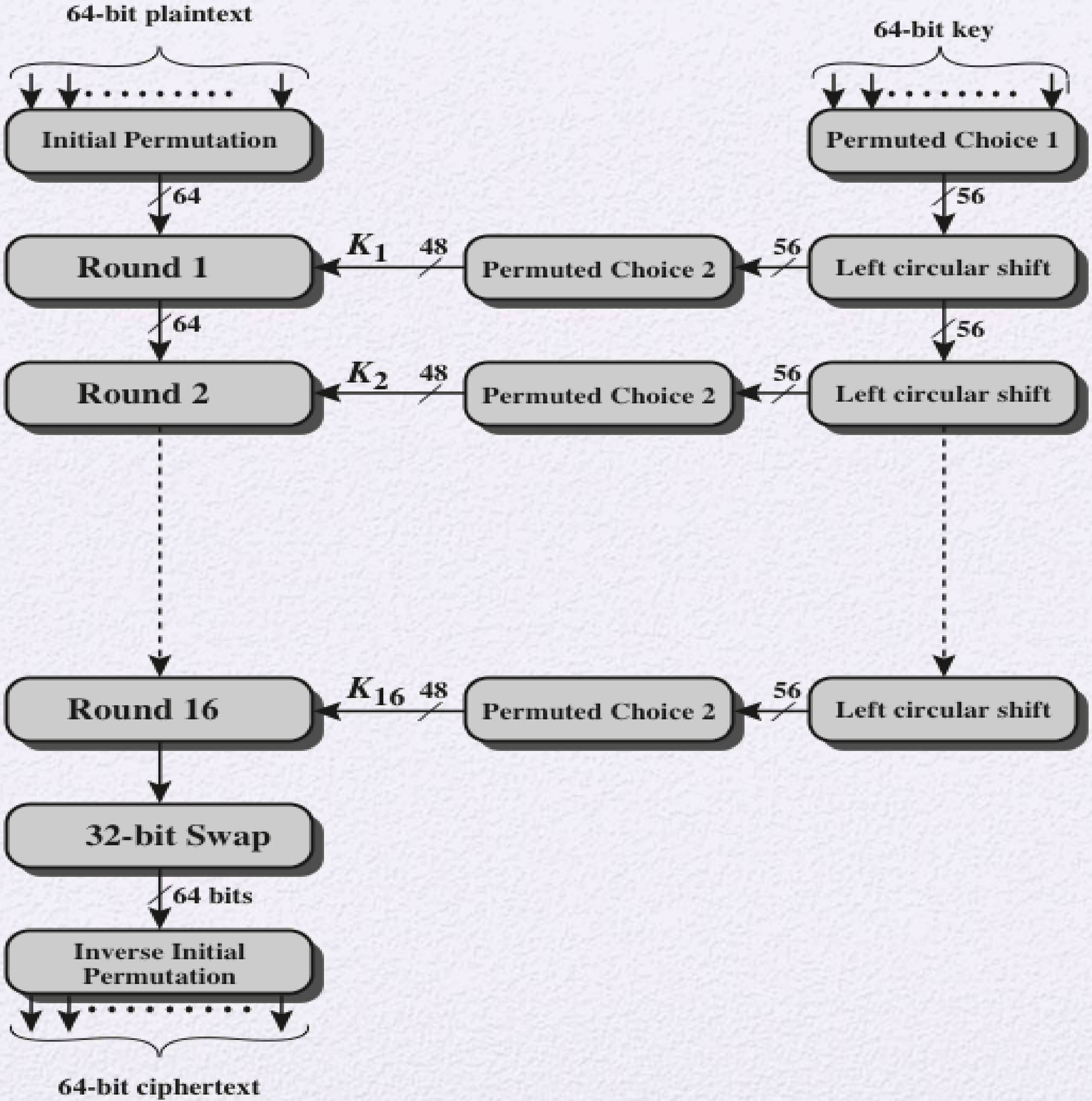

Input (plaintext)
LE_0
RE_0
Round 1
F
K_1
LE_1
RE_1
Round 2
F
K_2
LE_2
RE_2
LE_{14}
RE_{14}
Round 15
F
K_{15}
LE_{15}
RE_{15}
Round 16
F
K_{16}
LE_{16}
RE_{16}
LE_{17}
RE_{17}
Output (ciphertext)
Output (plaintext)
$RD_{17} = LE_0$
$LD_{17} = RE_0$
$LD_{16} = RE_0$
$RD_{16} = LE_0$
Round 16
F
K_1
$LD_{15} = RE_1$
$RD_{15} = LE_1$
Round 15
F
K_2
$LD_{14} = RE_2$
$RD_{14} = LE_2$
$LD_2 = RE_{14}$
$RD_2 = LE_{14}$
Round 2
F
K_{15}
$LD_1 = RE_{15}$
$RD_1 = LE_{15}$
Round 1
F
K_{16}
$LD_0 = RE_{16}$
$RD_0 = LE_{16}$
Input (ciphertext)

Feistel Cipher: Factors

- Speed (hardware/software) and security concerns
  - Block size
  - Key size
  - Number of rounds
  - Round function F
  - Subkey generation algorithm
  - Security analysis

Data Encryption Standard (DES)

- National Bureau of Standards (now NIST) 1977, Federal Information Processing Standard 46 (FIPS-46), 1977
- Data Encryption Algorithm (DEA)
  - Plaintext, ciphertext: 64 bits
  - Key size: 56-bit key
  - 16 rounds
  - Feistel cipher
- Replaced by Advanced Encryption Standard (AES) in 2001, FIPS 197


64-bit plaintext
64-bit key
Initial Permutation
Permuted Choice 1
64
56
Round 1
K_1
48
Permuted Choice 2
56
Left circular shift
64
56
Round 2
K_2
48
Permuted Choice 2
56
Left circular shift
Round 16
K_{16}
48
Permuted Choice 2
56
Left circular shift
32-bit Swap
64 bits
Inverse Initial Permutation
64-bit ciphertext

DES : initial permutation

- Initial permutation: IP (64 bits → 64 bits)
- Final permutation: IP^{-1} (64 bits → 64 bits)

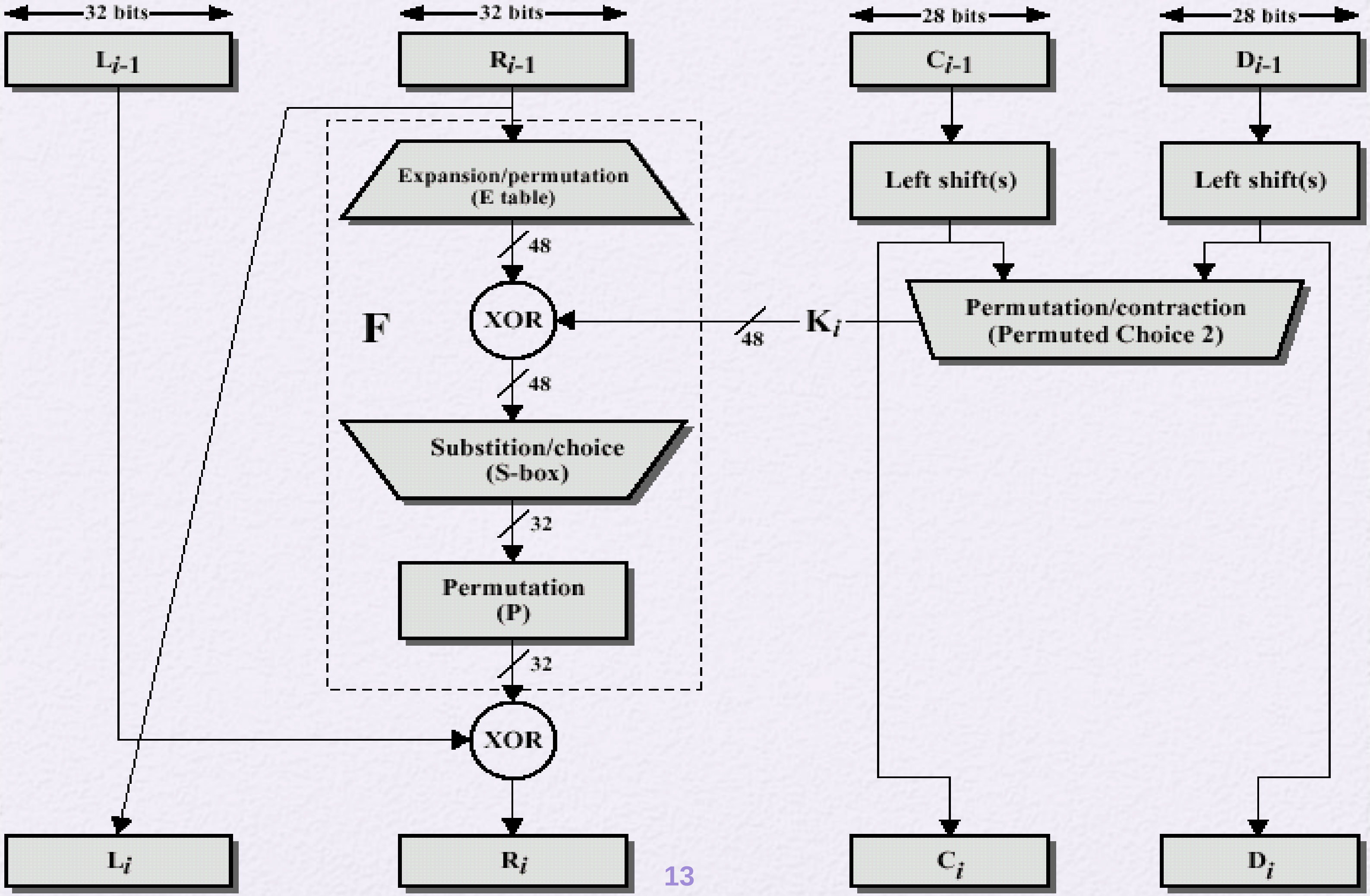
IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

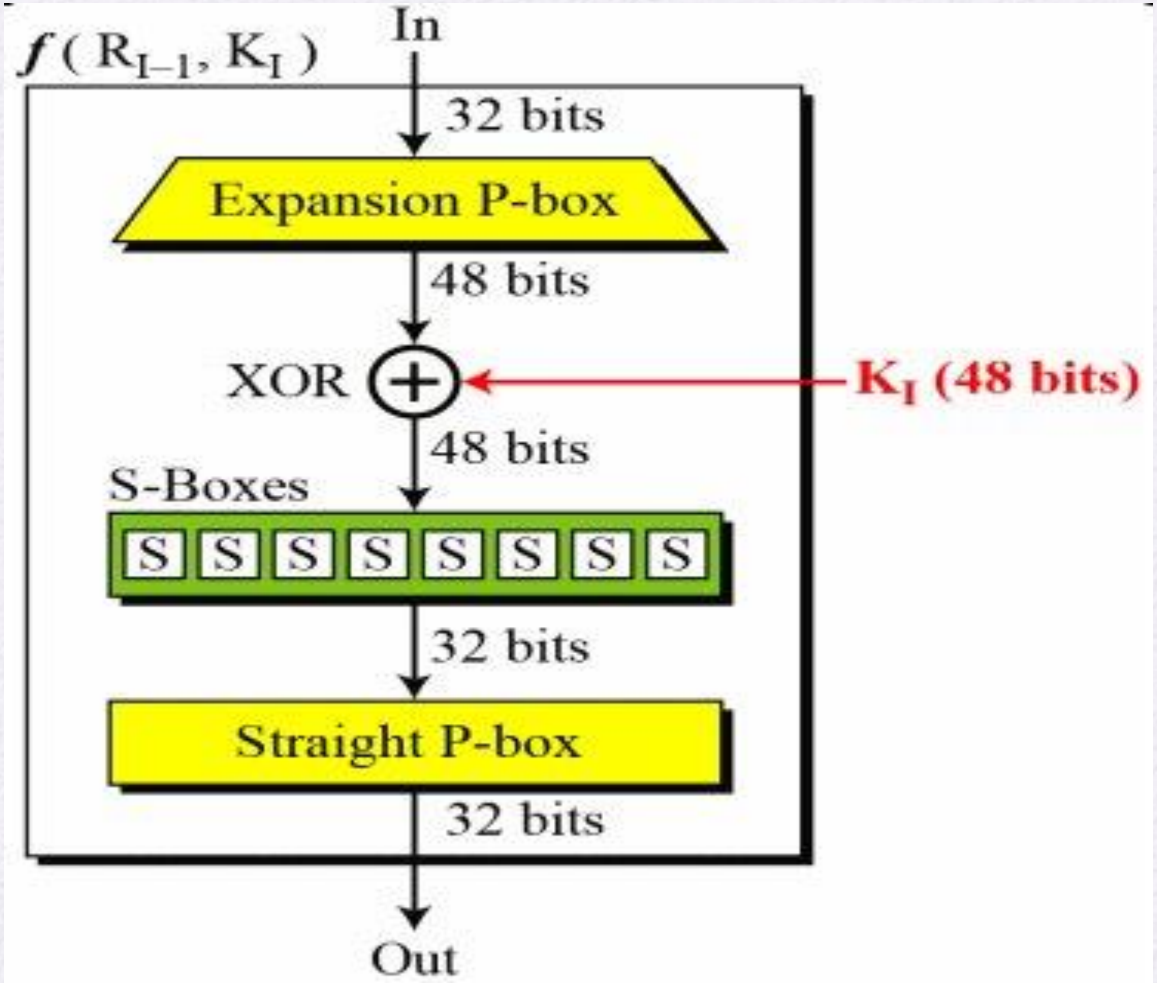
IP^{-1}

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

DES: a single round

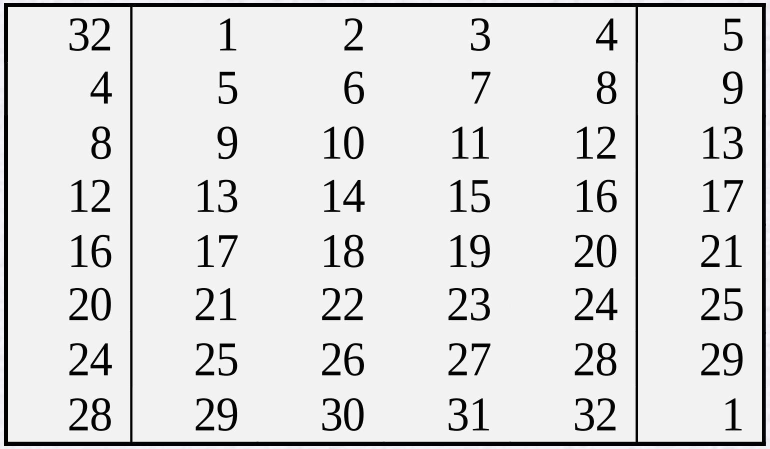


F function


In
$f(R_{I-1}, K_I)$
32 bits
Expansion P-box
48 bits
XOR
K_I (48 bits)
48 bits
S-Boxes
S S S S S S S S
32 bits
Straight P-box
32 bits
Out

DES: E

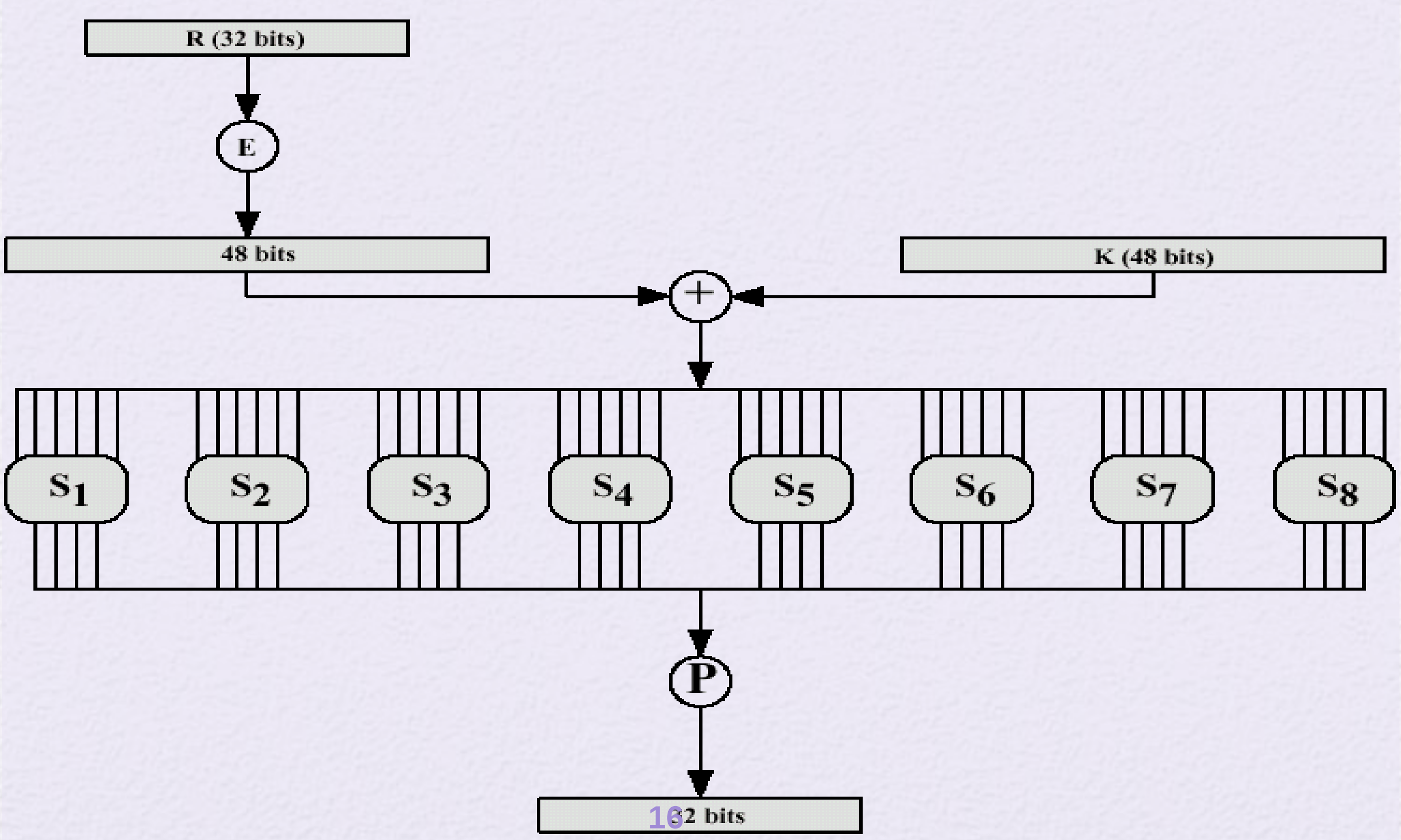
- Expansion permutation E: 32 bits→48bits
- Input bits: 1 2 3 …   32



32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

DES: S-box

- The only non-linear relation between input and output
- The core of security

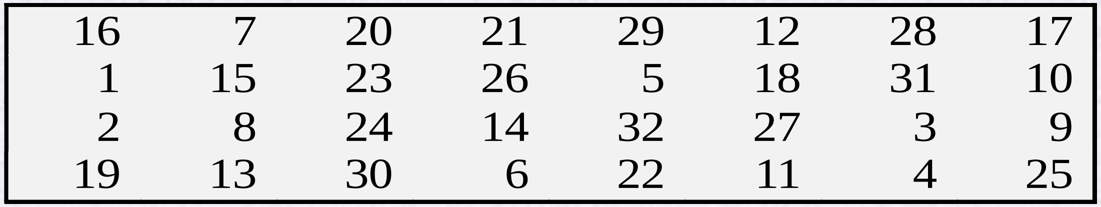


DES: S-box

i	S_i															
1	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
2	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
3	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
4	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
5	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
6	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
7	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
8	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

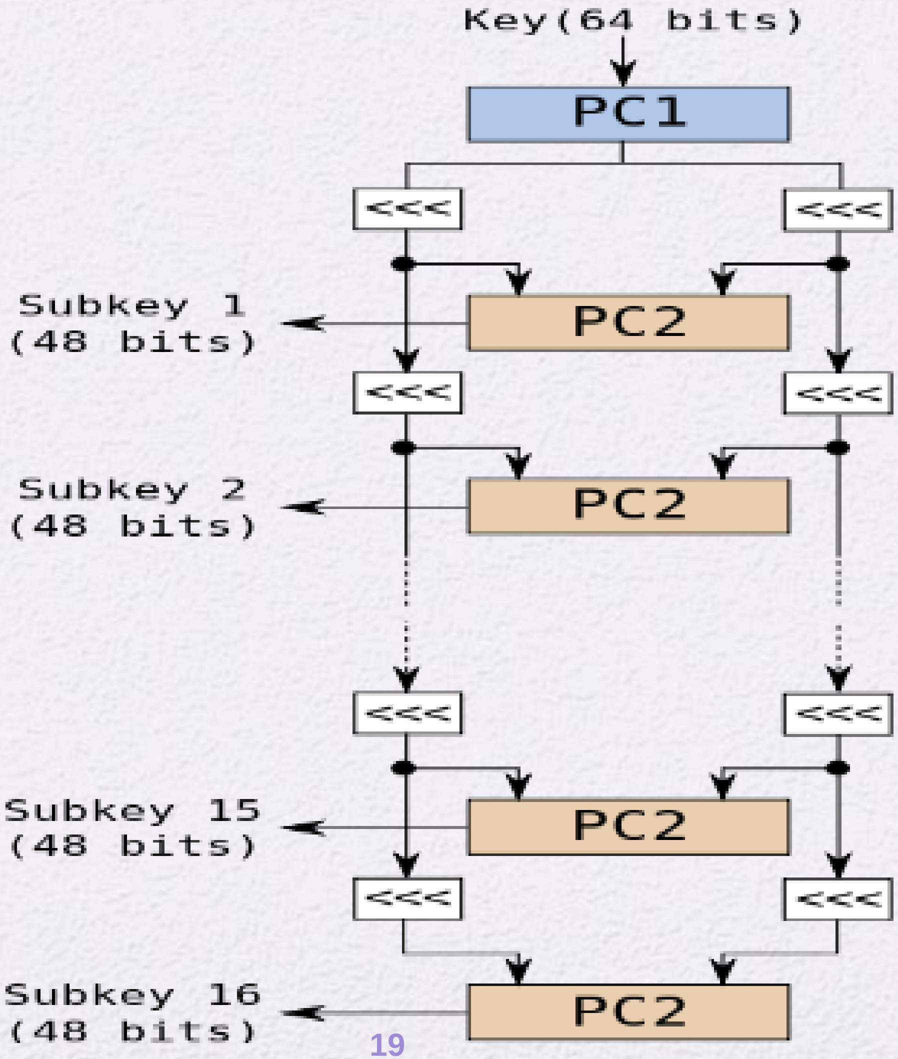
DES: P

- Permutation function P: 32 bits→32 bits

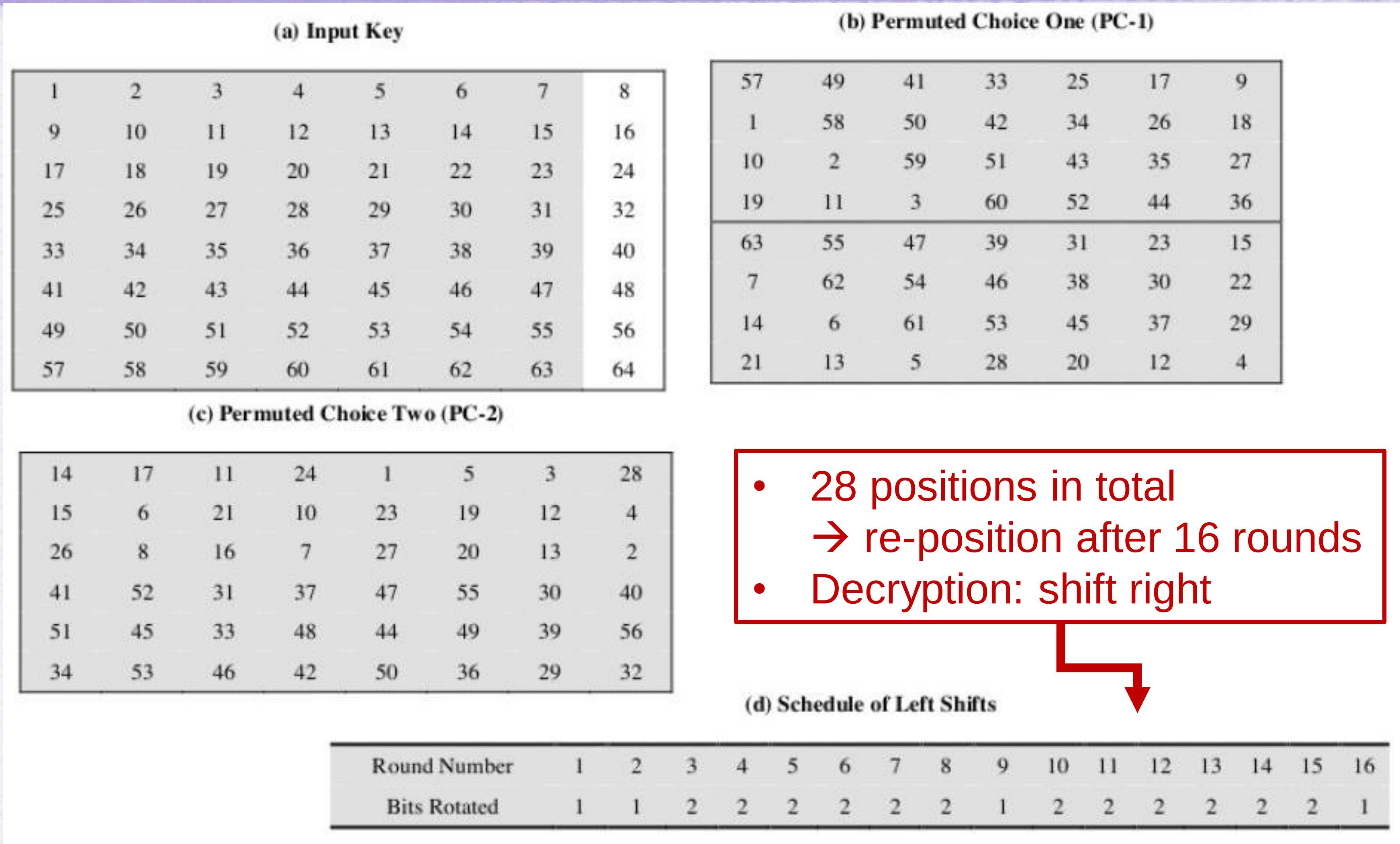


16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

Key scheduling



Key scheduling



(a) Input Key

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

(b) Permuted Choice One (PC-1)

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

(c) Permuted Choice Two (PC-2)

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

- 28 positions in total
  → re-position after 16 rounds
- Decryption: shift right

(d) Schedule of Left Shifts

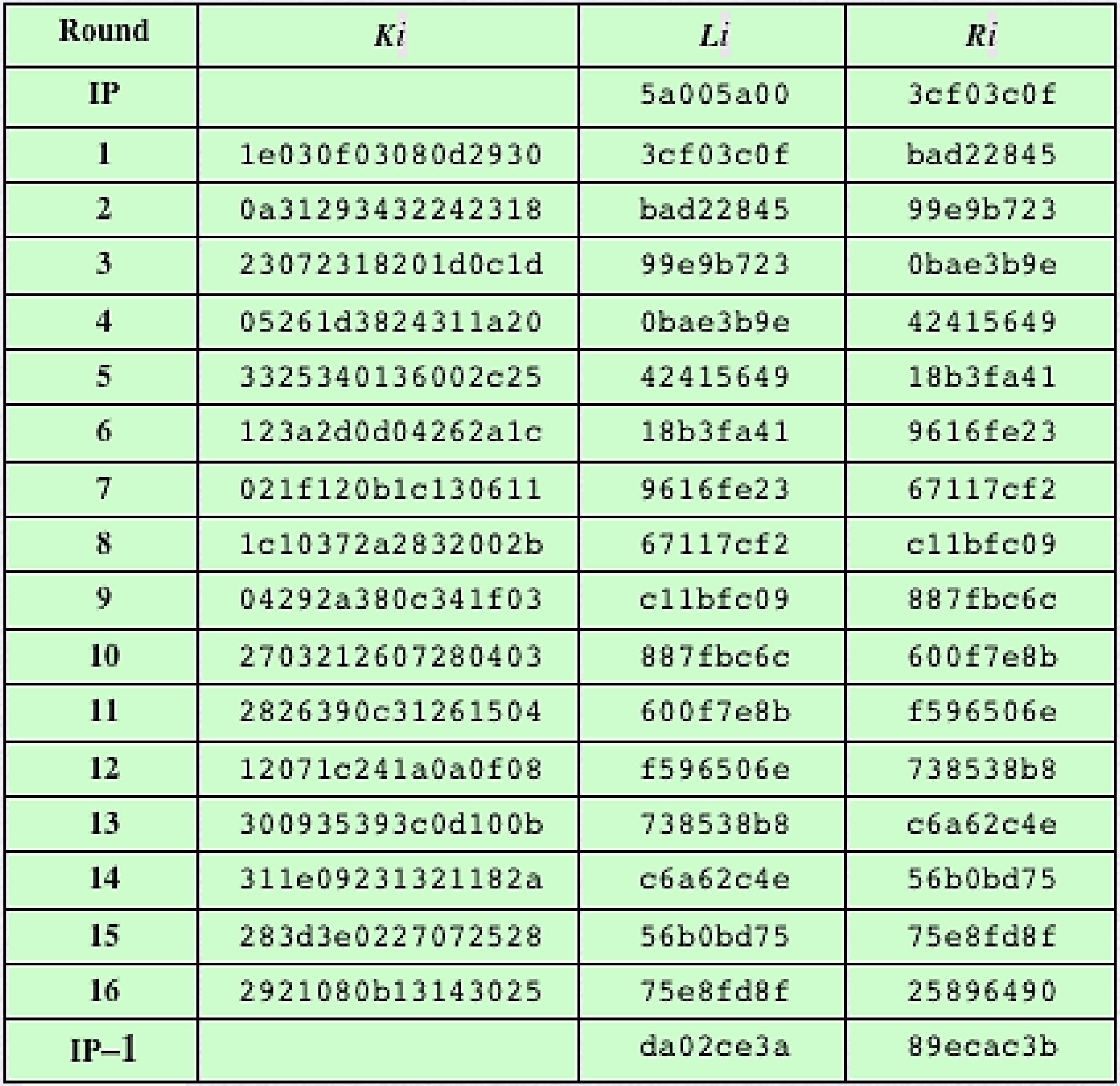
Round Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bits Rotated	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

DES Example

plaintext:
02468aceeca86420

key:
0f1571c947d9e859

ciphertext:
da02cd3a89ecac3b



Round	*Ki*	*Li*	*Ri*
IP		5a005a00	3cf03c0f
1	1e030f03080d2930	3cf03c0f	bad22845
2	0a31293432242318	bad22845	99e9b723
3	23072318201d0c1d	99e9b723	0bae3b9e
4	05261d3824311a20	0bae3b9e	42415649
5	3325340136002c25	42415649	18b3fa41
6	123a2d0d04262a1c	18b3fa41	9616fe23
7	021f120b1c130611	9616fe23	67117cf2
8	1c10372a2832002b	67117cf2	c11bfc09
9	04292a380c341f03	c11bfc09	887fbc6c
10	2703212607280403	887fbc6c	600f7e8b
11	2826390c31261504	600f7e8b	f596506e
12	12071c241a0a0f08	f596506e	738538b8
13	300935393c0d100b	738538b8	c6a62c4e
14	311e09231321182a	c6a62c4e	56b0bd75
15	283d3e0227072528	56b0bd75	75e8fd8f
16	2921080b13143025	75e8fd8f	25896490
IP–1		da02ce3a	89ecac3b

DES security

- The core of security is the non-linear mapping of S-boxes
- Key size: to defend the brute-force attack
- Avalanche effect
- Bit independence effect

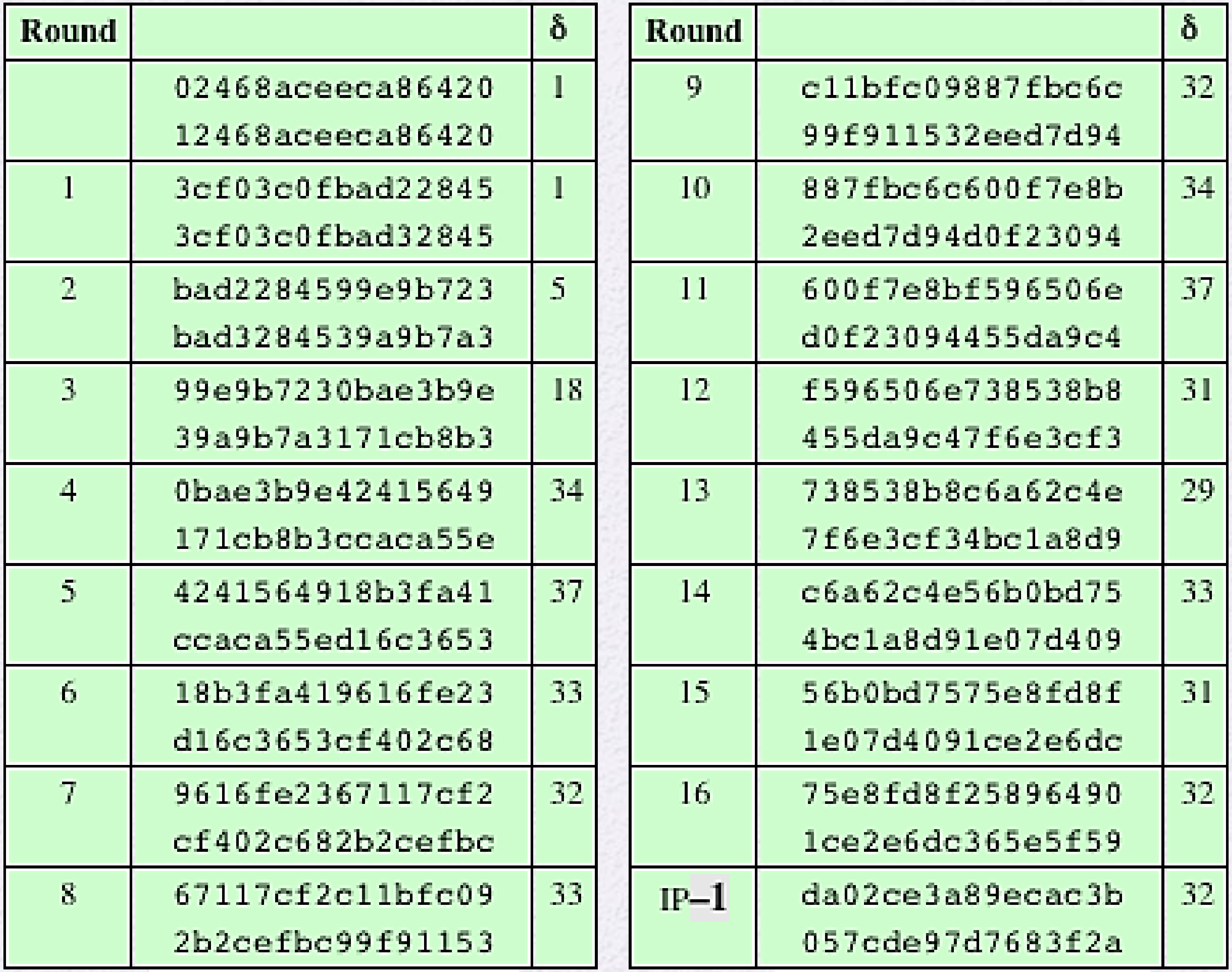
Avalanche effect

- A **small change** in either the plaintext or the key should produce **a significant change in the ciphertext**

- In particular, **one bit change** in either the plaintext or the key ➔ **half bits change** in ciphertext

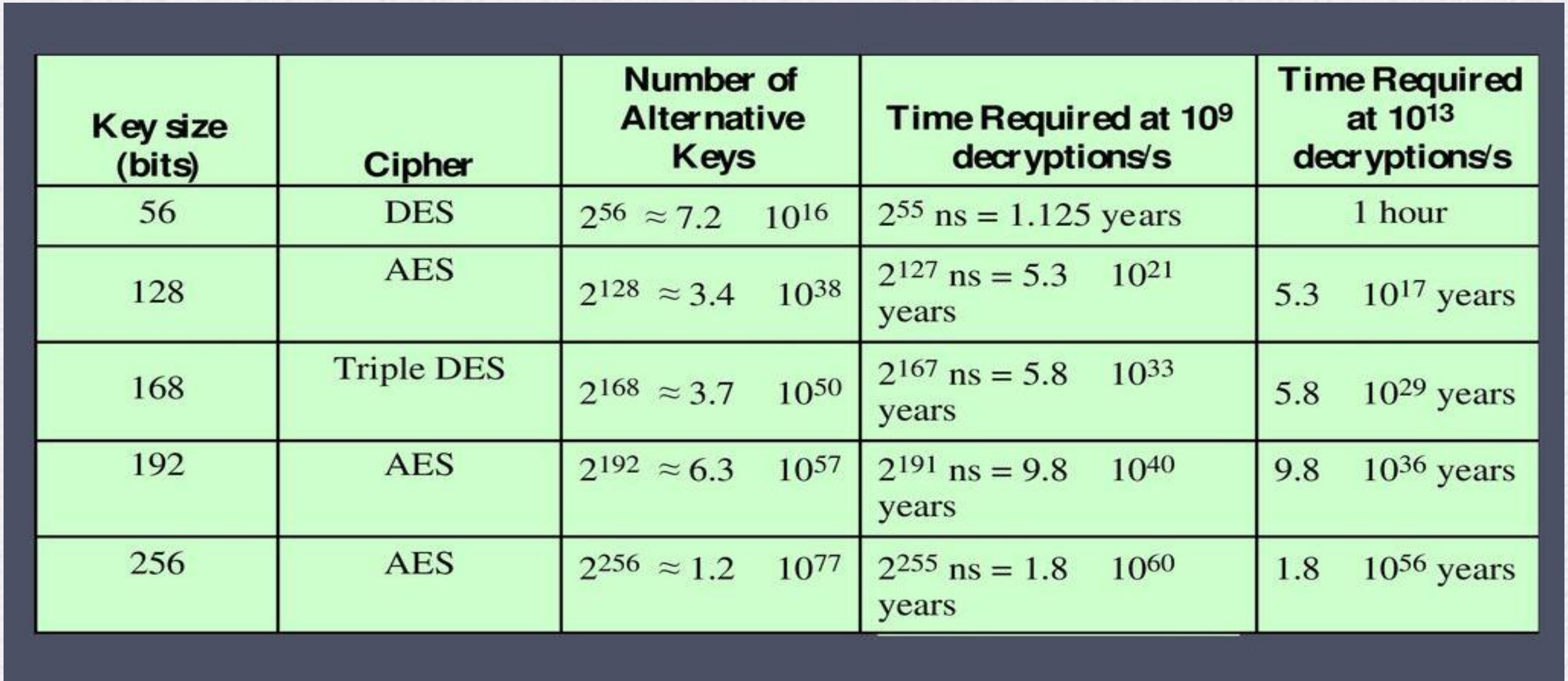
Fast avalanche effect

- Example
  - Altered plaintext = 12468aceeca86420
- δ: number of different bits



Round		δ
	02468aceeca86420 12468aceeca86420	1
1	3cf03c0fbad22845 3cf03c0fbad32845	1
2	bad2284599e9b723 bad3284539a9b7a3	5
3	99e9b7230bae3b9e 39a9b7a3171cb8b3	18
4	0bae3b9e42415649 171cb8b3ccaca55e	34
5	4241564918b3fa41 ccaca55ed16c3653	37
6	18b3fa419616fe23 d16c3653cf402c68	33
7	9616fe2367117cf2 cf402c682b2cefbc	32
8	67117cf2c11bfc09 2b2cefbc99f91153	33
9	c11bfc09887fbc6c 99f911532eed7d94	32
10	887fbc6c600f7e8b 2eed7d94d0f23094	34
11	600f7e8bf596506e d0f23094455da9c4	37
12	f596506e738538b8 455da9c47f6e3cf3	31
13	738538b8c6a62c4e 7f6e3cf34bc1a8d9	29
14	c6a62c4e56b0bd75 4bc1a8d91e07d409	33
15	56b0bd7575e8fd8f 1e07d4091ce2e6dc	31
16	75e8fd8f25896490 1ce2e6dc365e5f59	32
IP–1	da02ce3a89ecac3b 057cde97d7683f2a	32

Exhaustive Key Search



Key size (bits)	Cipher	Number of Alternative Keys	Time Required at 10^9 decryptions/s	Time Required at 10^{13} decryptions/s
56	DES	$2^{56} \approx 7.2 \quad 10^{16}$	2^{55} ns = 1.125 years	1 hour
128	AES	$2^{128} \approx 3.4 \quad 10^{38}$	2^{127} ns = 5.3 10^{21} years	5.3 10^{17} years
168	Triple DES	$2^{168} \approx 3.7 \quad 10^{50}$	2^{167} ns = 5.8 10^{33} years	5.8 10^{29} years
192	AES	$2^{192} \approx 6.3 \quad 10^{57}$	2^{191} ns = 9.8 10^{40} years	9.8 10^{36} years
256	AES	$2^{256} \approx 1.2 \quad 10^{77}$	2^{255} ns = 1.8 10^{60} years	1.8 10^{56} years

Average Time Required for Exhaustive Key Search

S-box security

- Strict avalanche criterion (SAC)
  - When an input bit i is inverted, an output bit j of an S-box changes with probability 0.5

- Bit independence criterion (BIC)
  - When an input bit i is inverted, output bits j and k change independently, for all i , j , and k

S_5		Middle 4 bits of input															
		0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
Outer bits	00	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1111	1101	0000	1110	1001
	01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	1000	0110
	10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000	1110
	11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101	0011

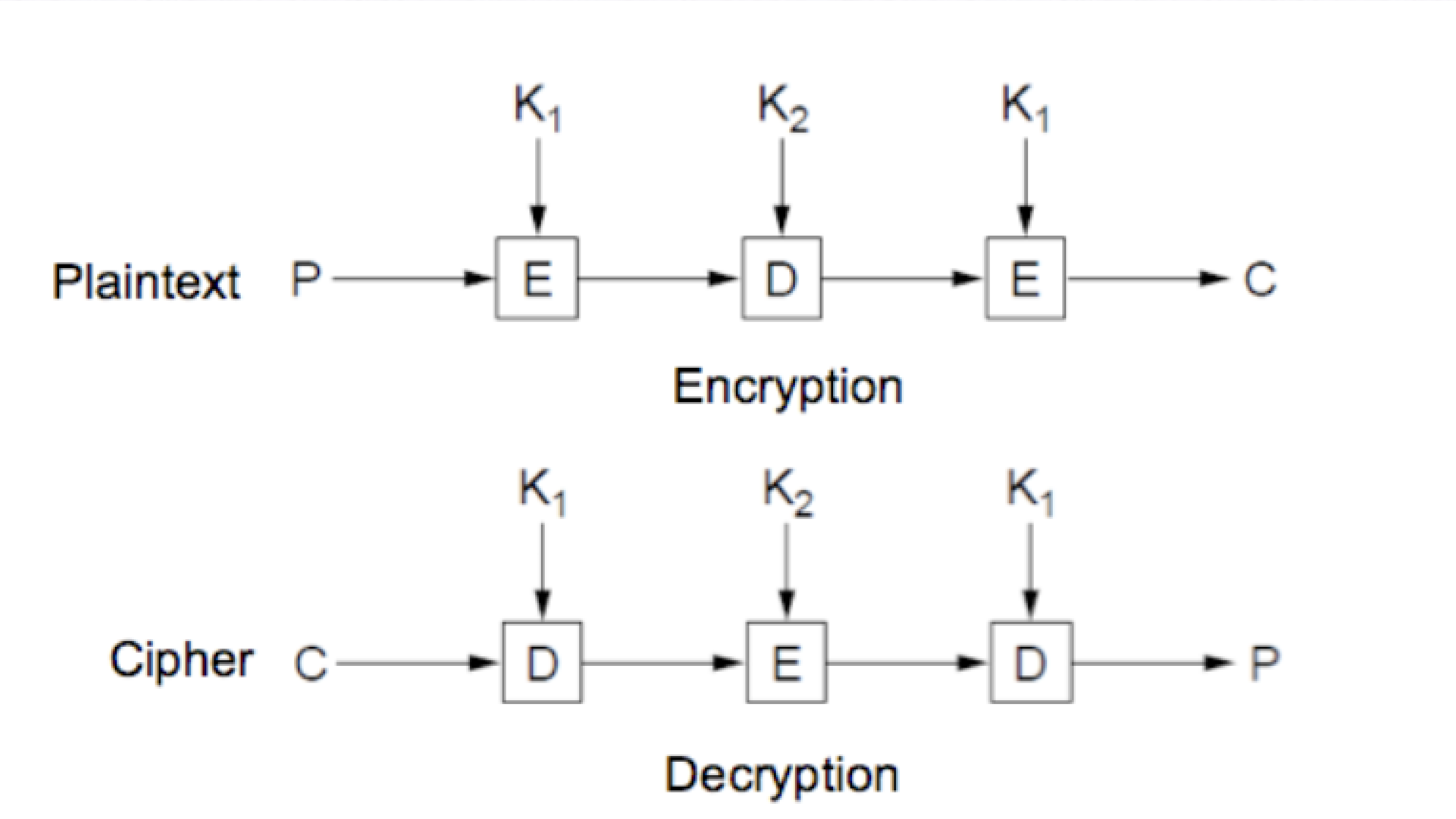
Key Schedule

- One subkey is generated in each round
- It is difficult to deduce individual subkeys and the main key from a subkey
- Meet the SAC and BIC conditions

DES: weakness

- Key complementation: C = DES(P, K) ➔ $\bar{C} = DES(\bar{P}, \bar{K})$
- Differential cryptanalysis
  - Δ_x=P1⊕P2 and Δ_y=S(P_1)⊕S(P_2) have some relation
  - Chosen plaintext attack: need 2^{47} pair of plaintexts and 2^{37} DES calls
  - Significantly less than 2^{55} exhaustive key search.
- 16 rounds are the boundary for current known attacks
- 56-bit is too small in current technology
  - Quantum computers reduces the key search to 2^{28}
  - Should use 3DES with 112-bit keys at least

2-Key Triple DES



Attack on 3-key Triple-DES

Given (P, C)

- Naive attack
  - For all K_1, K_2, K_3, if $E(D(E(P, K_1), K_2), K_3)=C$, then output (K_1, K_2, K_3)
  - Time: $O(2^{56x3})$
- Meet-in-the-middle attack
  - For all K_1, K_2, store $D(E(P, K_1), K_2)$ in Table I
  - For all K_3, store $D(C, K_3)$ in Table II
  - Match Tables I & II and output matched K_1, K_2, K_3
  - Time: $O(2^{56x2}+2^{56}+\text{matched time})$

Summary

- Traditional Block Cipher Structure
  - Stream ciphers
  - Block ciphers
  - Motivation for the Feistel cipher structure
  - Feistel cipher
- The Data Encryption Standard (DES)
  - Encryption
  - Decryption
  - Avalanche effect
- The strength of DES
  - Use of 56-bit keys
  - Nature of the DES algorithm
  - Timing attacks
- Block cipher design principles
  - Number of rounds
  - Design of function F
  - Key schedule algorithm