DES: Data Encryption Standard

block of size 64 bit

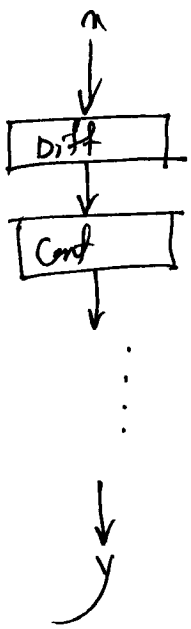
IBM 1977 NSA

key 56 bit

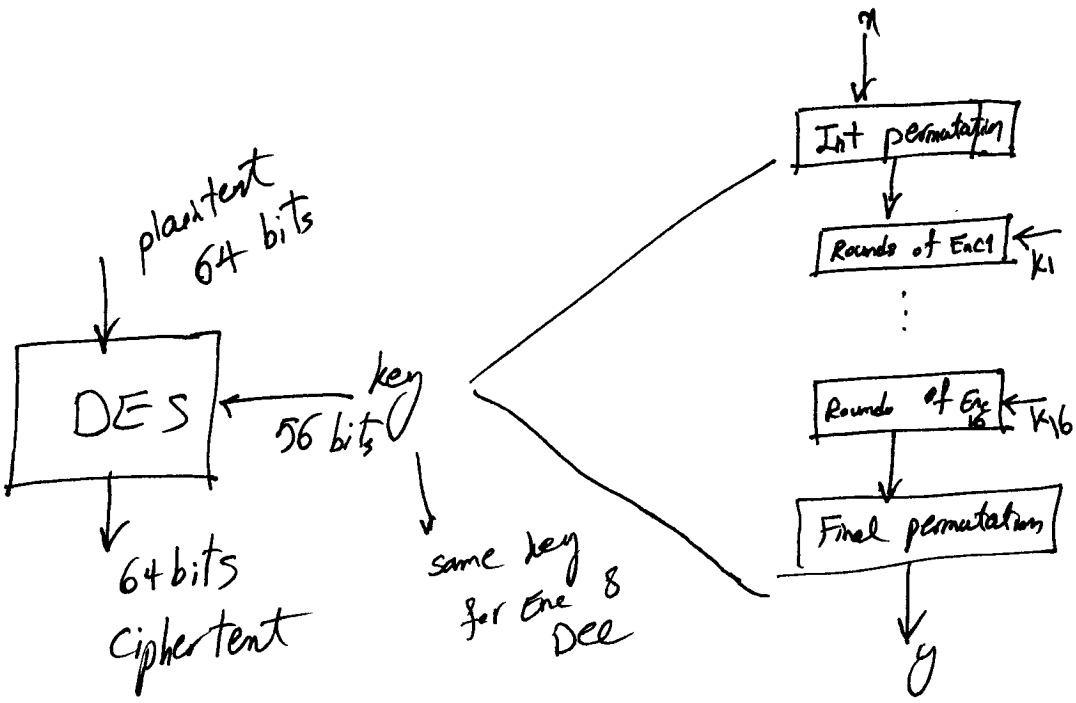
2000 was replaced by AES (Advanced Enc Standard)

Confusion: an Enc operation where the relationship between key & ciphertext is obscured.

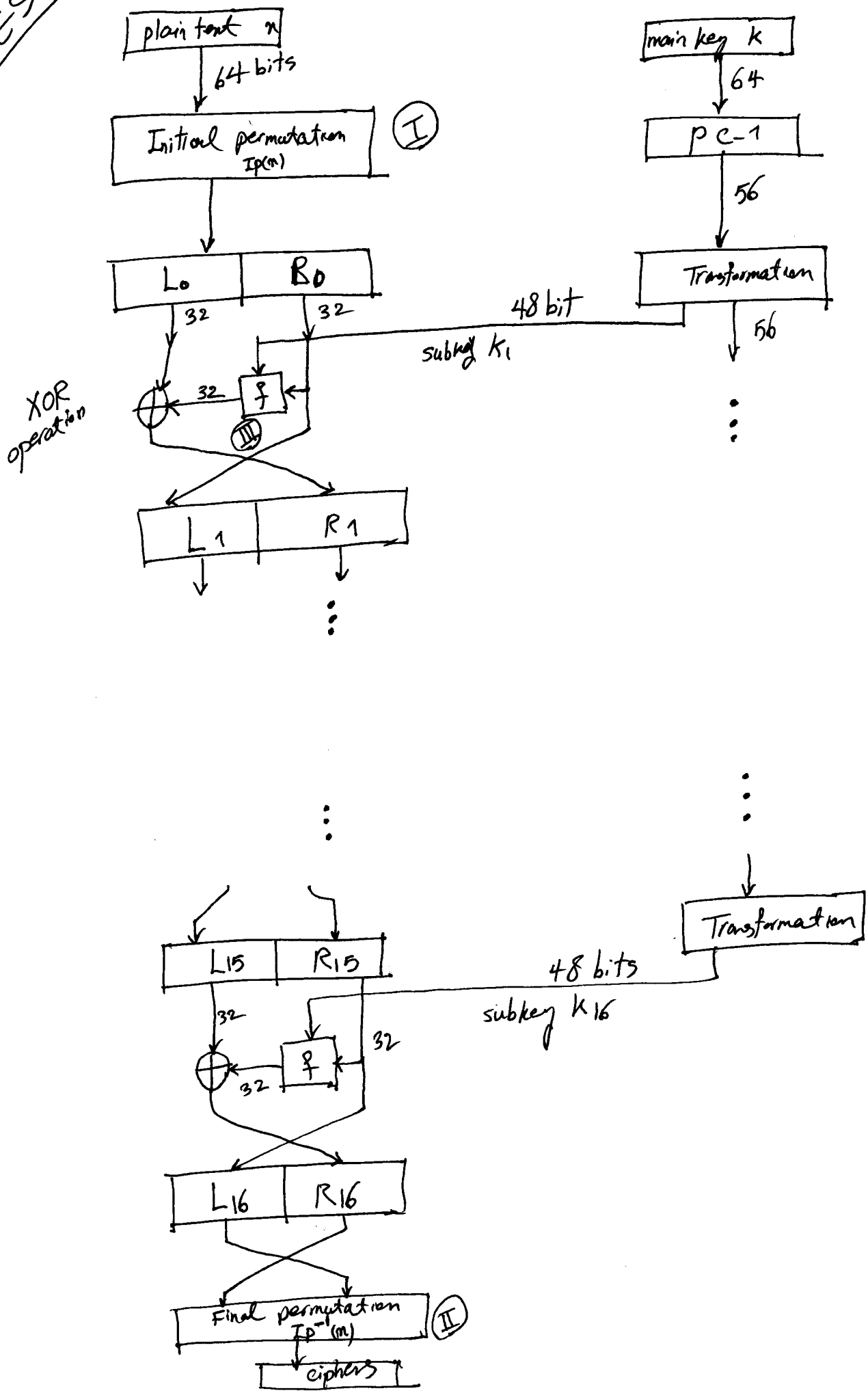
Diffusion: an Enc operation where the influence of one plaintext symbol is spread over many ciphertext symbols. → hide statistical properties of the plaintext



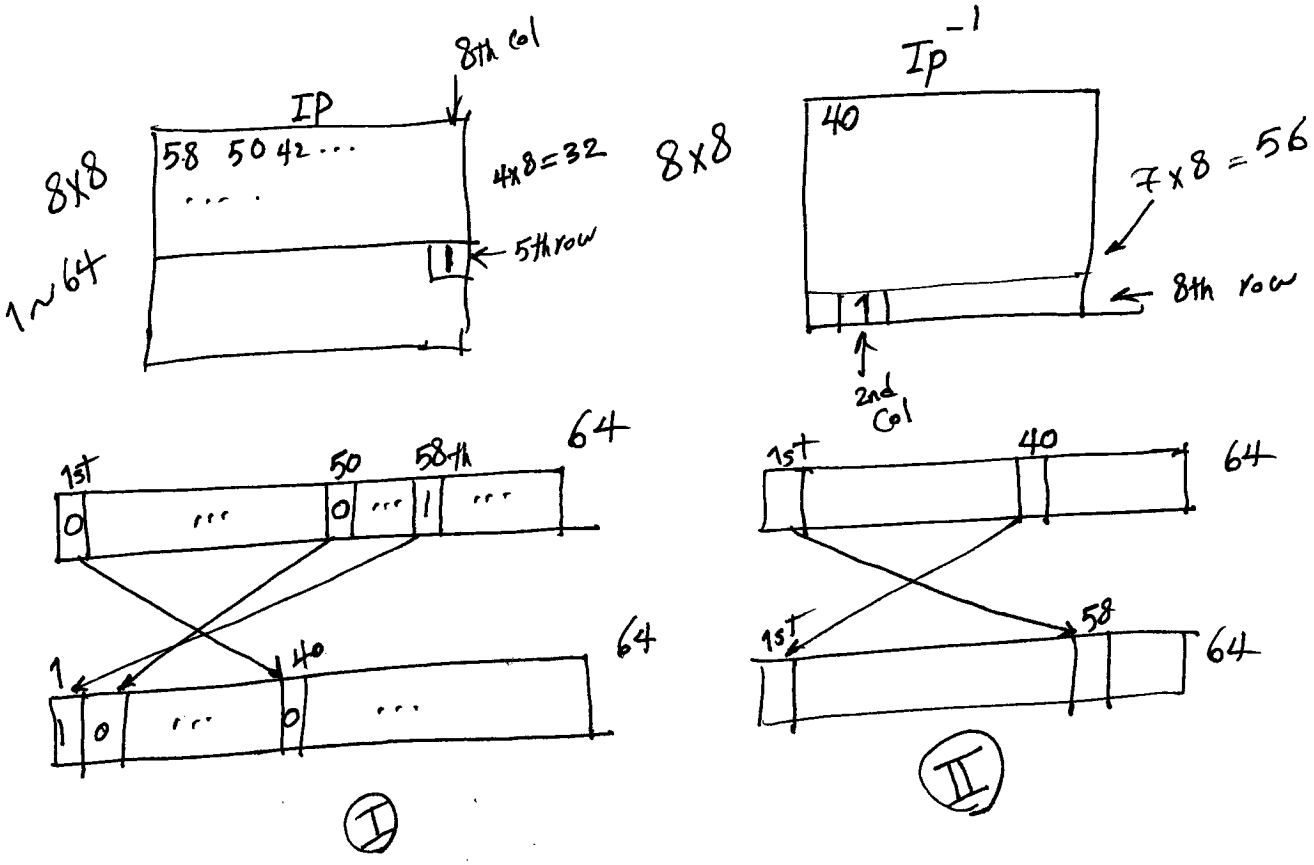
* a good diff. ope: changing 1 bits results in change of half of the bits in the ciphertext



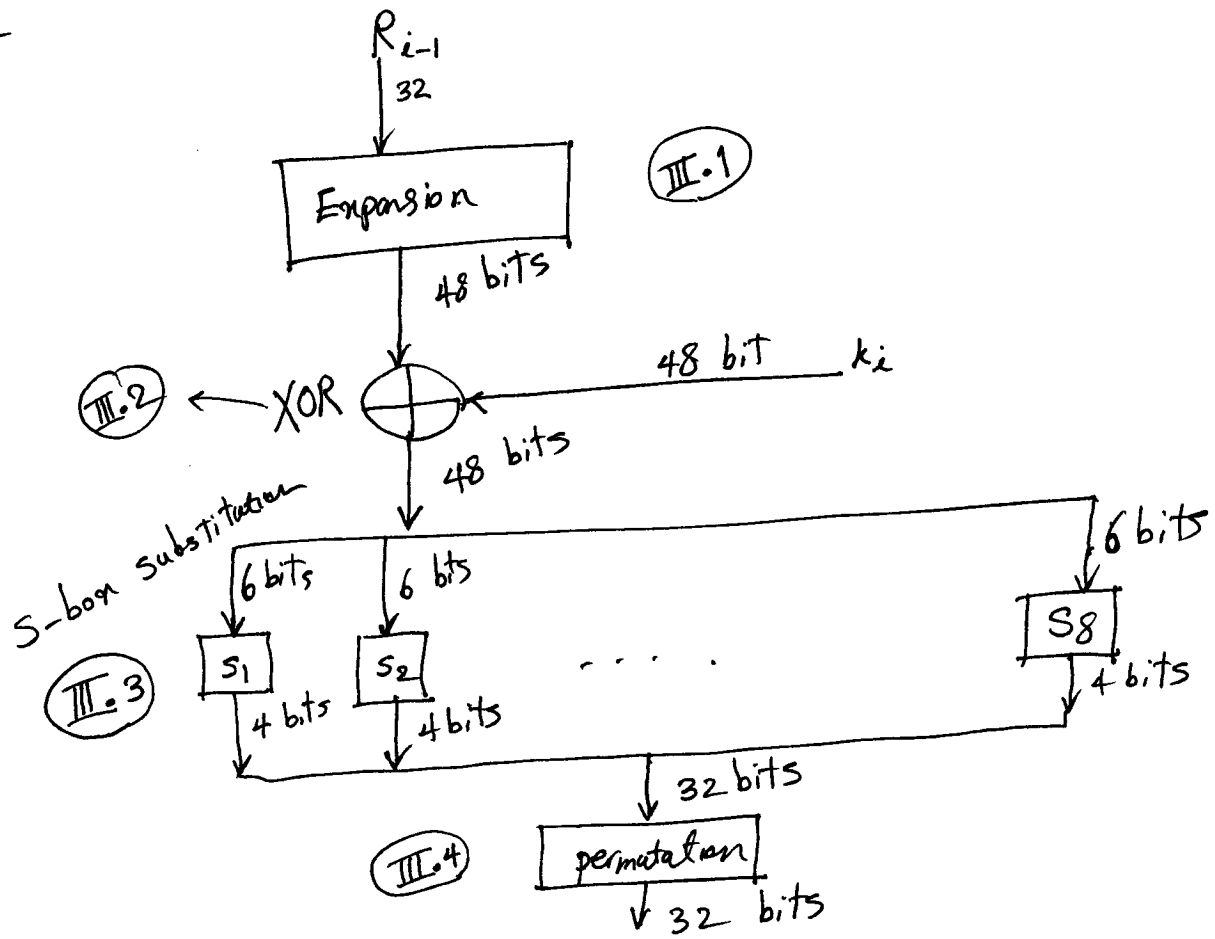
DES


plain text x
64 bits
Initial permutation
Ip(x)
I
main key k
64
PC-1
56
Transformation
48 bit
subkey K1
56
L0
R0
32
32
XOR operation
32
f
II
L1
R1
L15
R15
32
32
32
f
48 bits
subkey K16
Transformation
L16
R16
Final permutation
Ip-1(x)
II
ciphers

Initial & Final permutation functions

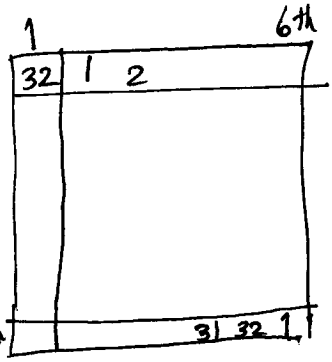


III ƒ

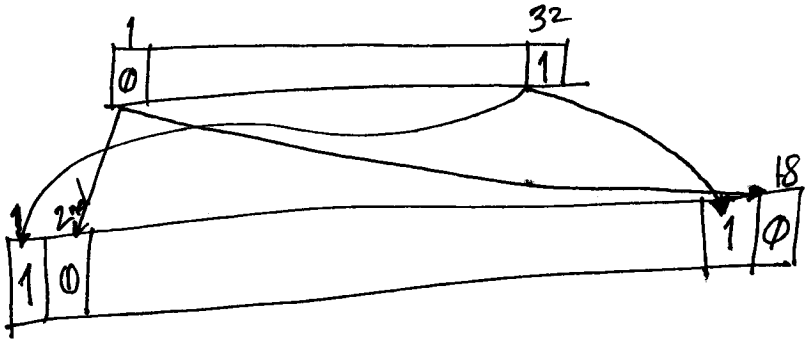


III.1

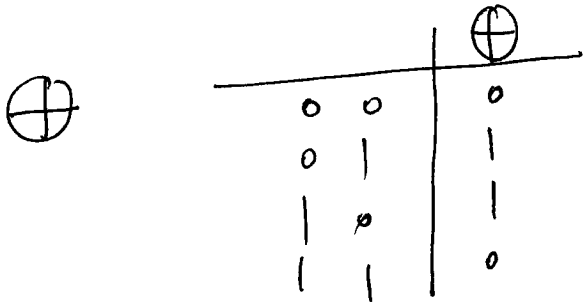
8 x 6



1 ~ 32 all these numbers in your table



III.2

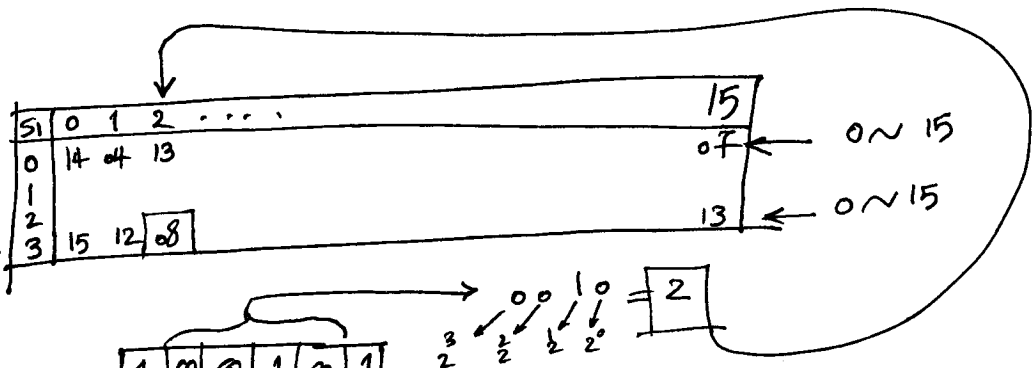


III.3 S-box

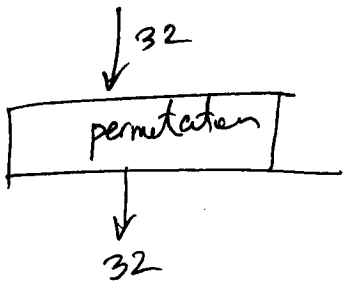
for every single box you need a table

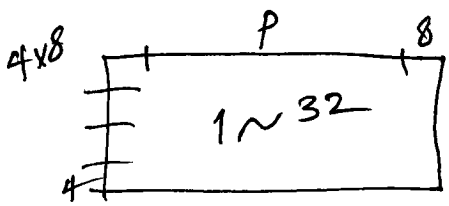
6 bits → S1 → 4 bits

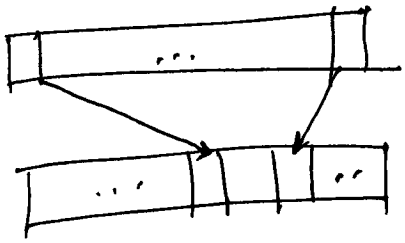
we need eight 8 tables like this



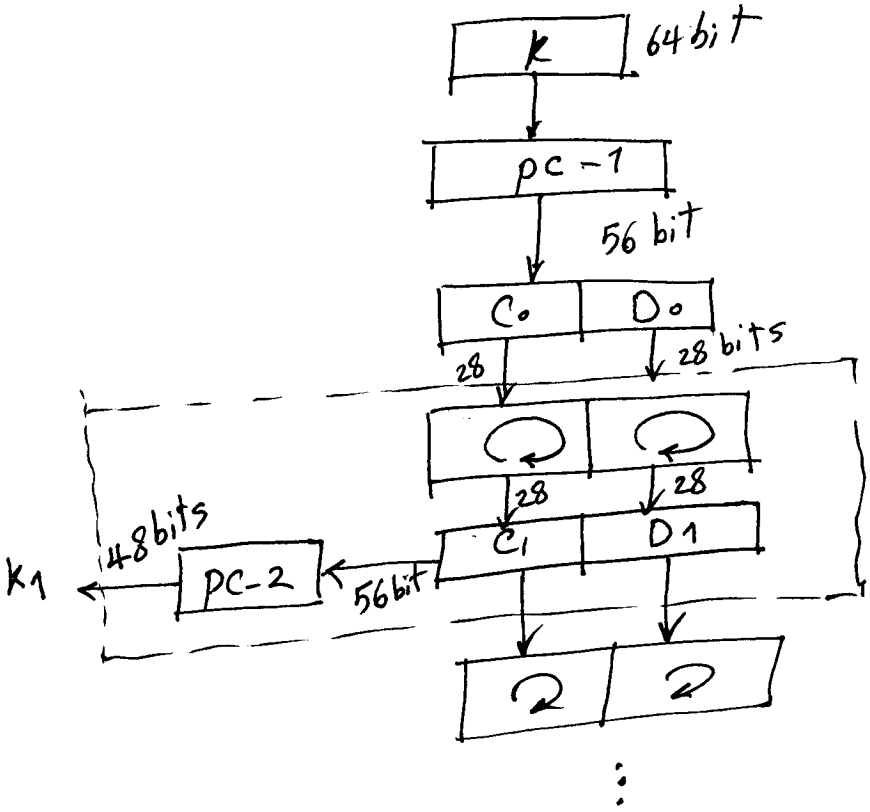
III.4

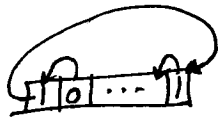




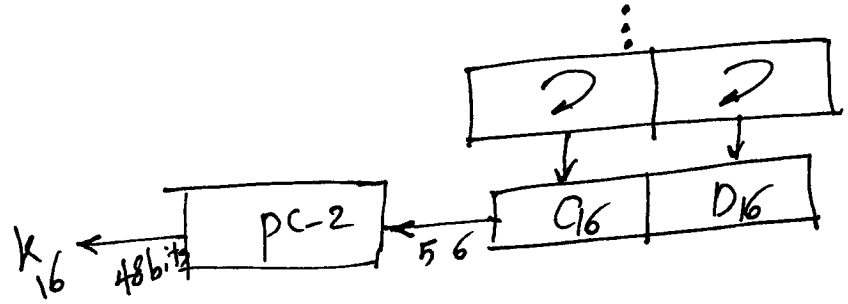


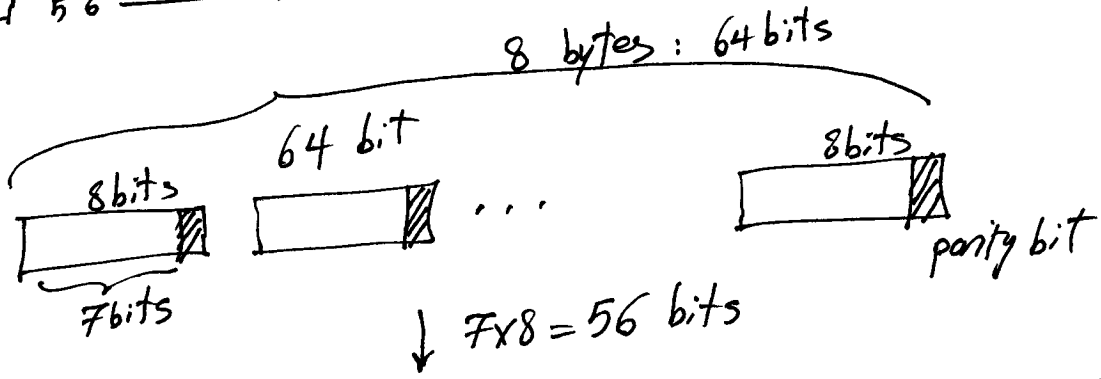
key schedule for DES

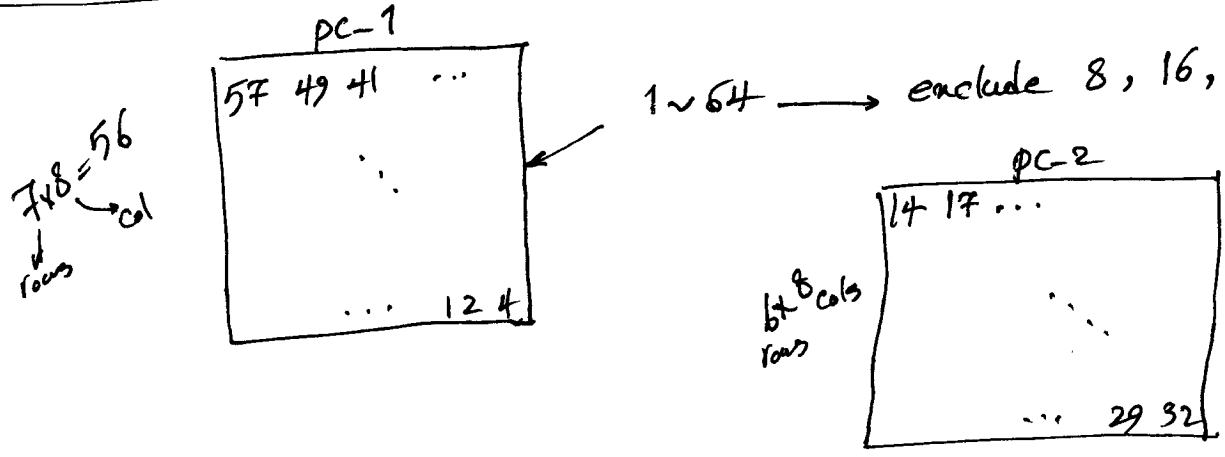




1. In rounds $i=1, 2, 9, 16$, two halves are each rotated left by one bit
2. In all other rounds, two bits will be rotated to left

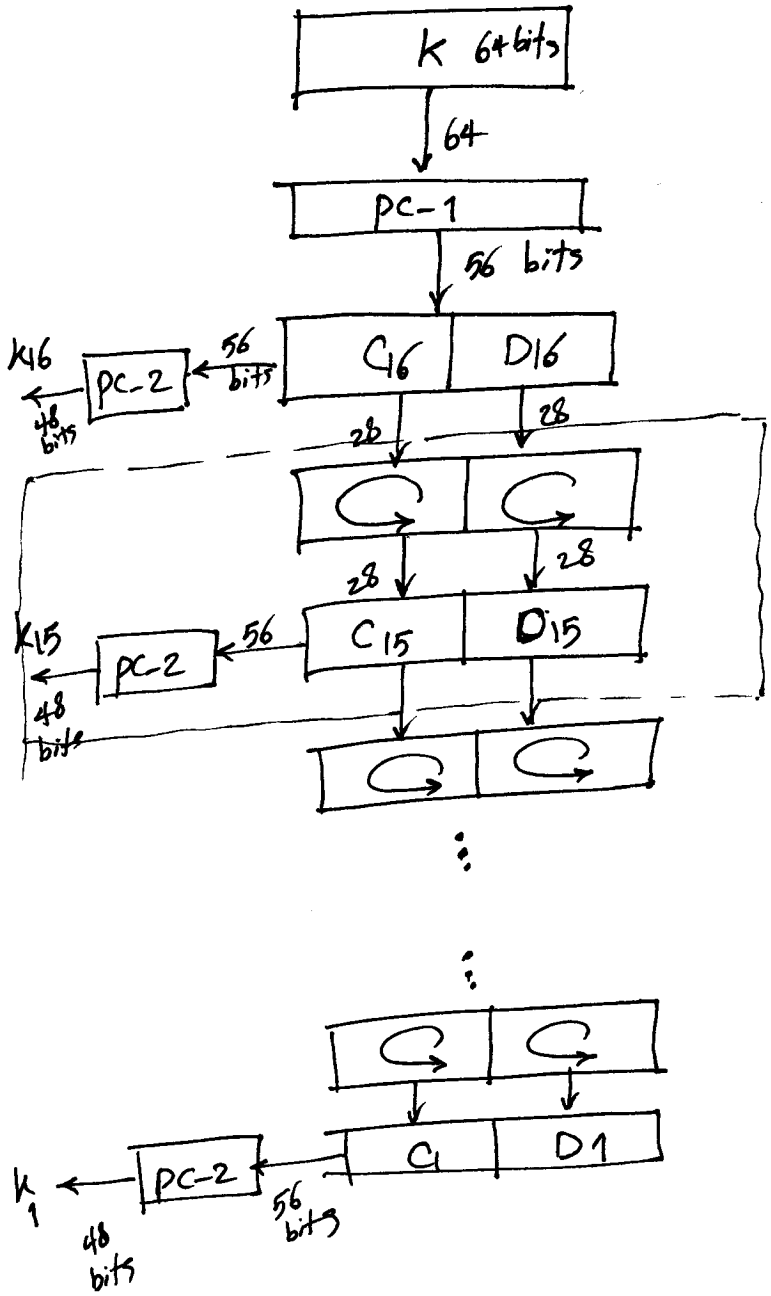






decryption — key schedule : we need to generate same key

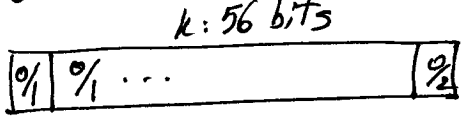
$K_1 \sim K_{16}$ in reverse order



1. No rotation in round 1
2. one bit rotation to the right in rounds 2, 9, 16
3. Two bit rotation to the right in all other rounds

---

1. key space is very small



2^{56} : total # of possible keys that one can generate

2. S-box

---

attack → pair of plaintext-ciphertext → test all 2^{56} keys

Jan 1997 ⟶ 4.5 months of distributed search

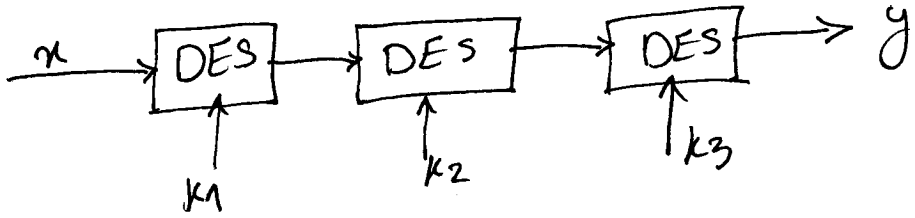
Feb 1998 ⟶ 39 days

Jul 1998 ⟶ 15 days ⟶ 24 search engines (EFF)

Jan 1999 ⟶ 22 h 15 min

2006–2008 ~~germany~~ 6.4 days at a very low cost $10,000

alternative sol : Triple DES – 3DES



Banking system

* DES was the dominant sym Enc scheme from mid-1970s to mid-1990s ⟶ Advanced Enc Standard
* 56 bits, the key can be broken by plaintext-ciphertext attack very fast through an Exhaustive key Search
* No practial attack is currenty known against 3DES.