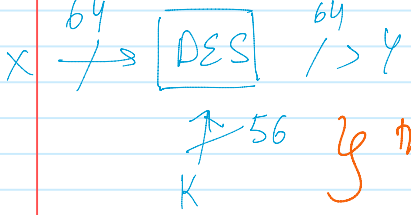
DES

Tuesday, 12 November 2019 11:09 AM

Source : https://www.youtube.com/watch?v=kPBJIhpcZgE



that why its not secure

Q → how do we build a block cipher ?

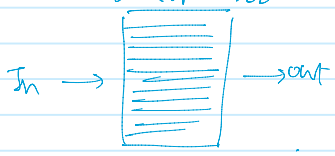
SHANNON

Every block cipher should perform 2 basic operations:

(a) CONFUSION - Relationship b/w PT & CT should be OBSCURRED (hidden)

eg substitution table

LOOK UP TABLE

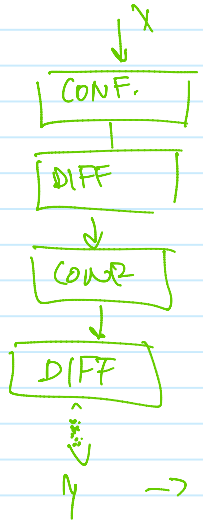


but ceasars cipher is not good enough

(b) DIFFUSION : The influence of one such PT bit is spread over many different bits

eg PERMUTATION

combine confusion and diffusion many times to build a strong block cipher.



DES has 16 rounds

1 round : 1 diff and 1 conf. etc etc

changing of one bit of PT results on an average in the change of half the output bits eg.

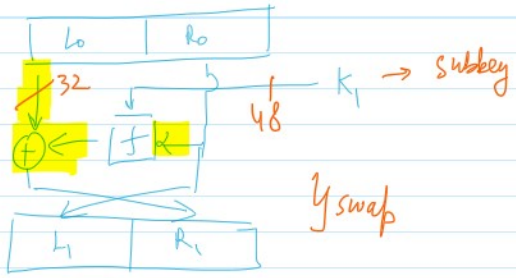
$x_1 = 00101011$ → block cipher → $y_1 = 10111001$

$x_2 = 00001011$ → block cipher → $y_2 = 01101100$

single bit i/p → many bit o/p

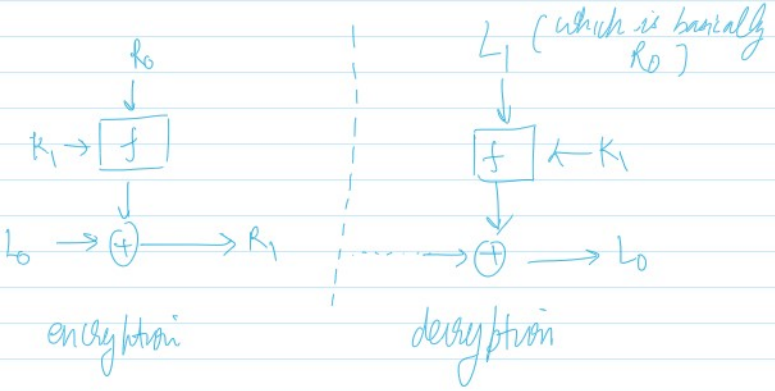
PRODUCT CIPHER → rounds which are applied repeatedly to the data

FEISTEL NETWORKS:



only L_0 is encrypted using XOR operation

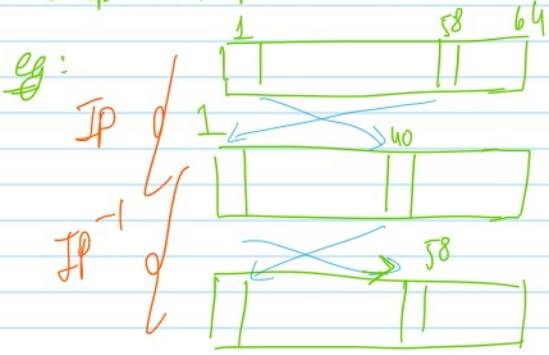
(R_0 is not being encrypted here)



DES - Internals:

(a) IP and IP^{-1} → simple bit permutation.

eg:

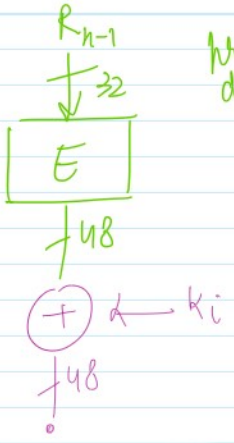


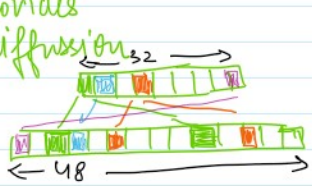
Q: why permute?

Obviously, it doesn't directly add to security as the IP & IP^{-1} tables are publicly known

The reason behind is just electrical wiring systems (no relation to cryptography)

(b) The "f" function





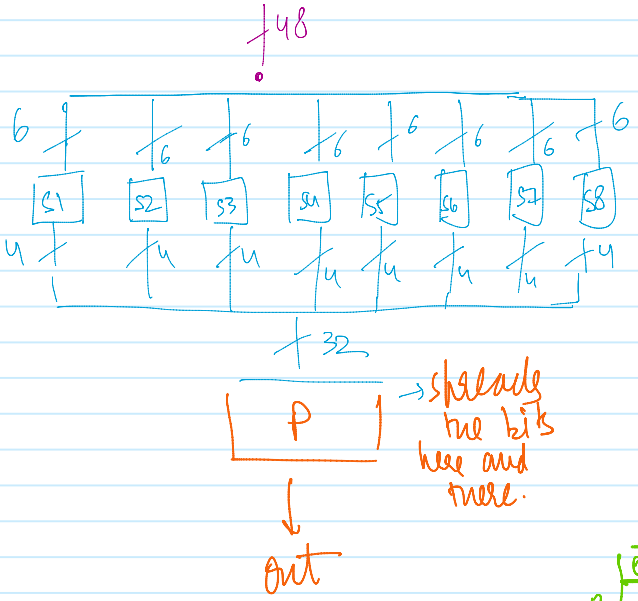
4 steps:

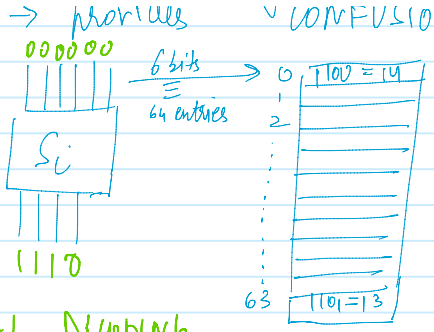
(1) Expansion E
(2) XOR with round key
(3) S-box substitution
(4) Permutation

S box

→ the heart of DES

→ provides CONFUSION





UNUSUAL DECODING OF SBOX INPUT BITS:

XXXXXX

column select → Row select

every entry here is 4 bit ∴ b/w 0 and 15

eg: S(37)

S(100101)

⇒ 0010 column 11 row

⇒ 2 column 3rd row

∴ entry no → (3,2)

which is 08 in the given table (or 1000)

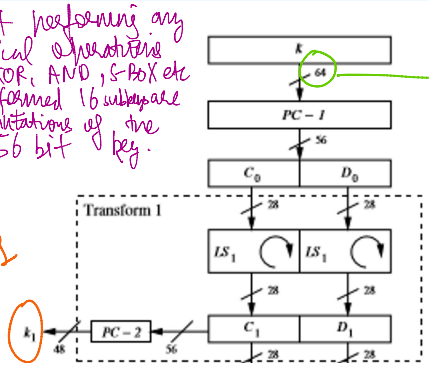
The S box are ANTI-DIFFERENTIAL CRYPT ANALYSIS in nature ie the values of this table are chosen s.t. the above technique cannot break it.

Source : https://youtu.be/I-7YW06BFNs

KEY SCHEDULE

→ getting the 16 roundkeys / subkeys $K_1, K_2, \ldots K_{16}$

we are not performing any mathematical operations such as XOR, AND, S-BOX etc on the newly formed 16 subkeys are just permutations of the original 56 bit key.



Subkey 1

(a) PC-1 Permutated Choice 1

→ drops bits 8, 16, 24, ..., 64

→ effective key length of DES = 64 − 8 = 56

(b) LS_i $i = 1, 2, 3, \ldots 16$ [happens in the 2 28 bit blocks]

Left shift → just a left rotate.

We shift as

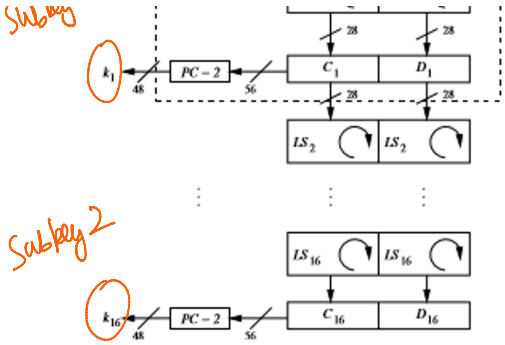


Fig. 3.14 Key schedule for DES encryption

Left shift → just a left rotate.

They shift as

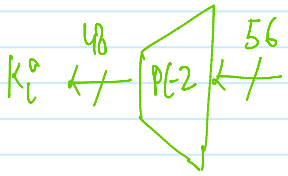
$$LS_i = \begin{cases} 1 \text{ position shift}, & i = 1,2,9,16 \\ 2 \text{ position shift}, & \forall \text{ other } i \end{cases}$$

note: (1) total number of bit position shifted $= \underbrace{4 \times 1}_{i=1,2,9,16} + \underbrace{12 \times 2}_{\text{other } i's}$

$= 28$ [28 is coming a lot of times in true implementation]

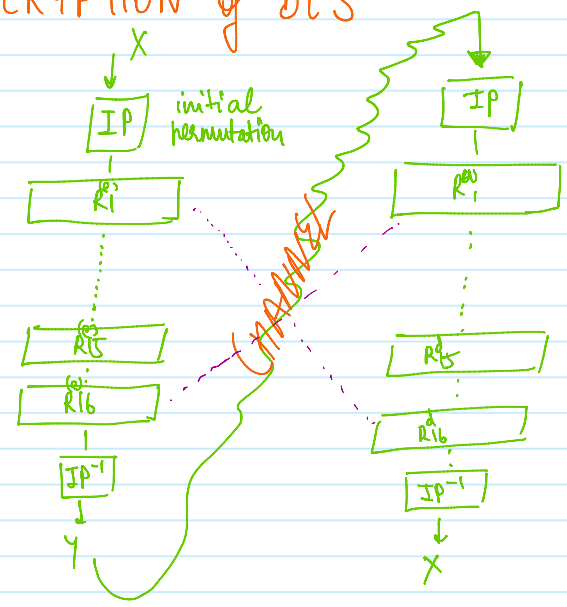
(2) By the time, we do all the shifts and reach LS_{16}, the bits in the C_0 block have rotated 28 time i.e. $C_{16} = C_0$ and $D_{16} = D_0$

(b) PC-2 Permuted Choice 2



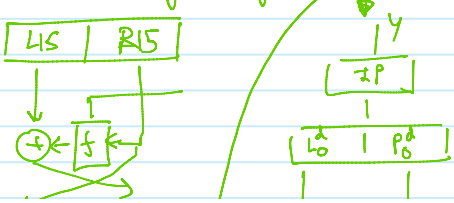
i.e. 8 bits are dropped and the remaining 48 bits are permuted.

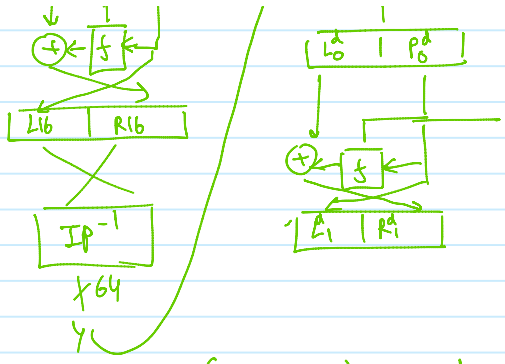
DECRYPTION of DES



Q: how to reverse R_{16} to get R_1?

Soln: at the end of encrypt





to show: $(L_1^d = R_{15}^e) \wedge (R_1^d = L_{15}^e)$

since R15 is L16 and IP & IP^{-1} cancel ∴ L16 is L_0^d and due to f and XOR [same as discussed before]

$$L_1^d = R_{15}^e$$

Illy $R_1^d = \underbrace{L_0^d}_{\text{actually } R_{16}^e \text{ (since IP \& IP}^{-1}\text{ cancel)}} \oplus f(K_i, R_0^d)$

$= L_{15}^e \oplus f(K_{16}, R_{15}^e) \oplus f(K_i, R_0^d)$

$=$ since $R_0^d = R_{15}^e$

now if i chose i to be 16 then

$= L_{15}^e \oplus f(K_{16}, R_{15}^e) \oplus f(K_{16}, R_{15}^e)$

$= L_{15}^e \oplus (\overbrace{000\ldots00}^{32})$

$= L_{15}^e$

$= L_5^e$

QED

note: this explains why f doesn't need to be invertible (↓) since we never use f^{-1} ... (↓)

∴ Illy for remaining round reversals work the same:

Round 2^d reverses Round 15^e

⋮ ⋮ ⋮ ⋮ ⋮

Round 16^d reverses Round 1^e

Security of DES:

2 types of attacks:

(1) ANALYTICAL ATTACKS:

→ Differential cryptanalysis attack requires 2^{47} (X,Y) pairs (as opposed to 2^{56} before)

→ Linear cryptanalysis attack requires 2^{43} (X,Y) pairs (better but not that better)

(2) BRUTE FORCE ATTACK

given: (X_0, Y_0)

$$DES^{-1}_{K_i}(Y_0) \stackrel{?}{=} X_0 \; ; \; i = 0, 1, \ldots 2^{56} - 1$$

Deepcrack (1998) → special purpose DES hardware cracker. → $250,000 machine showed DES is no longer secure.

COPACOBANA (2007) → did it in $10,000

DES Alternatives:

cipher	comment
AES	de facto world standard
3 DES	still very secure
AES - Finalists	4 ciphers all very secure RC6, serpent etc