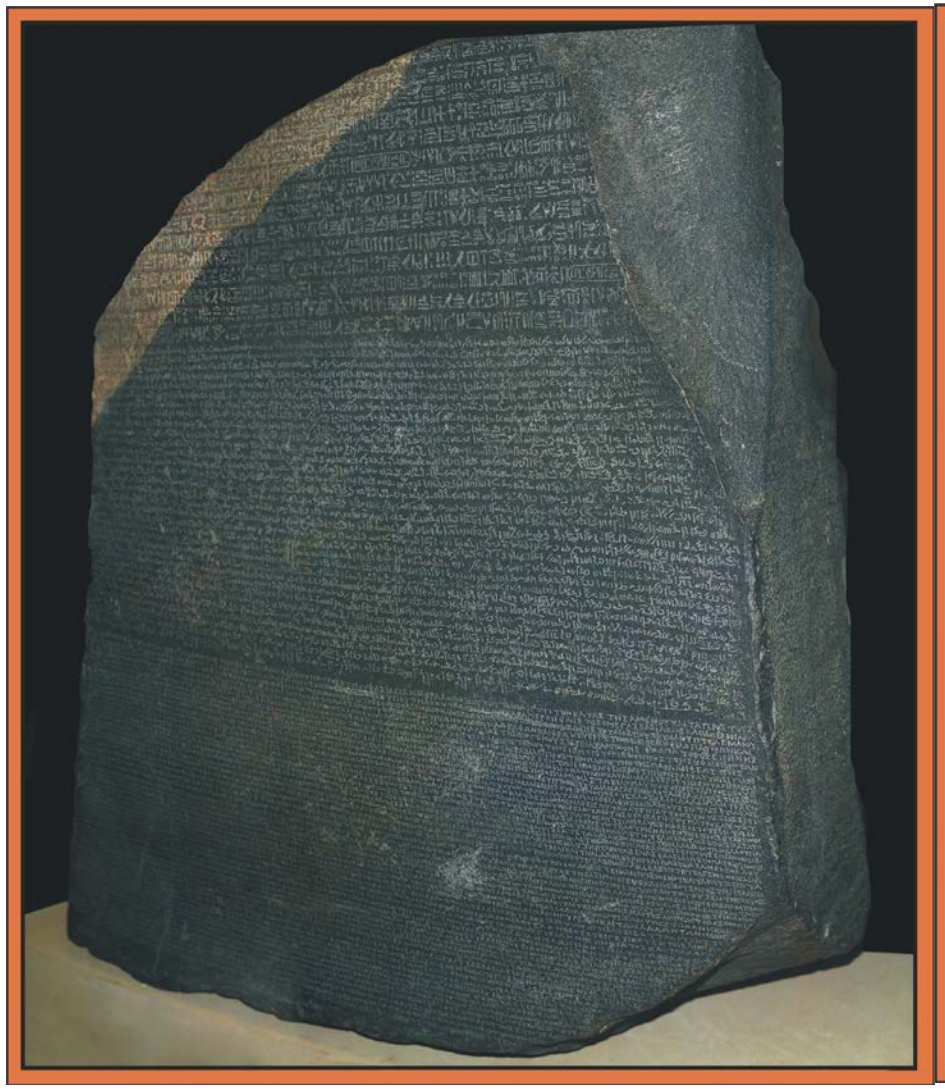
Cryptography

Prof. Dr. Eşref ADALI

www. Adalı.net

History (Reşit (Rosetta, 1799)

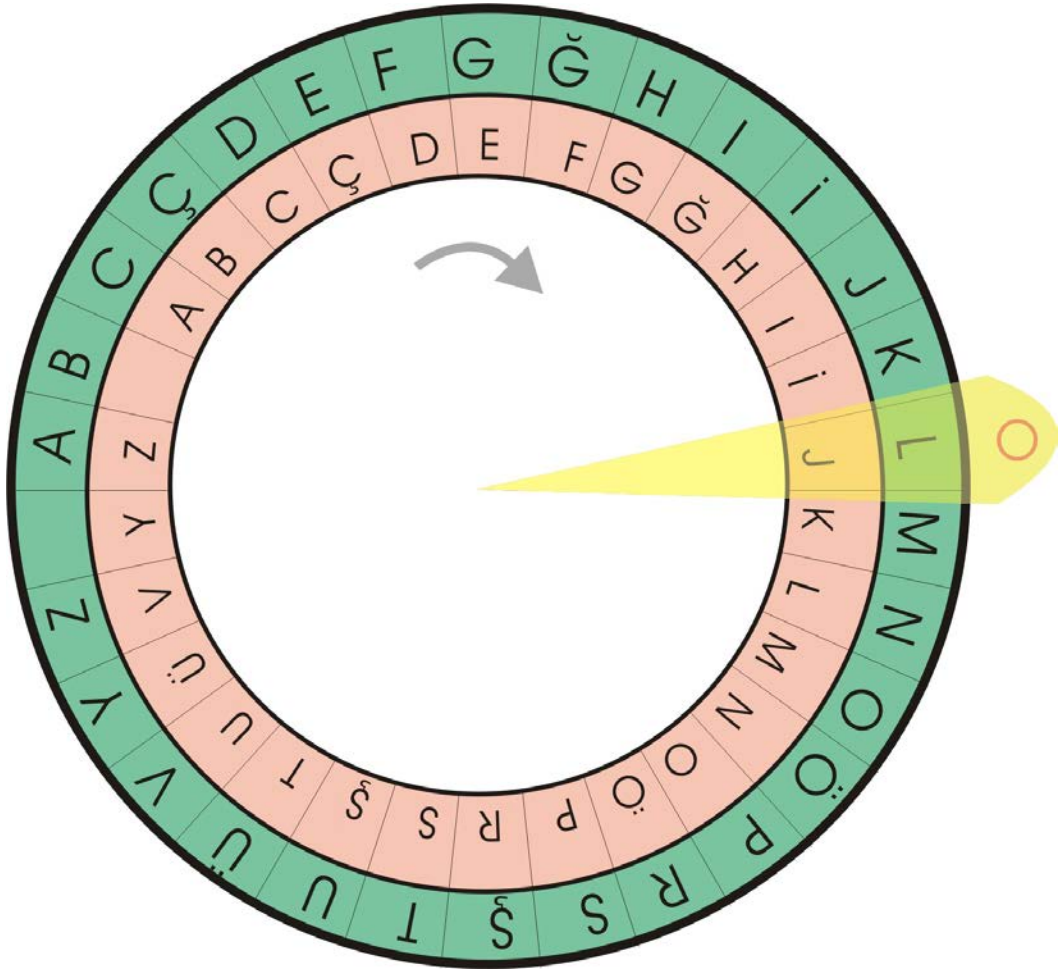
Greek Demotic hieroglyph



Sezar’s Algorithm

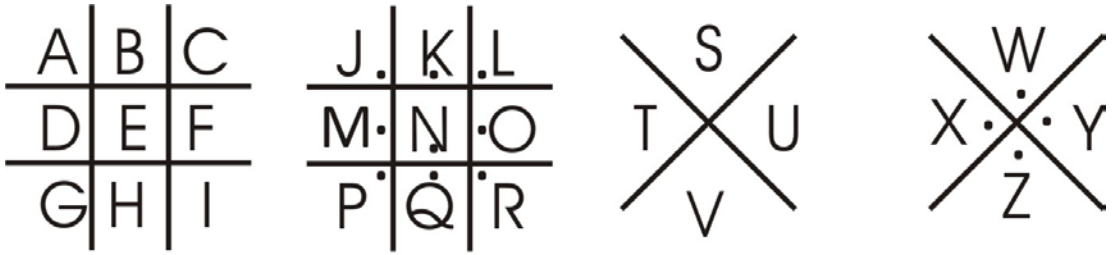
Uses alphabet (Phoenician, Latin or Arabic)

Each character is shifted n step



Pigpen Cipher

This cipher method was used in Masonic community



Old Turkish Cipher

(Ebced)

A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L
1	20	30	40	700	500	2	50	4	3	600	800	70	60	1000
M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	space
70	200	300	80	400	8	6	9	7	10	900	5	90	100	2000

Plain text: Eren okula gidecek

Enciphered text : 50085 00200 30060 10100 01508 00700 50030 50060

Ertuğ Cipher

Basic Terms of Cryptography

Plain text : Original form of text . It can be read.

Encrypting : Operation of encrypting of plain text. Produce encrypted text that cannot be read.

Decrypting : Operation of decrypting of encrypted text. Produce plain that can be read.

Key : Key for encryption and also decryption.

Algorithm : The algorithm for encryption and decryption process

Cryptography : Science of cryptography

Cryptanalysis : Study of solving a cryptography algorithm.

Zimmermann Telegram

	A	D	F	G	V	X
A	B	2	E	5	R	L
D	I	9	N	A	1	C
F	3	D	4	F	6	G
G	7	H	8	J	O	K
V	M	O	P	Q	S	T
X	U	V	W	X	Y	Z

E	R	E	N	O	K	U	L	A	G	İ	D	E	C	E	K
AF	AV	AF	DF	GV	GX	XA	AX	DG	FX	DA	FD	AF	DX	AF	GX

AFAVAF DFGVGX XAAXDG FXDAFD AFDXAF GX

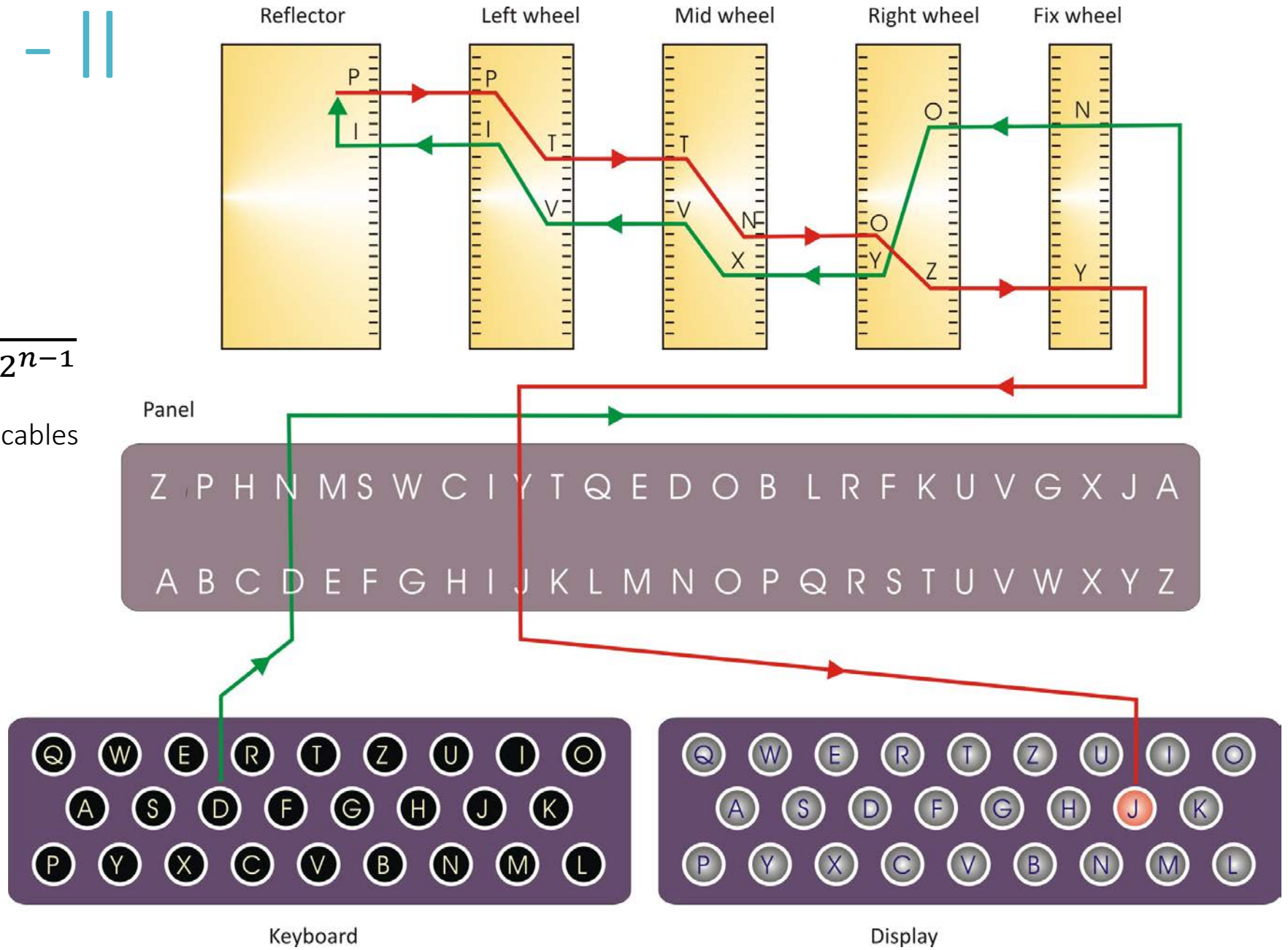
Enigma - I

- Design and developed by Artur Scherbius, in 1918 and widely used in II. War.
- It was the first electromechanical cryptography machine.
- It was the first nonlinear cryptography machine

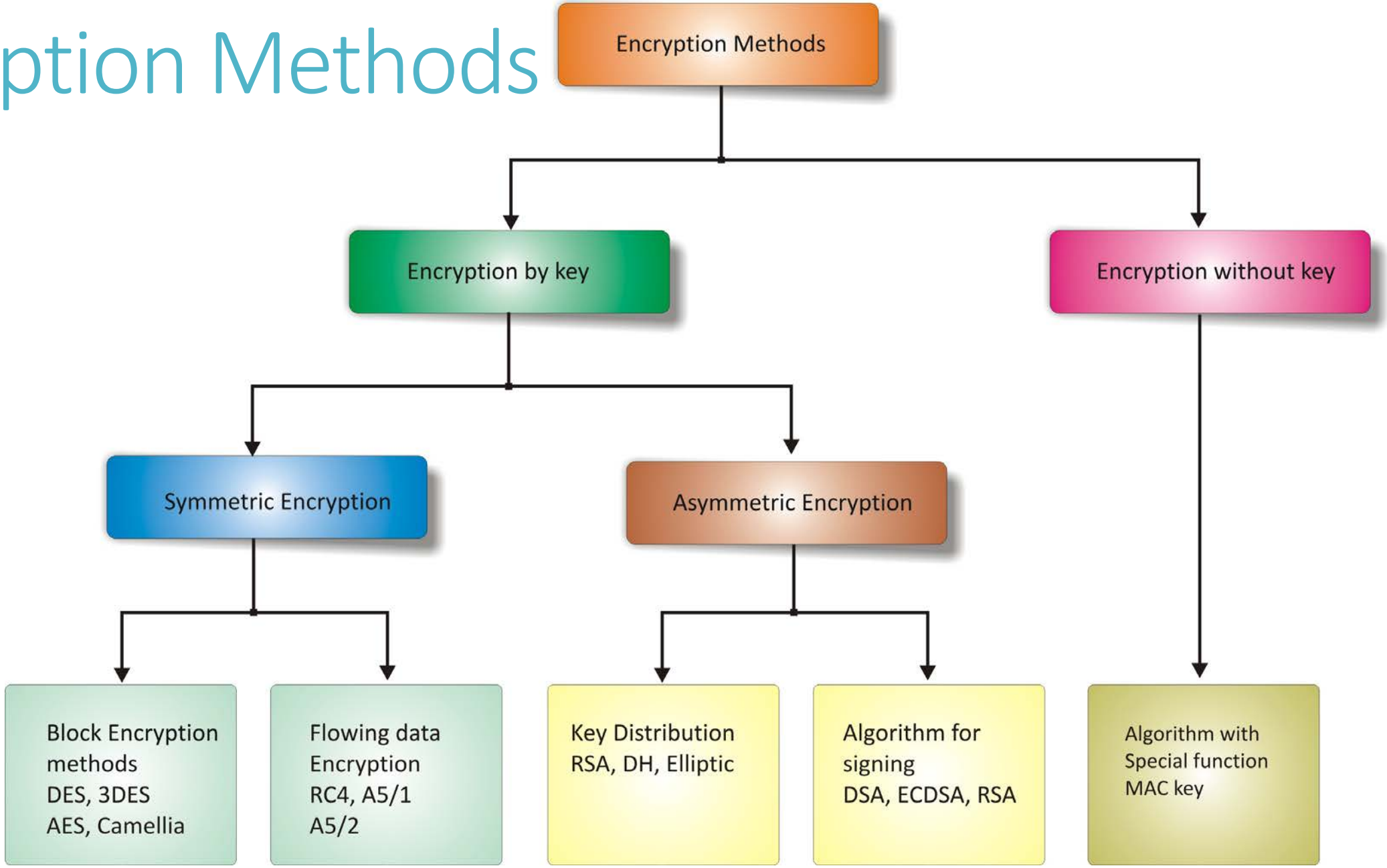
Enigma - II

$$n = \frac{26!}{n!(26-2n)!2^{n-1}}$$

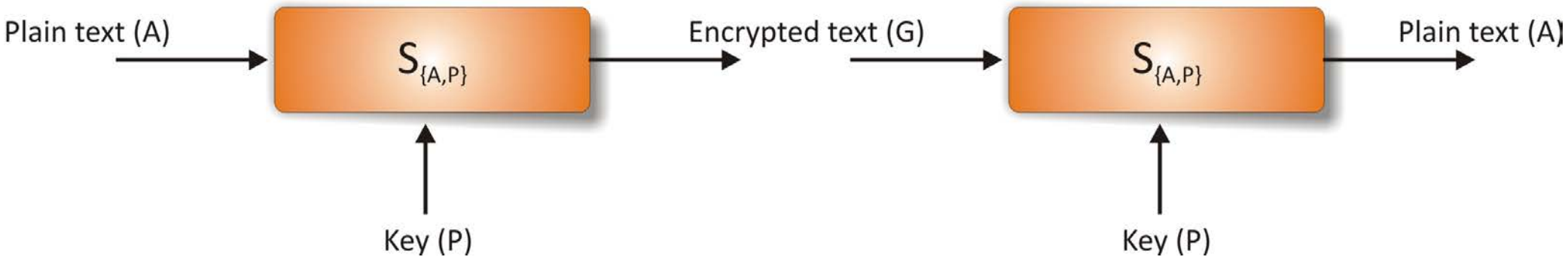
n is the number of cables



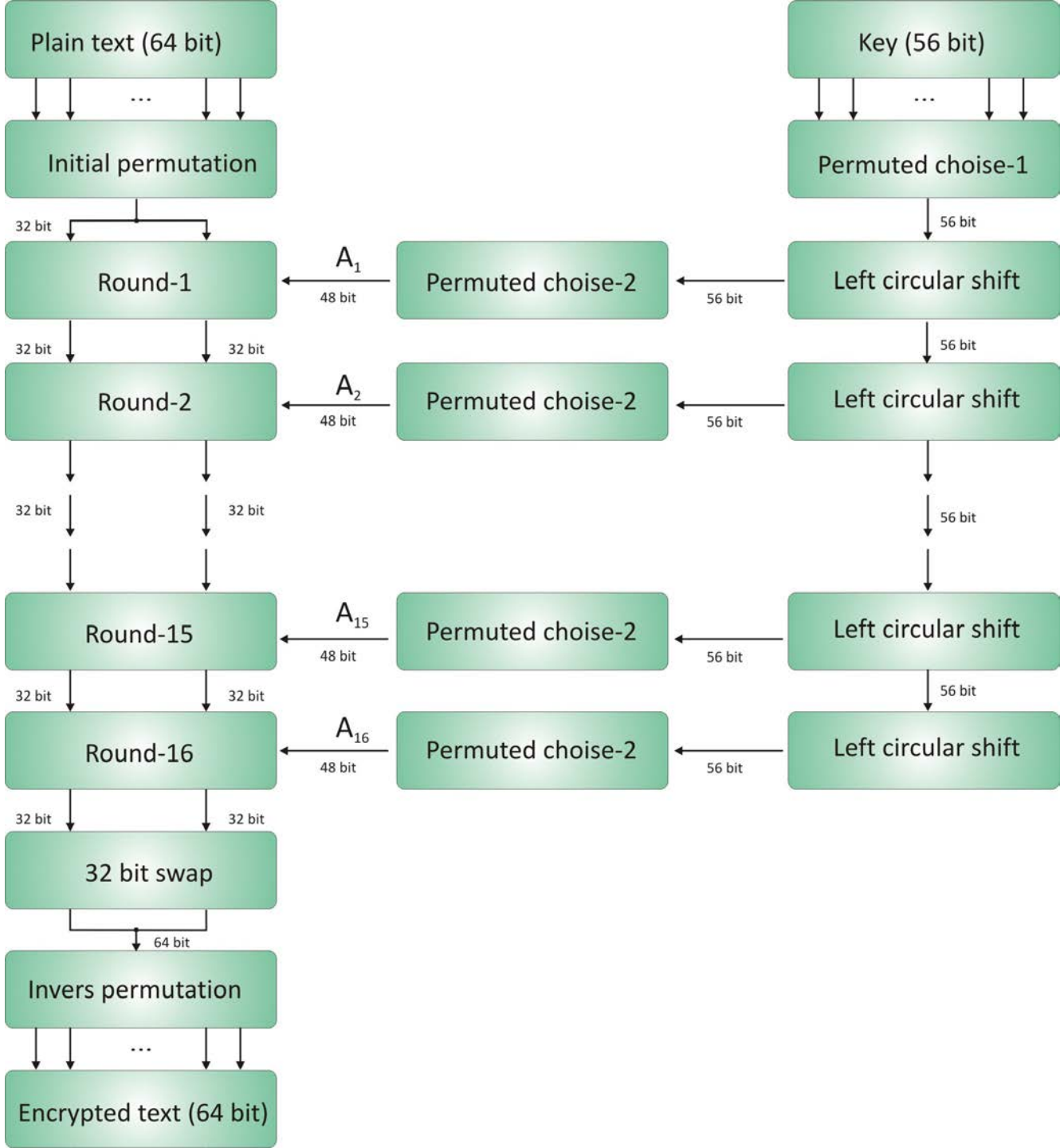
Encryption Methods



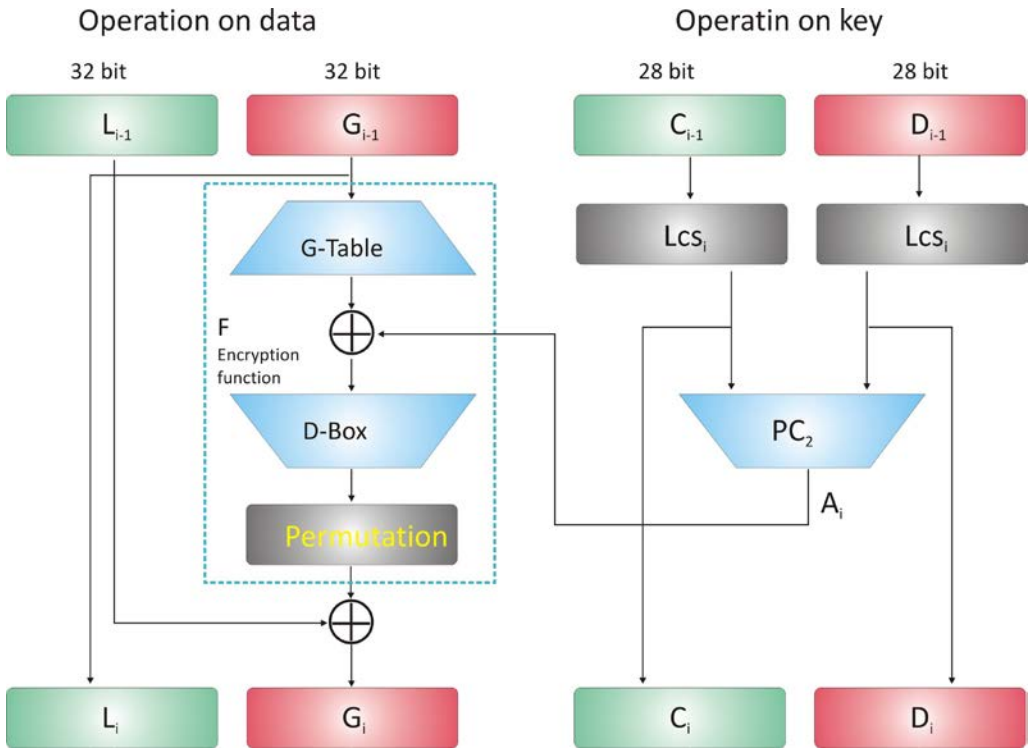
Symmetric Algorithm



DES - I

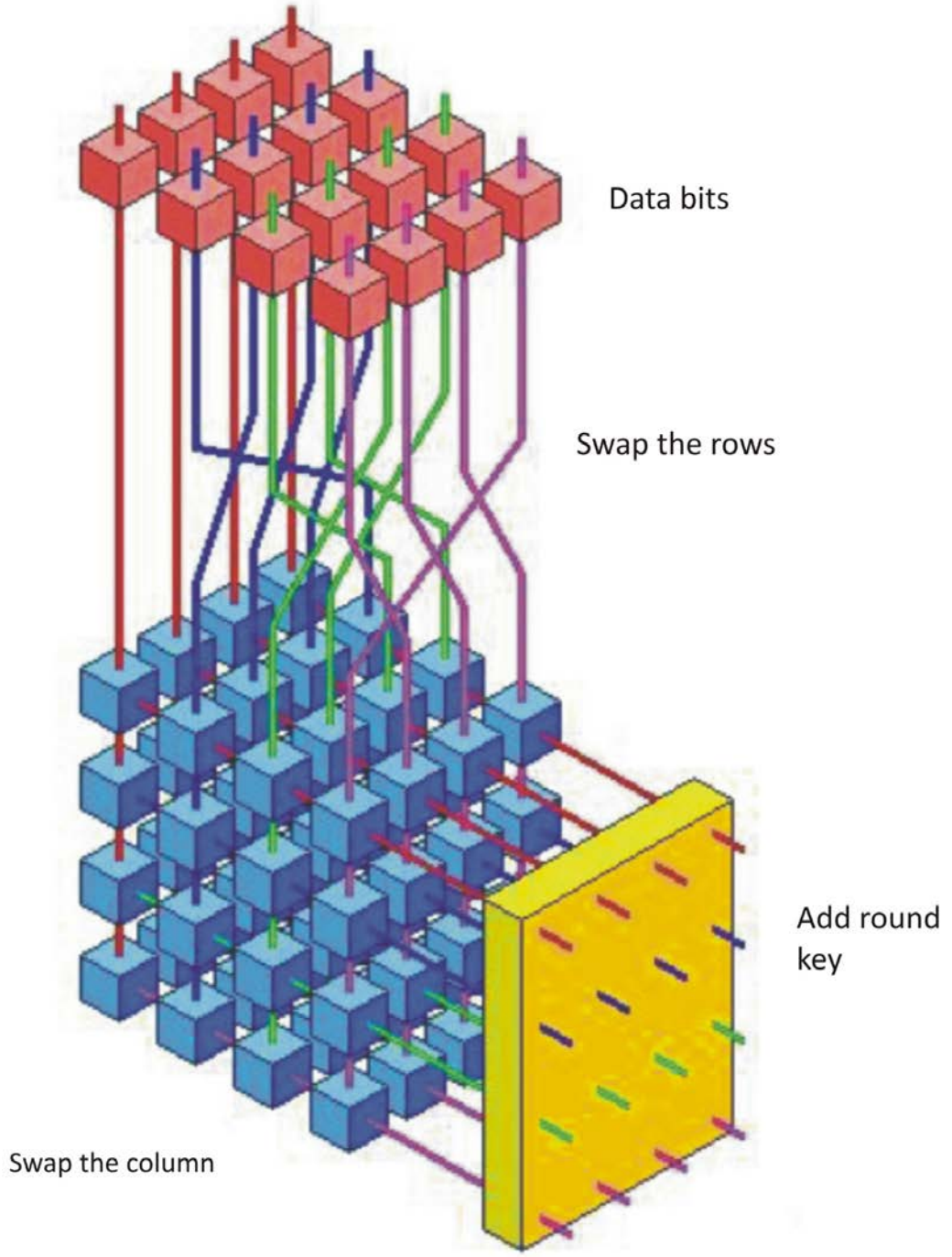

Plain text (64 bit)
Initial permutation
32 bit
Round-1
32 bit
32 bit
Round-2
32 bit
32 bit
Round-15
32 bit
32 bit
Round-16
32 bit
32 bit
32 bit swap
64 bit
Invers permutation
Encrypted text (64 bit)
A1
48 bit
A2
48 bit
A15
48 bit
A16
48 bit
Permuted choise-2
56 bit
Permuted choise-2
56 bit
Permuted choise-2
56 bit
Permuted choise-2
56 bit
Key (56 bit)
Permuted choise-1
56 bit
Left circular shift
56 bit
Left circular shift
56 bit
Left circular shift
56 bit
Left circular shift

DES - II



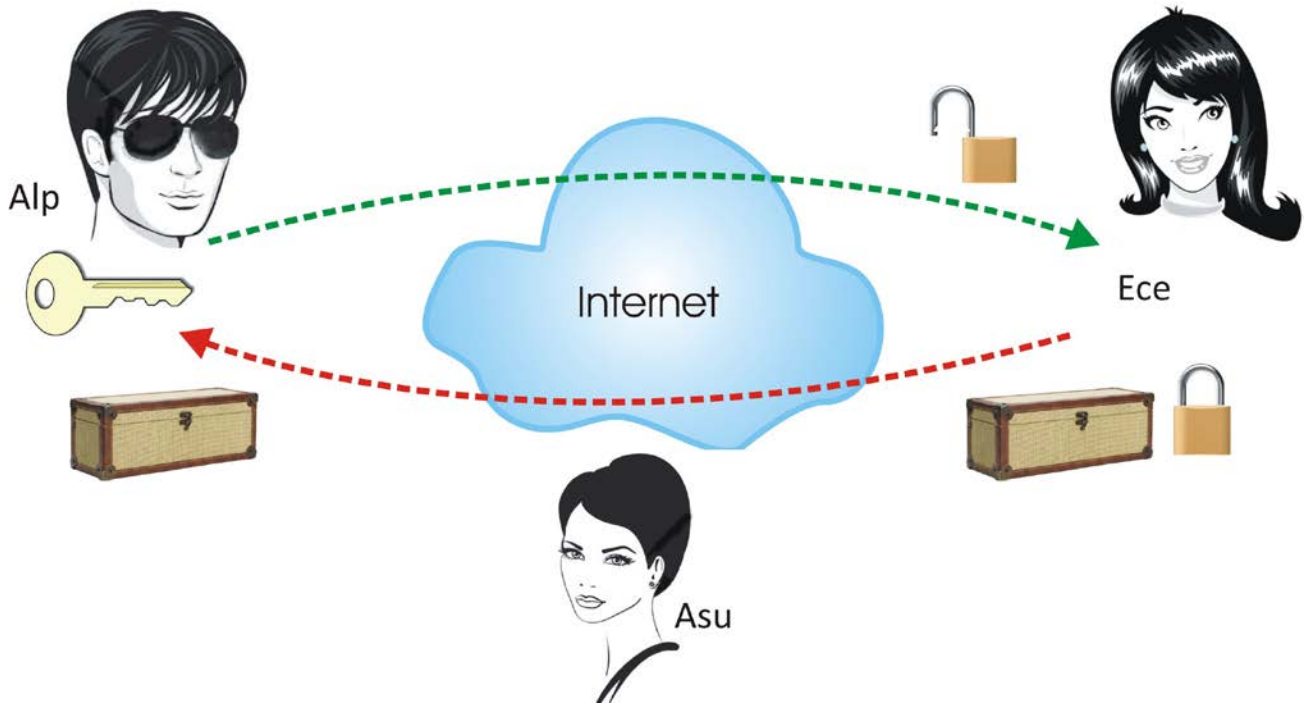
One round operation of DES

$L_i = R_{i-1}$ $R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$



Asymmetric Algorithm (RSA)

- The first work had been started by James Ellis at GCHQ'de (Government Communication Headquarter), 1960. This Project was completed by contribution of Clifford Cocks and Malcolm Williamson, in 1975. The report of this Project was published in 1997.
- Diffie-Hellman published a theoretical paper, in 1976, title "New Directions in Cryptography". His theory was implemented by Ralph Marke, in 2002.
- In 1977 , three young sciences Ron Rivest, Adi Samir and Len Adleman worked on Diffi-Hellman theory and implement it and gave the name RSA to the methods.



P and d are prime number

$n = p \times q$

$\varphi(n) = (p-1)(q-1)$

$1 < e < \varphi(n)$ e is integer and not divider of n. n and e are elements of public key

d is private key

$$d = \frac{2\varphi(n) + 1}{e}$$

Example for RSA)

p = 53 and q = 59 are chosen

n = p x q = 53 x 59 = 3127

$\varphi(n) = (p-1)(q-1) = (53-1)(59-1) = 3016$

1 < e < (n)

for simplicity e = 3 chosen.

So the component of public key are n = 3127 and e = 3

and private key is

$$d = \frac{2\varphi(n)+1}{e} = \frac{2(3016)+1}{3} = 2011$$

Encryption Phase

Ece want to send 'A' to Alp

ASCII code of 'A' is 65

$C = 65^e \bmod n = 65^3 \bmod 3127 = 274.625 \bmod 3127 = 2.576$

C represents ciphered character. It is residue of 2.576 mod 3127

Ece sent to Alp 'C'

Decryption Phase

Alp read 2.576 with his private key

Plain text is $= C^d \bmod n$

Plain text $= 2.574^{2011} \bmod 3127 = 65$

So Alp read 'A'

Performance of Algorithm

Test-1	Data length (KB)	Algorithm	Encryption time (s)	Decryption time (s)
1	153	DES	3	1,1
		AES	1,6	1
		RSA	7,3	4,9
2	196	DES	2	1,24
		AES	1,7	1,4
		RSA	8,5	5,9
3	312	DES	3	1,3
		AES	1,8	1,6
		RSA	7,8	5,1
4	868	DES	4	1,2
		AES	2	1,8
		RSA	8,2	5,1

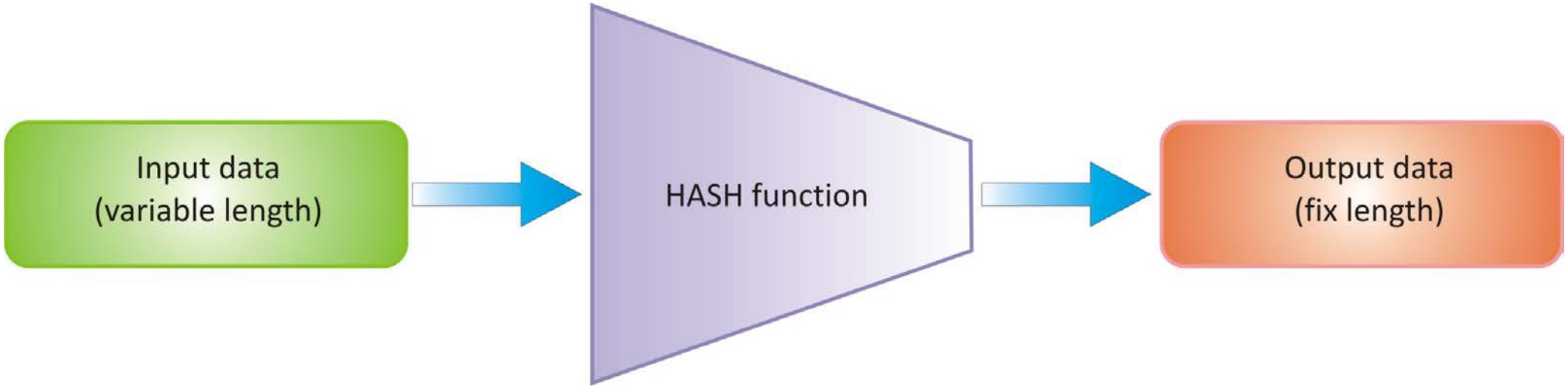
Data Integrity

- Data integrity in database
- Data integrity in communication

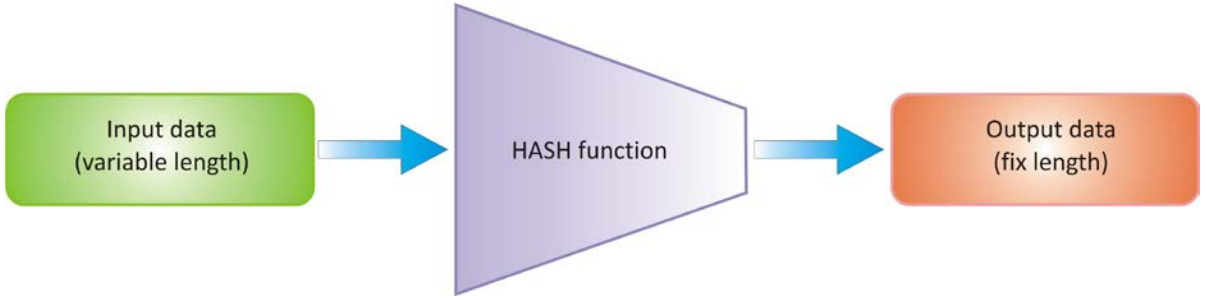
- Hashing for data integrity

Some checking methods

- Parity bit,
- Horizontal parity
- Vertical parity
- Hamming code
- CRC



HASH Function - 1



Hash function is written as

y = h(x) ; x is input and y is output

Hash function is one way function and Collision resistant

One way function : A one-way hash function is a function h satisfying the following conditions:

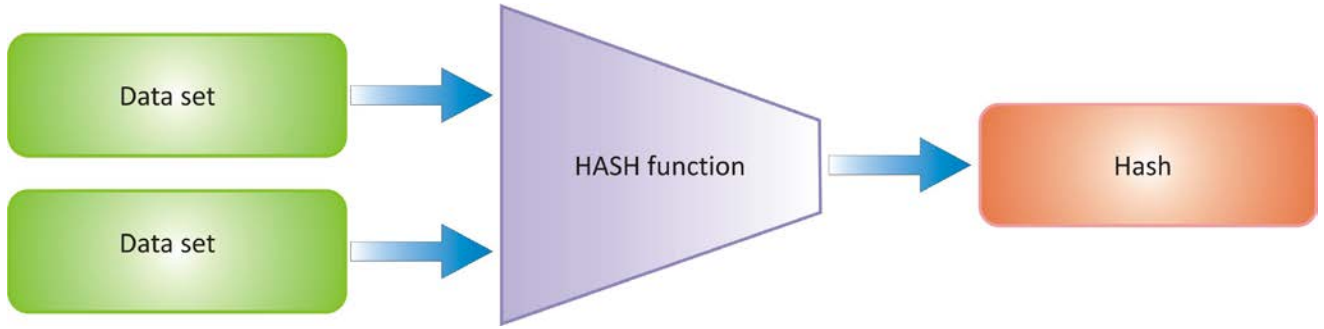
1. The argument x can be of arbitrary length and the result h(x) has a fixed length of n bits (with n ≥64).
2. The hash function must be one-way in the sense that given a y in the image of h, it is “hard” to find a message x such that h(x)=y, and given x and h(x) it is “hard” to find a message x’≠ x such that h(x’)=h(x)

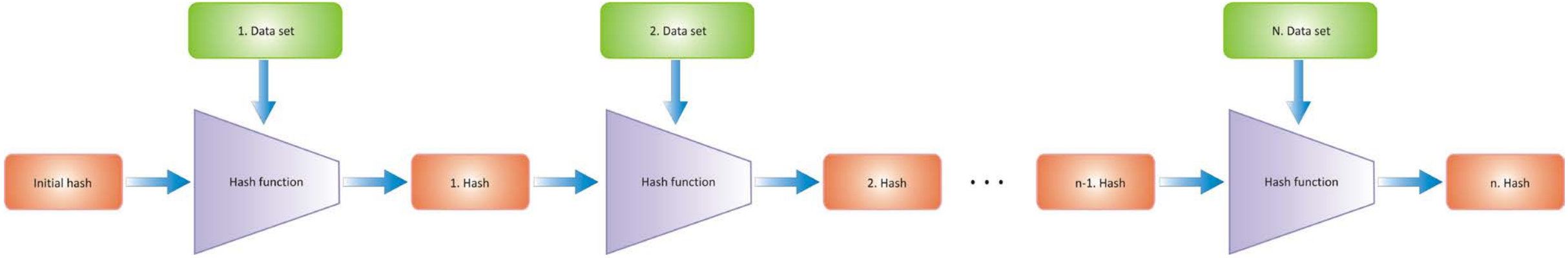
Collision resistant : The hash function must be collision resistant: this means that it is “hard” to find two distinct messages that hash to the same result.

If $y_1=h(x_1)$ and $y_2=h(x_2)$ then $y_1 \neq y_2$

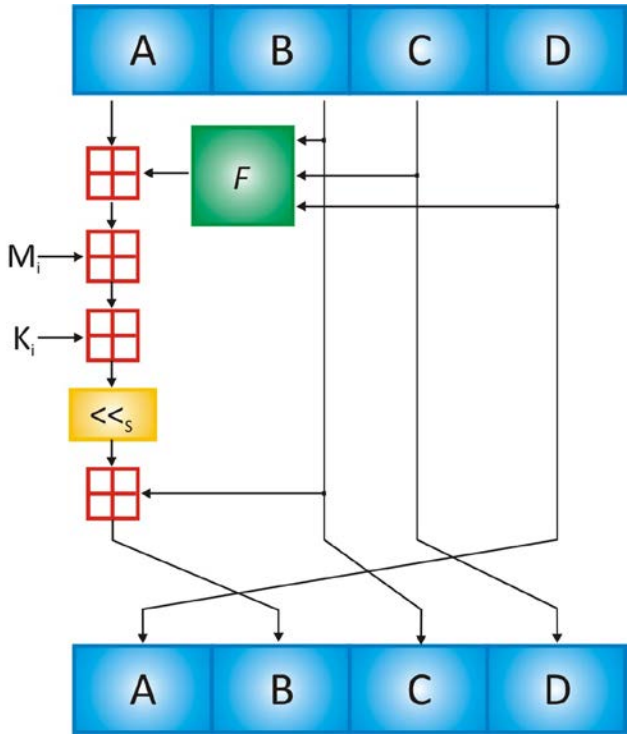
HASH Function - 2

- Hashing algorithm XOR two data set and left rotate then apply to nonlinear function
- Firstly, input data is divided blocks then applied to hash function





MD5 Hash Function

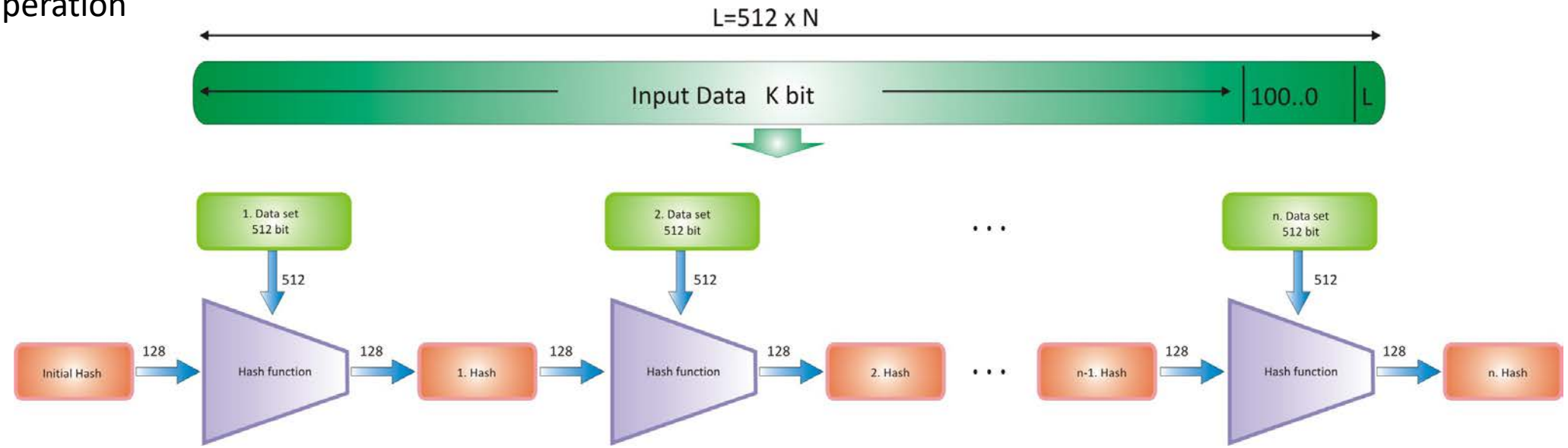


$F(B,C,D) = (B \wedge C) \vee (\neg B \wedge D)$
$G(B,C,D) = (B \wedge D) \vee (C \wedge \neg D)$
$H(B,C,D) = B \oplus C \oplus D$
$I(B,C,D) = C \oplus (B \vee \neg D)$

M_i is current data set, K_i is a constant for each round

⊞ is 32 bit adder

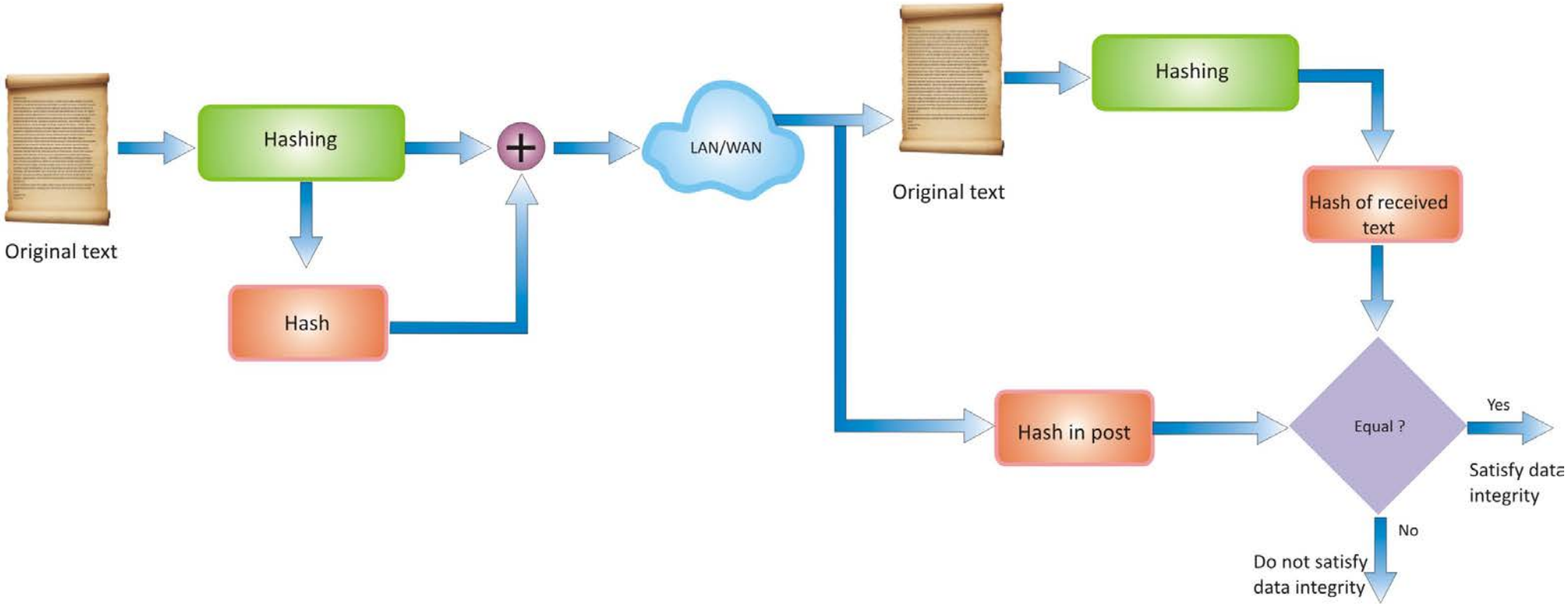
$<<_s$ shift operation



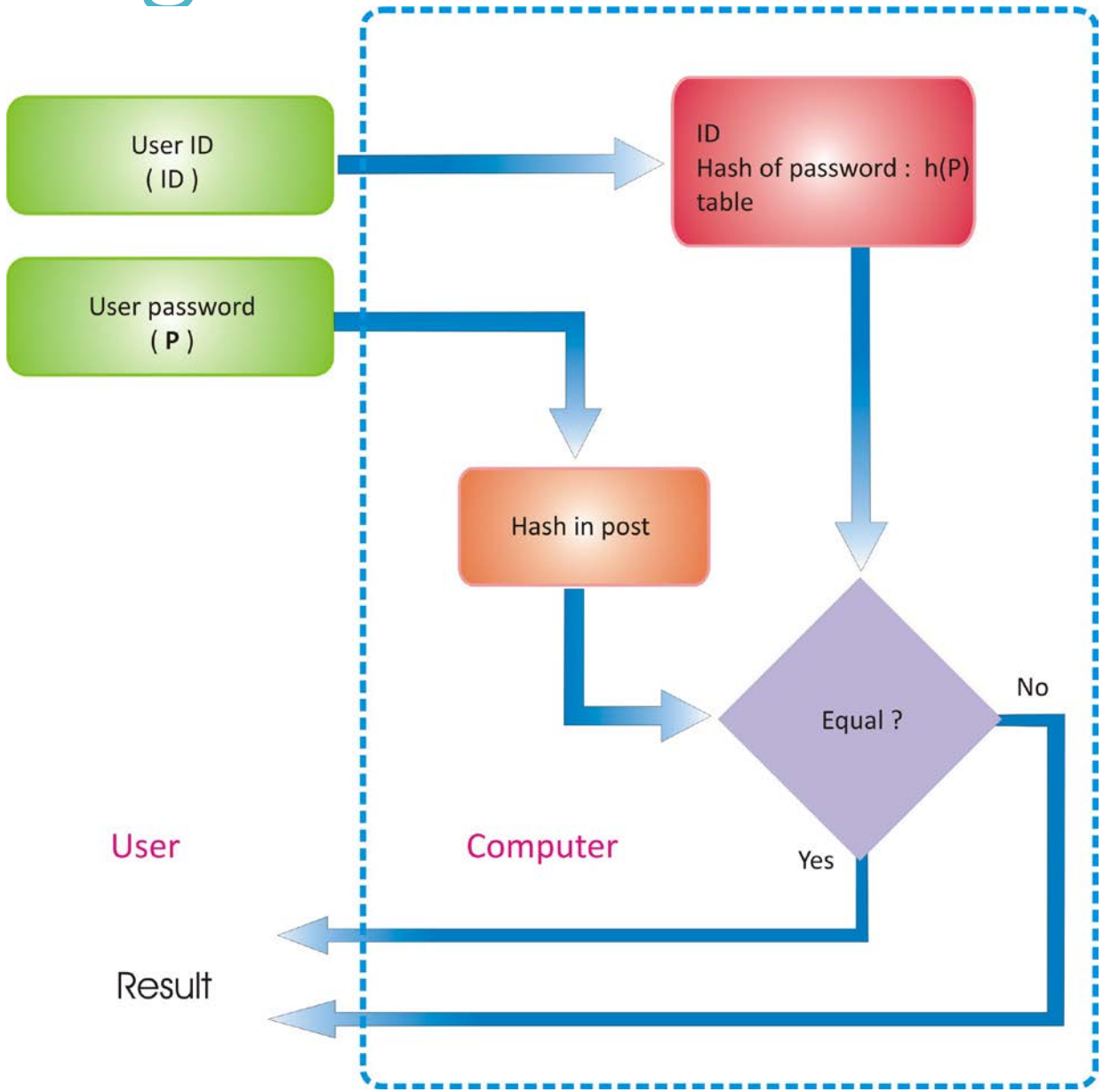
Application of Hash Function

- Data integrity
- Message verification
- One Time Password
- Digital signature

Data Integrity



Password Disguise



One Time Password