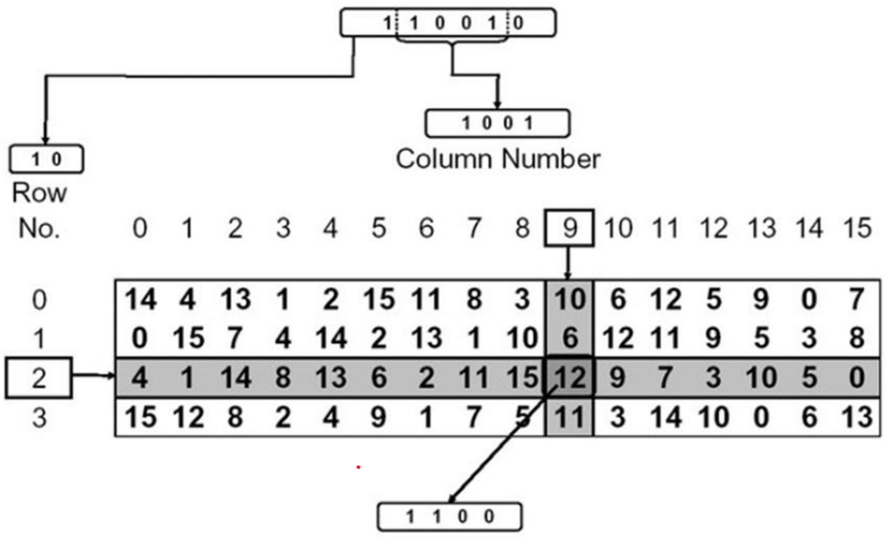
- DES bystkhdm 2 basic techniques Confusion w Diffusion
- Diffusion  => permutations
- Confusion => XOR
- Plain text btb2a 64 bits
- Key byb2a 56 bits
- Byb2a feh 16 round  kol round leha key w feha function
- B3ml awl haga initial permutation ll 64 bits plain text.
- Bakhod el result mn permutation a2smo l right hand side (32) w left hand side (32)
- Bakhod el rhs adkhlo 3la expansion permutation 3shan akhleh 48 bits zy el key 3shan a3rf b3dha a3mlhm XOR.()
- El hytl3 mn XOR 48 bits 3yza arg3hm 32 bits zy m kano 3shan lma ahothm 3la lhs yrg3o 64 bits f hdkhlhm 3la 8 Subsitution Boxes kol 8 yroho l box.
- Msln awl Sbox khad 110010 9 bits dol bakhod awl rkm w akhr rkm yb2o row number w el fl nos hyb2o col number w ashof fl gdwl dh f kol box hytl3 4 bits 8x4=32 bits.

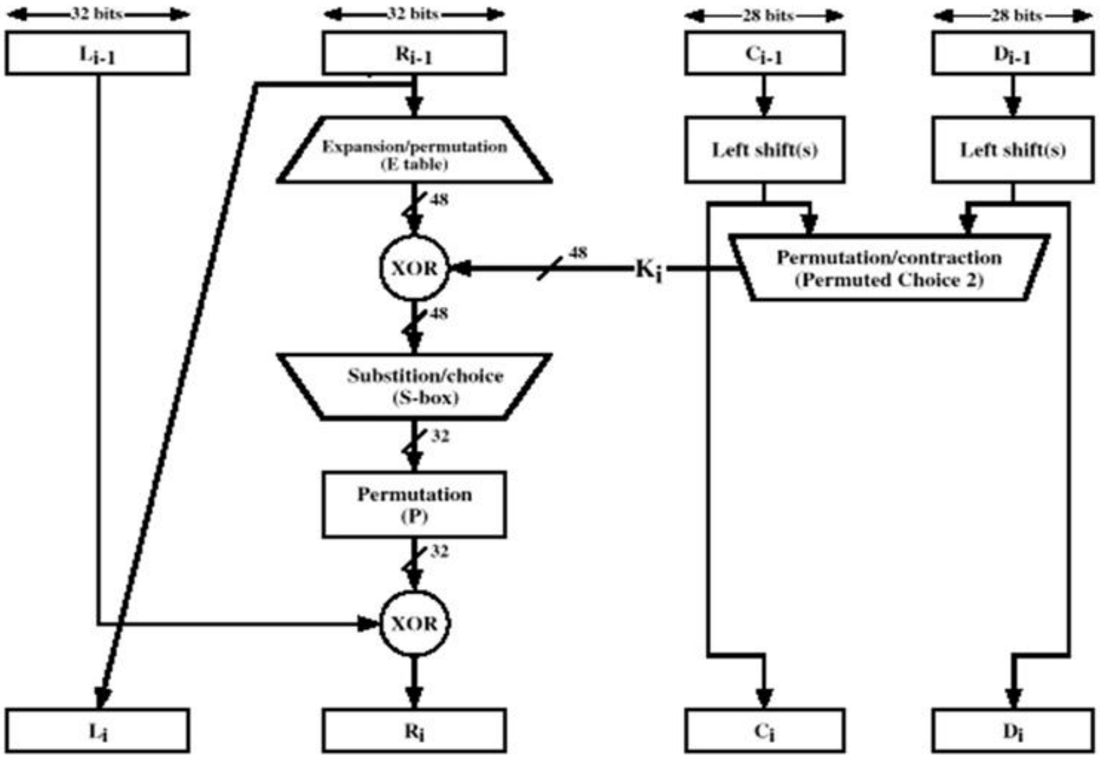


| Row No. | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 14 | 4 | 13 | 1 | 2 | 15 | 11 | 8 | 3 | 10 | 6 | 12 | 5 | 9 | 0 | 7 |
| 1 | 0 | 15 | 7 | 4 | 14 | 2 | 13 | 1 | 10 | 6 | 12 | 11 | 9 | 5 | 3 | 8 |
| 2 | 4 | 1 | 14 | 8 | 13 | 6 | 2 | 11 | 15 | 12 | 9 | 7 | 3 | 10 | 5 | 0 |
| 3 | 15 | 12 | 8 | 2 | 4 | 9 | 1 | 7 | 5 | 11 | 3 | 14 | 10 | 0 | 6 | 13 |

- B3den hdkhl 32 bits 3la permutation tany 3shan yghyr el amakn bta3t bits w akhr haga el ytl3 XOR m3 LHS w el ytl3 hbd2 beh round el gdeda k LHS w RHS.
- B3d akhr round (round 16) b3ml 32 bit swap b3dha inverse permutation w el ytl3 yb2a cipher.
- avalanche effect: dh lw ghyrt bit fl input yghyr fl output ehna 3yzeno effect yb2a kber y3ni lw ghyr bit fl input yghyr kaza bit fl outout 3shan hacker my3rfsh y3ml decryption b sohola.
- General remarks in the DES:
  1- The S-boxes provide the core of the security of DES
  and the cipher would be linear, and trivially breakable
  without them.
  2- The substitution and permutation in the DES provide
  confusion and diffusion.

  - El key byegy 64 bits b3ml PC1 yb2a 56 bits w a2sm left w right b3den shift 3la hasb el round b3dha pc2 f yb2a 48 bits a2dr a3mlo XOR m3 el PT.

# The 16 Iterations/Rounds of F Consist Of:



32 bits
32 bits
28 bits
28 bits
$L_{i-1}$
$R_{i-1}$
$C_{i-1}$
$D_{i-1}$
Expansion/permutation (E table)
Left shift(s)
Left shift(s)
48
XOR
48
$K_i$
Permutation/contraction (Permuted Choice 2)
48
Substition/choice (S-box)
32
Permutation (P)
32
XOR
$L_i$
$R_i$
$C_i$
$D_i$