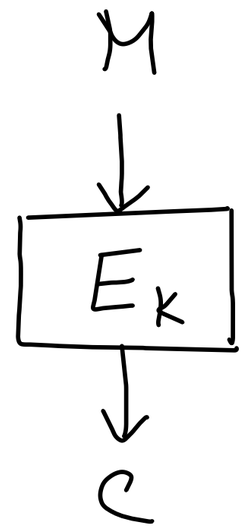
Block Cipher

Block: An n-bit string.

$$E: \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$$

k: Key; $\{0,1\}^n$: i/p block; $\{0,1\}^n$: o/p block



$\forall K \in \{0,1\}^k$, the map $E_K(\cdot)$ should be a permutation.

$\begin{cases} E^{-1} := D \\ \uparrow \\ \text{(decryption)} \end{cases}$

Attacks against A block-Cipher

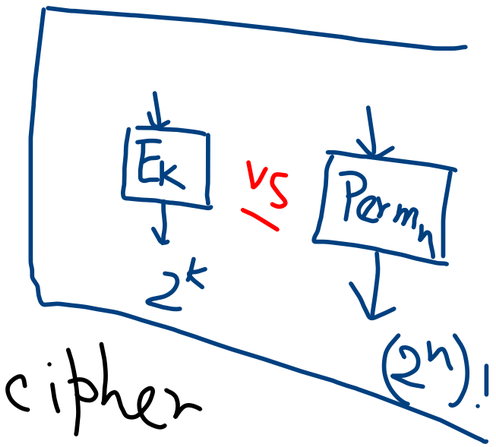
- Key Recovery
- Message Recovery
- Distinguish from a random permutation

Power
- Known P/T
- Chosen P/T
- Chosen C/T

Security

An adversary should not be able to (computationally) distinguish the block cipher from a random permutation.

(Strongest Notion)



Designing Block-Ciphers

$$C_1 = K_1 M_1 + K_2 M_2 + K_3 M_3 + K_4 K_1 M_4$$

$$C_1 = K_1 K_2 K_3 K_4 M_1 + (K_2 K_3 + K_1 K_4) M_2 + \text{---}$$

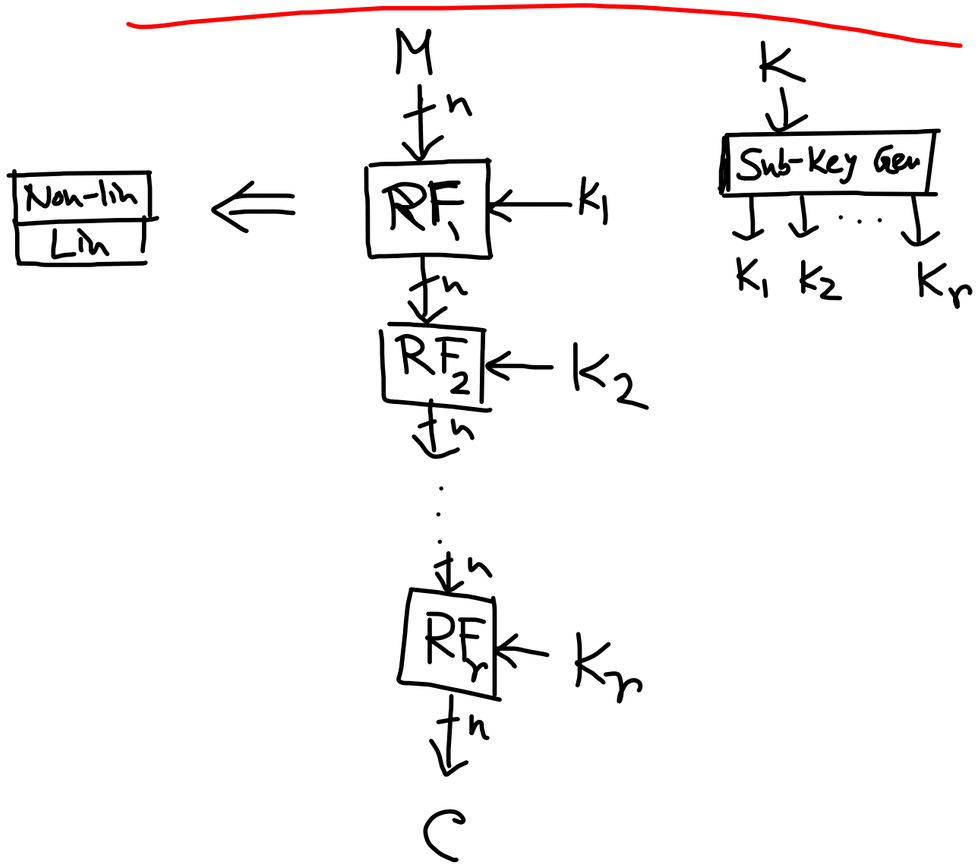
Shannon [1949]

- Confusion
- Diffusion

(Confusion: It would be very difficult to have a relation between the key & the ciphertext) → Non-linearity

(Diffusion: A single-bit change in the I/P should change roughly half of the C/T bits) → Linear

Iterative Structure

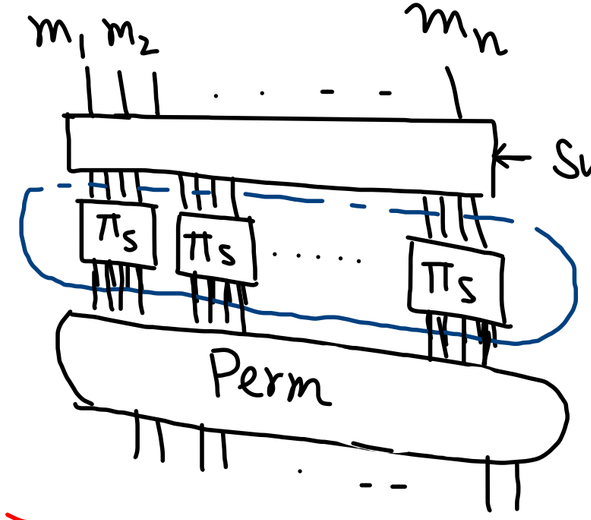


Block Cipher Design

└ SPN based (Substitution-Permutation Network)

└ Feistel

SPN



Assume, $n = s.b$

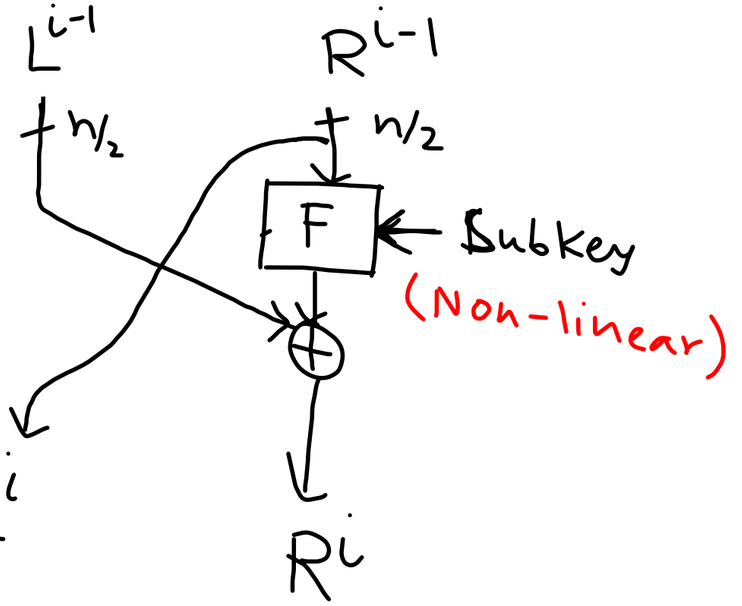
$\pi_S : \{0,1\}^s \rightarrow \{0,1\}^s$

Typical choices

$\begin{cases} n = 128 \Rightarrow s = 4/8 \\ n = 64 \Rightarrow s = 4 \end{cases}$

Feistel

(Luby-Rackoff construction)



- F^{-1} not required
- F is applied partially on the state.
- F is a non-linear function on n/2 bits.

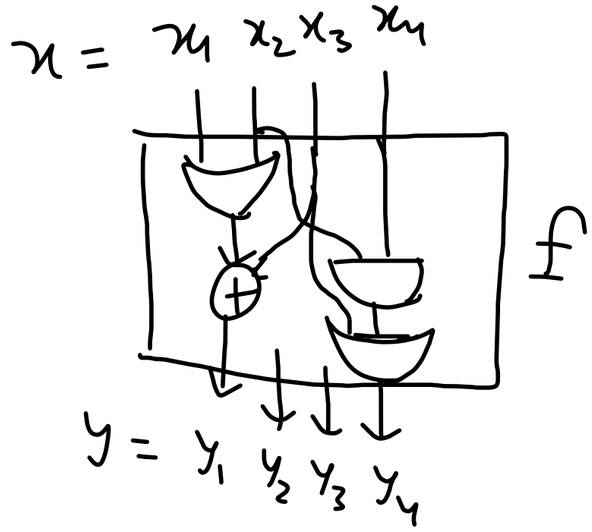
Non-linear functions

$GF(2^n)$

- Boolean functions (AND, OR gate)
- Integer addition
- Inverse / Field Multiplication
- S-Box (Substitution Box)

x	0	1	2	. . . .	F
S(x)	A	2	4		B

Look-up table representation



$y = f(x)$

f is Linear when

$f(x \oplus x') = f(x) \oplus f(x')$

$y_1 = x_1 \oplus x_3$
$y_2 = x_4$
$y_3 = x_4 \oplus x_2 \oplus x_4$
$y_4 = x_2 \oplus x_3$

$y_1 = x_1 x_2 x_3 \oplus x_3 x_4 \oplus 1$
$y_2 = x_3 x_4$
$y_3 = x_2$
$y_4 = x_1 x_2$

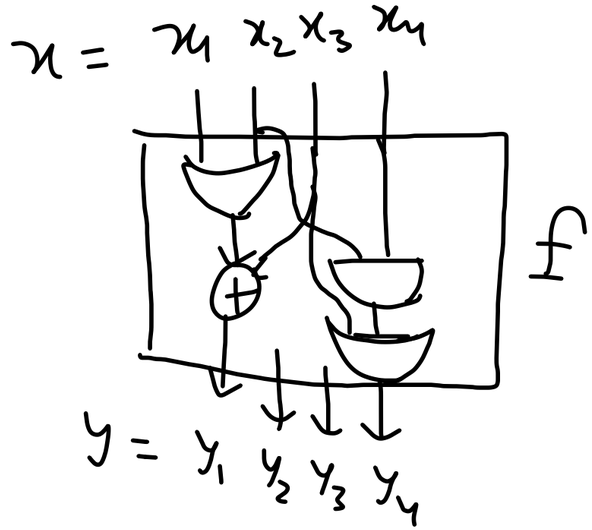
Non-linear functions

$GF(2^n)$

- Boolean functions (AND, OR gate)
- Integer addition
- Inverse / Field Multiplication
- S-Box (Substitution Box)

x	0	1	2	. . . .	F
S(x)	A	2	4		B

Look-up table representation



$y = f(x)$

f is Linear when

$f(x \oplus x') = f(x) \oplus f(x')$

$y_1 = x_1 \oplus x_3$
$y_2 = x_4$
$y_3 = x_4 \oplus x_2 \oplus x_4$
$y_4 = x_2 \oplus x_3$

$y_1 = x_1 x_2 x_3 \oplus x_3 x_4 \oplus 1$
$y_2 = x_3 x_4$
$y_3 = x_2$
$y_4 = x_1 x_2$

$GF(2^8) \Rightarrow x^8 \oplus x^4 \oplus x^3 \oplus x \oplus 1$ (primitive polynomial)

Binary Representation	Hex representation	Polynomial Representation
(19) 0001 0011	13	$(x^4 \oplus x \oplus 1)$
1100 1011	CB	$(x^7 \oplus x^6 \oplus x^3 \oplus x \oplus 1)$

02 ⊙ CB (Mult) → NL

$= x(x^7 \oplus x^6 \oplus x^3 \oplus x \oplus 1)$

$= x^8 \oplus x^7 \oplus x^4 \oplus x^2 \oplus x$

$= (x^4 \oplus x^3 \oplus x \oplus 1) \oplus x^7 \oplus x^4 \oplus x^2 \oplus x$

$= x^7 \oplus x^3 \oplus x^2 \oplus 1$

$= 8D$

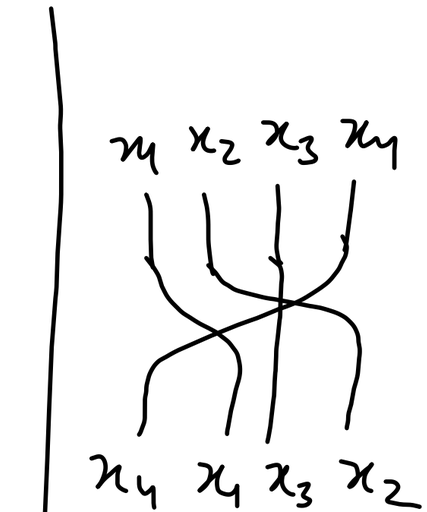
$(02)^{-1}$ inverse → NL

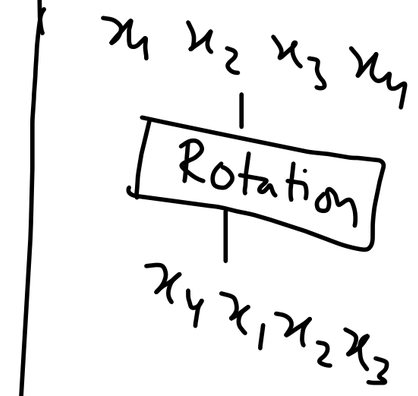
$(02) \cdot \alpha = 01$

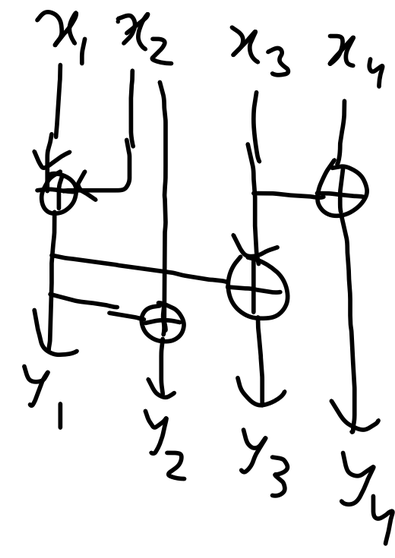
Hex
0000 → 0
.
.
.
1000 → 8
1001 → 9
1010 → A
1011 → B
1100 → C
1101 → D
1110 → E
1111 → F

Linear Operations

- Bit Permutation
- XOR
- Rotation (BP)
- Matrix Multiplication







Linear Operations

- Bit Permutation
- XOR
- Rotation (BP)
- Matrix Multiplication

✓

Ref: - Sasaki (Book)
- Rijndael Block Cipher