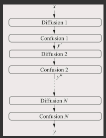


all block ciphers ← product cipher = Conf + Diff = strong

Data Encryption Standard (DES).

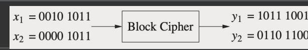
→ There are 2 primitive operations w/ which strong encryption algorithms can be built

→ Confusion: operation where the relationship between key & ciphertext is obscured via substitution

→ Diffusion: operation where influence of one plaintext symbol spread over many ciphertext symbols to hide statistical properties of plaintext

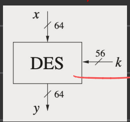
DES uses bit permutation
AES uses MixColumn.

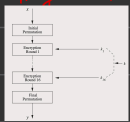
→ Modern Block Ciphers possess good diffusion properties → Cipher Level: Change one bit of plaintext → Change avg. of ciphertext → Ex:



→ DES: Symmetric cipher encrypting blocks of 64 bit length w/ a key length of 56 bits (Round-Based) → each block → 16 rounds performing identical op

each round, diff. subsets of the main key are used





→ Feistel Network: used for strong ciphers → allows encryption & decryption to have similar procedure

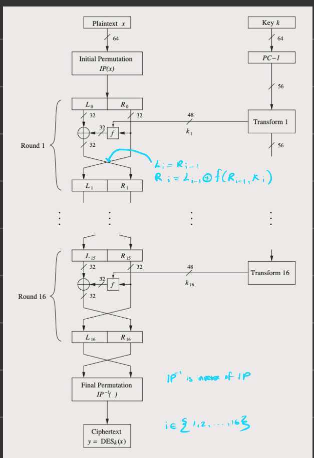
* Only encrypts 1/2 of input bits each round (LEFT) where right side is copied → Decryption requires reversed key schedule.

→ f: pseudorandom generator w/ R_{i-1} & k_i → used to encrypt L_{i-1} w/ XOR   f not predictable ⇒ strong

↳ includes confusion & diffusion

→ Feistel Network bijectively maps 64 bit block → 64 bit output for some arbitrary f ≠ f (in DES, is surjective)

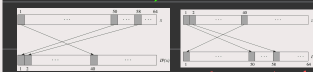
→ IP (Initial Permutation) & IP^{-1} (Final Permutation) are bitwise permutations



$L_i = R_{i-1}$
$R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$

IP^{-1} is inverse of IP

$i \in \{1, 2, \ldots, 16\}$



Bit 58 mapped to pos 1

Table 3.1 Initial permutation *IP*

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

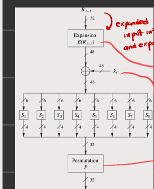
⟹

Table 3.2 Final permutation IP^{-1}

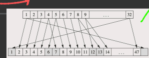
IP^{-1}							
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Ex: S box input
$b = (100101)_2$ ⇒ row $11_2 = 3$ (4th row)
⇒ column $0010_2 = 2$
∴ $S(b) = 8 = 1000_2$
4×2

→ In each round i, f takes R_{i-1} and k_i where output is XORed w/ L_{i-1}



expanded by partitioning input into 4 bit blocks and expanding each block to 6 bits



E					
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

exactly 16/32 = 1/2 bits appear twice after E but input bit is not repeated in the block its in

Expansion improves diffusion since some input bits influence 2 output locations.

→ S-Box: Map 6 bit input to 4 bit output (2^6 entries ≈ 4×16 matrix)   Each entry is 4-bit value

48-bit expanded result XORed w/ k_i ⇒ fed into 8 Substitution / S-boxes   all are unique

Core of DES providing confusion

MSB and LSB of each 6 bit input select row while inner 4 bits select column

$\mathbb{Z}_{15}$ of each entry table ≡ decimal notation of 4 bit value

→ S-boxes designed according to criteria:

1. Each S-box has six input bits and four output bits.
2. No single output bit should be too close to a linear combination of the input bits.
3. If the lowest and the highest bits of the input are fixed and the four middle bits are varied, each of the possible 4-bit output values must occur exactly once.
4. If two inputs to an S-box differ in exactly one bit, their outputs must differ in at least two bits.
5. If two inputs to an S-box differ in the two middle bits, their outputs must differ in at least two bits.
6. If two inputs to an S-box differ in their first two bits and are identical in their last two bits, the two outputs must be different.
7. For any nonzero 6-bit difference between inputs, no more than 8 of the 32 pairs of inputs exhibiting that difference may result in the same output difference.
8. A collision (zero output difference) at the 32-bit output of the eight S-boxes is only possible for three adjacent S-boxes.

→ S-boxes introduce non-linearity: $S(a) \oplus S(b) \neq S(a \oplus b)$ For DES, requires differential cryptoanalysis

Without them, attacker can express input & output as sys. of linear equations to solve for unknowns.

→ P introduces diffusion as 4 output bits of each S-box permuted s.t. they affect S-boxes in next round

↳ E + P ⇒ Diffusion w/ confusion caused by S-boxes

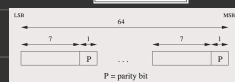
⇒ f = of every plaintext & key bit   Avalanche Effect

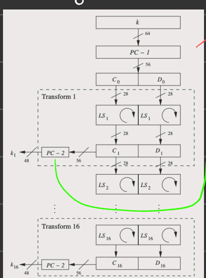
→ Key Schedule: Derives 16 round keys k_i, each of 48 bits, from 56 bit original key

64 bit key reduced to 56 bit by ignoring every 8th bit → PC−1:

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

↳ Resulting 56-bit key split in half ⇒ C_0 & D_0 cyclically shifted by 1 or 2 positions depending on round number
i = 1, 2, 9, 16 ⇒ shifted left by 1 bit
otherwise ⇒ shifted left 2 bits

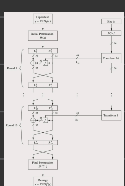




Total # of Rotation Pos = 4·1 + 12·2 = 28 ⇒ $C_0 = C_{16}$ ∧ $D_0 = D_{16}$ → useful for Decryption Key Schedule

To derive k_i, 2 halves C_i & D_i permuted bitwise via PC−2 which permutes 56 bits from C_i & D_i & ignoring 8 bits

→ Advantage of DES: Encryption uses same f as Decryption → Property of Feistel Ciphers → Key schedule reversed



We know $C_0 = C_{16}$ ∧ $D_0 = D_{16}$ ⇒ k_{16} derived from PC−1 $k_1, \ldots, k_{16}$ ⇒ $k_{16}, \ldots, k_1$

$k_{16} = PC\text{-}2(C_{16}, D_{16})$
$= PC\text{-}2(C_0, D_0)$
$= PC\text{-}2(PC\text{-}1(k))$

$k_{15} = PC\text{-}2(C_{15}, D_{15})$
$= PC\text{-}2(RS_2(C_{16}), RS_2(D_{16}))$
$= PC\text{-}2(RS_2(C_0), RS_2(D_0))$

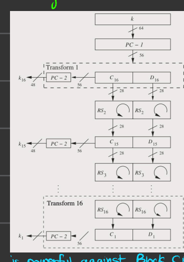
i = 1: not rotated
i = 2, 9, 16: rotate right 1 bit
otherwise: rotate right 2 bits

→ For k_{15}, we need C_{15} & D_{15} derived from C_{16}, D_{16} via right shifts

$(L_0^d, R_0^d) = IP(Y) = IP(IP^{-1}(R_{16}, L_{16})) = (R_{16}, L_{16})$ ∴ $L_0^d = R_{16}$ $R_0^d = L_{16} = R_{15}$

$L_1^d = R_0^d = L_{16} = R_{15}$

$R_1^d = L_0^d \oplus f(R_0^d, k_{16})$
$= R_{16} \oplus f(L_{16}, k_{16})$
$= [L_{15} \oplus f(R_{15}, k_{16})] \oplus f(R_{15}, k_{16})$
$= L_{15} \oplus [f(R_{15}, k_{16}) \oplus f(R_{15}, k_{16})]$
$= L_{15}$



∴ as we go on, $L_i^d = R_{16-i}$, $R_i^d = L_{16-i}$ > $IP^{-1}(R_{16}^d, L_{16}^d) = IP^{-1}(L_0, R_0)$
$= IP^{-1}(IP(x))$
$= x$

→ 2 major criticisms of DES:

↳ Key space too small ⇒ BFA

↳ Design Criteria of S boxes are secret but could lead to analytical attack

DES Exhaustive Key Search:
Input: At least one pair of plain-cipher (x, y)
Output: k s.t. $y = DES_k(x)$
Attack: Test all 2^{56} possible keys until:

$DES^{-1}_{k_i}(y) \stackrel{?}{=} x$ for $i \in \mathbb{Z}_{2^{56}}$

can be done.

→ Differential Cryptoanalysis is powerful against Block Ciphers but S-boxes are resistant

→ Hypothetical Attack: Attacker would need 2^{47} pc pairs but only recovers one key