Modern Symmetric Key Ciphers

Part II: Fiestel Ciphers and the DES

Priyank Kalla
Professor
Electrical & Computer Engineering

Product Ciphers

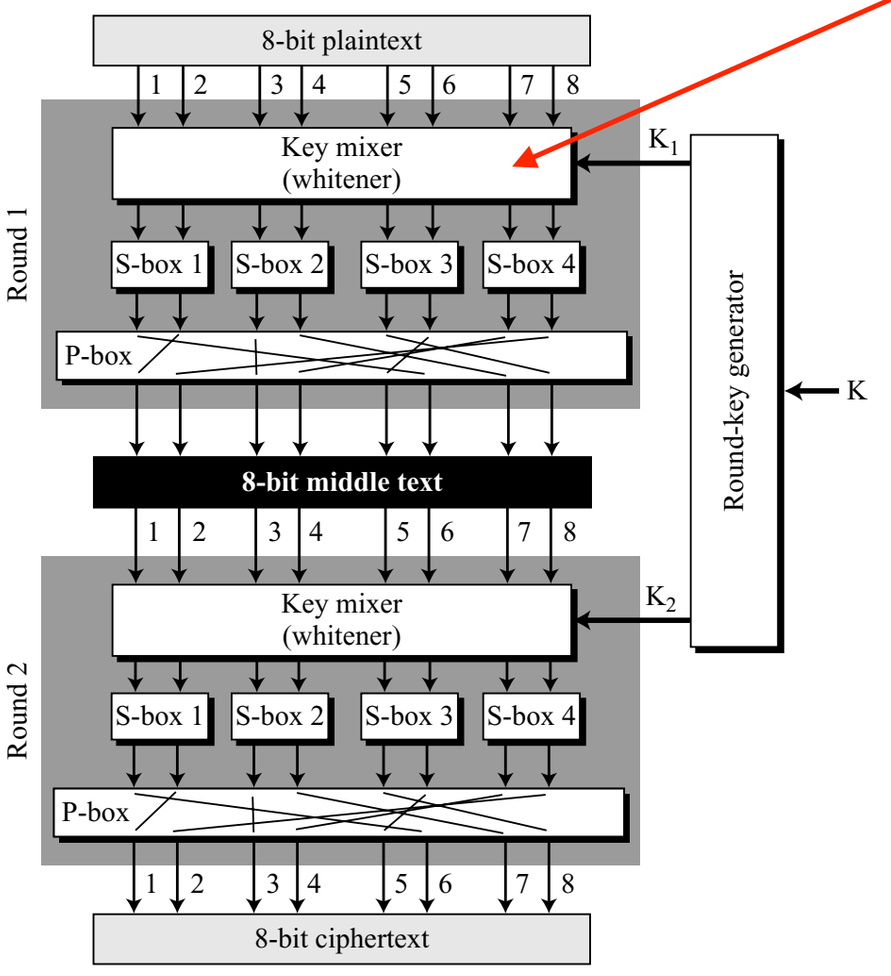
- Product Cipher: Combines S-Boxes, P-Boxes and Mixers, and may use multiple rounds for encipherment

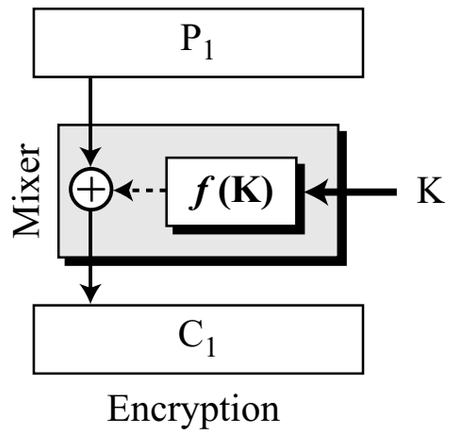
- Two types of Product Ciphers
  - Feistel Cipher: Includes invertible and noninvertible components
  - DES = Feistel Cipher (uses non-invertible mixers and compression P-Boxes)
  - Non-Feistel Cipher: Includes only invertible components
  - AES = Non-Feistel Cipher

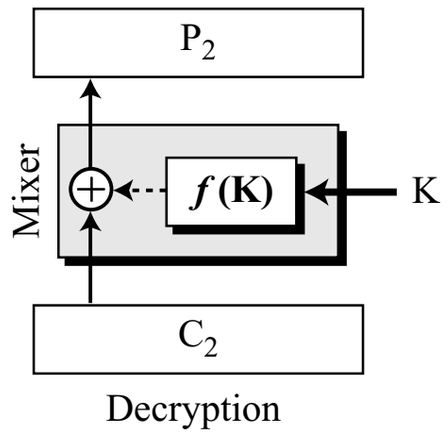
Example Product Cipher

Key Mixer: P[7:0] XOR K1[7:0]

A product cipher made of two rounds







- Mixer: Use a non-invertible function $f(K)$: can be linear or polynomial in $\mathbb{F}_{2^k}$
- But the Mixer is "self-invertible":

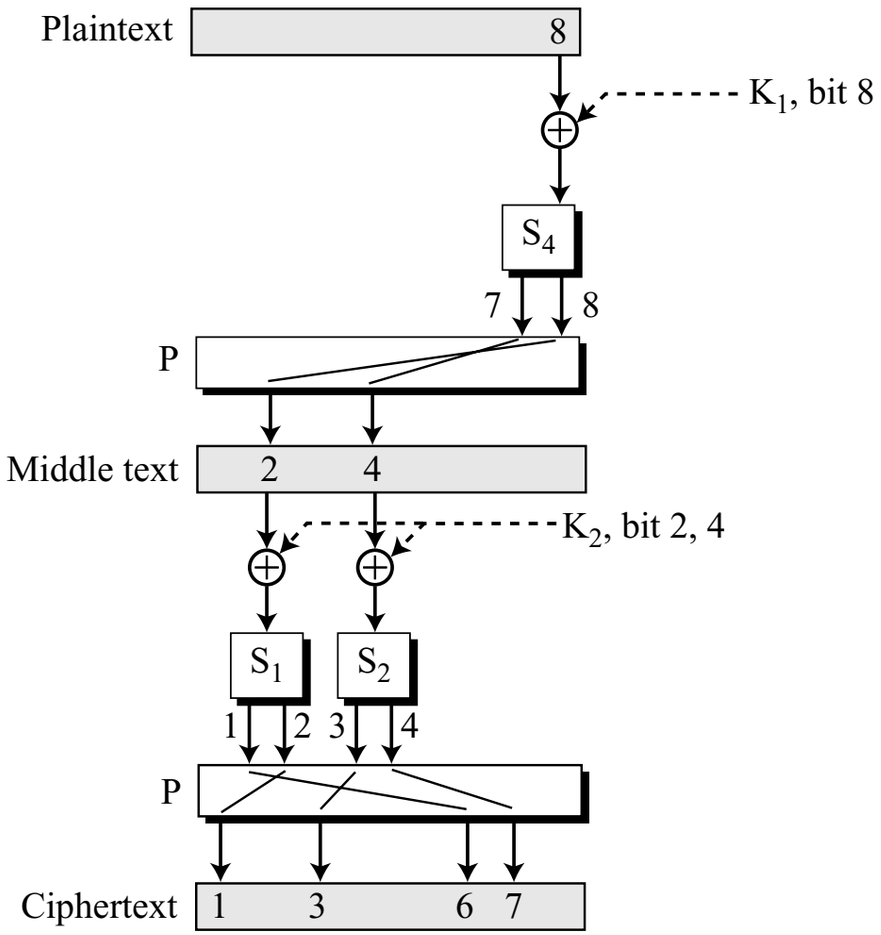
$$C = P \oplus f(K)$$

- $P = C \oplus f(K)$

Encryption: $C_1 = P_1 \oplus f(K)$

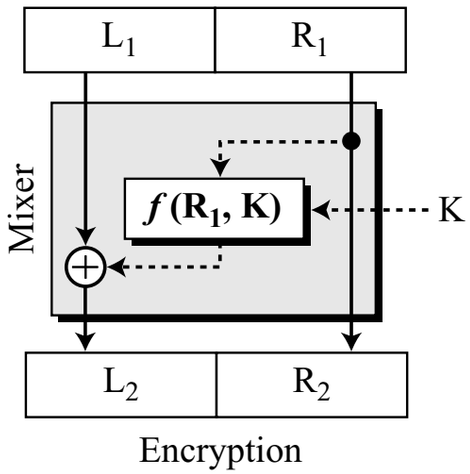
Decryption: $P_2 = C_2 \oplus f(K) = C_1 \oplus f(K) = P_1 \oplus f(K) \oplus f(K) = P_1 \oplus (00\ldots0) = P_1$

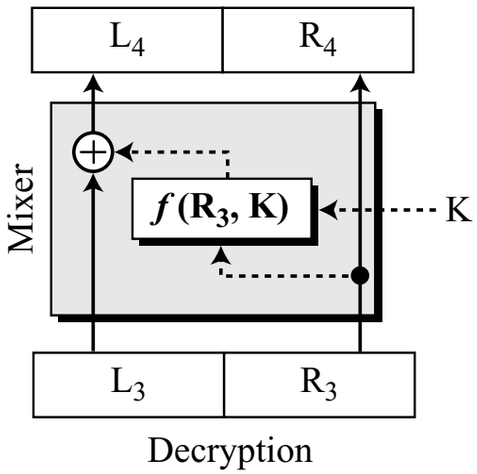
Example of Diffusion and Confusion

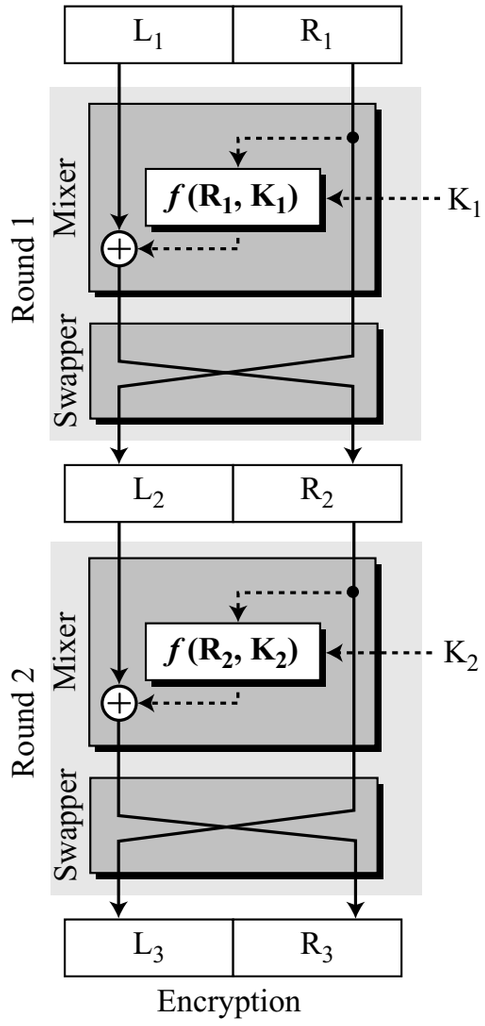


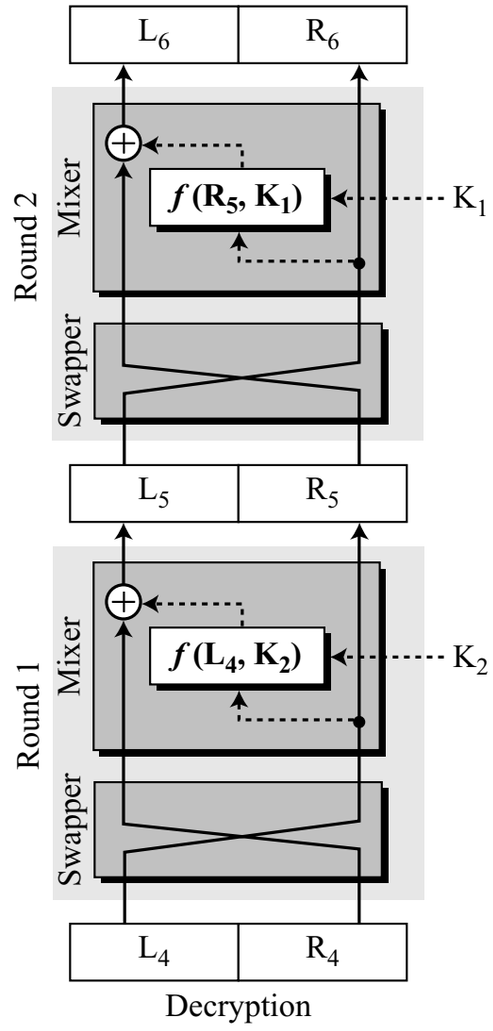
- Diffusion:
  - Bit-8 in P has affected bits 1, 3, 6,7 in C
  - Similarly, each bit in C is affected by several bits in P
- Confusion:
  - Bits 1, 3, 6, 7 in C affected by bit 8 in K_1 and bits 2, 4 in K_2

An Example Product Cipher: Feistel Cipher





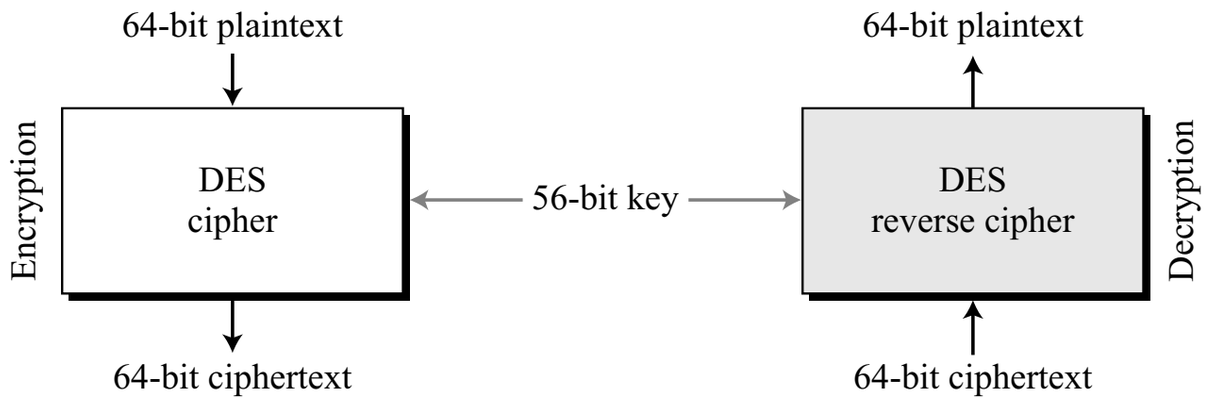




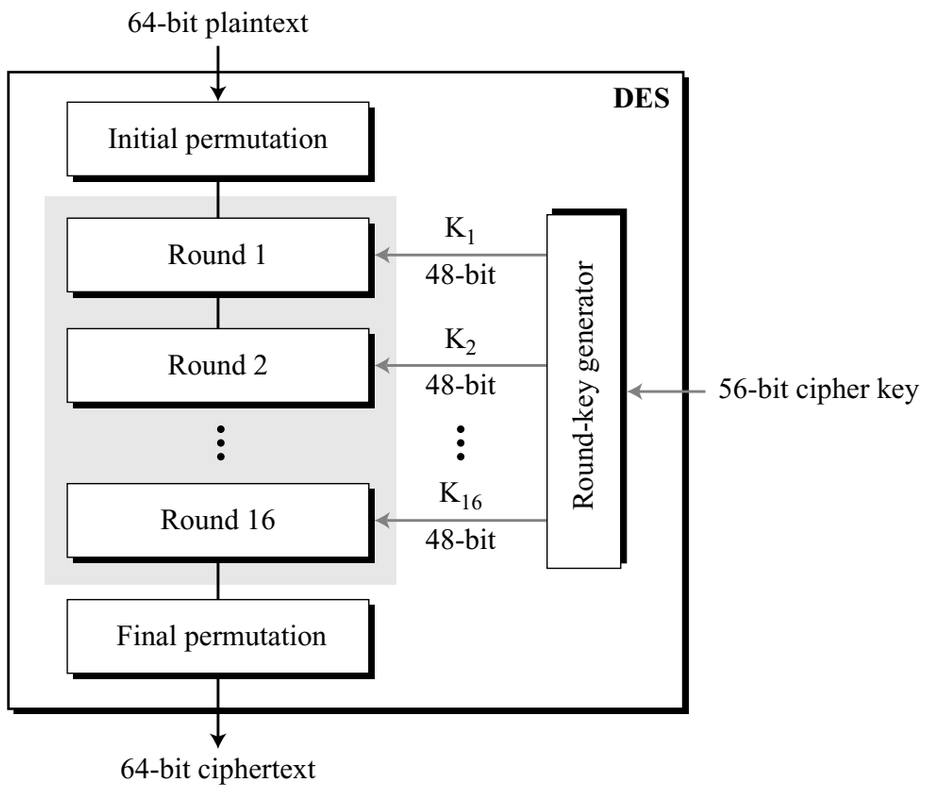
- $L_3 = L_2, R_3 = R_2$

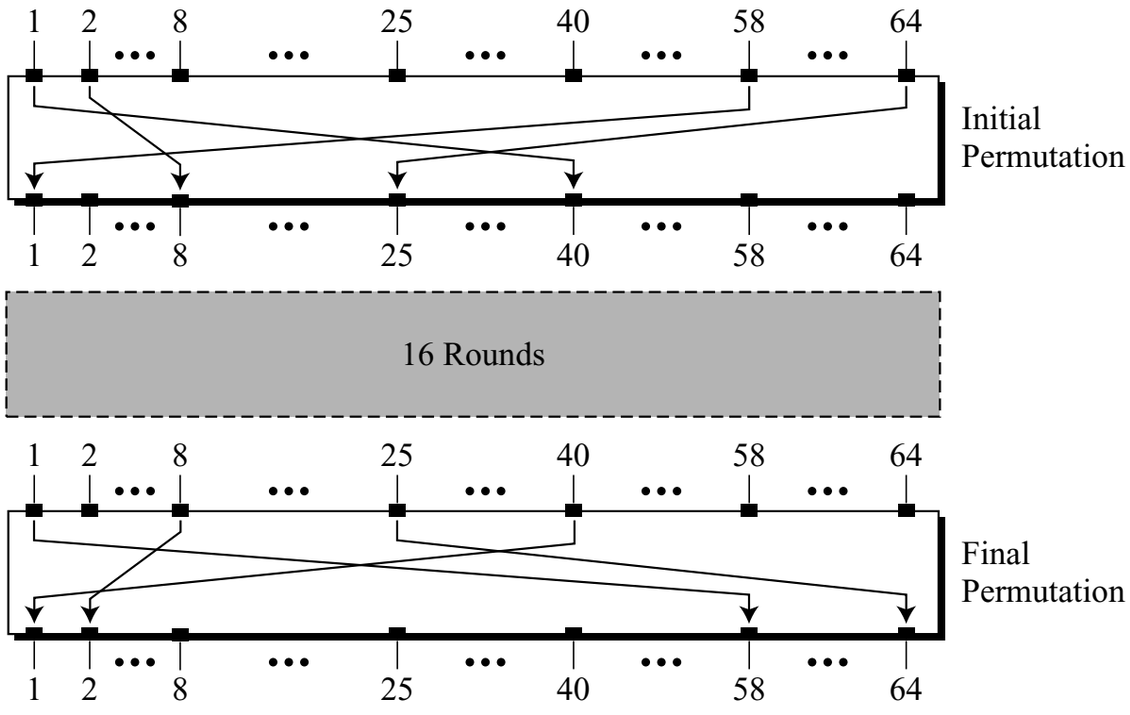
Data Encryption Standard (DES)

- DES was published by NIST ~1977, original proposal by IBM
- 64-bit block cipher (64-bit data block), and 56-bit key
- Proof (by IBM?) that the 56-bit partial size key cipher is not a subgroup of the full size key



High-Level Structure of DES

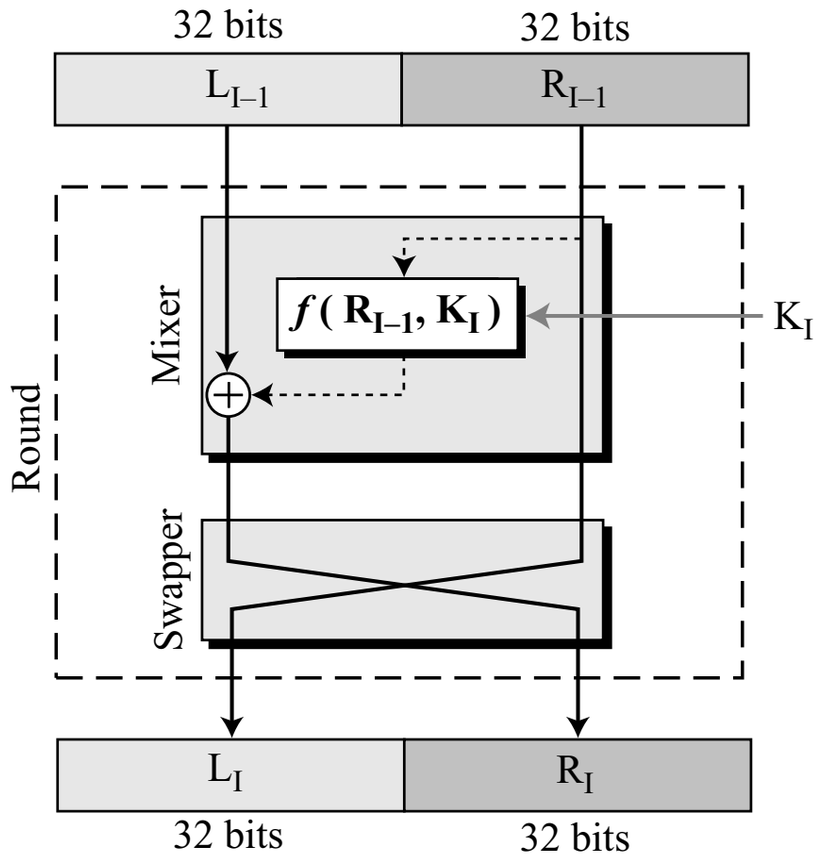




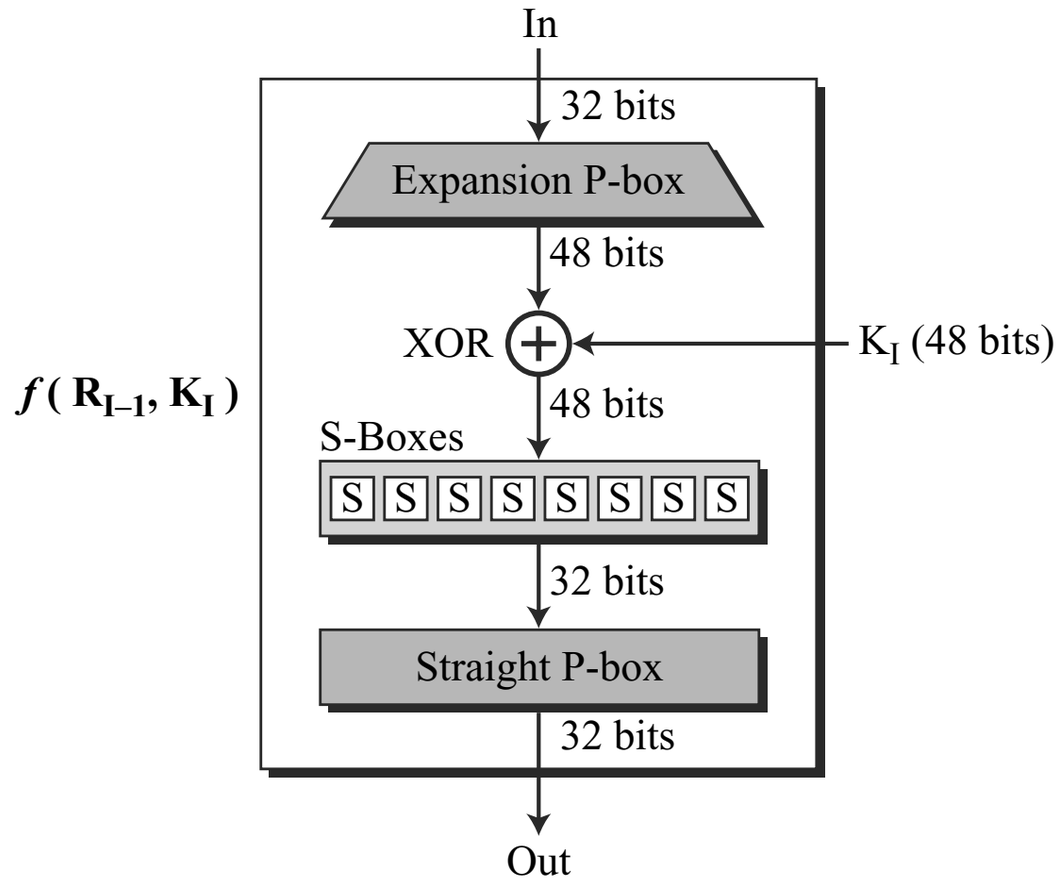
Initial Permutation								*Final Permutation*							
58	50	42	34	26	18	10	02	40	08	48	16	56	24	64	32
60	52	44	36	28	20	12	04	39	07	47	15	55	23	63	31
62	54	46	38	30	22	14	06	38	06	46	14	54	22	62	30
64	56	48	40	32	24	16	08	37	05	45	13	53	21	61	29
57	49	41	33	25	17	09	01	36	04	44	12	52	20	60	28
59	51	43	35	27	19	11	03	35	03	43	11	51	19	59	27
61	53	45	37	29	21	13	05	34	02	42	10	50	18	58	26
63	55	47	39	31	23	15	07	33	01	41	09	49	17	57	25

- Output bit 1 = input bit 58, and so on…
- There's been debate on the security significance of initial and final permutations — don't seem to add to security
- Each DES Round = Feistel Cipher
- 16 DES Rounds

DES Round & Mixer Function



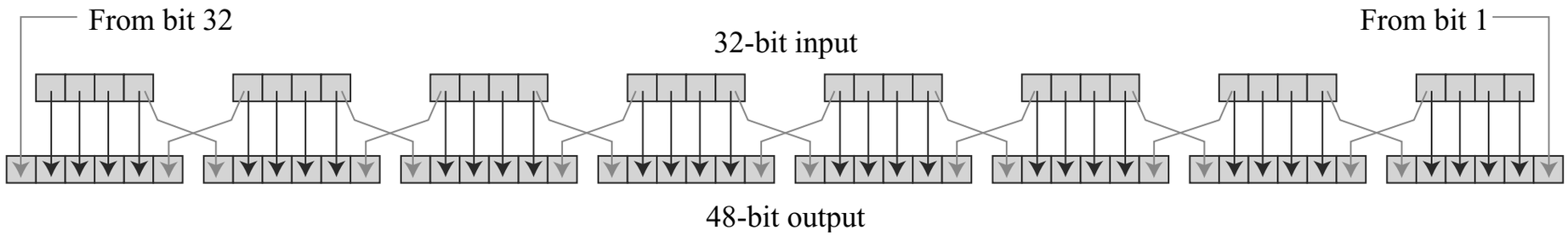
A Round in DES



The Mixer Function in DES

- The Expansion P-Box has a specified table (routing)
- Each of the 8 S-boxes has a separate 6-bit → 4-bit table
- The last P-box is also a permutation table (routing)

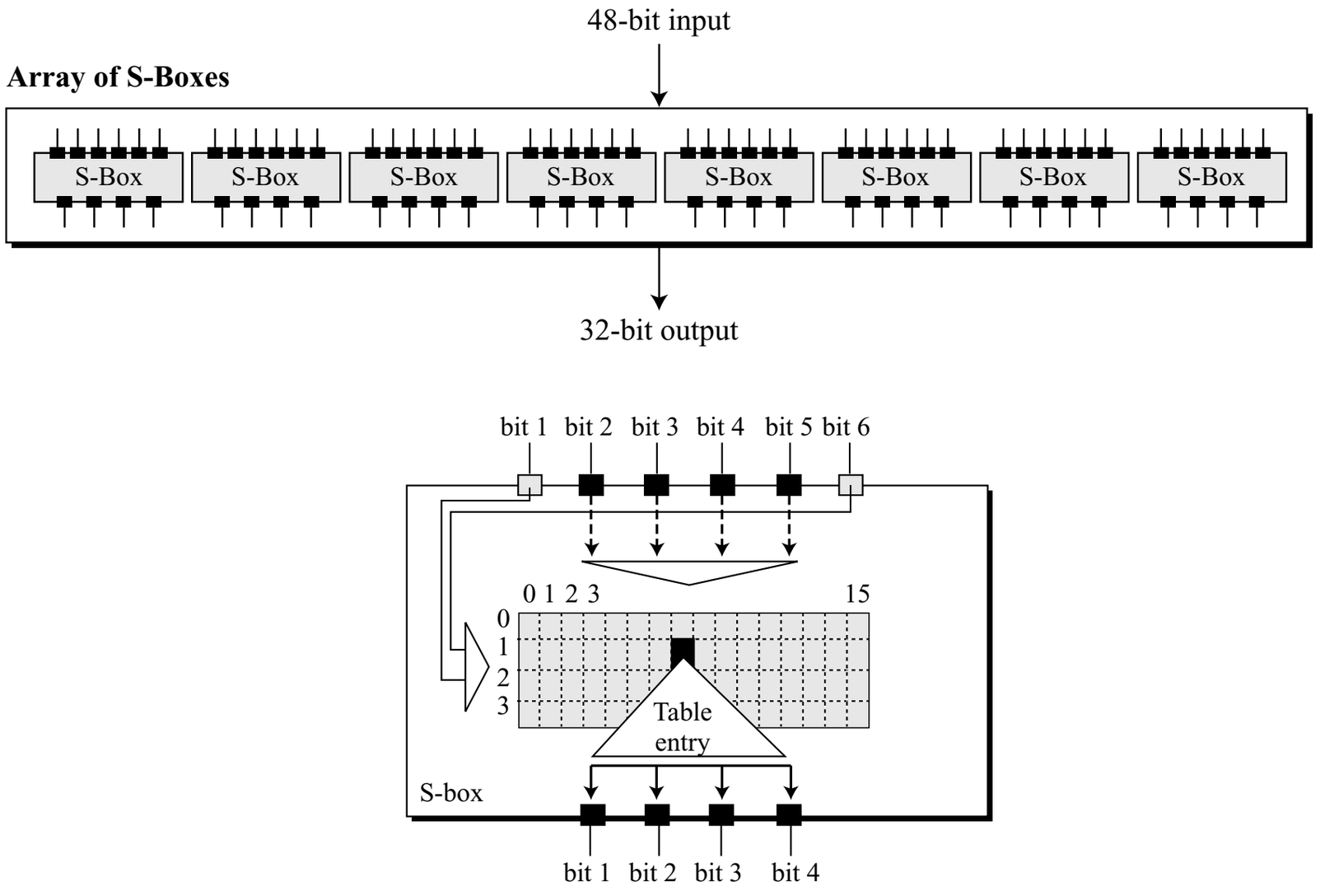
Details of DES Function: Expansion P-Box



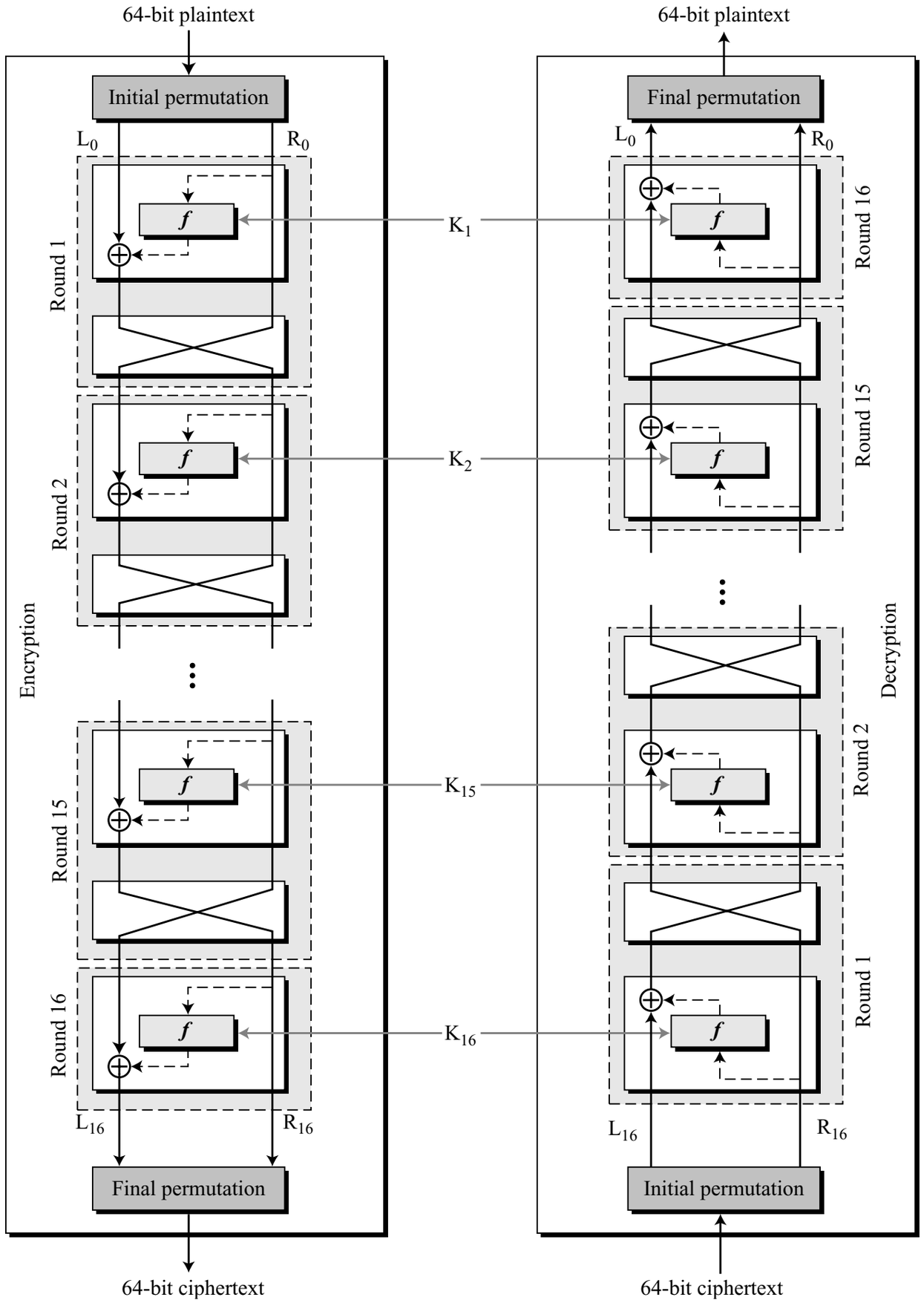
32	01	02	03	04	05
04	05	06	07	08	09
08	09	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	01

- The Expansion Permutation P-Box of the DES function
- It’s just wiring…

Details of DES Function: S-Boxes



- Each S-Box is a different polynomial function: $\mathbb{F}_{2^6} \rightarrow \mathbb{F}_{2^4}$
- Or as a truth table of a 6-input, 4 output Boolean function: $\mathbb{B}^6 \rightarrow \mathbb{B}^4$
- Each of the 8 truth tables are different — are provided in the DES Spec



- The Final DES Cipher and Reverse Cipher
- Round 16 does not have a swap

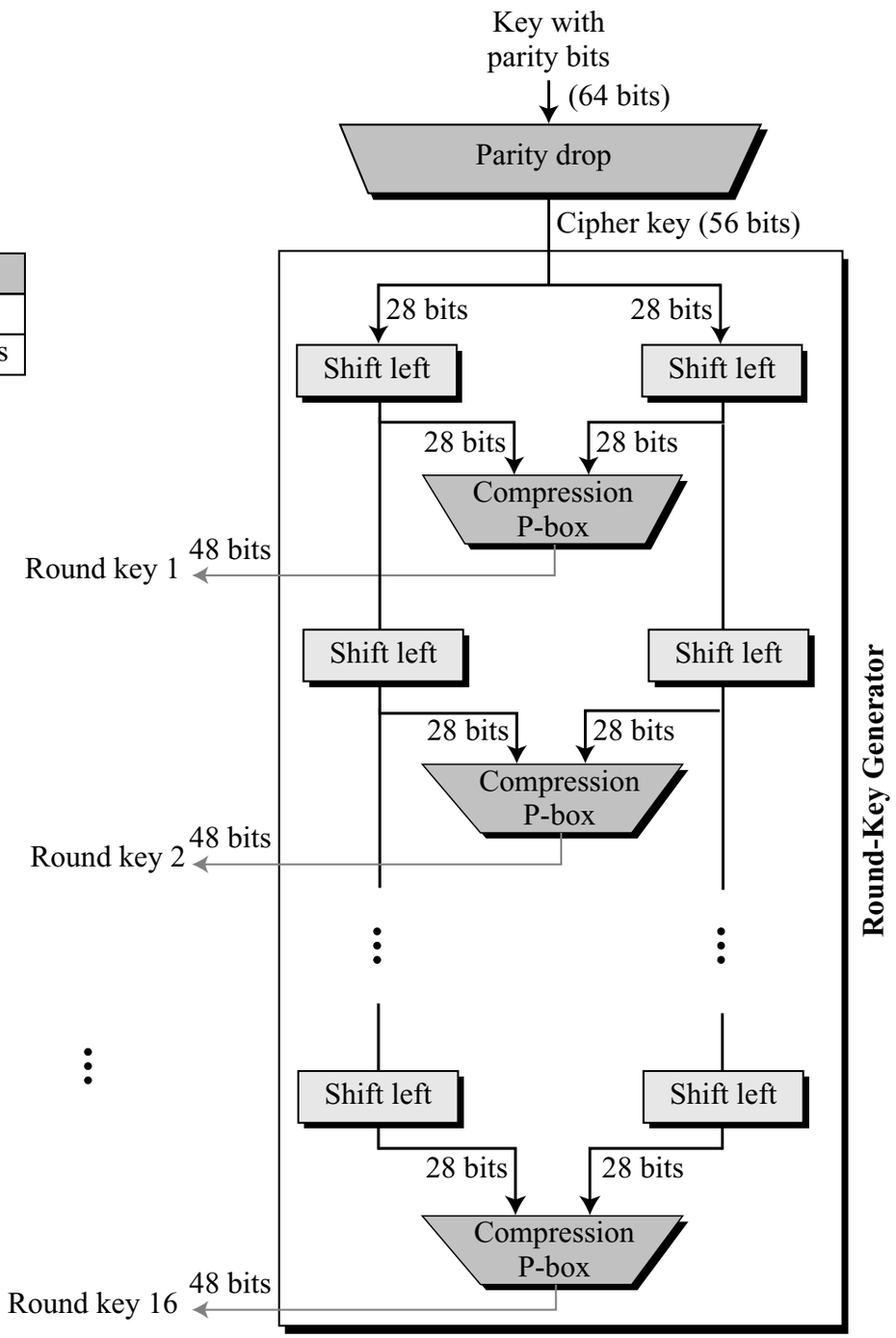
Key Generation for Each Round

- Key Generator takes a 56-bit Key (K)
- Keys are usually provided with 8 parity bits: Adds 8 parity bits to get 64-bit key after every 7 key bits
- These parity bits are dropped before the real key generation
- Generates 16 48-bit Keys (K1, …, K16) from K

Key Generation View

Shifting

Rounds	Shift
1, 2, 9, 16	one bit
Others	two bits



- Shifts = circular shifts
- All compression P-Box Truth Tables are specified
- Verilog Code for DES is available on the internet
- Never been a good HW problem :)
- I have a DES.blif logic circuit (which can transformed into Verilog)

Other Aspects of DES

- IBM released the design rationale for choices of DES blocks ~1994, as well as their effects
- **Avalanche** effects: Small change in input, significant change in the output:

Plaintext: 0000000000000000 Key: 22234512987ABB23
Ciphertext: 4789FD476E82A5F1

Plaintext: 0000000000000001 Key: 22234512987ABB23
Ciphertext: 0A4ED5C15A63FEA3

- **Completeness effect:** Each bit in C depends on various bits of P
- Various publications have also found weaknesses in DES
- Significant criticism came about Key size & Weak Keys

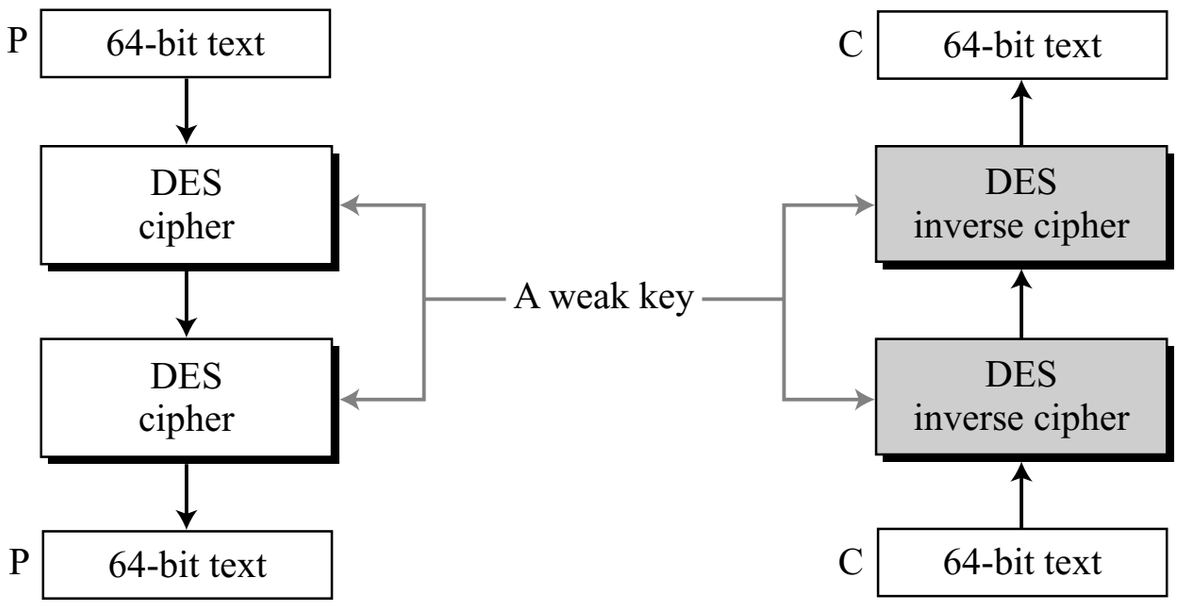
Weakness in DES w.r.t. Keys

- Key size is considered to be small
- Brute force attack: in 1977, RSA Labs threw up a key-challenge
- Networked computers reverse engineered the key in 120 days, and a super computer broke the cipher in 112 hours in 1998
- Weak Keys: 4 out of 2^{56} keys are weak
- All 0 key: Each round key is the same
  - 1st Key: All round keys are 0s
  - 2nd key: Same pattern as the cipher Key
  - Half 0s and half 1s

Actual key (56 bits)
0000000 0000000
0000000 FFFFFFF
FFFFFFF 0000000
FFFFFFF FFFFFFF

Weak Key Issues

Double encryption and decryption with a weak key



- Each weak key = inverse of itself
- $E_k(E_k(P)) = P$
- Avoid weak keys, of course

Key: 0x0101010101010101
Plaintext: *0x1234567887654321* Ciphertext: 0x814FE938589154F7

Key: 0x0101010101010101
Plaintext: 0x814FE938589154F7 Ciphertext: *0x1234567887654321*

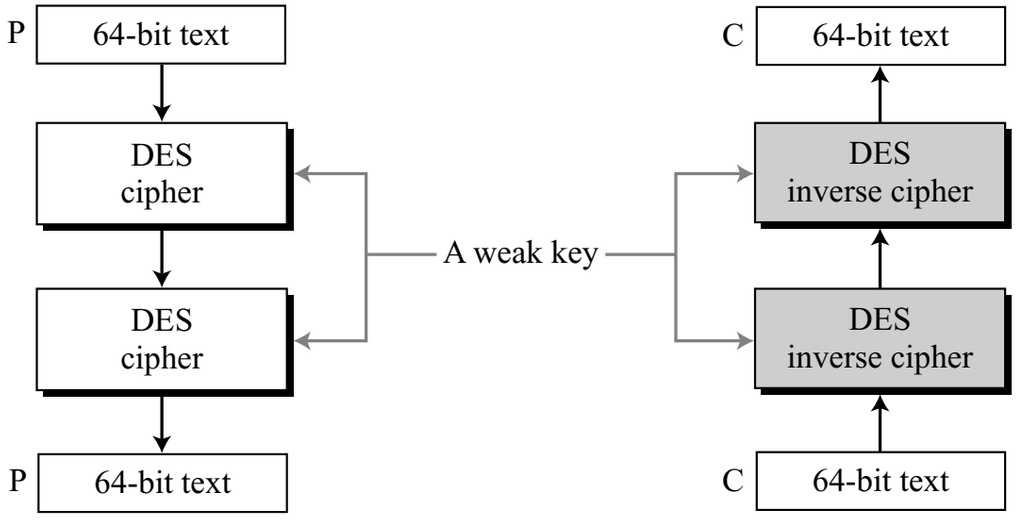
Semi-Weak Key

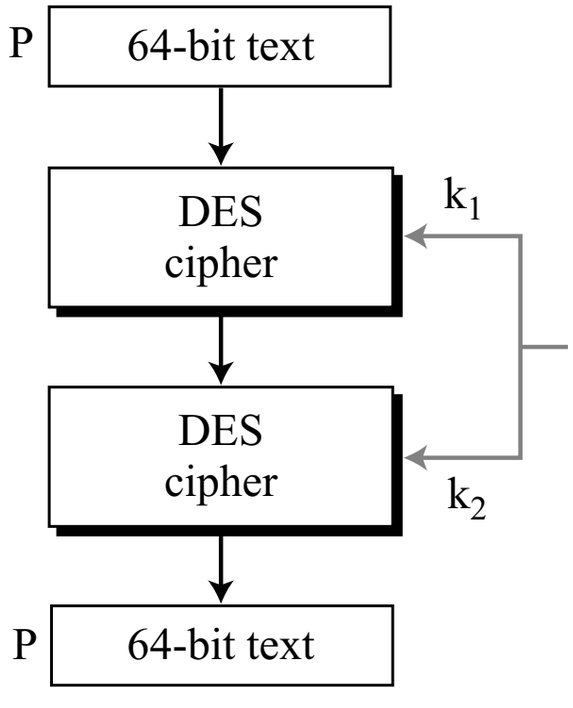
First key in the pair	*Second key in the pair*
01FE 01FE 01FE 01FE	FE01 FE01 FE01 FE01
1FE0 1FE0 0EF1 0EF1	E01F E01F F10E F10E
01E0 01E1 01F1 01F1	E001 E001 F101 F101
1FFE 1FFE 0EFE 0EFE	FE1F FE1F FE0E FE0E
011F 011F 010E 010E	1F01 1F01 0E01 0E01
E0FE E0FE F1FE F1FE	FEE0 FEE0 FEF1 FEF1

Round key 1	9153E54319BD	6EAC1ABCE642
Round key 2	6EAC1ABCE642	9153E54319BD
Round key 3	6EAC1ABCE642	9153E54319BD
Round key 4	6EAC1ABCE642	9153E54319BD
Round key 5	6EAC1ABCE642	9153E54319BD
Round key 6	6EAC1ABCE642	9153E54319BD
Round key 7	6EAC1ABCE642	9153E54319BD
Round key 8	6EAC1ABCE642	9153E54319BD
Round key 9	9153E54319BD	6EAC1ABCE642
Round key 10	9153E54319BD	6EAC1ABCE642
Round key 11	9153E54319BD	6EAC1ABCE642
Round key 12	9153E54319BD	6EAC1ABCE642
Round key 13	9153E54319BD	6EAC1ABCE642
Round key 14	9153E54319BD	6EAC1ABCE642
Round key 15	9153E54319BD	6EAC1ABCE642
Round key 16	6EAC1ABCE642	9153E54319BD

- Encrypt using the first key-pair

Double encryption and decryption with a weak key





$$E_{k1}(E_{k2}(P)) = P$$

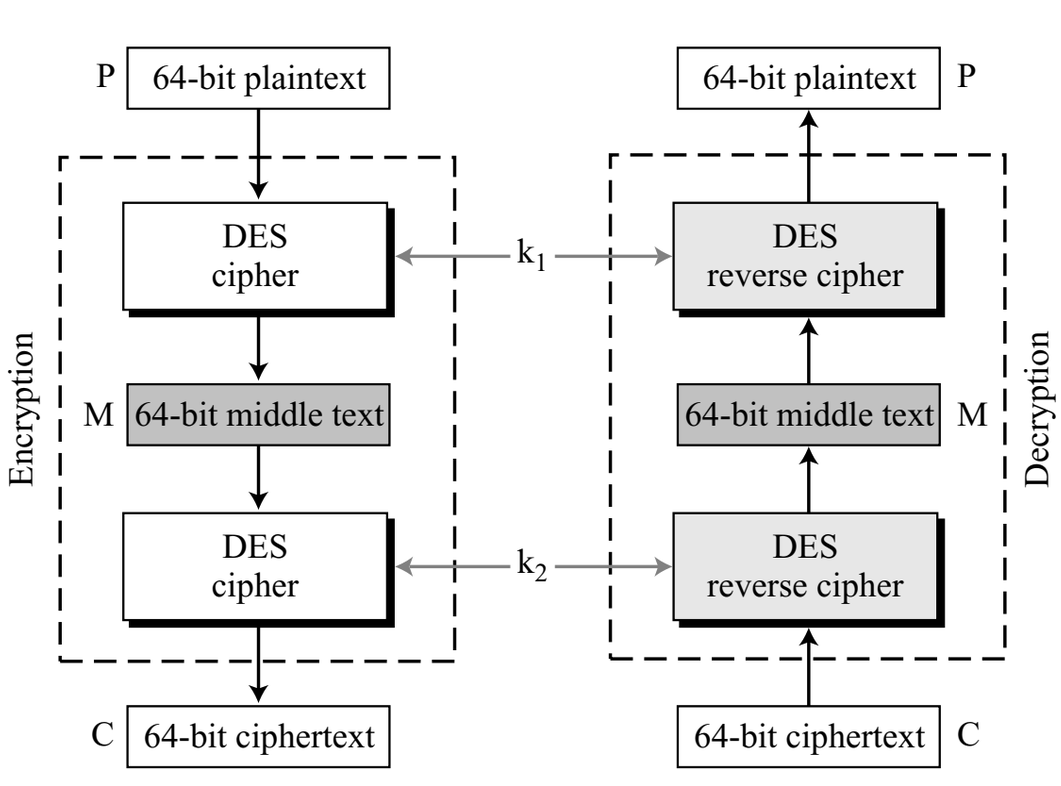
Key Complements

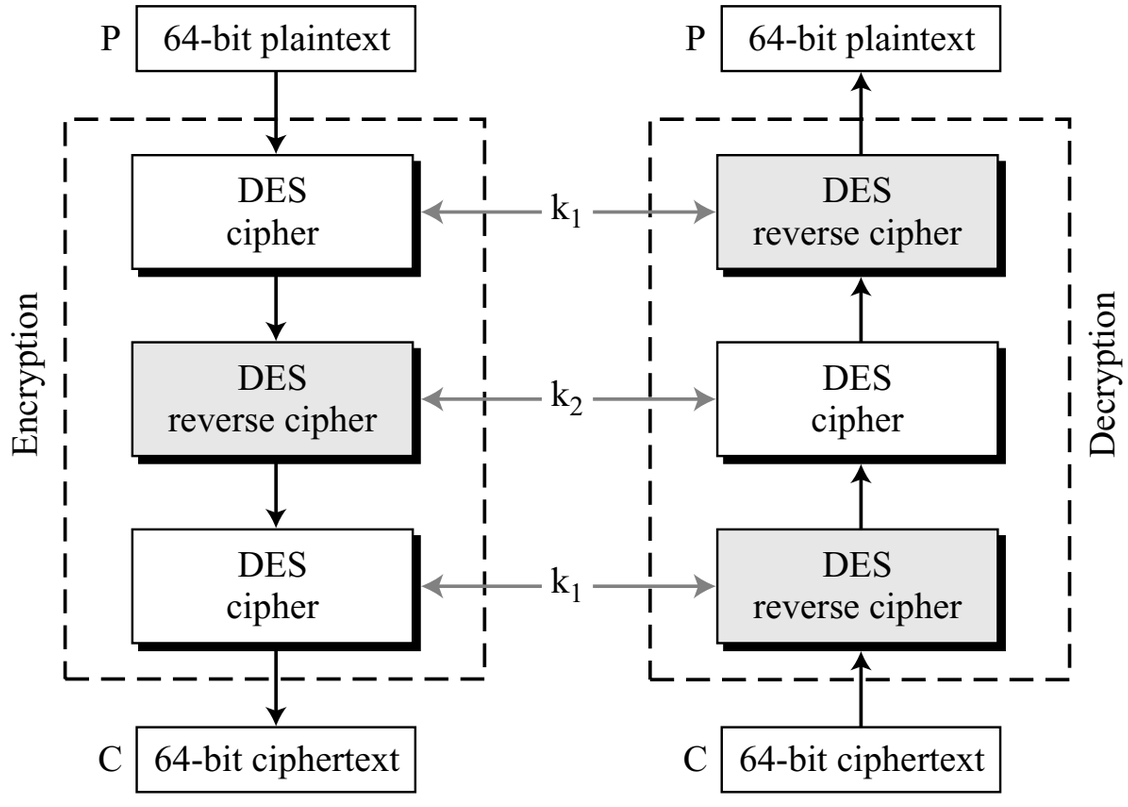
- 2^{56} keys: Actually, only 2^{55} Keys; others are bit-vector complements
- $$C = E(K, P) \quad \rightarrow \quad \overline{C} = E(\overline{K}, \overline{P})$$
- Brute-force or known-plaintext attack: 2^{55} keys

	Original	*Complement*
Key	`1234123412341234`	`EDCBEDCBEDCBEDCB`
Plaintext	`12345678ABCDEF12`	`EDCBA987543210ED`
Ciphertext	`E112BE1DEFC7A367`	`1EED41E210385C98`

Multiple DES

- DES is not known to be a permutation group
- Double DES with Two Keys: Was used in the Banking sector
- Tripple DES with 2 or 3 keys: Used in PGP (secure emails)
  - K1 = K2 = K3: compatibility with single DES

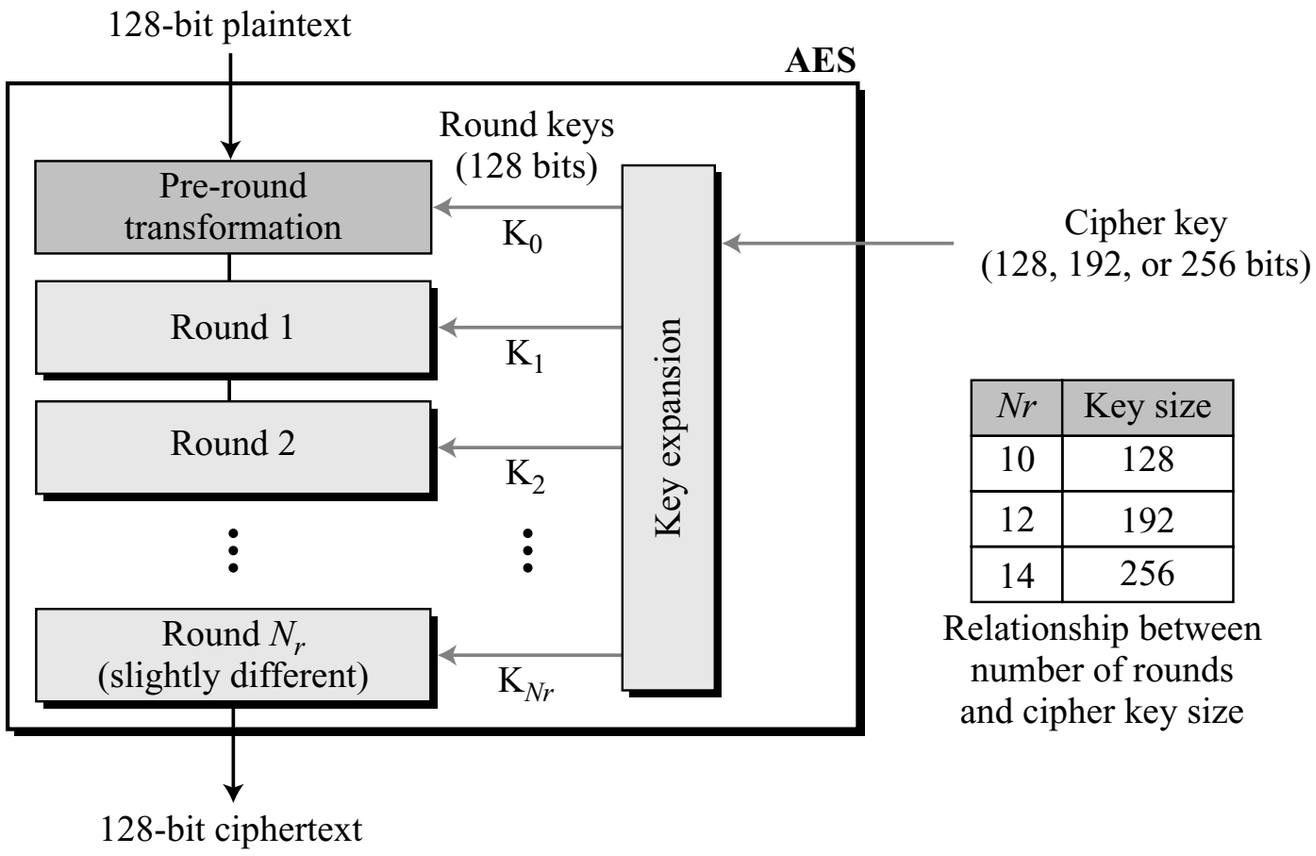




Will study Differential and Linear Cryptanalysis after AES

AES

- NIST Standard ~2001
- Based on Rijndael Proposal: J. Daemen & V. Rijment
- 128-bit Block Cipher, and 128-bit internal round keys
- Number of round keys: $N_r + 1$

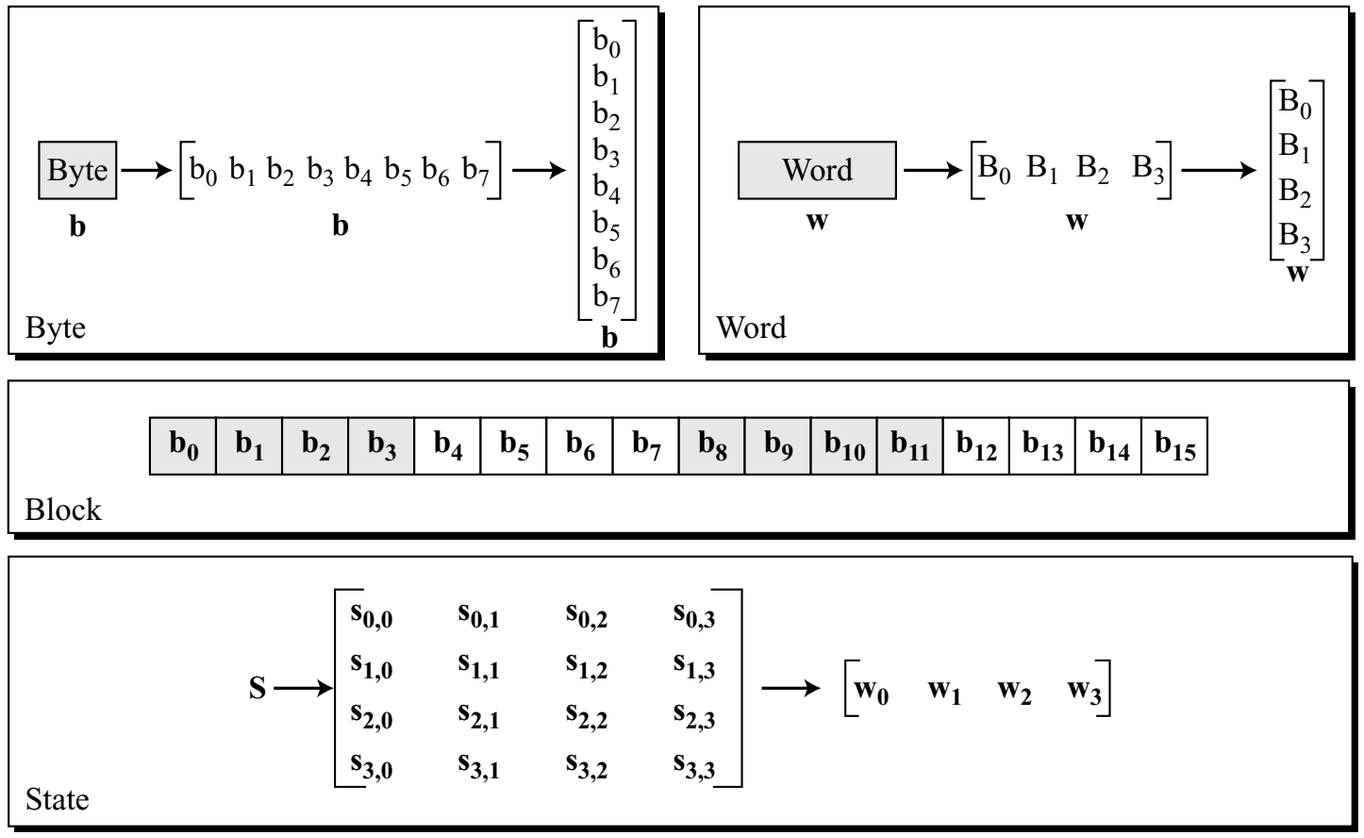


Nr	Key size
10	128
12	192
14	256

Relationship between number of rounds and cipher key size

Data Units in AES

- Bits, Byte, Word (32 bits), Block (128 bit), and State
- State = Block, but inside the stages of AES, it is called a State; operations are performed as matrices



Blocks and States in Matrices

Block-to-state and state-to-block transformation