Crypto – V2

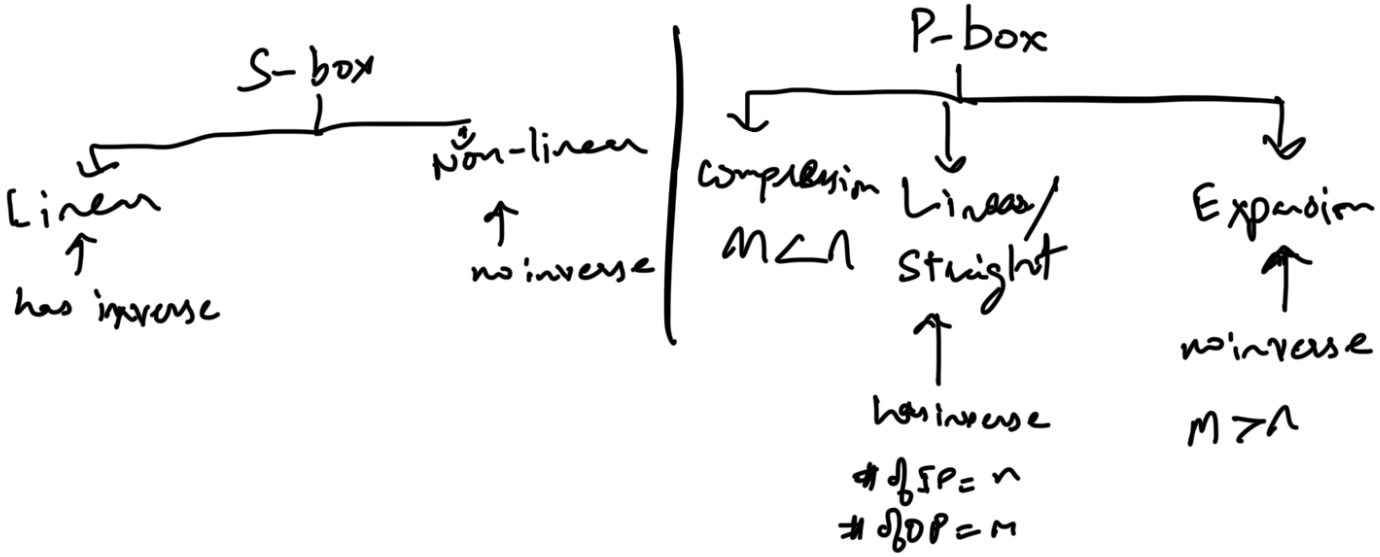
Introduction to Mordern Symmetric-key Cipher

S-box → Substitution box

P-box → Permutation box

XOR.

CS
DT



How many padding bits must be added to a message of 100 char if 8-bit ASCII is used for encryption & the block cipher accepts blocks of 64 bits?

$8 \times 100 = M$

$M + P \equiv 0 \bmod 64$

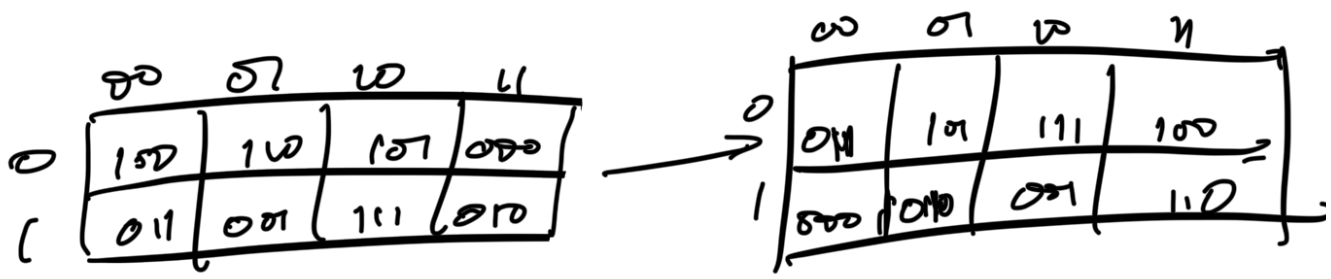
$800 + P \equiv 0 \bmod 64$

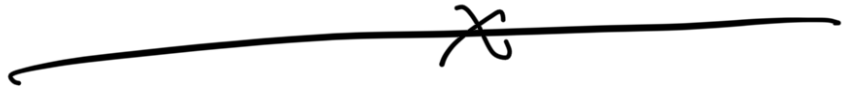
$P = -800 \bmod 64 = 32$ bits

	M	key	Ciphertext
T	n bits	$\log_2 n!$	$n!$
S	n bits	$\log_2 2^n!$	$2^n!$

Decrypt

$$\left.\begin{matrix} 634521 \\ 123456 \end{matrix}\right\} \rightarrow 652341$$



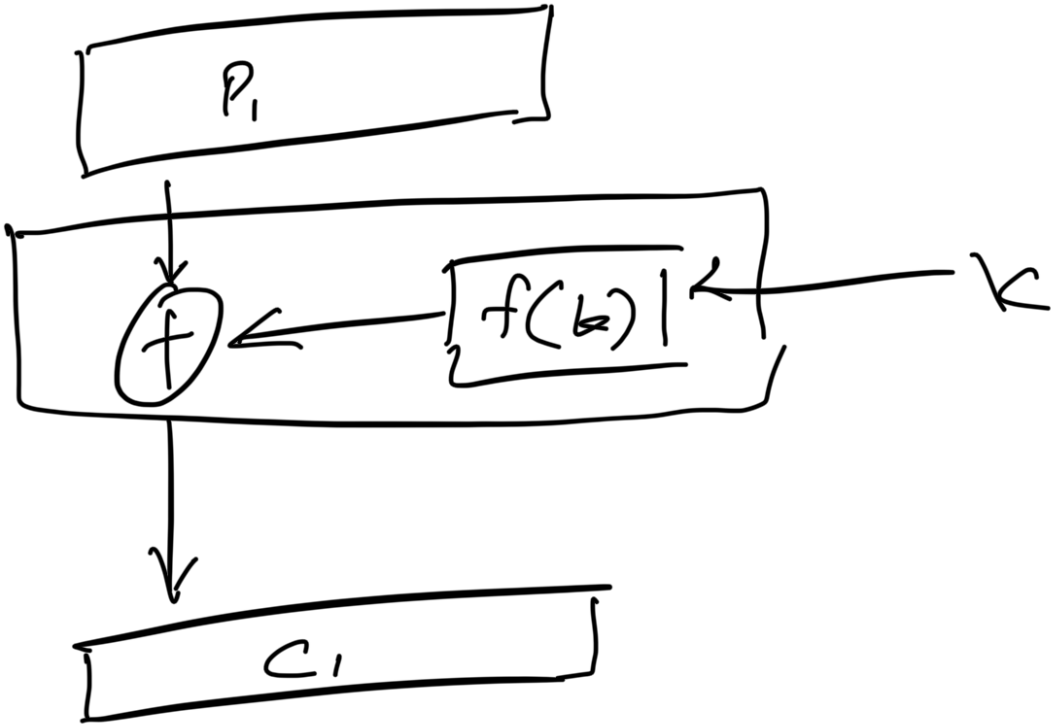


... ciphers are all product ciphers, but they

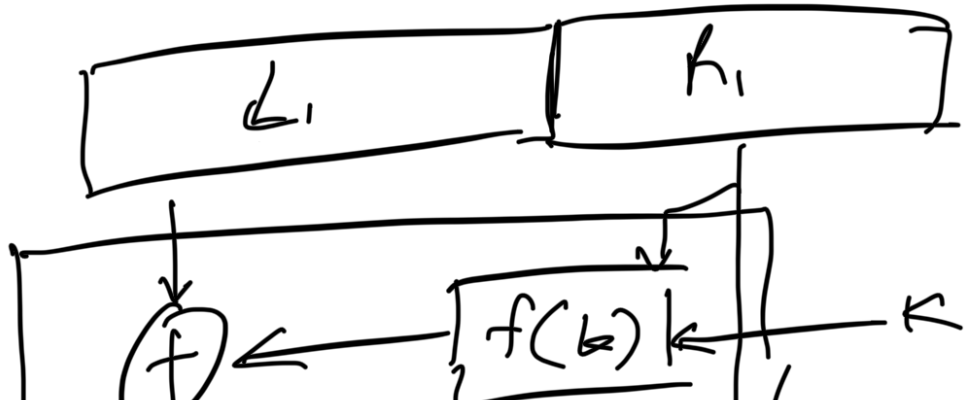
Mordern block ciphers
are divided into 2 classes:

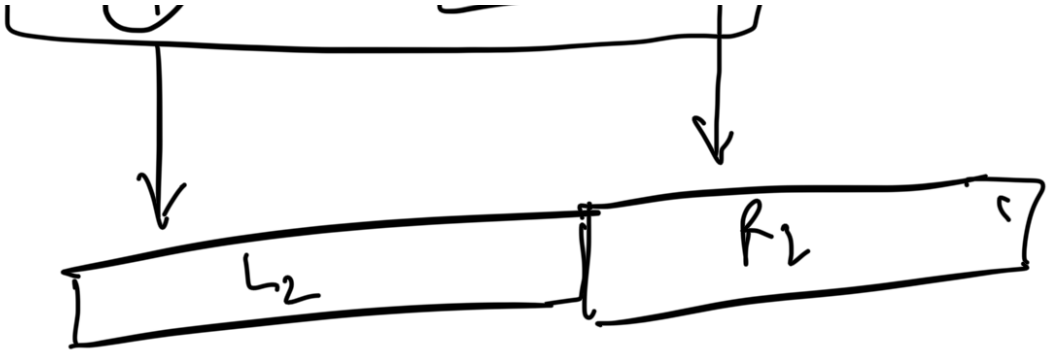
Fiestal

Non- "



Size matching





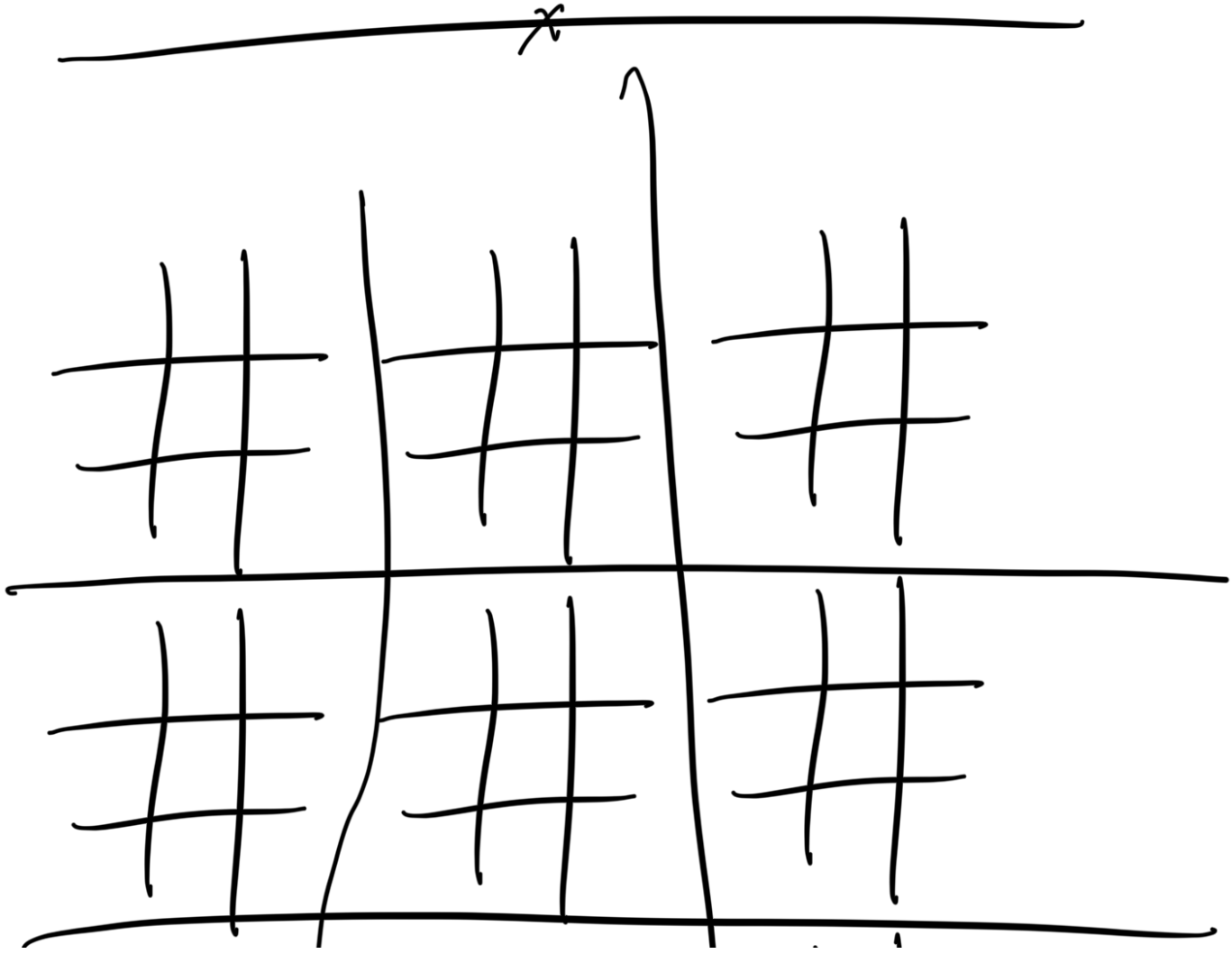
$C_0 = P_0 \oplus K_0 \oplus P_1 \oplus K_1$

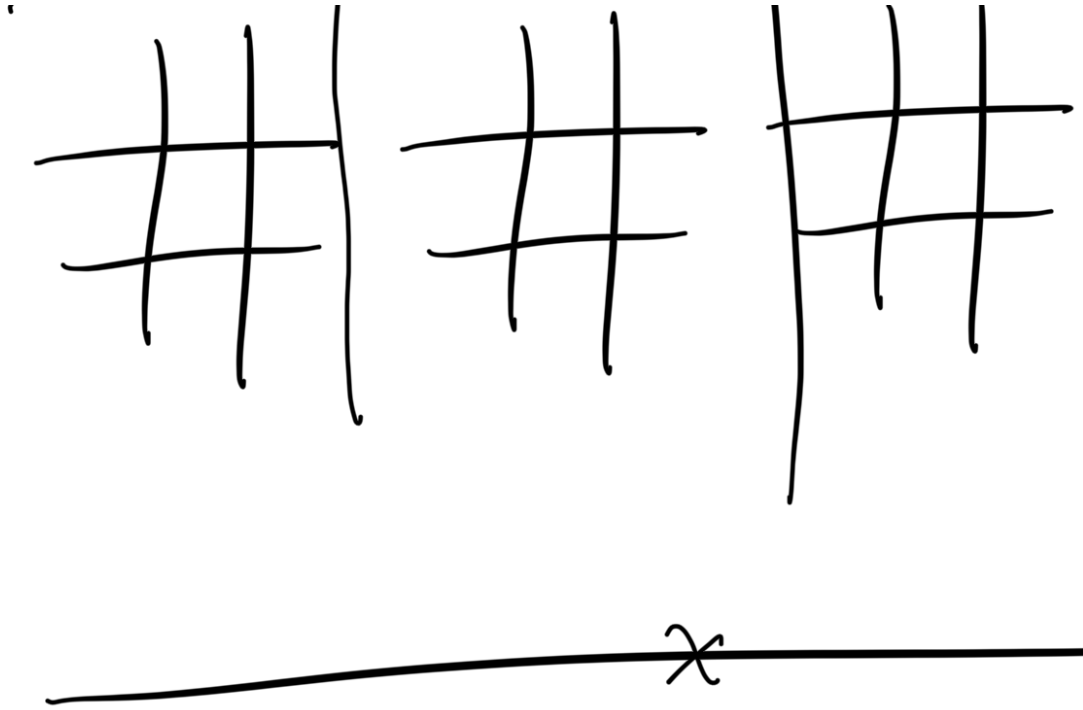
Differential Cryptanalysis → Choosen-plaintxt Attack

Linear " → known-plaintxt "

Stream Cipher:

- FSM
  - get polynomial





DES Algo

IP 0x0002 8000 0000 0001

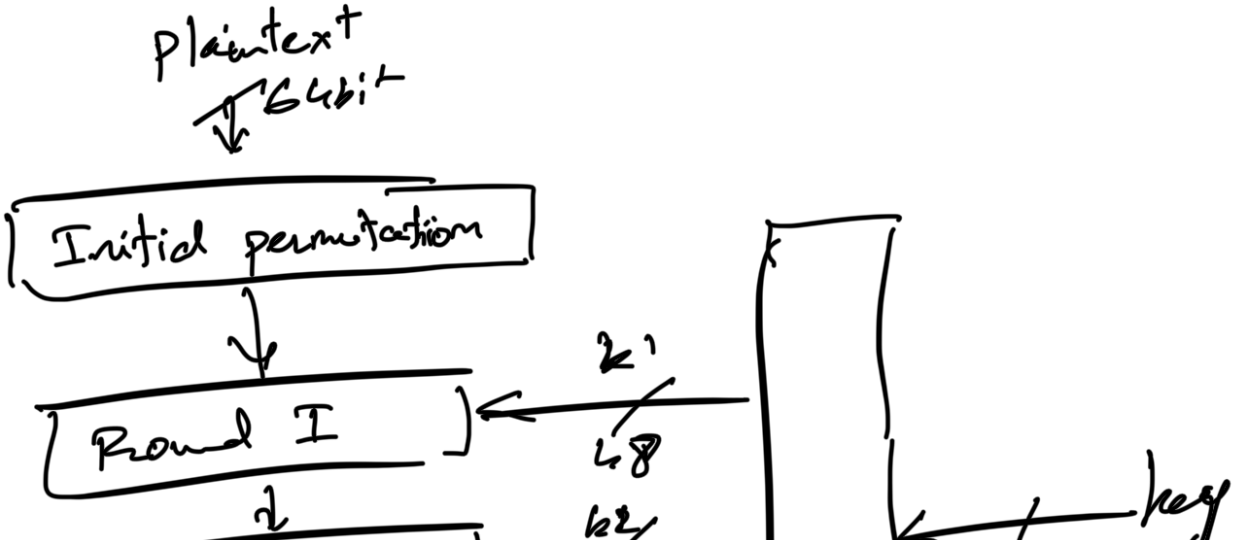
DES Algo → Feistal cipher

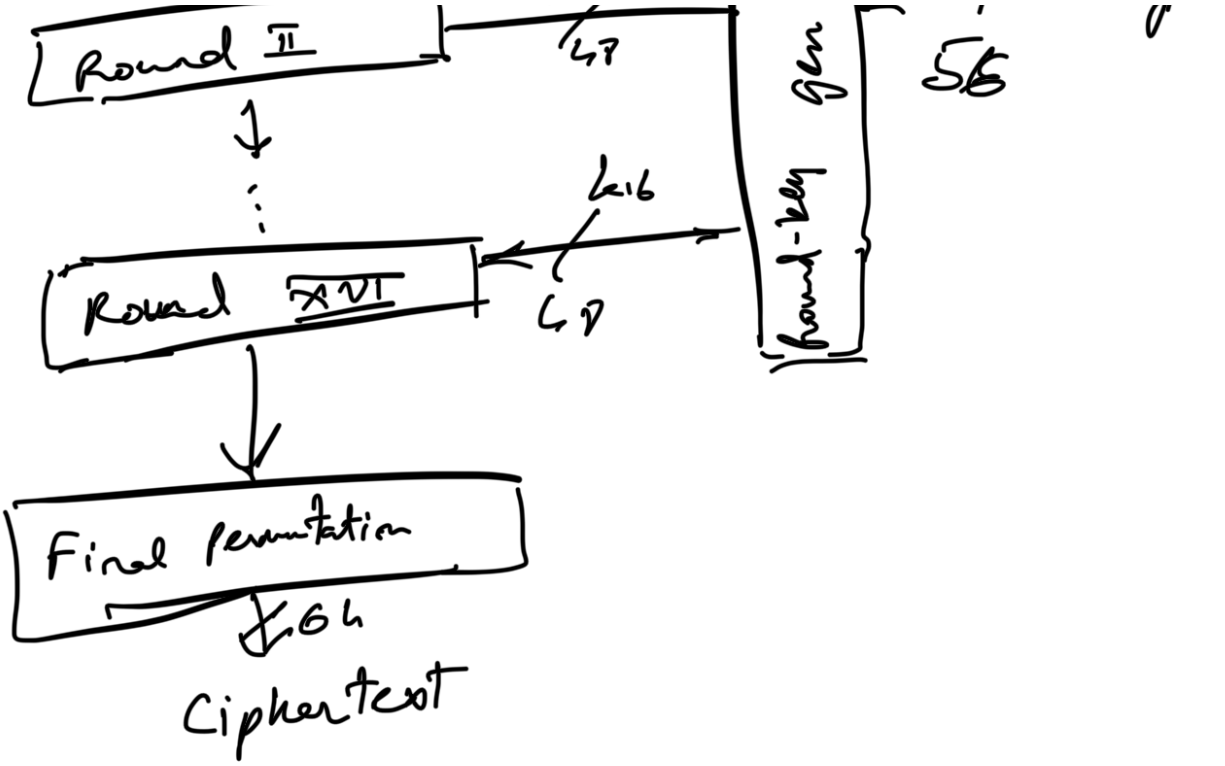
↳ Block cipher

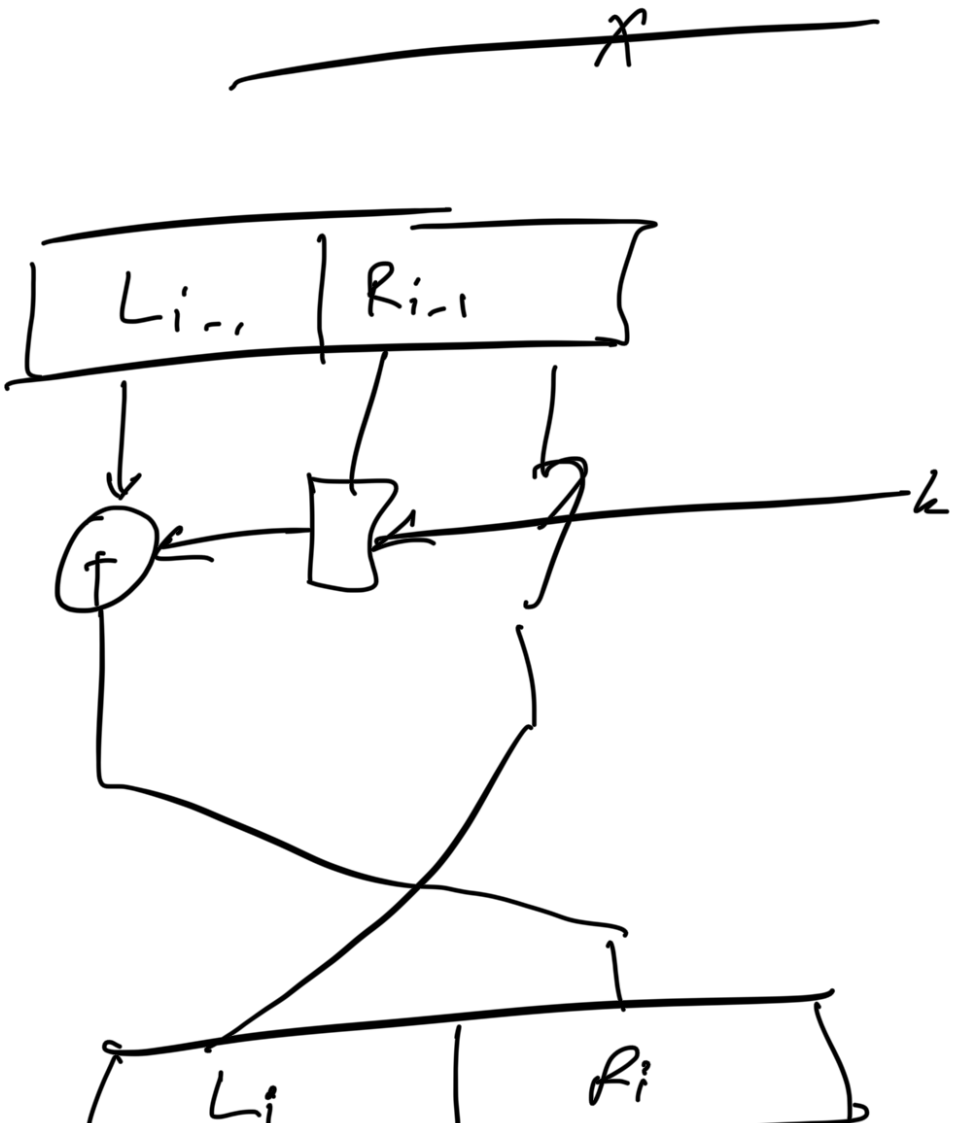
↳ 64 bits blocks, pad if needed

↳ 56 bit key

↳ 48 bit round key.




Round II
48
56
Round-key gen.
48
Round XVI
32
Final permutation
64
Ciphertext

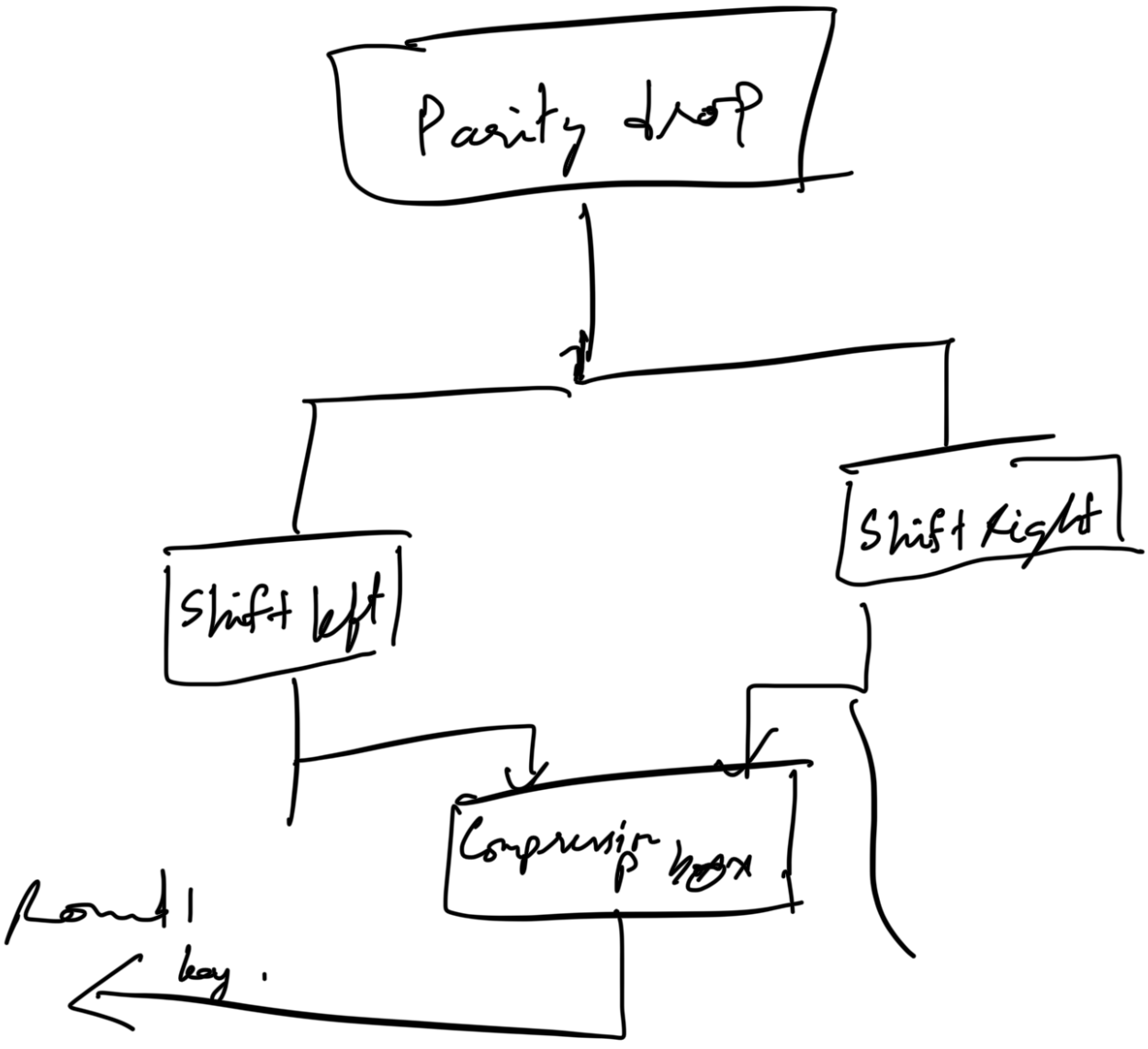

X
Li-1
Ri-1
f
k


32
P-box
48
K
f
48
S-box
32

E box

32

key gen →



The above repeats 16 times

in the DES also

4 weak keys in [illegible]
using them will give the plaintext back
not ciphertext.

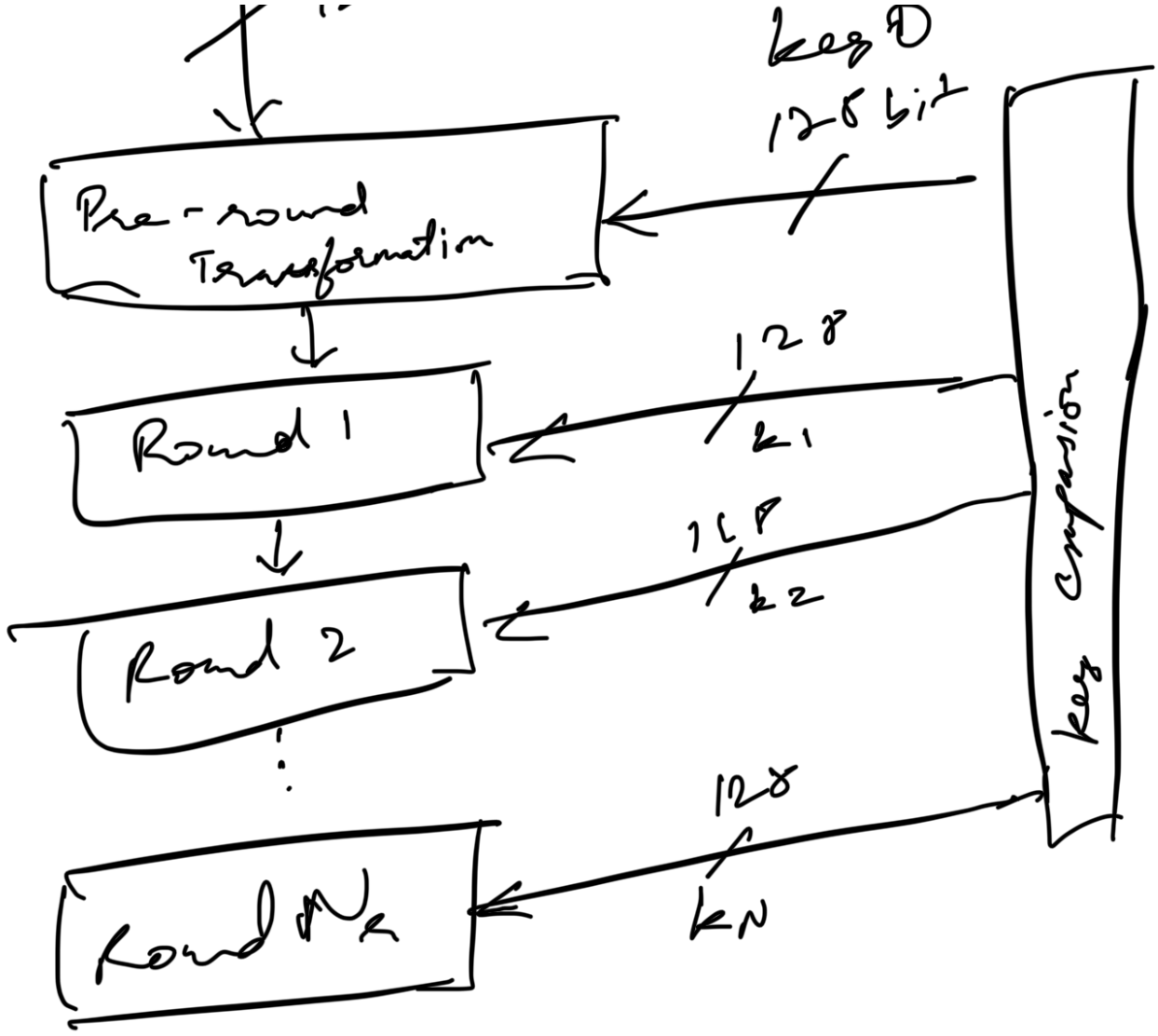
12 semi weak keys → pairs

48 strong weak keys

so out of 2^{56} → 64 keys are weak.

AES algo → non-feistal

Plaintext
↳ 128-bit



Nr	key Size
10	128
12	192
14	256

$$d = X\left(S_{RC}\right)^{-1} \oplus Y$$

Subbyte : →

$53 \rightarrow 00101011$

$x^5 + x^3 + x + 1$

$01 \quad x^8 + x^4 + x^3 + x + 1$

$x^3 \quad 10 \quad x^5 + x^3 + x + 1$

$0 + x^3 \qquad x^6 + 1$

x^3

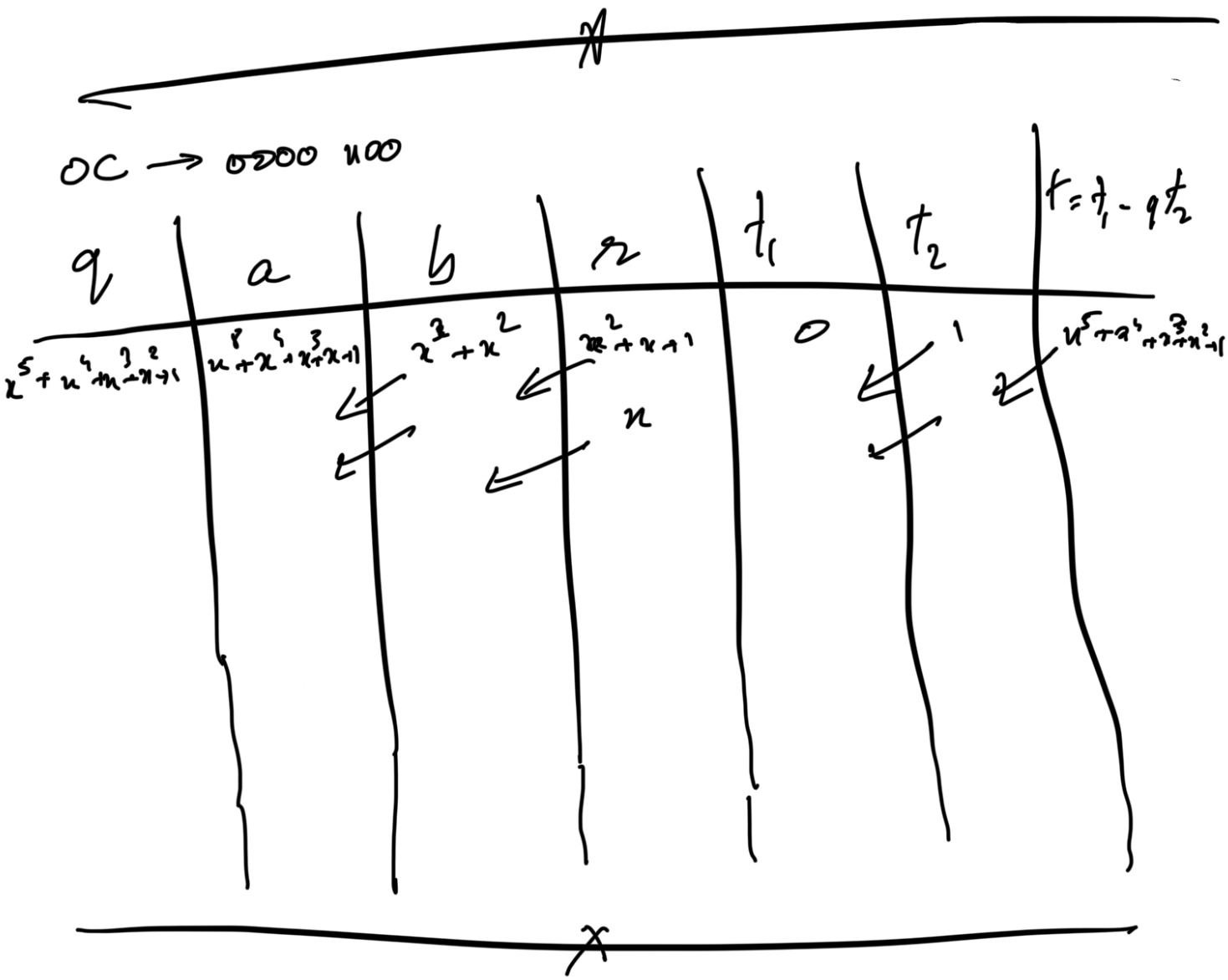
$x^5 + x^3 + x + 1 \;)\; x^8 + x^4 + x^3 + x + 1$

$x^8 + x^6 + x^4 + x^3$

$x^3 \;)\; x^6 + 1 \;(\; x^3$

$x^6 + x^3$

x^3



Shift Row

↳ Rolling left shift.

↳ Row 0 times

↳ " 1 "

↳ " 2 "

" 3 "

Mixed column

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$

Addround.