Modern Symmetric Cryptography

Part 1

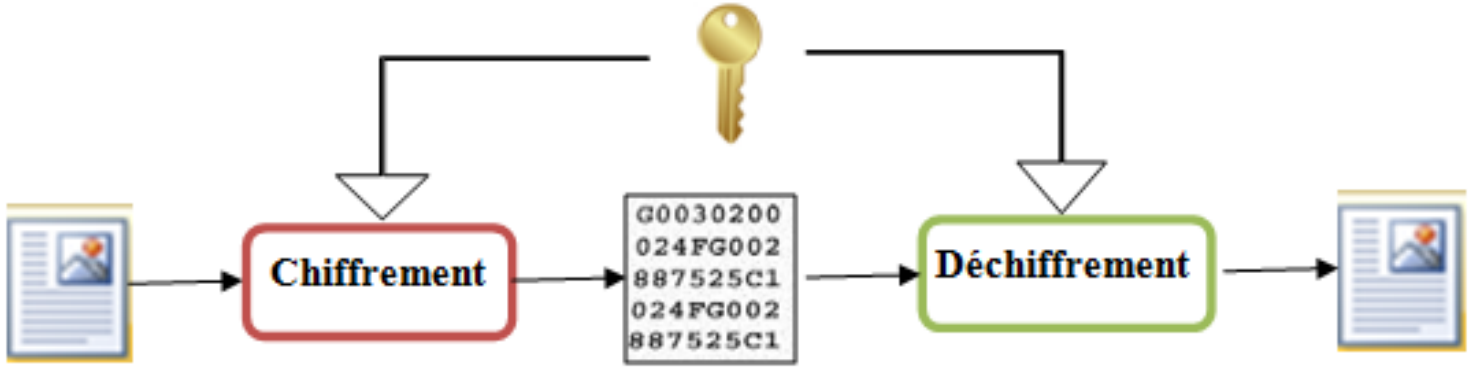
Pr. Noureddine Chikouche
noureddine.chikouche@univ-msila.dz
https://sites.google.com/view/chikouchenoureddine

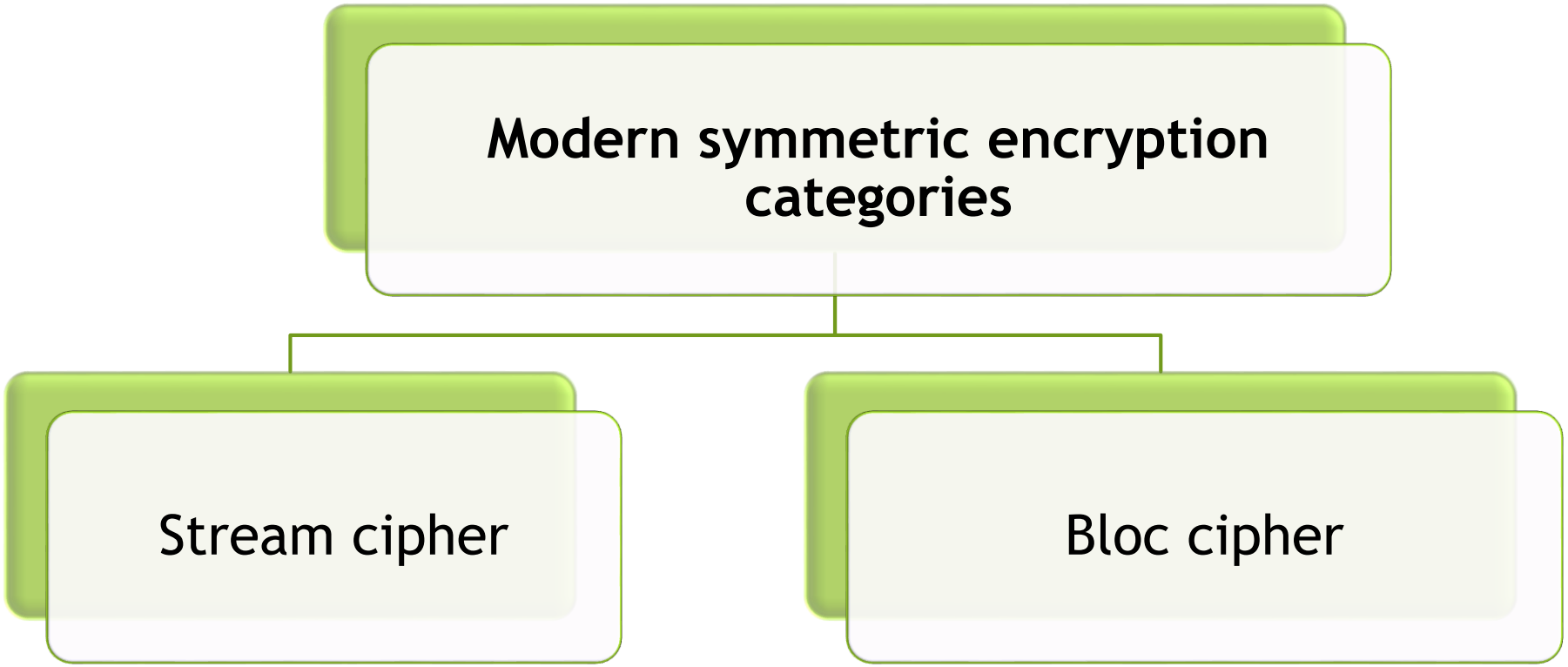
Course outline

- Introduction
- Modern symmetric encryption categories
  - Stream cipher
  - Block cipher
- Data Encryption Standard (DES)

Introduction

Symmetric cryptography




Modern symmetric encryption categories
Stream cipher
Bloc cipher

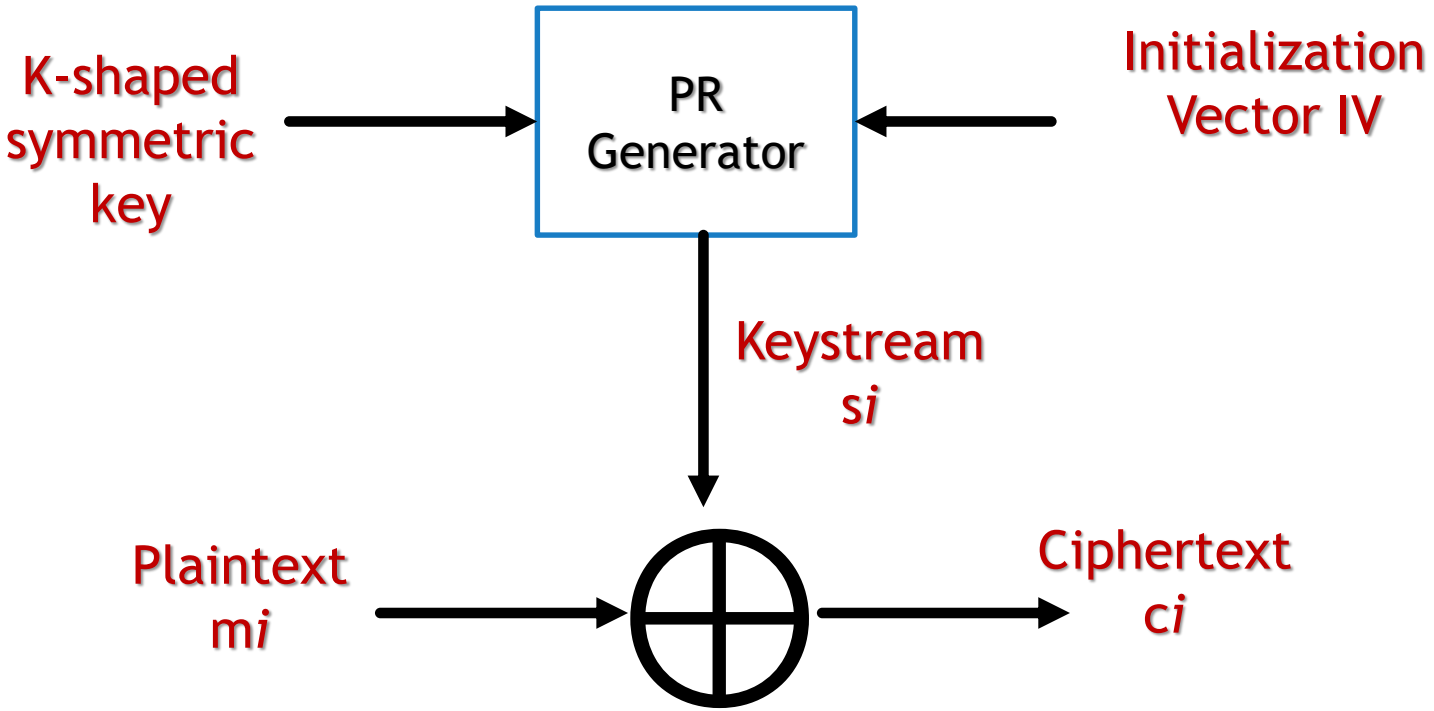
Stream cipher

- Each bit/byte of the clear message is encrypted with a new key called the *keystream*.
- Keystream is a sequence of bits generated from the symmetric key (K).

Stream cipher

- To generate a keystream we use a pseudo-random generator (PRG).
- The size of the generated key is equal to that of clear text.
- To encrypt a message, we use the principle of o*ne time pad (OTP*).
- Encryption function:
  - $c_i = E_{s_i}(m_i) = m_i \oplus s_i$
- Decryption function:
  - $m_i = D_{s_i}(c_i) = c_i \oplus s_i$

Stream cipher



Stream cipher: Example

- **Example:**
- Plaintext (*m*): 01010011 01000001
- Keystream(*s*) =01110111 01110111
- Encryption:

01010011 01000001

$\oplus$

01110111 01110111

=

0010010000110110

Stream cipher

- **Importance of stream ciphers:**
  - It is very fast.
  - Easy hardware and software implementation.
  - It is suitable for real-time applications.
- **Limitation:**
  - Error propagation problem (synchronization).

Stream cipher

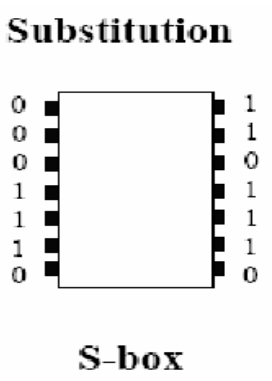
- RC4, used in particular by the protocol WEP to secure wireless networks.
- A5/1,used in mobile phones of the type GSM to encrypt radio communication between the mobile phone and the nearest cell tower,
- E0,used by the protocol Bluetooth.
- Others:

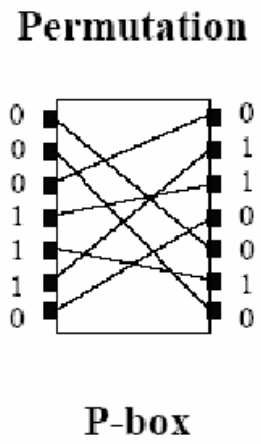
FISH - Helix·ISAAC·LEVIATHAN·MUGI·Panama·SEAL·SOBER·WAKE

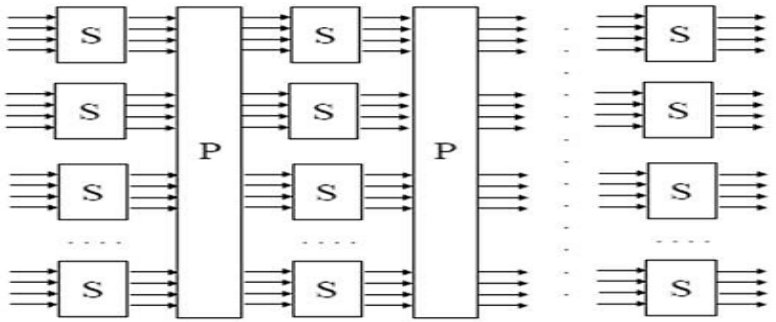
Block Cipher

Principle:

1. The message is divided into blocks of constant size,
2. The key is used to encrypt each block.
3. Each block is encrypted independently of the value of the other blocks.
4. It uses: substitution cipher (confusion) / transposition (broadcast)/ product (more robust).

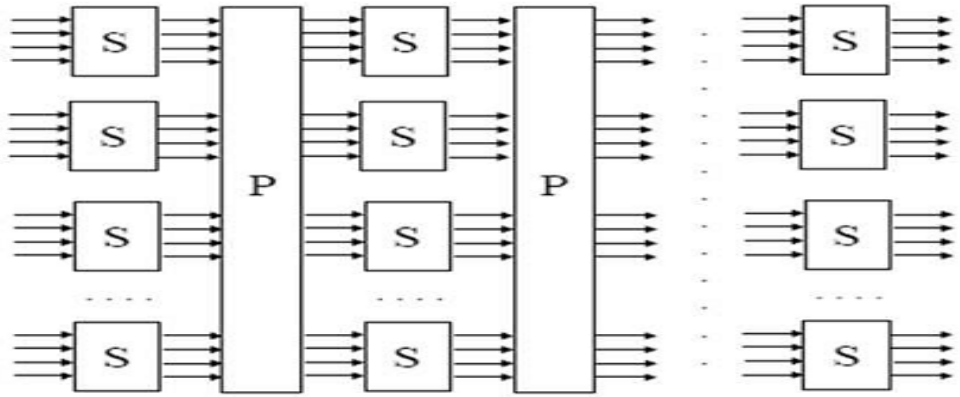






Block Cipher

- C. Shannon proved that the combination of confusion and diffusion provide adequate security.
  - Confusion (S-Box): hide the relationship between the plaintext and the ciphertext.
  - Distribution (P-Box): hide the redundancy by distributing the influence of one key bit over the entire ciphertext.

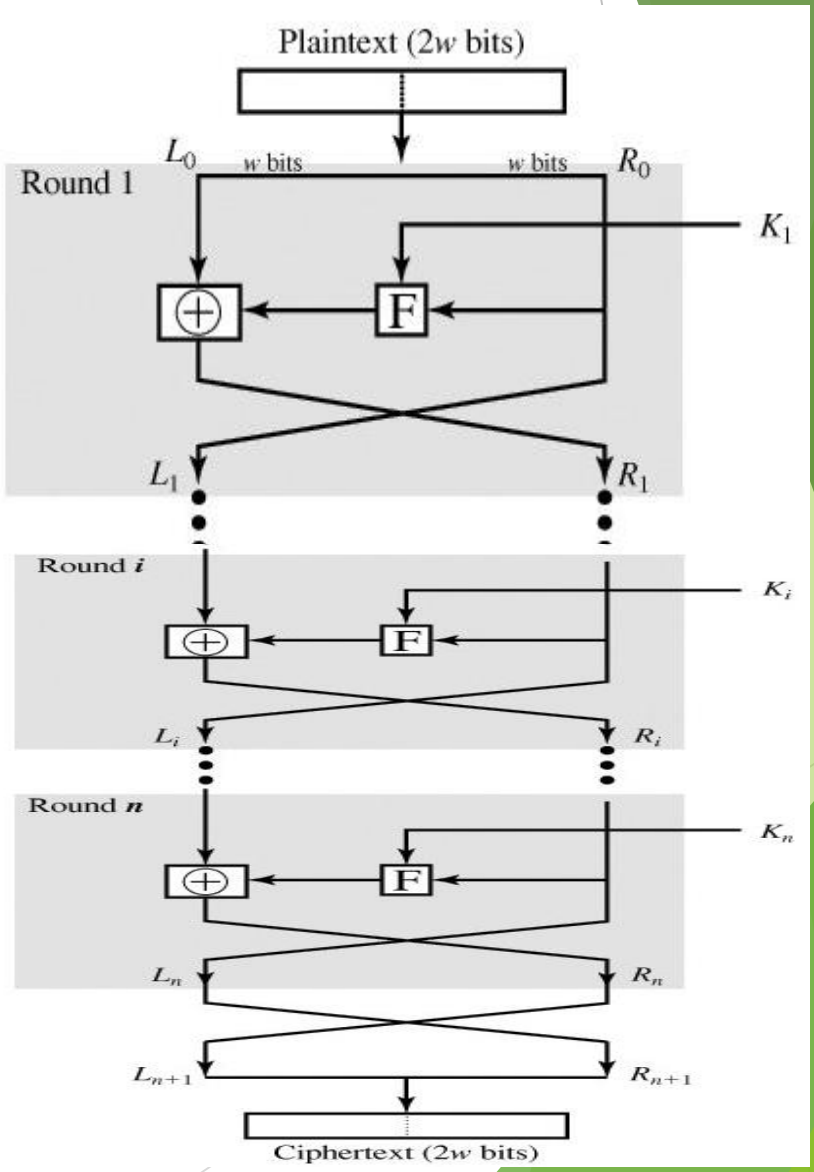


DES (Data Encryption Standard)

Feistel cipher structure

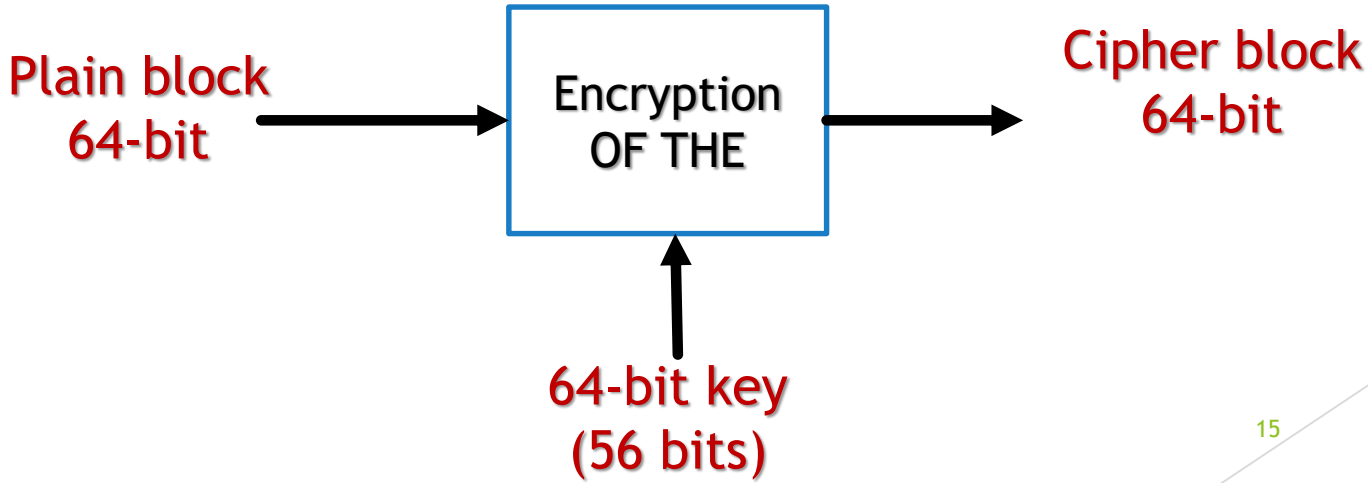
- Invented by Horst Feistel in 1973 (IBM).
- The length of the input is 2w (bits), that of the key is K.
- Divide the input into 2 halves L_{0} and R_{0}.
- For each round, we calculate the new, L_i and R_i.

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

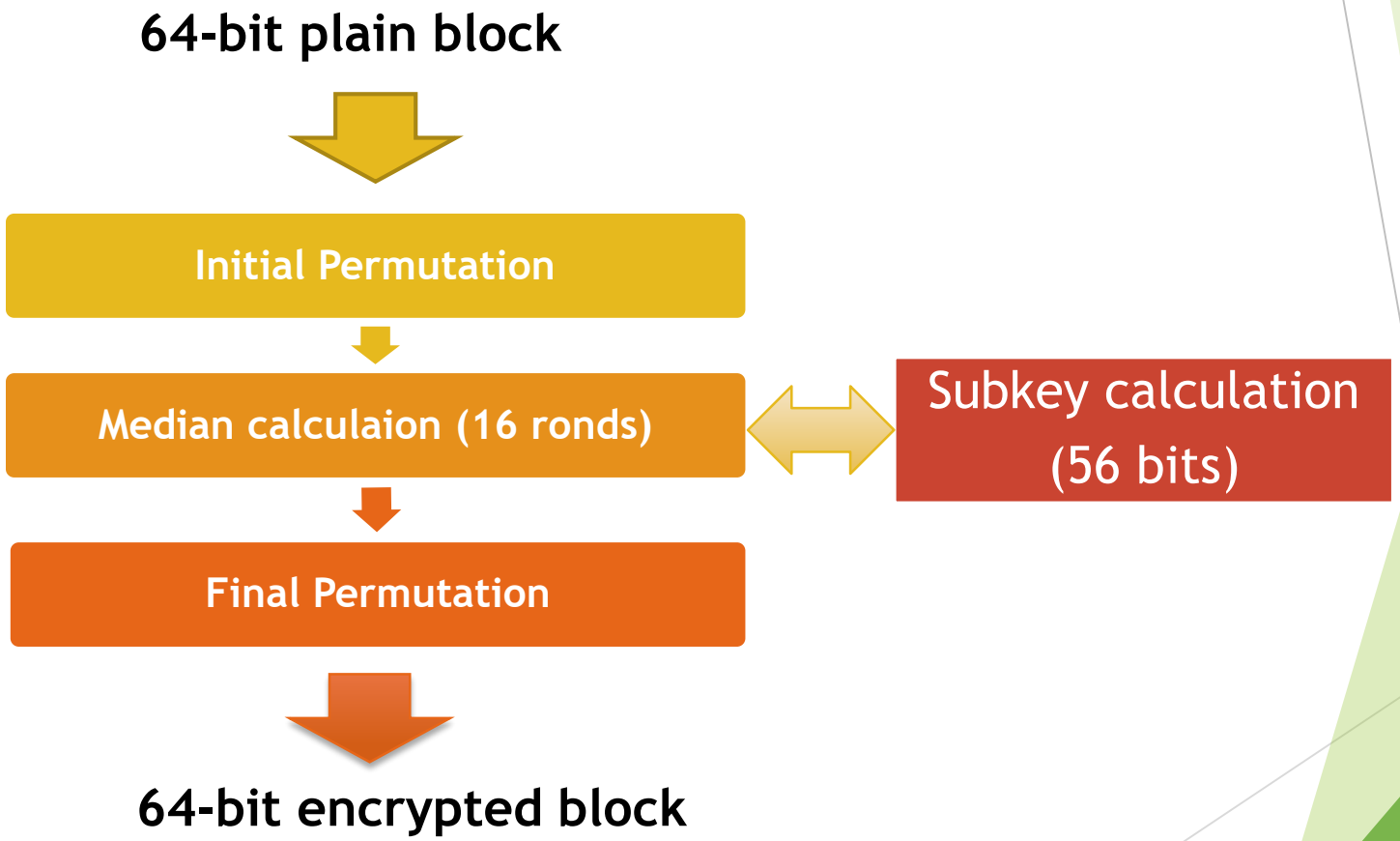


DES (Data Encryption Standard)

- Designed by IBM in 1973.
- DES adapted as a standard in1977.
- DES was the official algorithm of the US administration until 1999.
- DES is based on the encryption of Feistel, slightly modified with the alphabet {0,1} and the length of blocks 64.



DES (Data Encryption Standard)



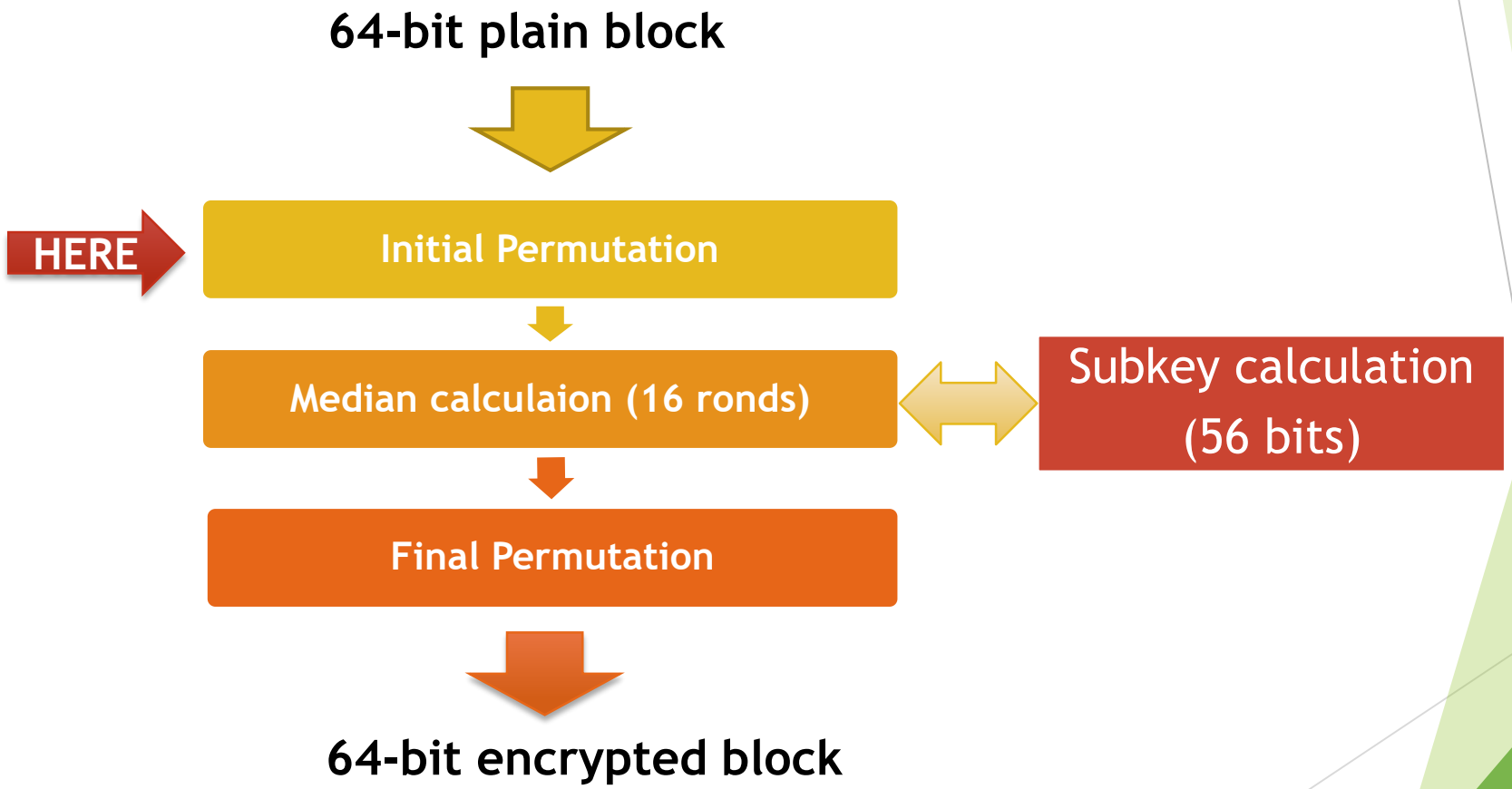
DES (Data Encryption Standard)

- Example block:

13345779 9BBCDFF1

0	0	0	1	0	0	1	1
0	0	1	1	0	1	0	0
0	1	0	1	0	1	1	1
0	1	1	1	1	0	0	1
1	0	0	1	1	0	1	1
1	0	1	1	1	1	0	0
1	1	0	1	1	1	1	1
1	1	1	1	0	0	0	1

DES (Data Encryption Standard)

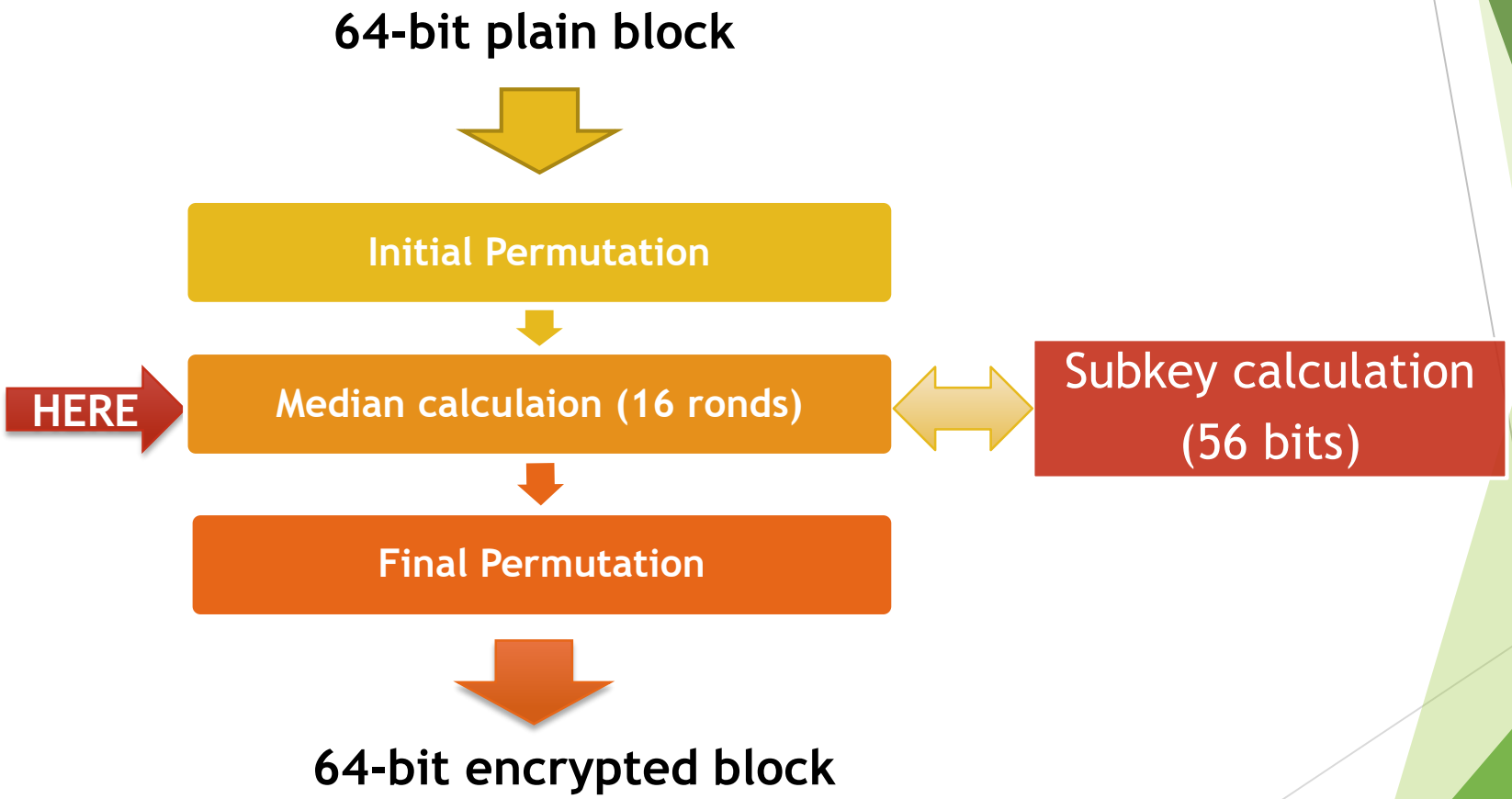


DES: Initial Permutation

- The 64 bits of plaintext are subjected to the initial permutation (IP) to produce the ciphertext according to the following table:

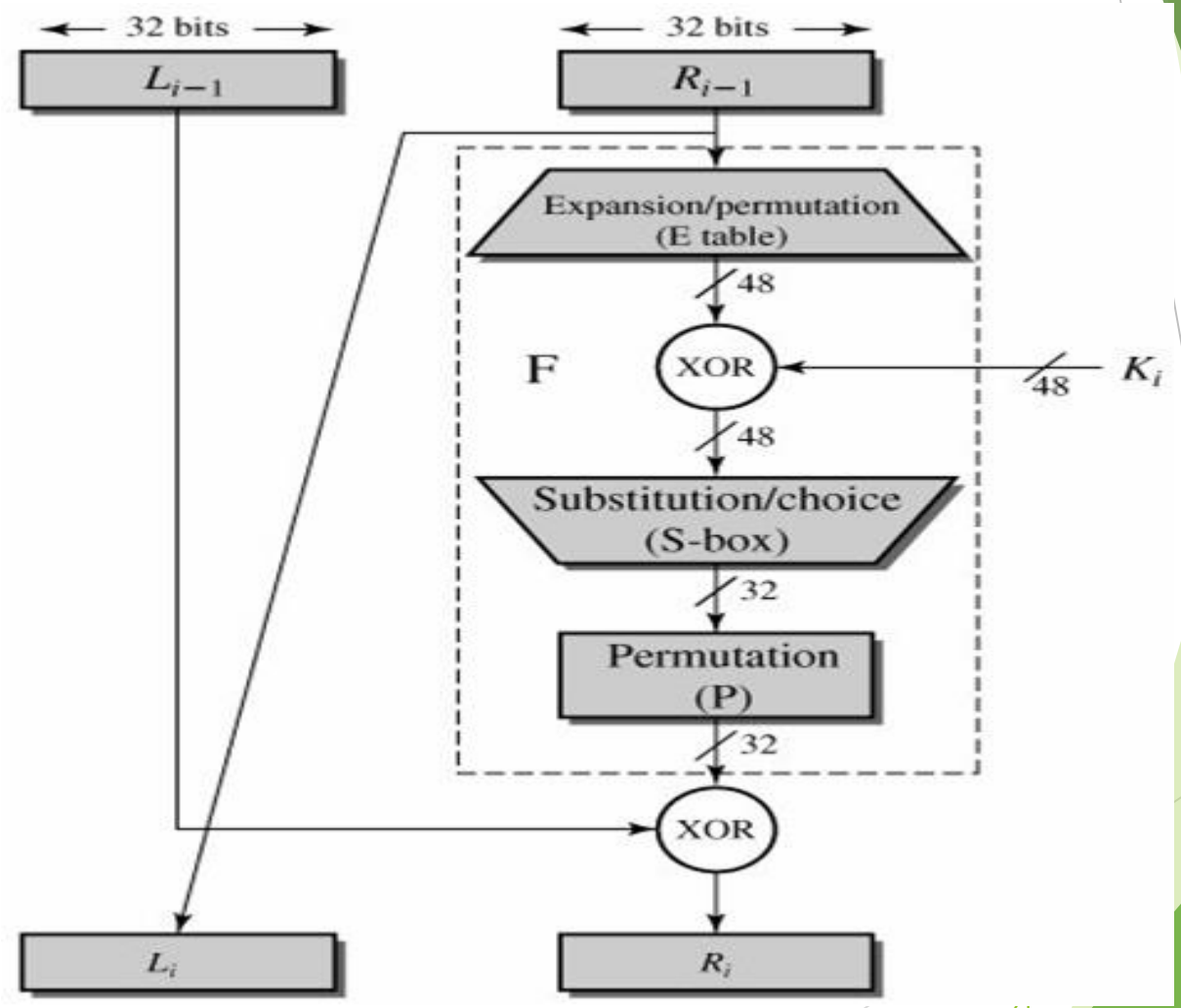
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

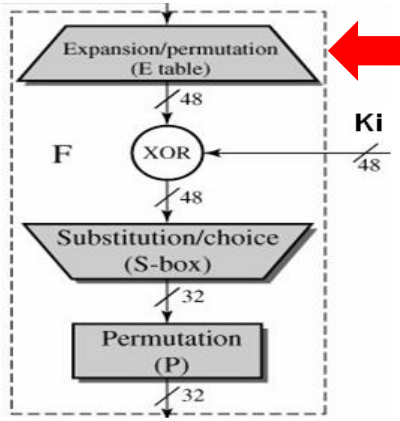
DES (Data Encryption Standard)



DES: Median Calculation

- Li = R_{i-1}
- $R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$
- Ki = G(K,i)





DES: Median Calculation

Expansion/Permutation (E table):

- Calculate the development function E:

  32-bit→ 48 bits.

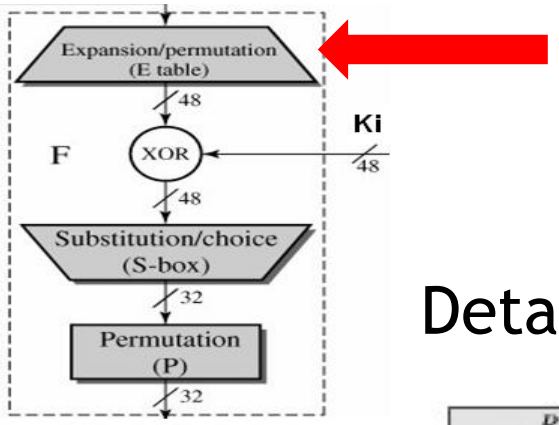
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

- Some bits of the input are duplicates.

- Next, $E(R) \oplus K$ is calculated and the result is divided into 8 Bi blocks of length 6, giving:

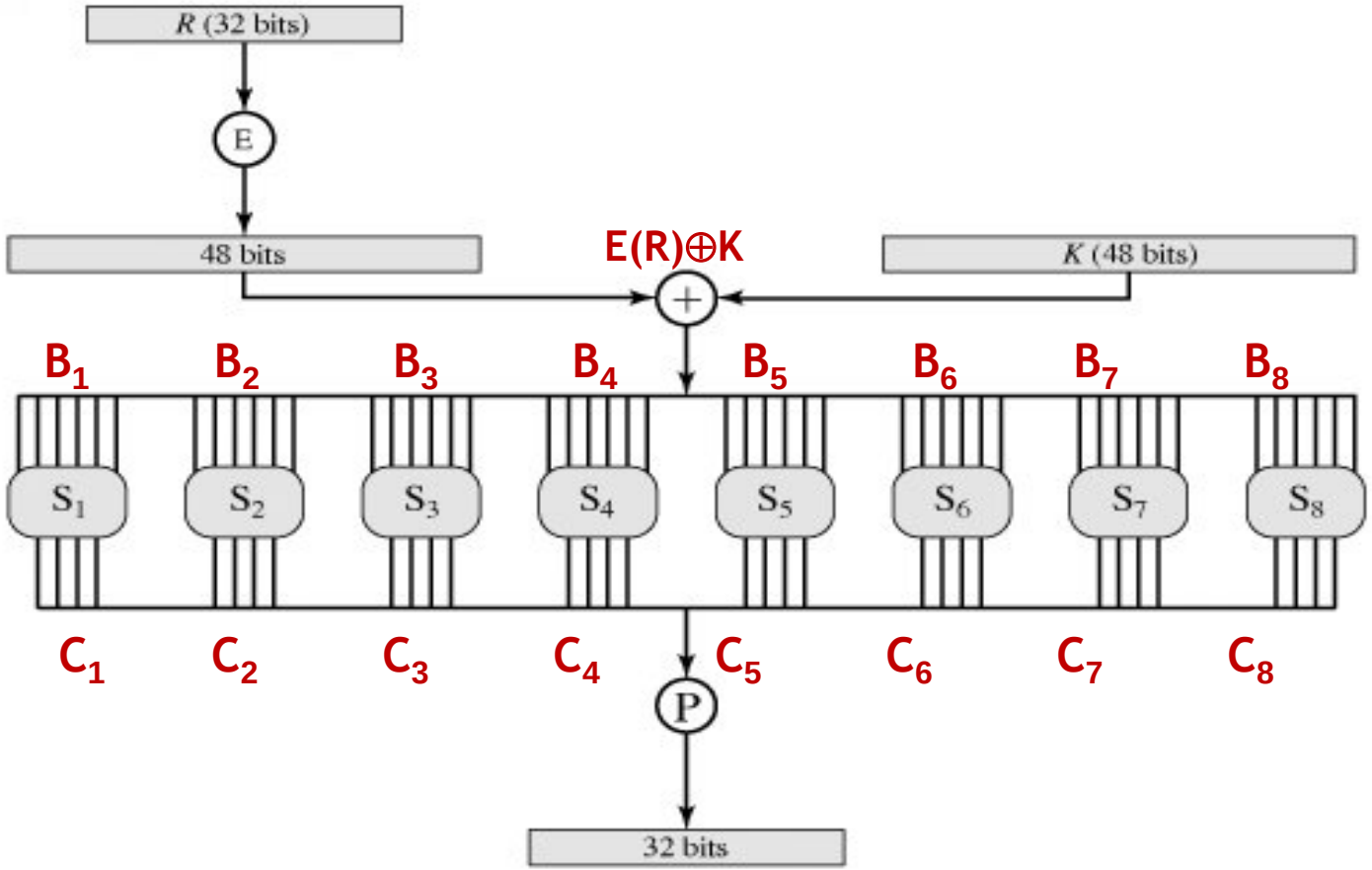
$$E(R) \oplus K = B_1 B_2 B_3 B_4 B_5 B_6 B_7 B_8$$

With $Bi \in \{0,1\}^6$

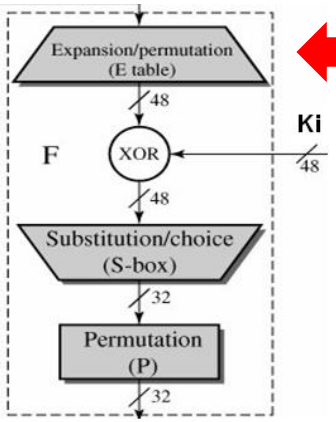


DES: Median Calculation

Details of function F:



E: Expansion,**P**: permutation



DES: Median Calculation

- **Substitution/choice (S-Box)**
- In the next stage, 8 functions are used:

$$S_i: \{0,1\}^6 \rightarrow \{0,1\}^4$$

$$i: 1 \ldots 8$$

They are called S-box:

- We calculate **Ci = Si (Bi),**

For $b_1b_2b_3b_4b_5b_6$→

b_1b_6➔ line

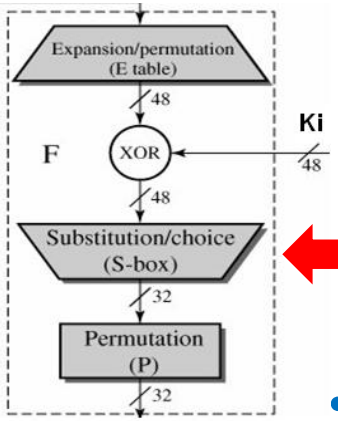
$b_2b_3b_4b_5$➔ column

- We obtains:

$C=C_1C_2C_3C_4C_5C_6C_7C_8$

It is a binary sequence of length 32 bits.

Lignes	Colonnes															
	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]	[13]	[14]	[15]
S_1																
[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
S_2																
[0]	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
[1]	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
[2]	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
[3]	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3																
[0]	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
[1]	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
[2]	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
[3]	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4																
[0]	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
[1]	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
[2]	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
[3]	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5																
[0]	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
[1]	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
[2]	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
[3]	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6																
[0]	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
[1]	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
[2]	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
[3]	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7																
[0]	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
[1]	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
[2]	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
[3]	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8																
[0]	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
[1]	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
[2]	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
[3]	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11



DES: Median Calculation

- **Example:**

We want to calculate C_1=? $S_1(B_1)$

Given B_1=**001001**

$b_1b_2b_3b_4b_5b_6$→**011001**

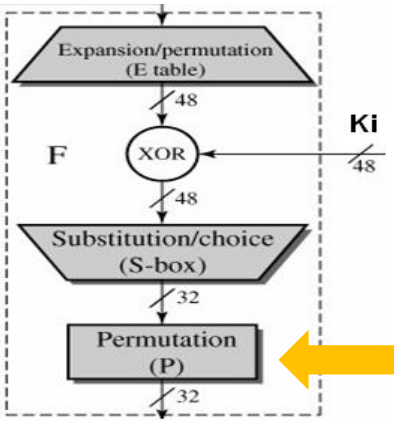
b_1b_6→ 01line (1)

$b_2b_3b_4b_5$→ 1100column (12)

Lignes	Colonnes															
	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]	[13]	[14]	[15]
S_1																
[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

- We obtain:

C_1= 9 = 1001



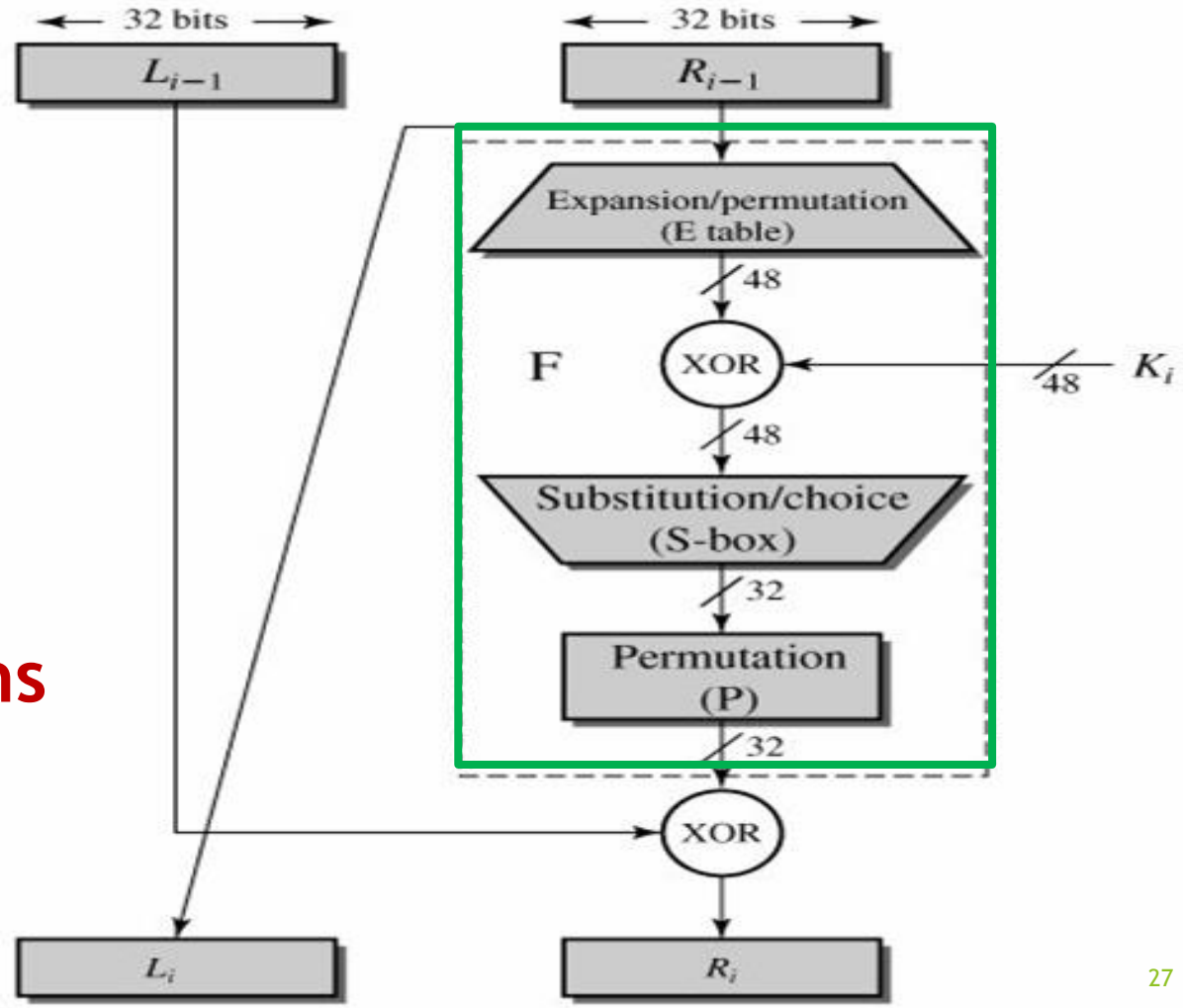
DES: Median Calculation

- **Permutation (P)**
- The permutation ***P*** is applied to the bit sequence C.
- Function P: 32-bit permutation

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

- At this point, we obtain the cryptogram $F(R_{i-1},K_i)$

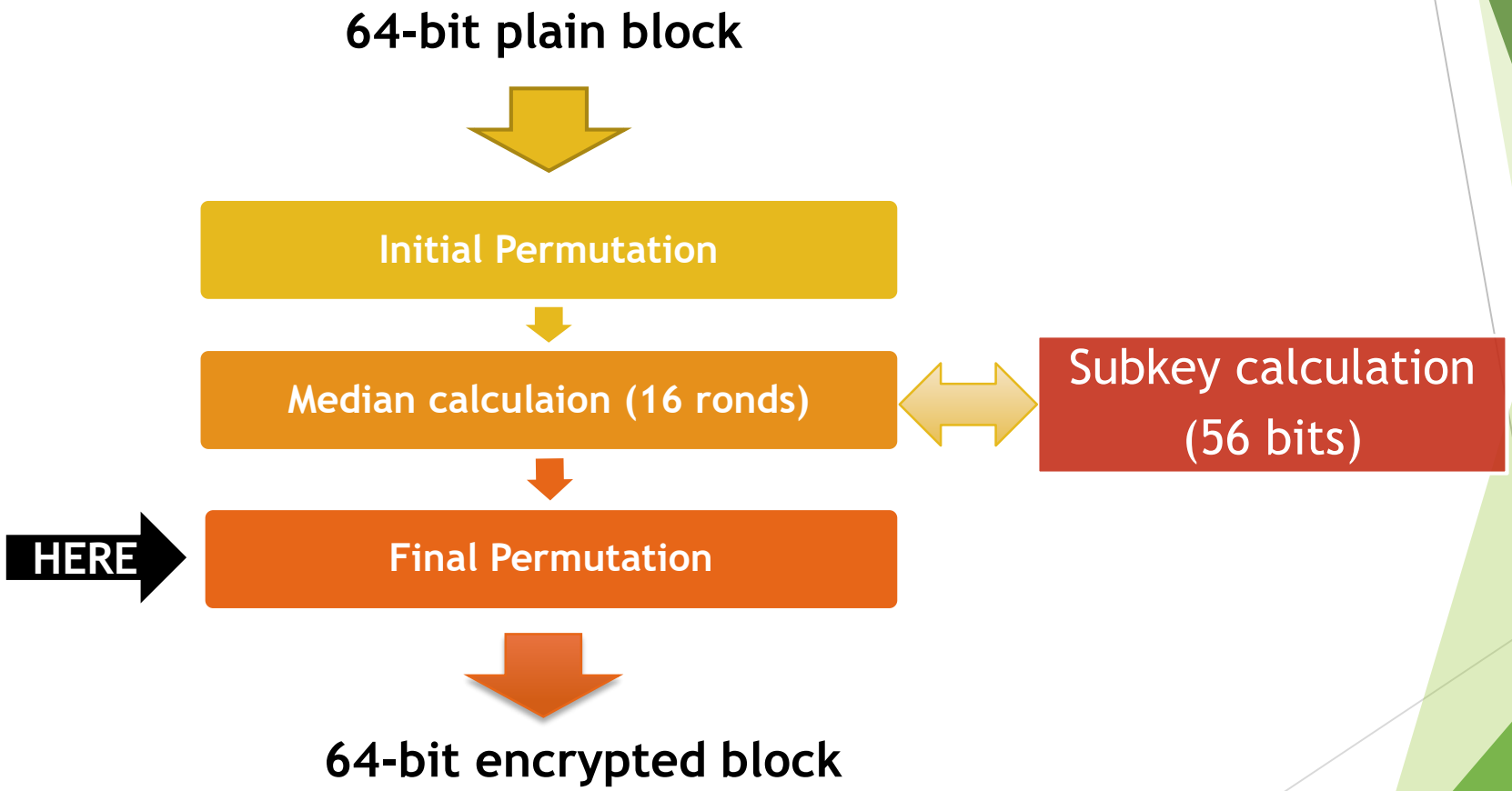
DES: Median Calculation



✓

16 iterations

DES (Data Encryption Standard)



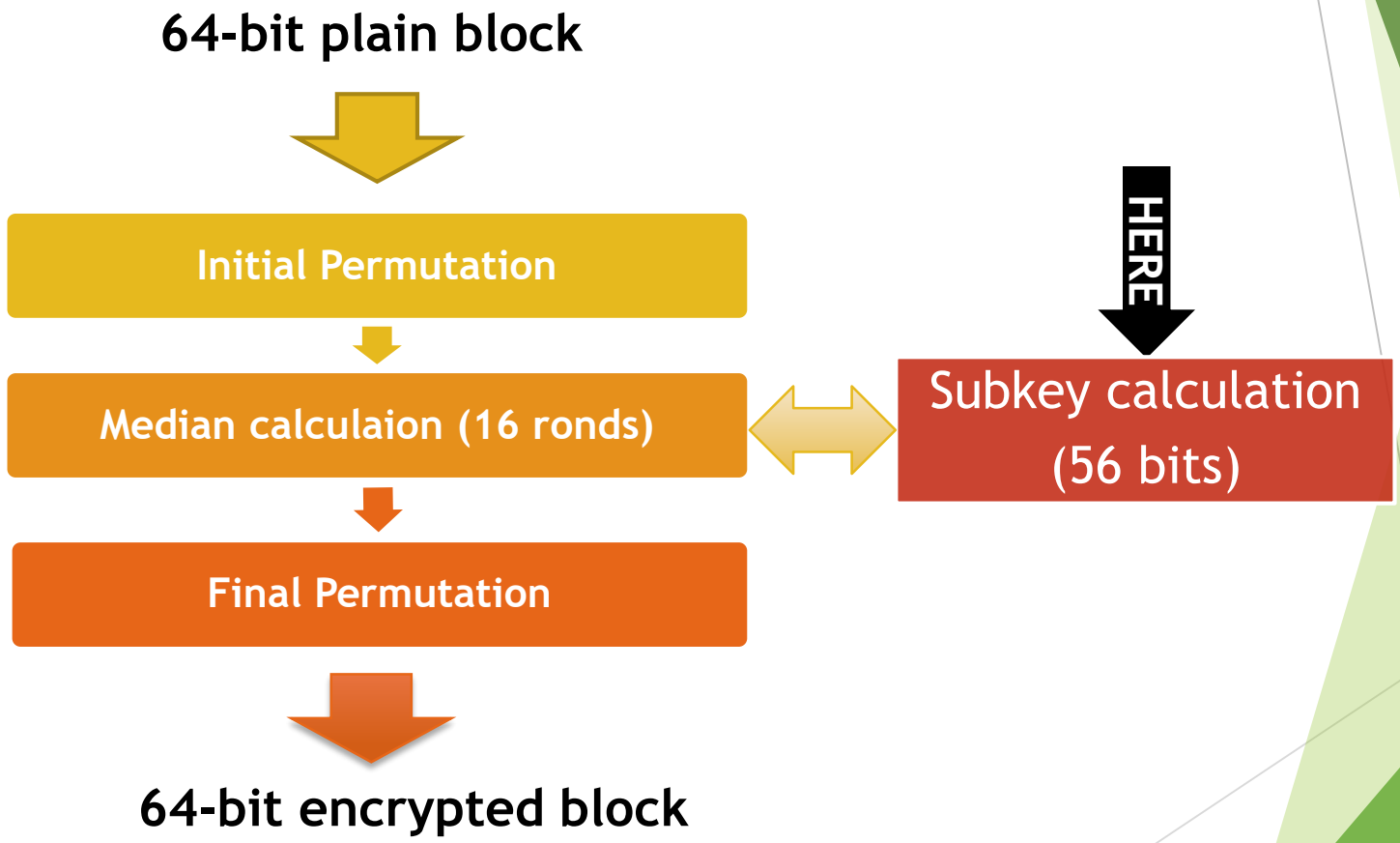
DES: Final Permutation

- According to the table PI^{-1} (the Inverse Permutation of the initial permutation):

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

- The result obtained is the encrypted block.

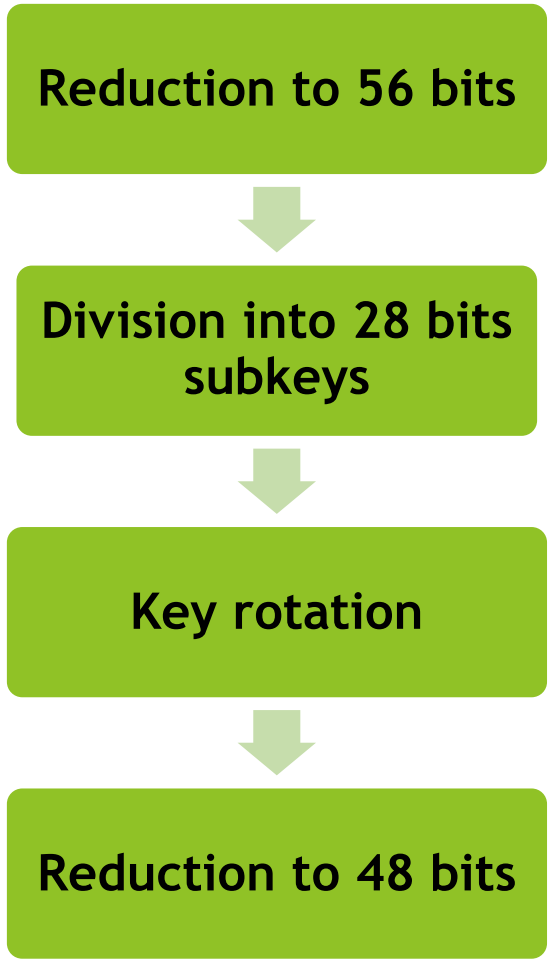
DES (Data Encryption Standard)



DES (Data Encryption Standard)

- The key has a length of **64** bits, (i.e. **8** characters), but only **56** bits are used (in the algorithm).
- The number of possible DES keys is $2^{56} \approx 7.2*10^{16}$

Algorithm for calculating the key G(K, n)



Algorithm for calculating the key G(K, n)

The calculation takes place in 4 steps:

1. **56-bit reduction:** we use the function PC1:

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Algorithm for calculating the key G(K, n)

❷ **Division into 28-bit subkeys:** the result of the previous step (56 bits) is divided into two 28 bits subkeys.

❸ **Key rotation:** At each round, the left rotation function is applied by 1 or 2 bits for each 28-bit subkey according to the following table:

Round number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bits rotated	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Algorithm for calculating the key G(K, n)

- **Reduction:** After concatenating the two previous subkeys, the function is applied PC2 to reduce the 56-bit subkey to a subkey of48 bits:

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

The result of this reduction is the subkey K_i added with $E(R_{i-1})$.

DES: Decryption

- We apply the same algorithm but we simply reverse the steps.
- For the Feistel structure, we use:
  - $R_{i-1} = L_i$
  - $L_{i-1} = R_i \oplus F(R_i, K_i)$

DES Cryptanalysis

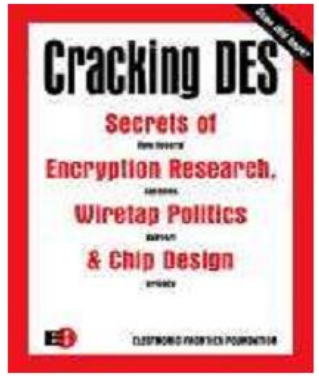
- Differential cryptanalysis (1991, 2^{47})
- Linear cryptanalysis (1994, 2^{43})
- DES has weak keys.
- Exhaustive search (2^{56})

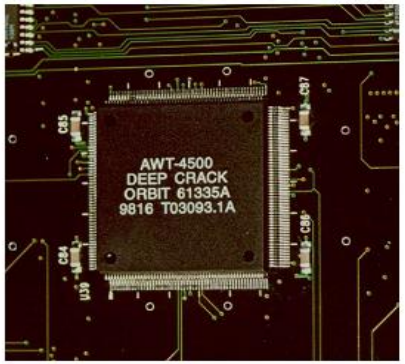
DES CryptanalysisWeak keys

- The keys that are considered weak keys in DES are:
  - 0101010101010101
  - FEFEFEFEFEFEFEFE
  - E0E0E0E0F1F1F1F1
  - 1F1F1F1F 0E0E0E0E
- **Solution:**These keys should be avoided during the key generation phase.

DES Cryptanalysis: Exhaustive Search

- In 1999,distributed.net and DeepCrack were able to break the key by 22 hours and 15 minutes.

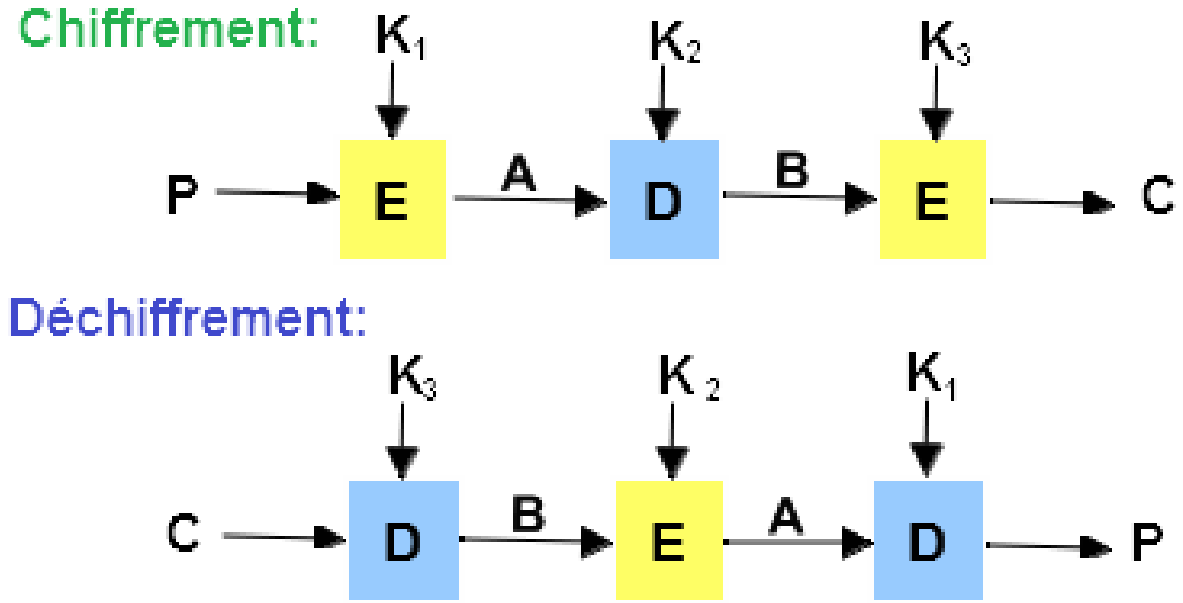




Triple DES (3DES)

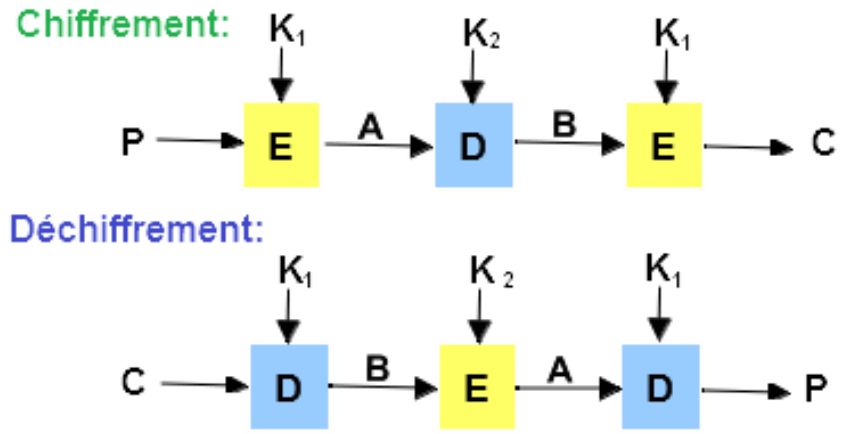
- It is developed by W.Tuchman (IBM) in 1999.
- It applies three successive operations of the DES cryptosystems using different keys.

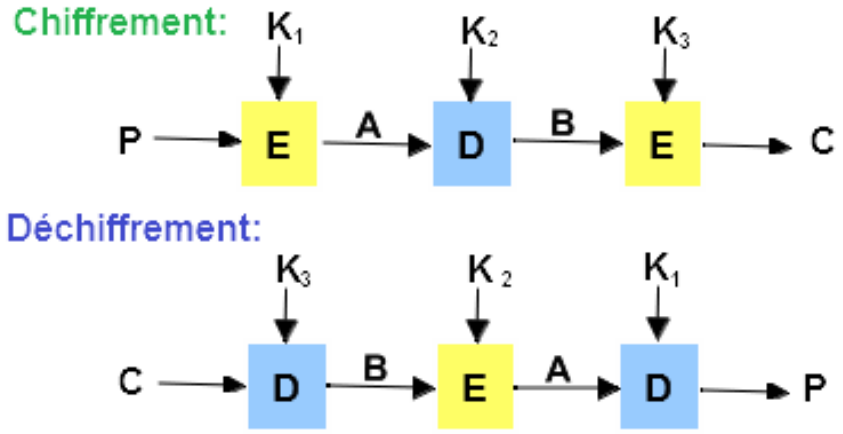
$$E(k_3,D(k_2,E(k_1,m))).$$



Triple DES (3DES)

- There are two versions:
  - $K_1 = K_3$ k, 112 bits key space
  - $K_1 \neq K_3$, 168 bits key space.





Triple DES (3DES)

- Features:
  - The key length is increased.
  - It resists all the known attacks (brute force, analytical, differential).
  - It is slower than DES because the operations are tripled.

Quiz

- Stream ciphers use the principle of:
  - Structure of Feistel
  - One time pad
  - Frequency analysis
  - No response correct
- The possible key sizes in 3DES are:
  - 112
  - 128
  - 168
  - 64

References

- HAS.Menezes, P. vanOorschot, and S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996. (Chapter 7)www.cacr.math.uwaterloo.ca/hac
- E.BerssonCryptography, Cryptography Laboratory.https://docplayer.fr/5870683-Cryptographie-chiffrement-symetrique.html
- R. Dumont, Cryptography and Computer Security, 2010.http://www.montefiore.ulg.ac.be/~dumont/pdf/crypto09-10.pdf
- NISTSpecialPublication 800-67Revision2, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, 2017.https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-67r2.pdf