Symmetric encryption: Block ciphers

CRYPTOGRAPHY AND COMPUTER SECURITY

Ana I. González-Tablas Ferreres
José M. de Fuentes García-Romero de Tejada
Lorena González Manzano
Sergio Pastrana Portillo

uc3m | Universidad Carlos III de Madrid

COSEC

OUTLINE

- 5. Symmetric encryption: Block ciphers
  - Modern encryption
  - Block ciphers
    - Introduction
    - Feistel scheme
    - Operation modes
    - Block ciphers: advantages and disadvantages
    - DES
    - AES

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

OUTLINE

- 5. Symmetric encryption: Block ciphers
  - Modern encryption
  - Block ciphers
    - Introduction
    - Feistel scheme
    - Operation modes
    - Block ciphers: advantages and disadvantages
    - DES
    - AES

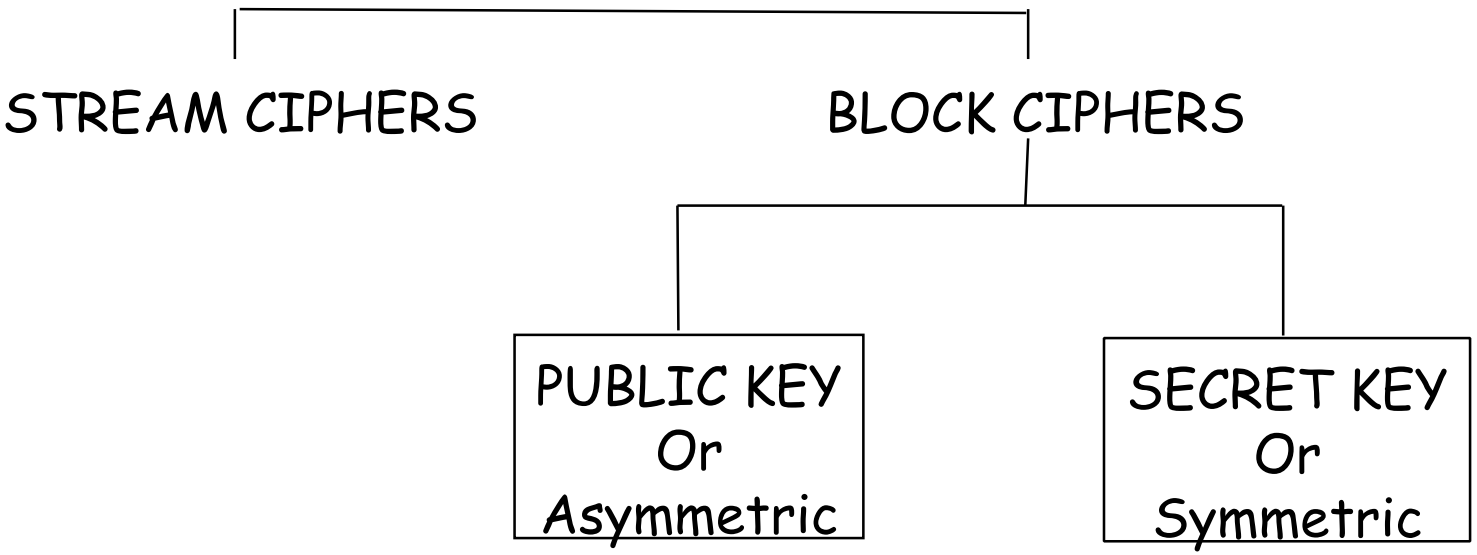
Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

Modern encryption

- Classification
  - Type of operations
    - In general, substitutions and transpositions
  - According to the key used:
    - Symmetric (Secret key)
    - Asymmetric (Public key)
  - According to the number of symbols encrypted at a time
    - Stream (1 symbol or a few)
    - Block (a set of symbols at a time)

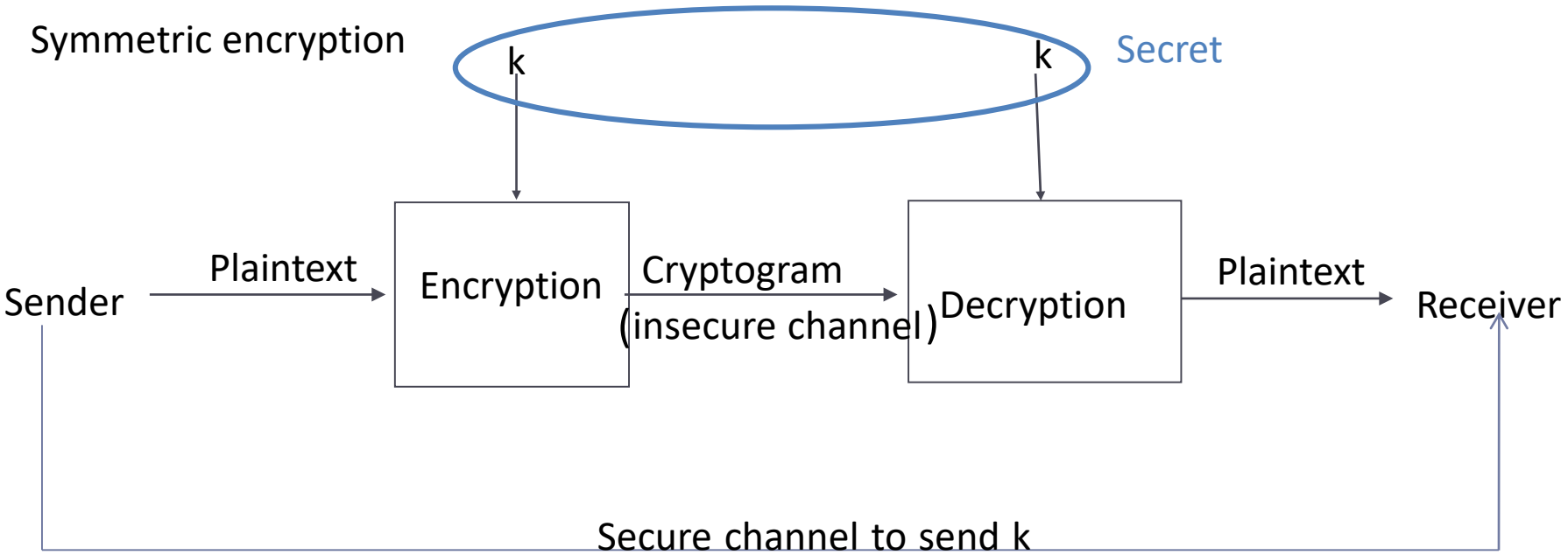
Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

Modern encryption



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

Modern encryption



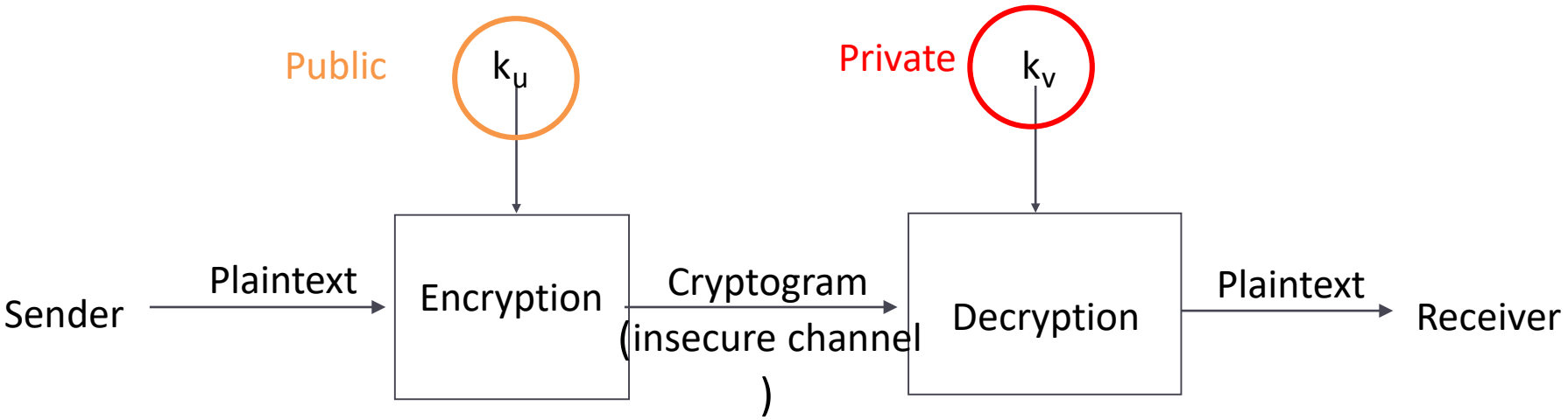
$$C = E(k, M) = E_k(M)$$

$$M = D(k, C) = D_k(C)$$

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

Modern encryption

Asymmetric encryption



$$C = E(k_u, M) = E_{ku}(M)$$

$$M = D(k_v, C) = D_{kv}(C)$$

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

OUTLINE

- 5. Symmetric encryption: Block ciphers
  - Modern encryption
  - Block ciphers
    - Introduction
    - Feistel scheme
    - Operation modes
    - Block ciphers: advantages and disadvantages
    - DES
    - AES

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

Block ciphers. Introduction

- M is divided in blocks of equal length:

  $M_1, M_2, \ldots M_n$

- Each block is encrypted with the same key

  $C = E_k(M) = E_k(M_1)\, E_k(M_2) \ldots E_k(M_n)$

- Typical block sizes 64, 128 or 256 bits
- Reversible mapping between M and C blocks

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

Block ciphers. Introduction

- Substitution of very long “characters”
  - 64 bits or more
- Ideal block cipher
  - n: block size. E.g.: 64
  - Substitution tables (mapping) of 2^n bits
  - $2^n!$ possible keys (matches C_i)
  - Not practical
    - Substitution table is the key, length = $n \cdot 2^n$ bits
    - For n = 64 -> key length 10^{21} bits aprox.

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

Block ciphers. Introduction

Algorithm	Block size (bits)	Key size (bits)	Rounds
Lucifer	128	128	16
DES	64	56	16
Twofish	128	variable	variable
RC2	64	variable	18
RC5	variable	variable	variable
SAFER	64	64	8
IDEA	64	128	8
Skipjack	64	80	32
RIJNDAEL	128	128 or more	flexible

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

OUTLINE

- 5. Symmetric encryption: Block ciphers
  - Modern encryption
  - Block ciphers
    - Introduction
    - Feistel scheme
    - Operation modes
    - Block ciphers: advantages and disadvantages
    - DES
    - AES

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

Block ciphers. Feistel scheme

- Block cipher (Feistel 1975)
  - Confine to a subset of $2^n!$ possible keys
    - n: block text size
    - k: key size
    - 2^k possible keys
  - Product cipher
    - Substitution (S-box)
    - Permutation (P-box)
  - Practical application of Shannon's proposal (1949)
    - High *diffusion*
    - High *confusion*

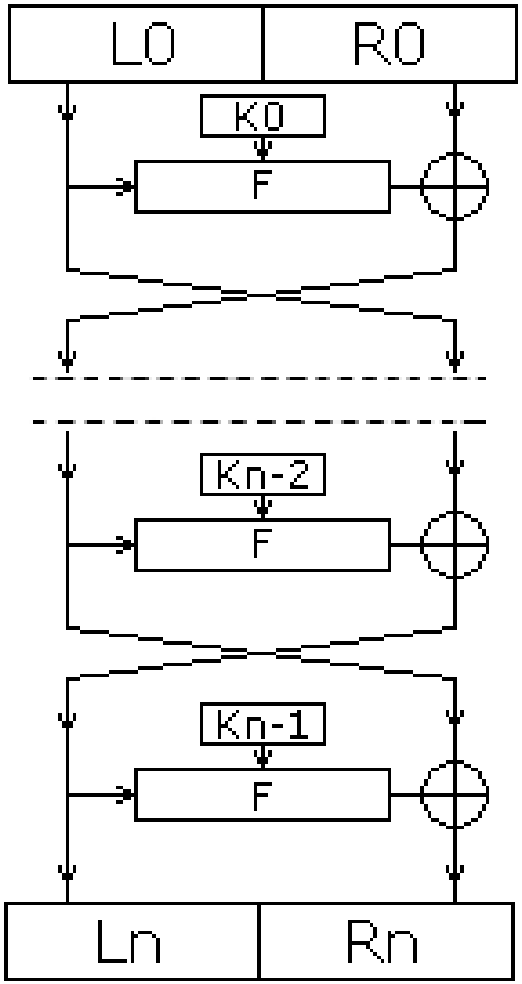
Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

Block ciphers. Feistel scheme

- Methods to thwart cryptanalysis
  - Diffusion
    - statistical structure of M is dissipated in C
    - each C bit is affected by many M bits
    - achieved performing some permutation on Mi followed by a function to that permutation
  - Confusion
    - seeks to make C - k statistical relationship as complex as poss.
    - achieved by the use of a complex substitution algorithm

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

Block ciphers. Feistel scheme



Author: Nibumbum
https://commons.wikimedia.org/wiki/File:Feistel_encryption.png

Block ciphers. Feistel scheme

- Divide the block into two halves L_0 and R_0
- Substitute the left half
  - Apply a *round function* F (non linear) to the right half of the data and then XOR the output and the left half
    - F is a function of the right half and the round subkey k_i
- Permute the two halves
- Repeat it n rounds

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

Block ciphers. Feistel scheme

- Same circuit to encrypt and decrypt
  - Just use the subkeys in reverse order
  - A final permutation is needed (fig. slide 15)
    - $L_{n+1} = R_n$
    - $R_{n+1} = L_n$
- In practice the design problem is reduced to:
  - Develop a good subkey generation algorithm
  - Develop a good round function F
- Many b.c. follows Feistel scheme but not all

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

Block ciphers. Feistel scheme

- Block size
  - Larger size, greater security, lower speed
  - 64 or more
- Key size
  - Larger size, greater security, lower speed
  - 128 or more
- Number of rounds
  - Higher number, greater security, lower speed
  - Typical value 16
- Subkey generation algorithm and round function F
  - Greater complexity, greater resistance to cryptoanalysis

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

OUTLINE

- 5. Symmetric encryption: Block ciphers
  - Modern encryption
  - Block ciphers
    - Introduction
    - Feistel scheme
    - Operation modes
    - Block ciphers: advantages and disadvantages
    - DES
    - AES

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

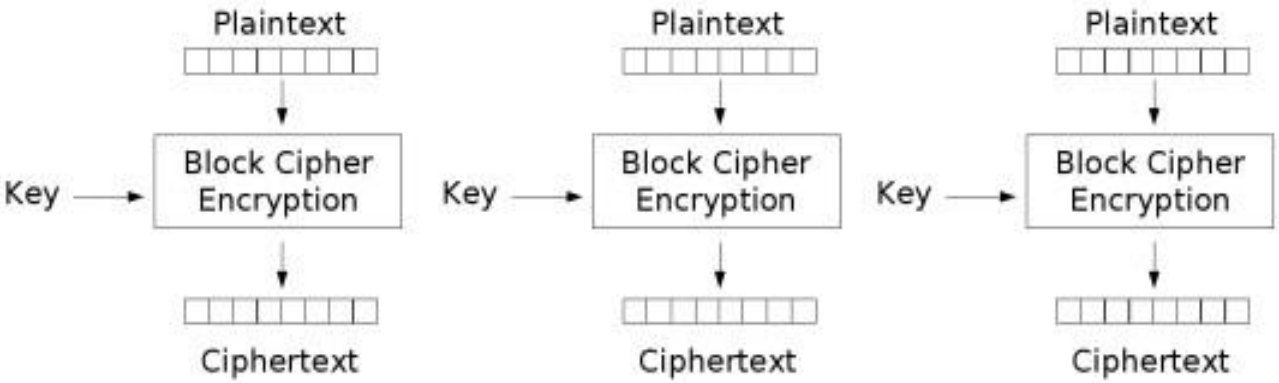
Block ciphers. Operation modes

- Technique for enhancing the effect of a cryptographic algorithm or adapting the algorithm for an application
- Intended for use with any symmetric block cipher
- Five modes defined by NIST (SP 800-38A)

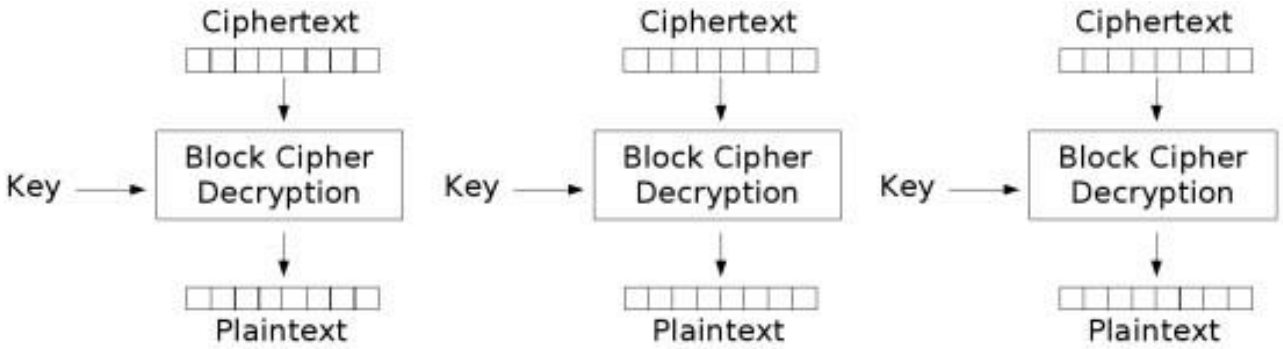
Electronic Code Book ECB
Cipher Block Chaining CBC
Cipher Feedback CFB
Output Feedback OFB
Counter Mode CTR (recommended)

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

Block ciphers. Electronic Code Book mode (ECB)



Electronic Codebook (ECB) mode encryption



Electronic Codebook (ECB) mode decryption

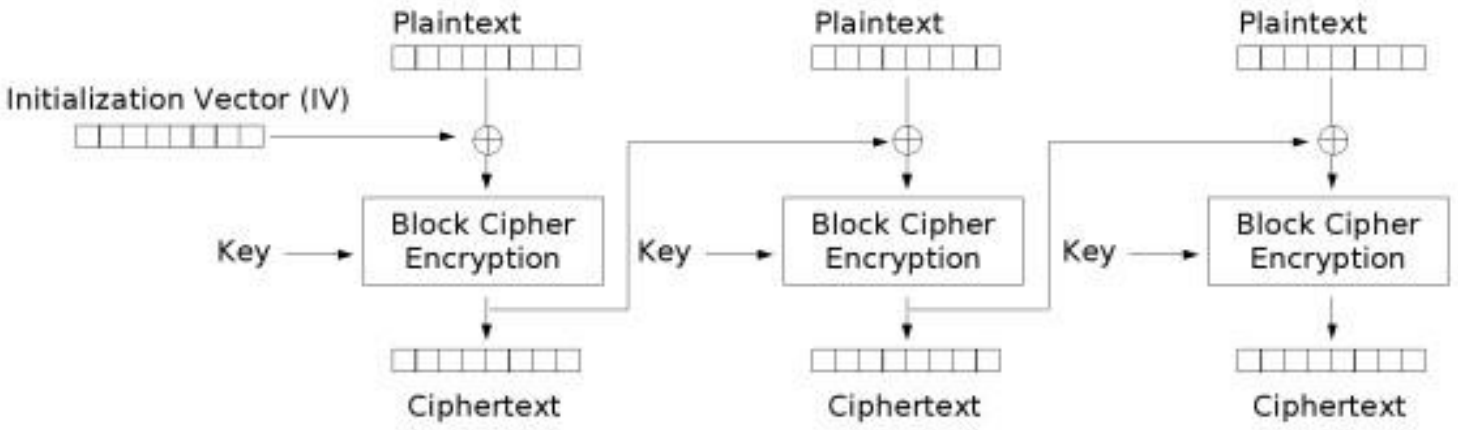
Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

Block ciphers. Electronic Code Book mode (ECB)

- Advantages:
  - Block encryption and decryption can be executed in parallel } Ideal for a short amount of data
  - e.g. symmetric key
  - Bit errors in transmission do not propagate
- Disadvantages:
  - Repeated plaintext blocks produce repeated ciphertext blocks
  - It is possible to modify the order of the blocks or eliminate them
  - ***Padding*** of the last block is neccesary
  - E.g.: add zero bytes and a last byte reporting #padding_bytes

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

Block ciphers. Electronic Code Book mode (ECB)



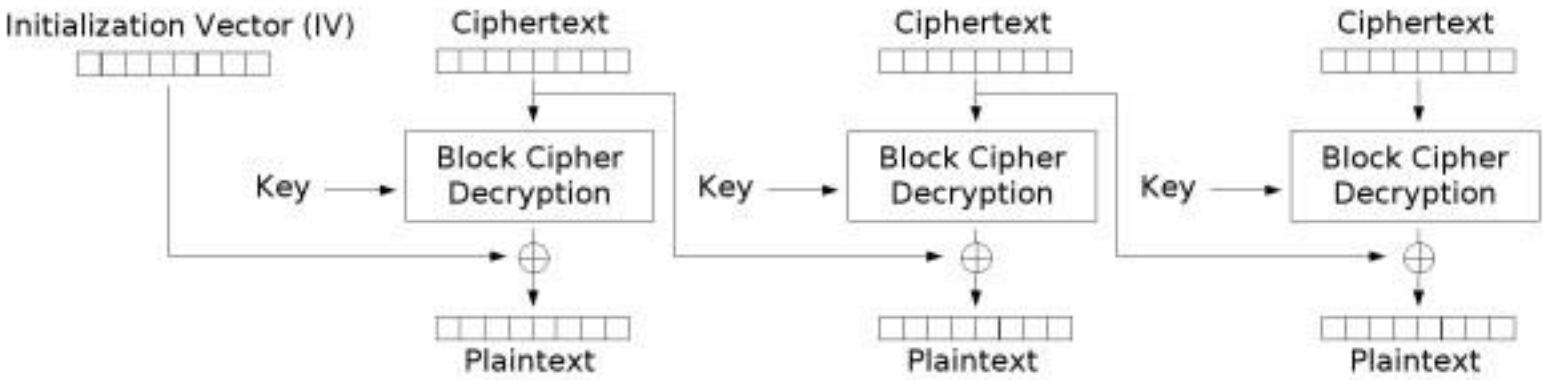
Cipher Block Chaining (CBC) mode encryption

$$C_i = E_K(P_i \oplus C_{i-1}), C_0 = IV$$

- IV confidential to parties (integrity reasons)

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

Block ciphers. Cipher Block Chaining mode (CBC)



Cipher Block Chaining (CBC) mode decryption

$$P_i = D_K(C_i) \oplus C_{i-1}, C_0 = IV$$

- A bit error in transmission affects two Mi
- ***Padding*** needed

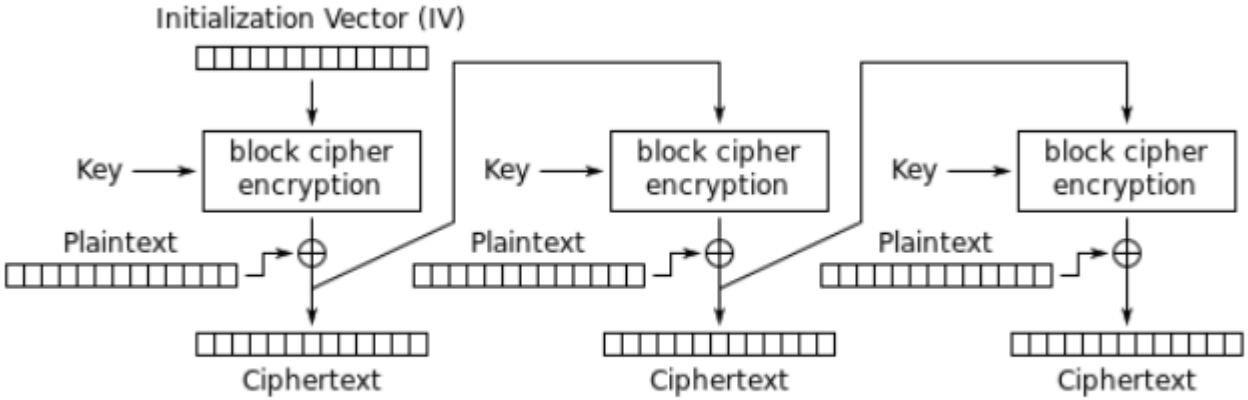
Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

Block ciphers. Cipher Feedback mode (CFB)

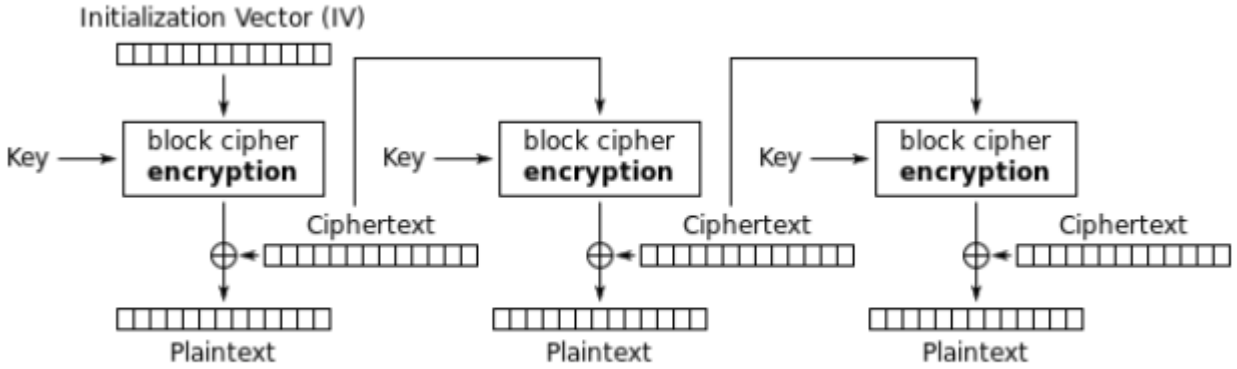
- Uses a shift register
- Plaintext is divided in *segments* (smaller than blocks)
- A bit error in transmission affects two Mi
- Converts a block cipher into a stream cipher
  - But keystream depends on the plaintext

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

Block ciphers. Cipher Feedback mode (CFB)



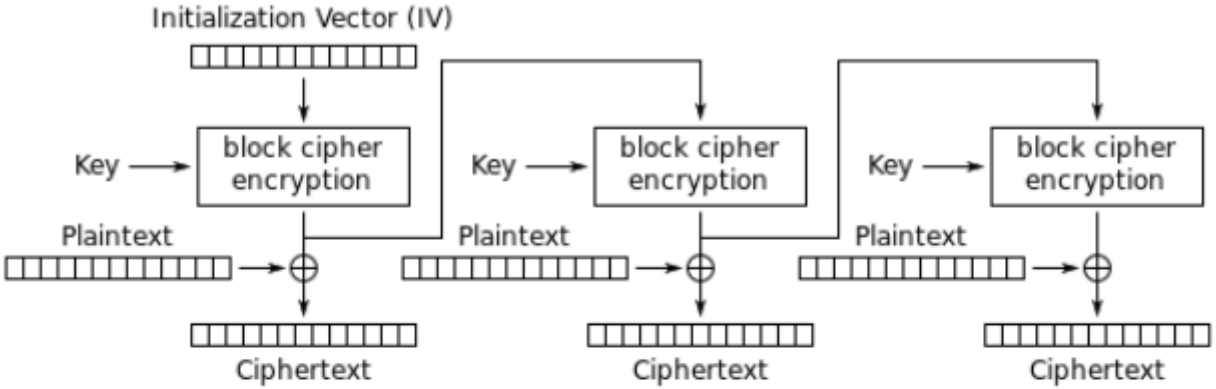
Cipher Feedback (CFB) mode encryption



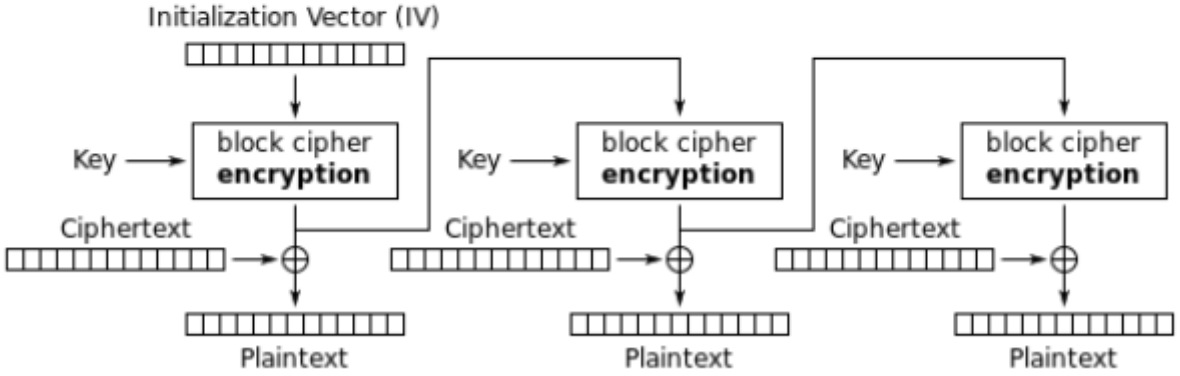
Cipher Feedback (CFB) mode decryption

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

Block ciphers. Output Feedback mode (OFB)



Output Feedback (OFB) mode encryption



Output Feedback (OFB) mode decryption

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

Block ciphers. Output Feedback mode (OFB)

- IV must be a *nonce*
- Bit error in transmission do not propagate
- Just affects a single bit of an Mi
- Does not need padding
- Remaining bits of the last output block are discarded
- Converts a block cipher into a stream cipher
  - Keystream does not depend on the plaintext
  - Works over blocks not over segments

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

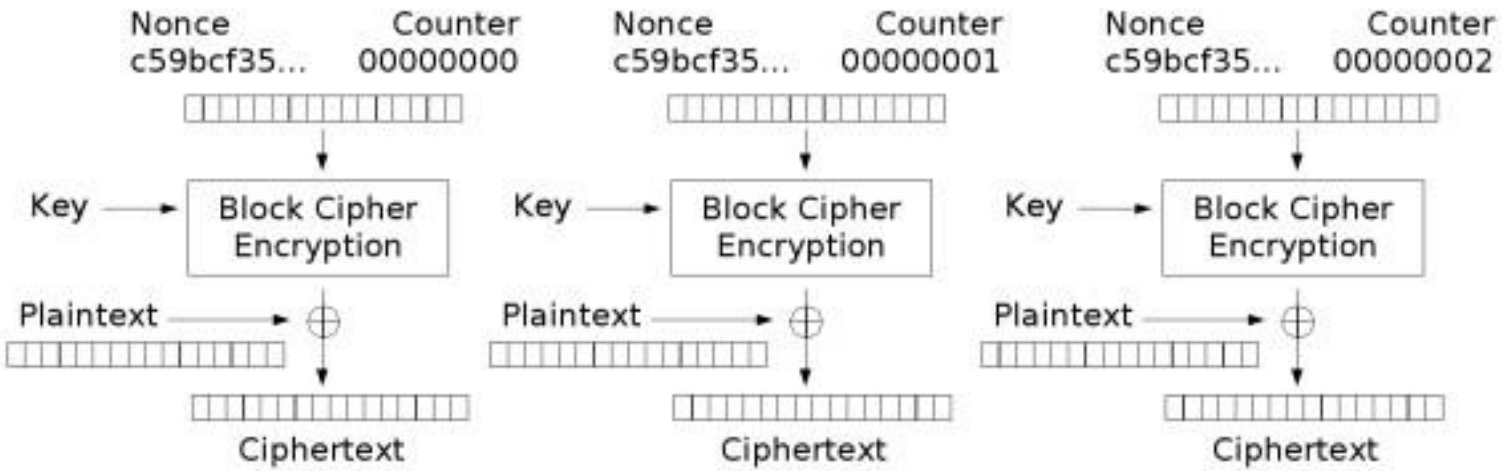
Block ciphers. Counter mode (CTR)

- Uses a counter of the size of a block (n)
- Incremented by 1 mod 2^n across consecutive blocks
- Remaining bits of the last output block are discarded
- Converts a block cipher into a stream cipher
  - Keystream does not depend on the plaintext
  - Works over blocks not over segments

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

Block ciphers. Counter mode (CTR)

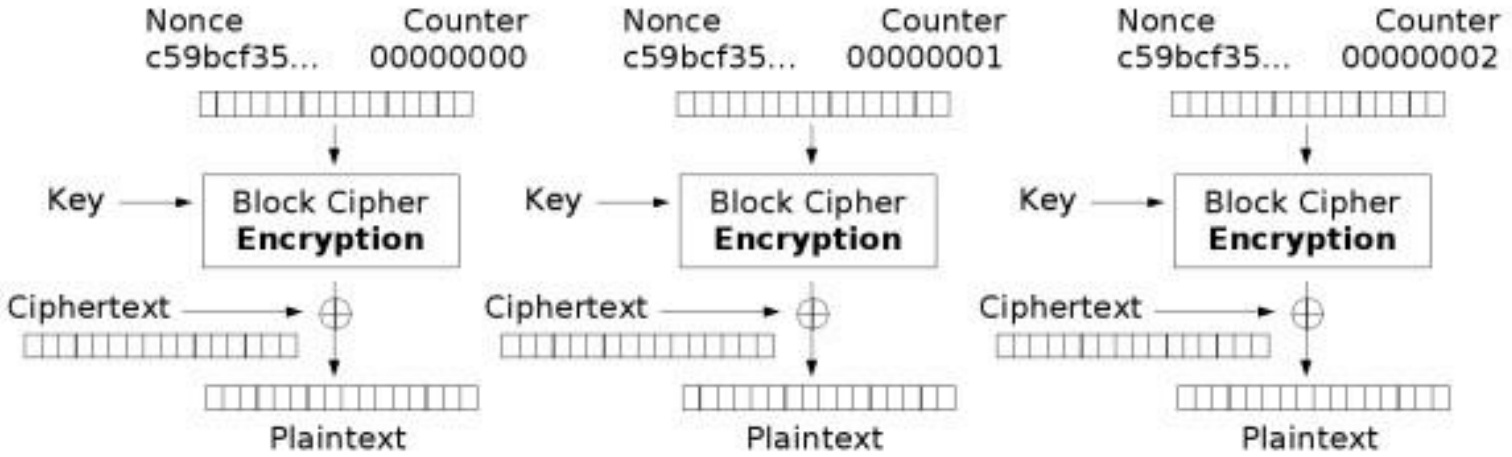
- Simplicity and random access



Counter (CTR) mode encryption

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

Block ciphers. Counter mode (CTR)



Counter (CTR) mode decryption

- A bit error in transmission does not propagate
- It only affects a single bit of a block

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

OUTLINE

- 5. Symmetric encryption: Block ciphers
  - Modern encryption
  - Block ciphers
    - Introduction
    - Feistel scheme
    - Operation modes
    - Block ciphers: advantages and disadvantages
    - DES
    - AES

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

Block ciphers. Advantages and disadvantages

- Use: confidentiality
- Advantages:
  - High diffusion and confusion
  - Simple implementation
  - Symmetry
    - Similar encryption and decryption processes
    - Same circuits to encrypt and decrypt (not always, e.g. AES)
  - Efficiency
    - Fast process

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

Block ciphers. Advantages and disadvantages

- Disadvantages:
  - Secure channel is required (key distribution)
  - Management of a high number of keys
  - Effectiveness
    - Slower than stream ciphers, the whole block should be read
    - If M length is not a multiple of the block size, C length is bigger
  - Security and robustness
    - Error propagation
    - Vulnerable to attacks if blocks are repeated
  - Padding gives clues to cryptanalysts

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

OUTLINE

- 5. Symmetric encryption: Block ciphers
  - Modern encryption
  - Block ciphers
    - Introduction
    - Feistel scheme
    - Operation modes
    - Block ciphers: advantages and disadvantages
    - DES
    - AES

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

Block ciphers. Data Encryption Standard (DES)

- 1971 LUCIFER: IBM research project finishes (Feistel)
  - Key size:128 bits
- 1974: NBS (now NIST) request for proposals for a national cipher standard
- 1976: A modified version of LUCIFER wins
  - Key size reduced to 56 in order to fit on a single chip
  - NSA changed de S- boxes
- 1977: DES standard for commercial, bank and unclassified communications
- 1983, 1988, 1993: NIST reaffirmed DES as a standard
  - Criticism
  - Key length
  - Obscure design
    - Suspicions of the National Security Agency (NSA)

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

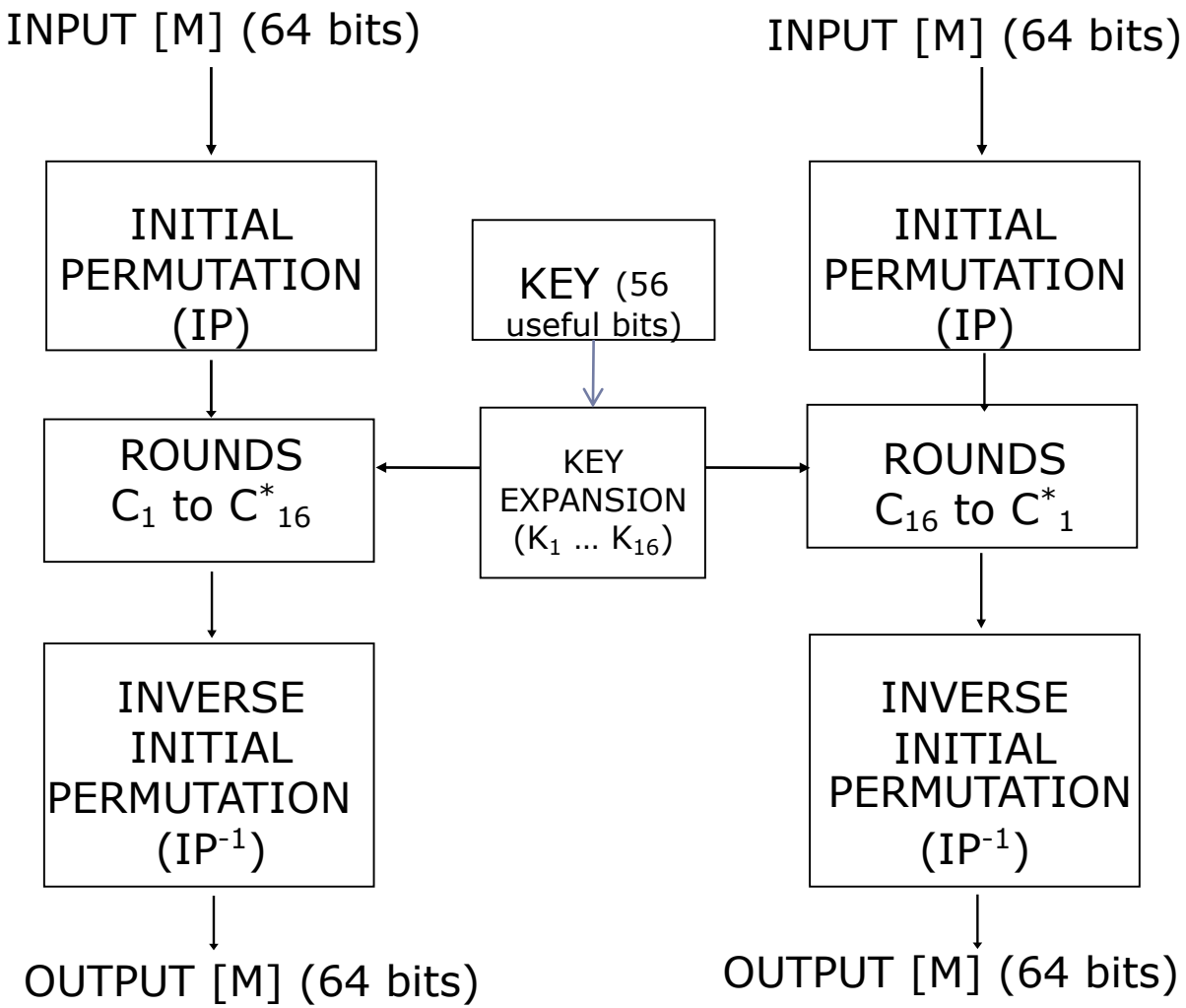
Block ciphers. Data Encryption Standard (DES)

- 1990: Differential cryptoanalysis (Biham and Shamir)
  - 2^{47} chosen paintexts needed. Effort on 2^{47} encryptions
  - Lucifer was vulnerable but DES is not
- 1993: Linear Cryptanalysis (Matsui)
  - 2^{43} knownplaintexts needed
- 1998: DES Cracker de la Electronic Frontier Foundation
  - 56 hours
  - Using 1536 dedicated chips
  - $250K, less than a year to build it
- 1999: DES Cracker version 2
  - 22 hours
  - Combines 100K PCs
- 1999:Triple DES as new standard
  - DES just for legacy systems
- **2001: new contest and new standard -> AES (Advanced Encryption Standard)**

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

DES: Encryption and decryption scheme

- Key: 64 bits
  - (8 parity bits)
- Block size: 64 bits
- Rounds: 16
  - Last one needs one additional permutation (*)
- Internal keys:
  - 16 48-bits keys
- Mathematical basis:
  - substitutions
    - lineal
    - non lineal
  - permutations



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

OUTLINE

- (…)
  - Data Encryption Standard (DES)
    - Encryption
    - Key expansion
    - Decryption
    - Triple DES
    - Security
  - AES
  - (…)

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

DES: Algorithm decription

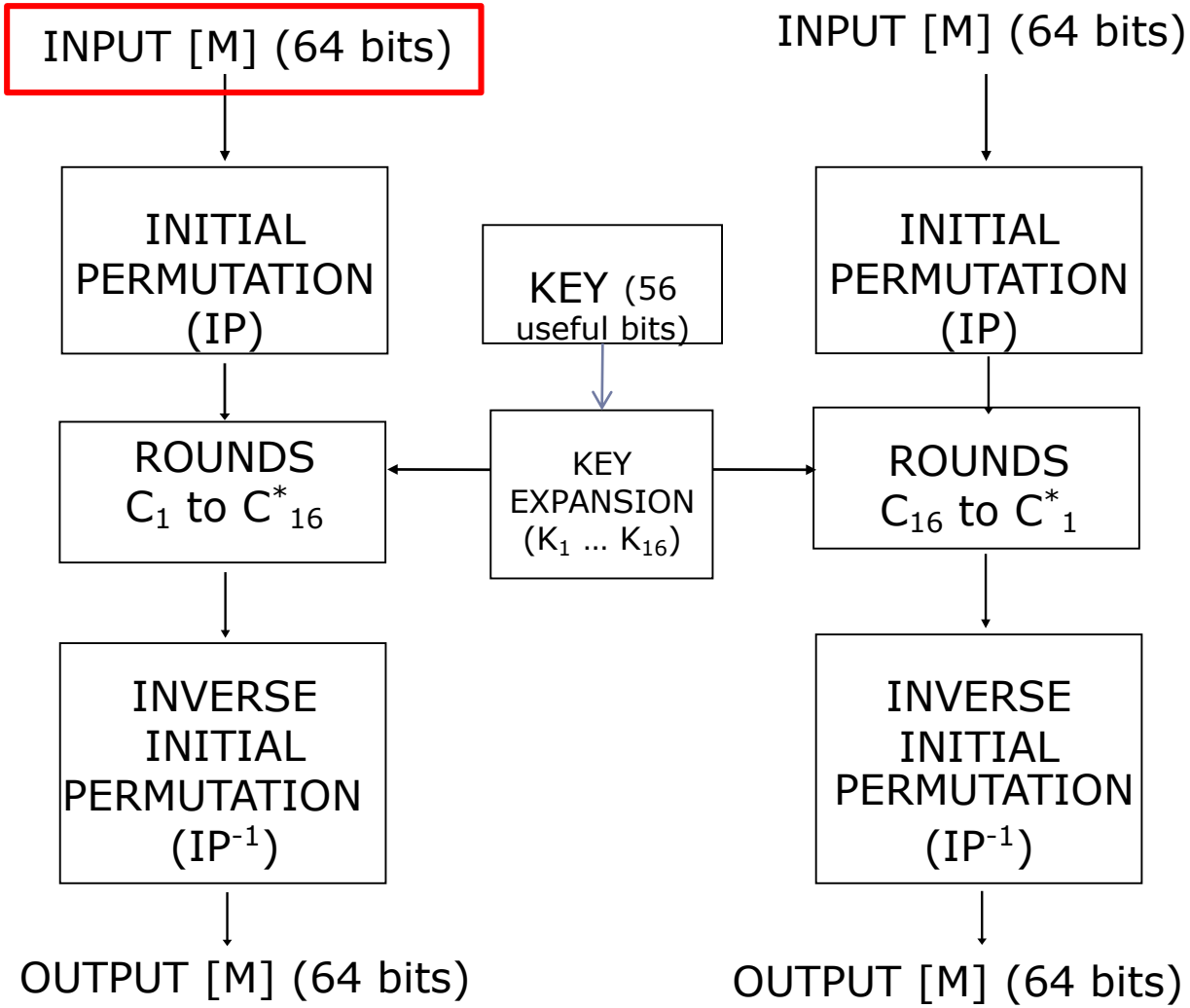
Cleartext

1. Select block M to be encrypted
2. Place the 64 bits of the cleartext as follows

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

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

DES: "Situational map"



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

DES: Algorithm decription

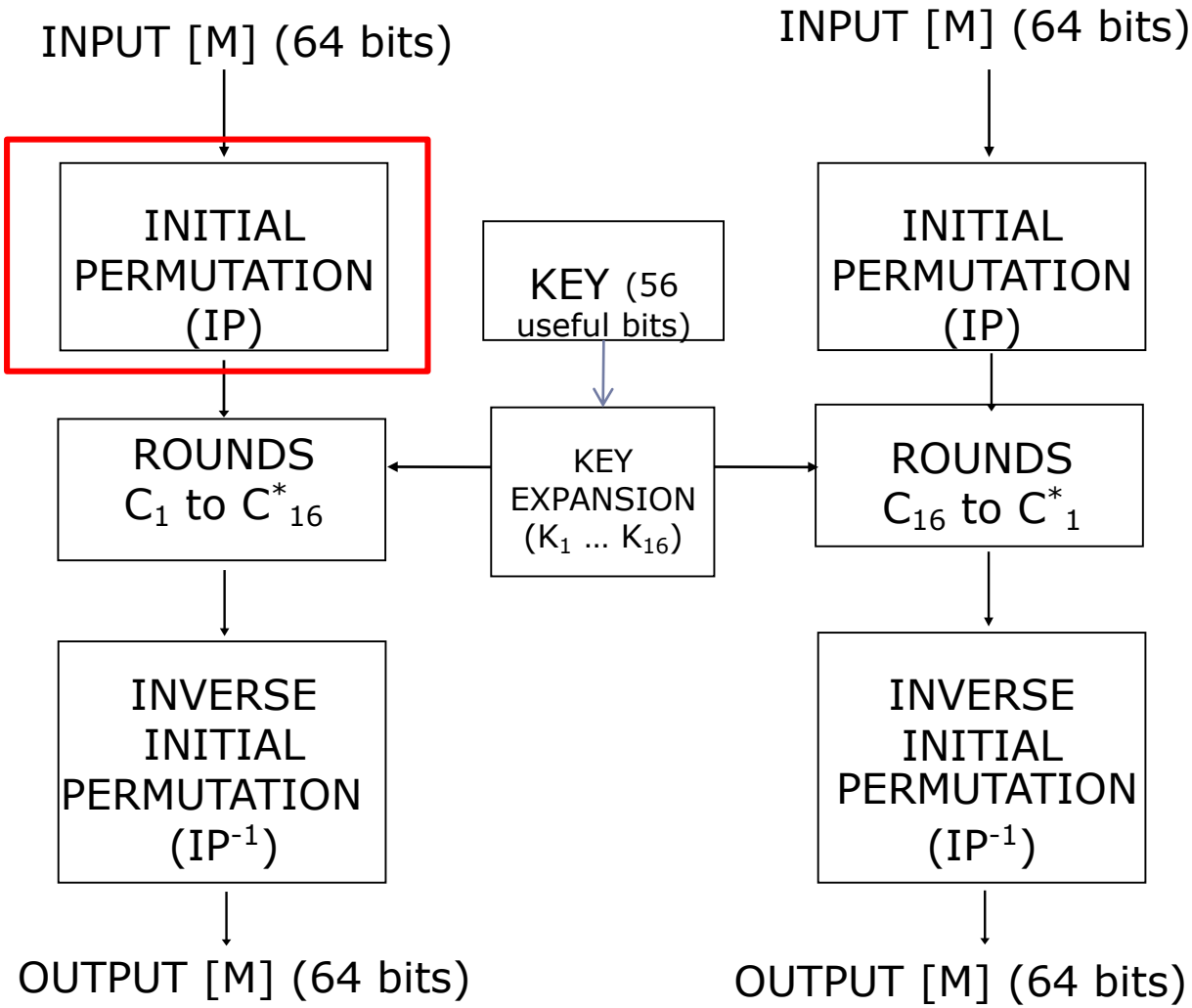
From cleartext to initial permutation

3. Initial Permutation, IP

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

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

DES: "Situational map"



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

DES: Algorithm decription

Operation before the initial round

4. Computation of left and right sub halves, L0 and R0, of 32 bits each

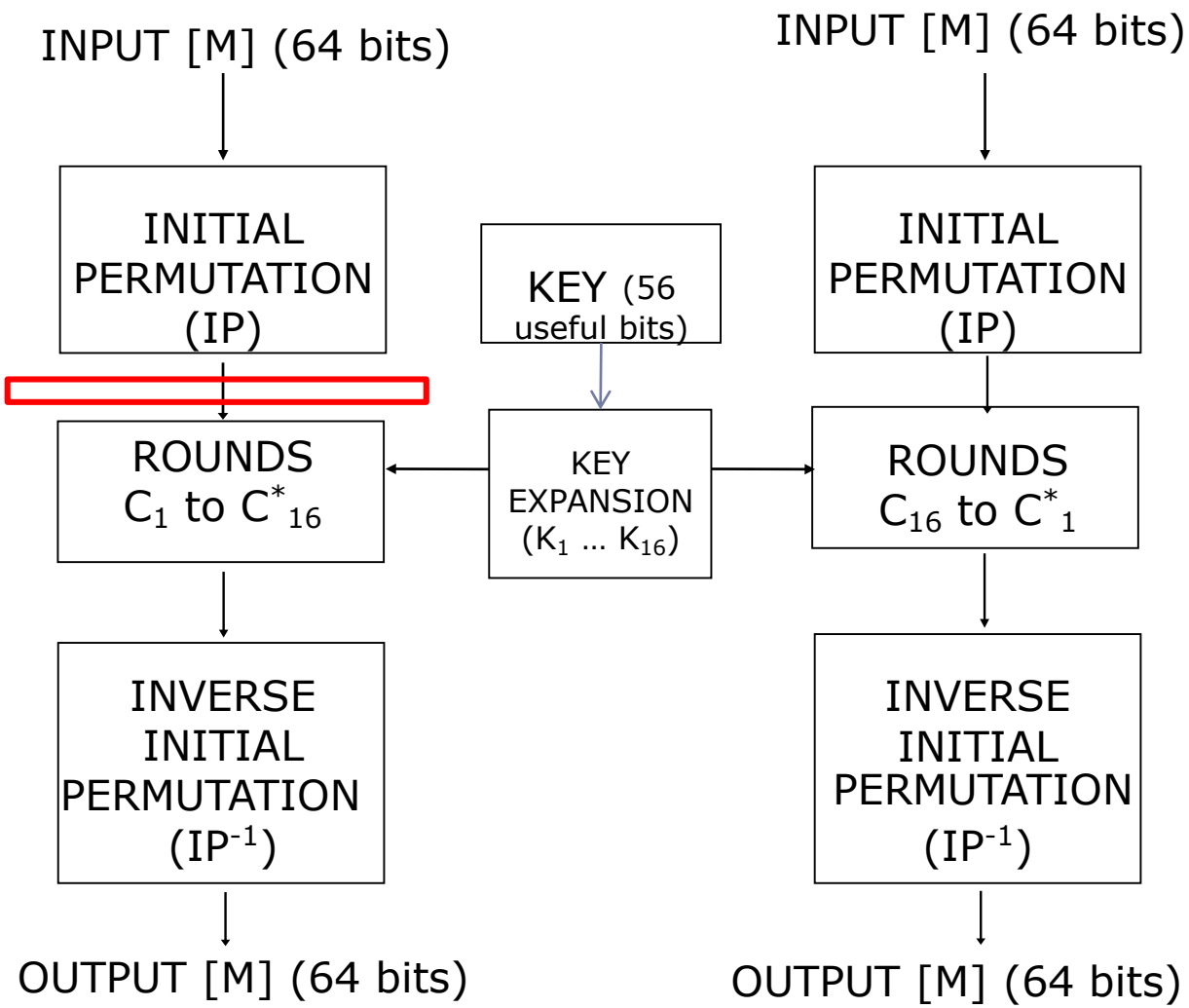
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

L_0 = 58 50 42 34 26 18 10 02 60 52 44
36 28 20 12 04 62 54 46 38 30 22 14
06 64 56 48 40 32 24 16 08

R_0 = 57 49 41 33 25 17 09 01 59 51
43 35 27 19 11 03 61 53 45 37 29 21
13 05 63 55 47 39 31 23 15 07

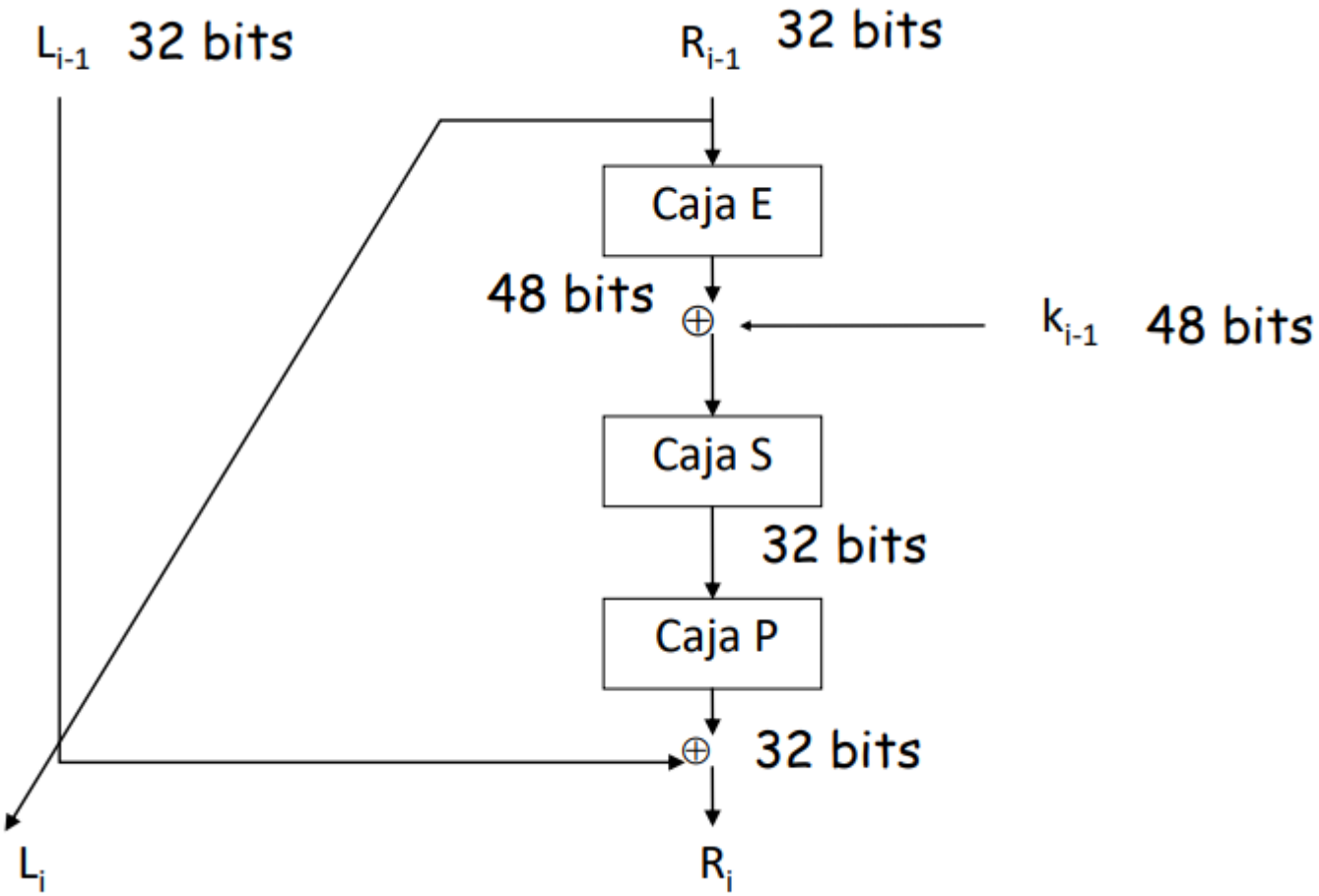
Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

DES: "Situational map"



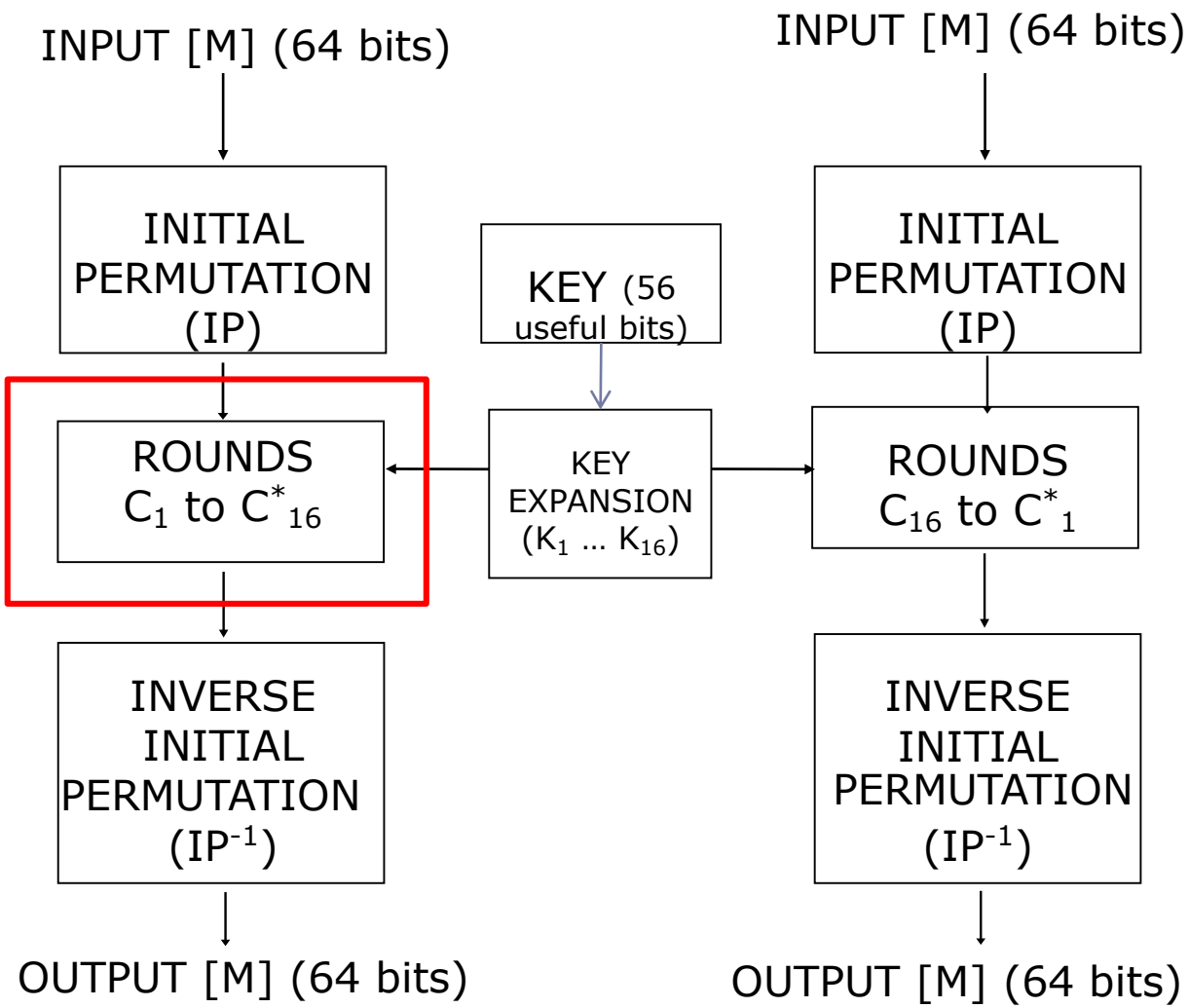
Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

DES: Round scheme



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

DES: "Situational map"



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

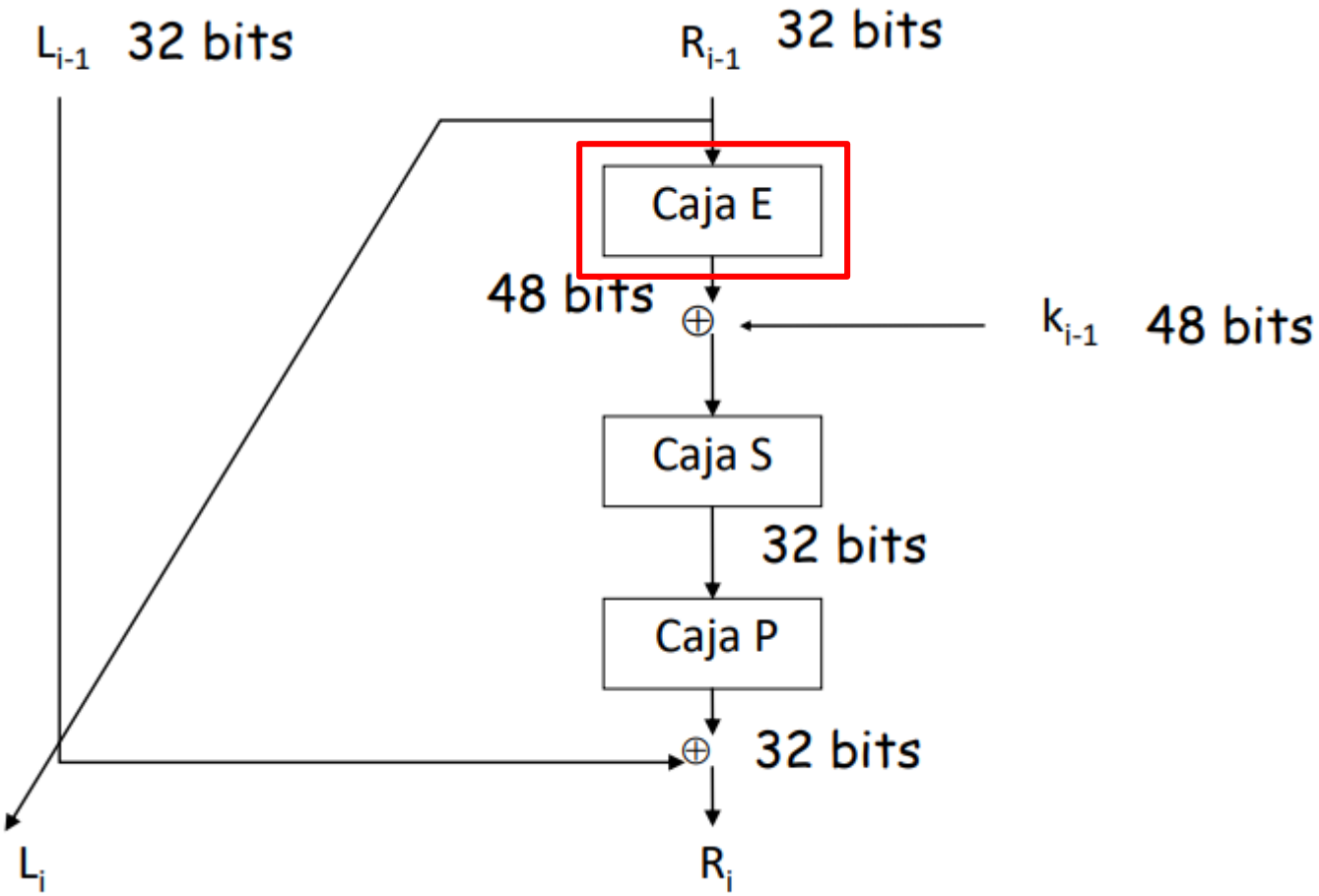
DES: Expansion (E) Box

- From 32 bits to 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

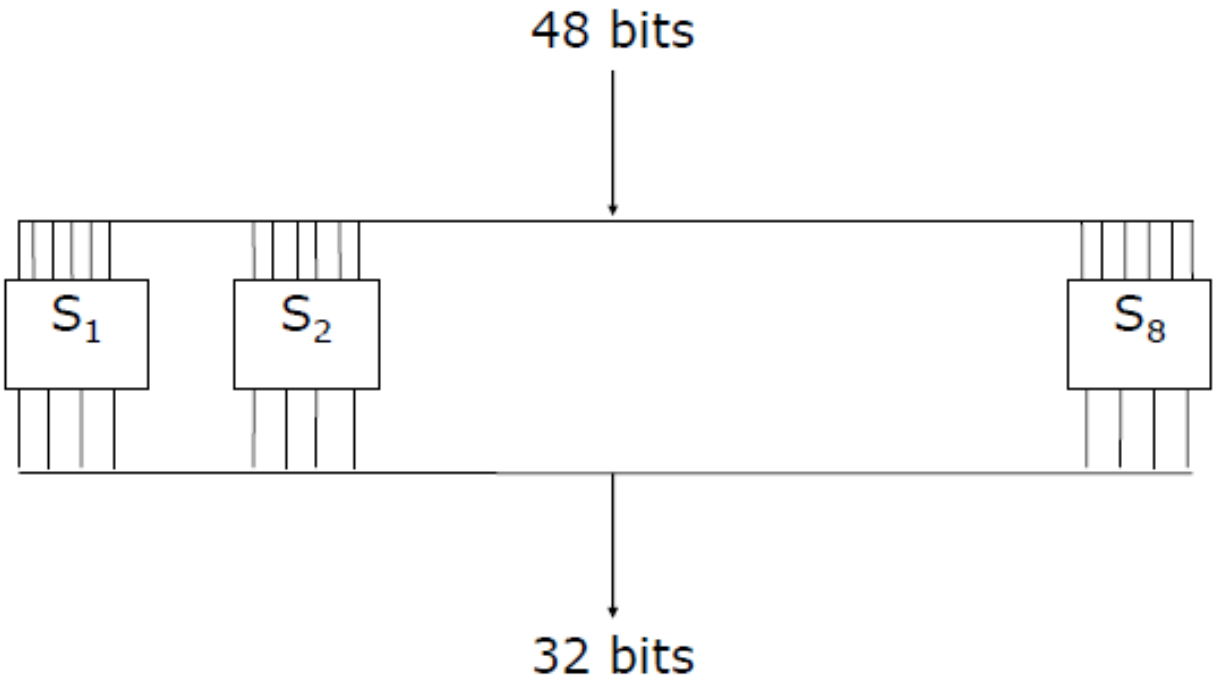
Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

DES: “Situational map” - Round



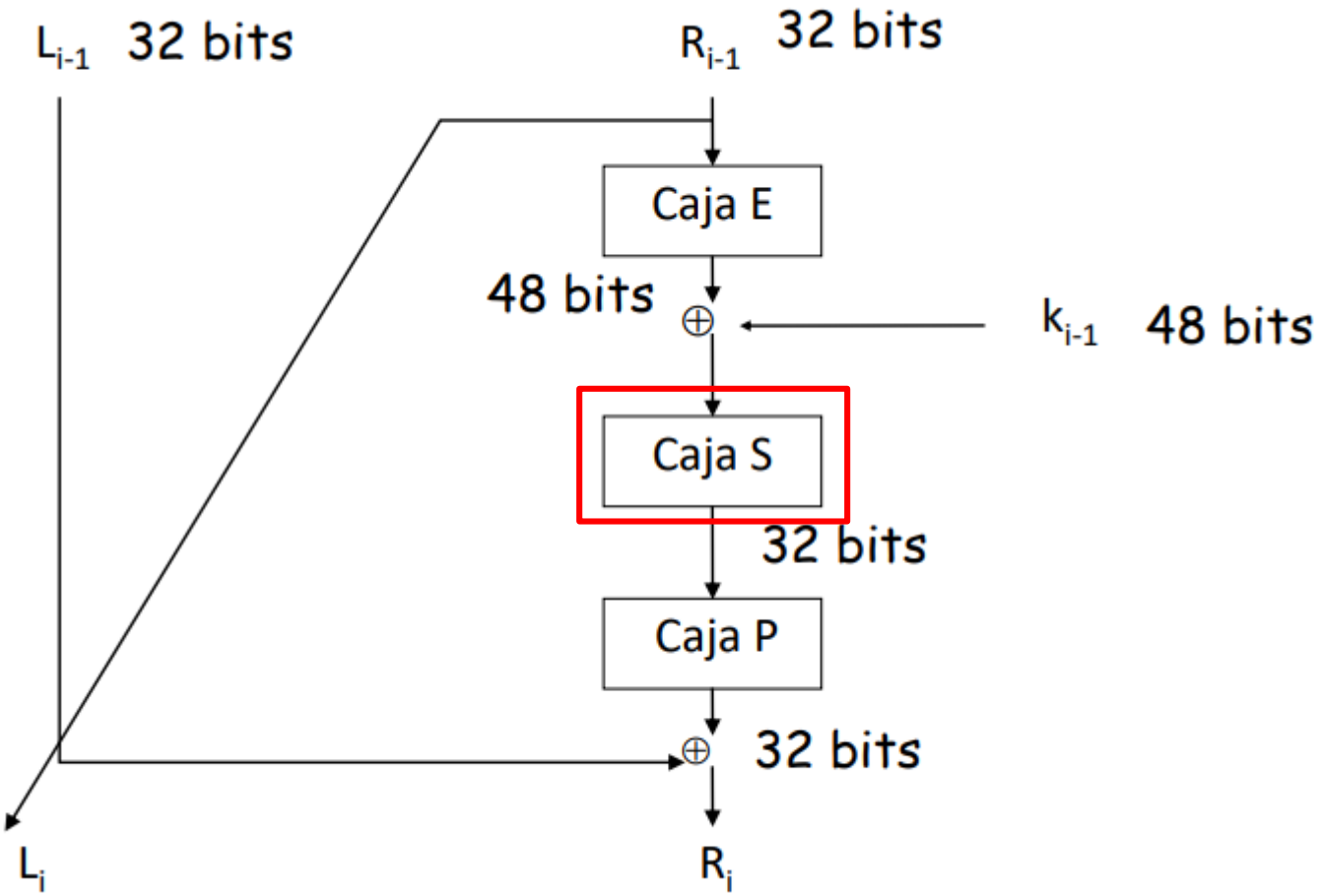
Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

DES: S boxes



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

DES: “Situational map” - Round



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

DES: S boxes

- **8 matrices S_1 , S_2 … S_8, where each S_i receives a 6-bit input b_0,b_1 … b_5**

Nº	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
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

- The decimal value of bit pair b_0 b_5 select a row in matrix S_i
- The decimal value of bits b_1 b_2 b_3 b_4 select a column in S_i
- The output in decimal is the value in the matrix given by the previously
- computed (row, column). Its 4-bit binary value is the output
- Eg: S_1 & input= 110011 -> row 3 (11) and column 9 (1001), with a decimal output of, 11, that corresponds to the binary string 1011

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

DES: S boxes

S_1

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
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

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S_3

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S_4

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

DES: S boxes

S_5

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
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

12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S_7

4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S_8

13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

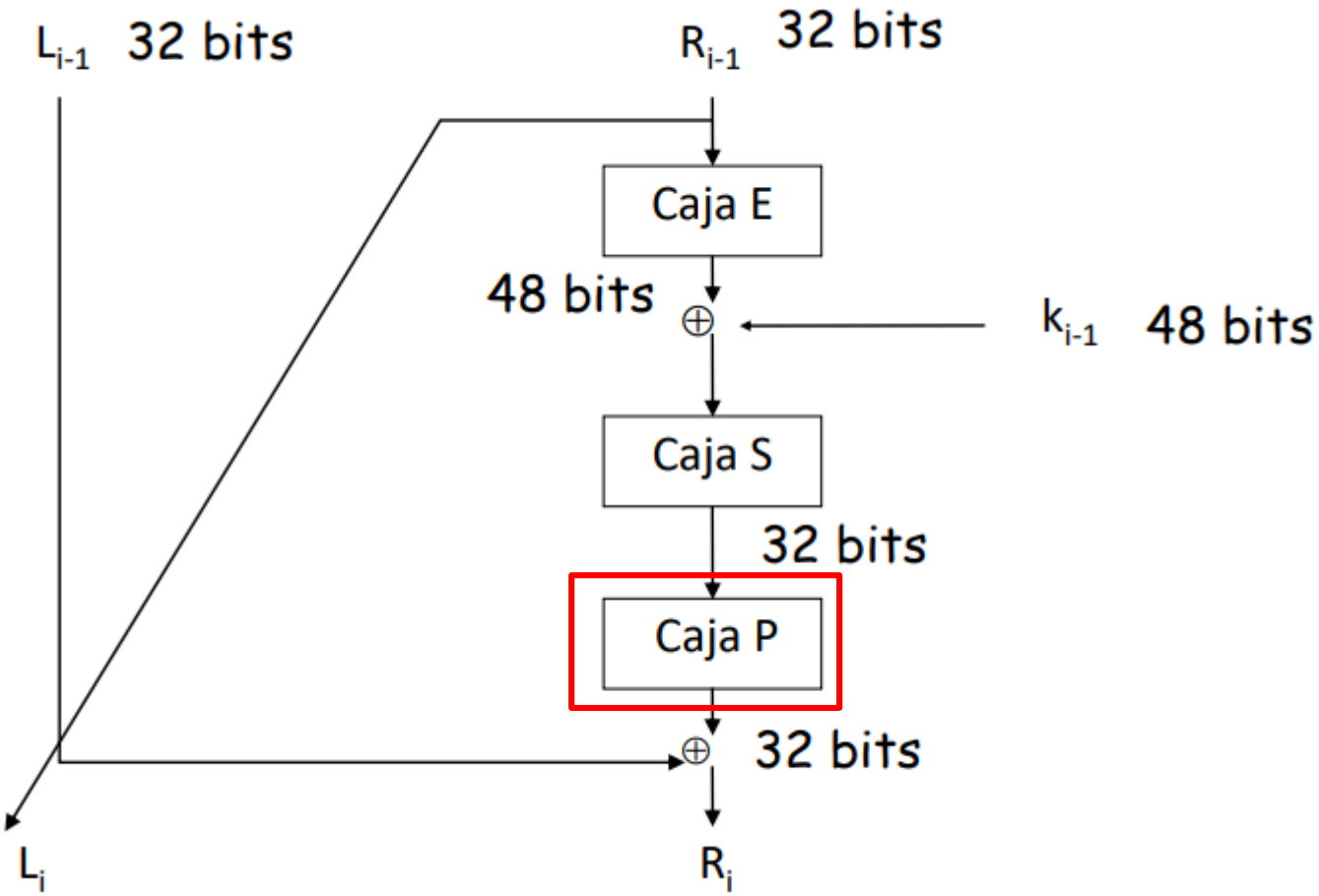
DES: Permutation (P) Box

- From 32 bits to 32 bits

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

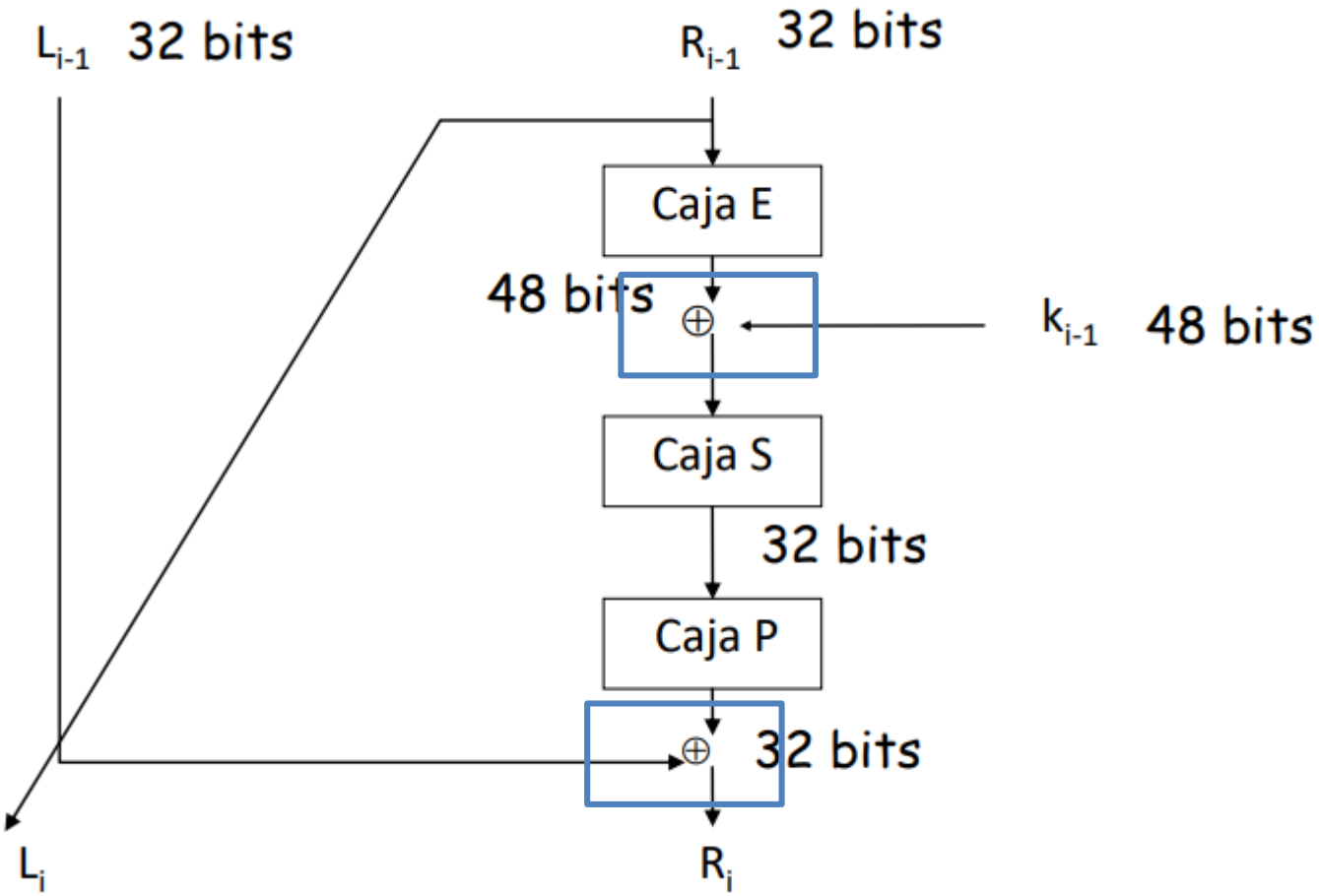
Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

DES: “Situational map” - Round



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

DES: “Situational map” - Round

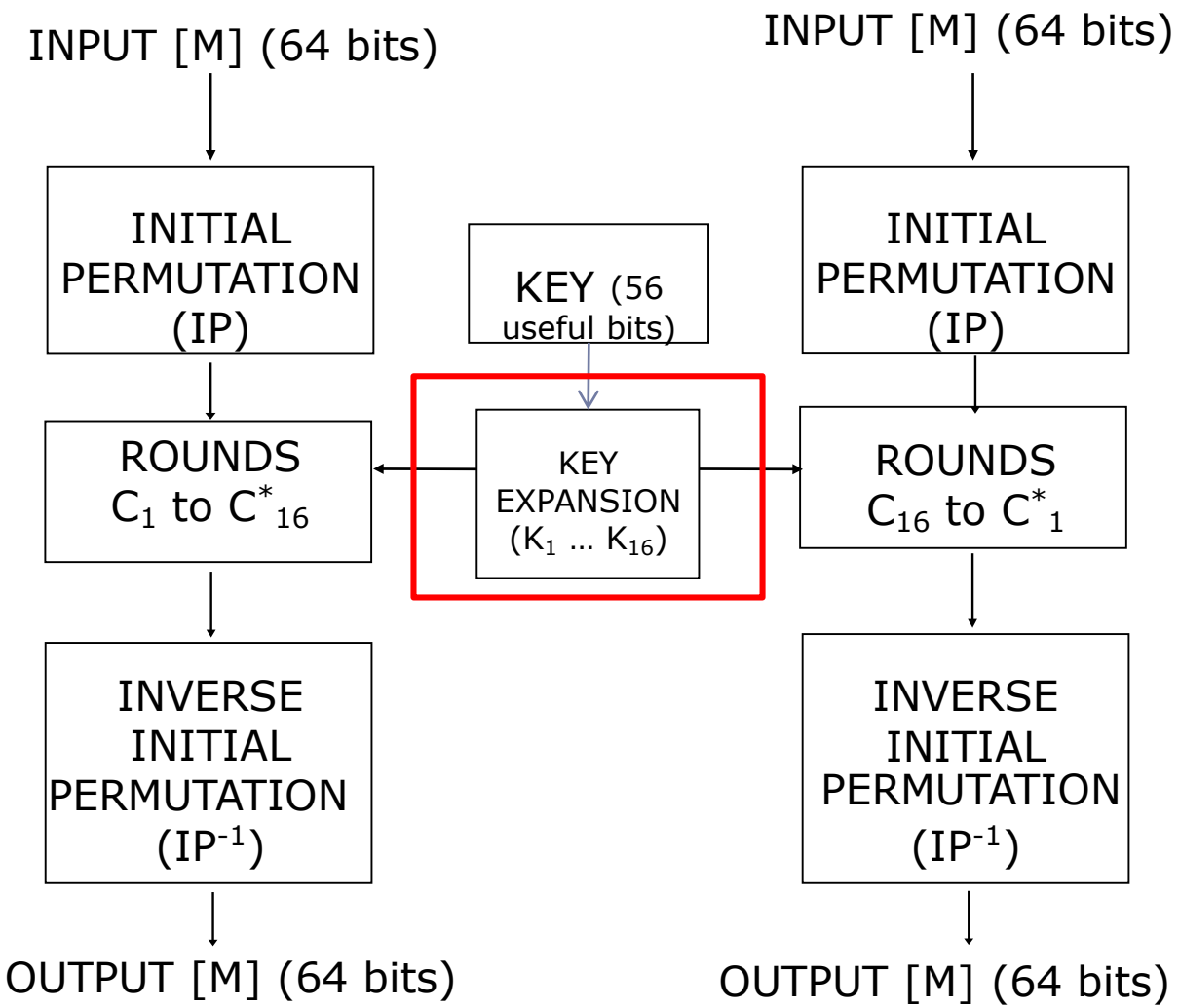


Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

OUTLINE

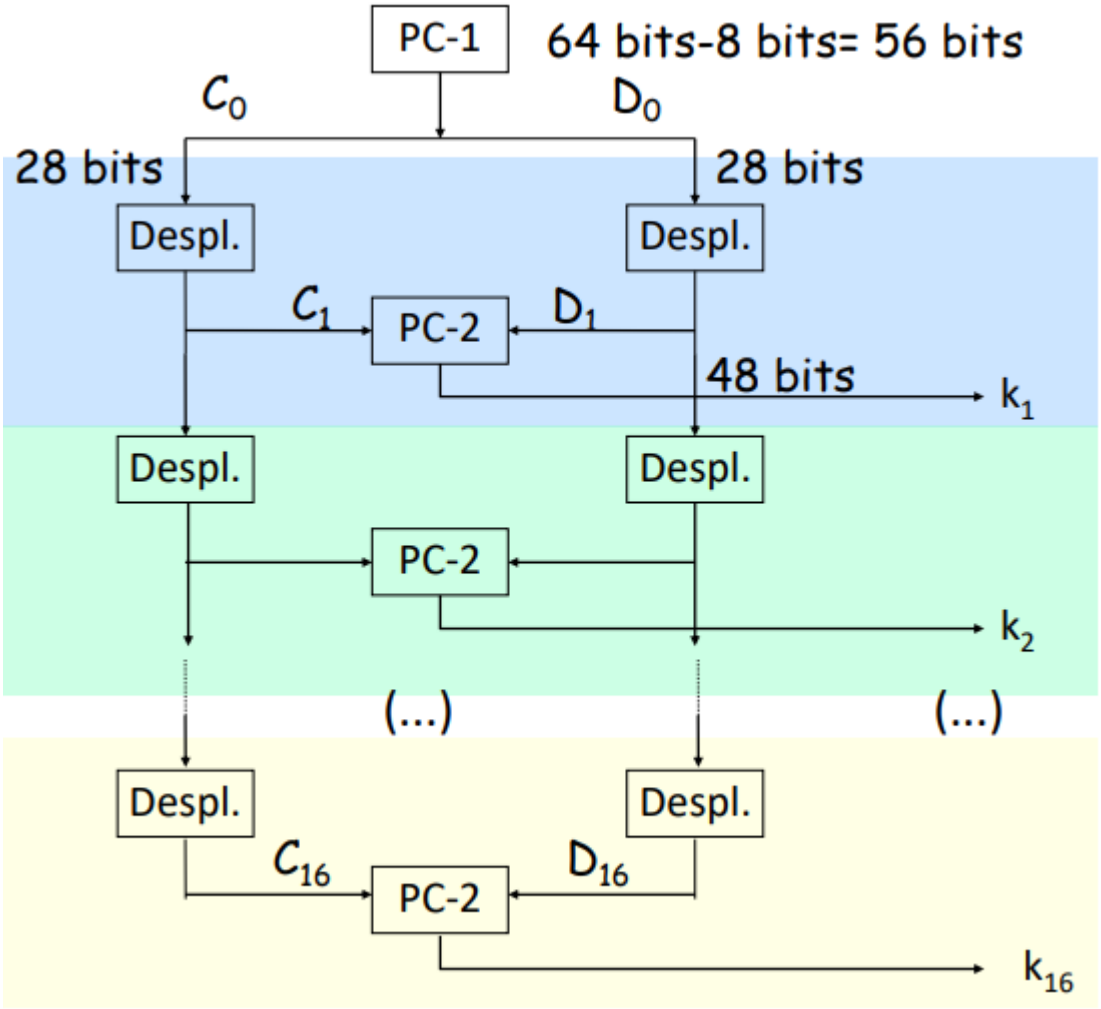
- (…)
  - Data Encryption Standard (DES)
    - Encryption
    - Key expansion
    - Decryption
    - Triple DES
    - Security
  - AES
  - (…)

DES: "Situational map"



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

DES: Generation of internal keys



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

DES: Generation of internal keys

1. Permutation of the key PC-1 => 56 bit.
2. Divide block in 28 bits.
3. i=1
4. Left swift of each block (1 or 2 bits depending on the round)
5. Internal key K_i generation
    1. Concatenation of the 2 blocks => 56 bits
    2. Permutation PC-2 => 48 bit = internal key k_i
    3. i= i +1
    4. Go back to 4 while i<=16
6. Result: 16 internal keys, 48 bits each of them
7. In the encryption process K_1-K_{16} (in the decryption, the inverse order K_{16}-K_1)

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

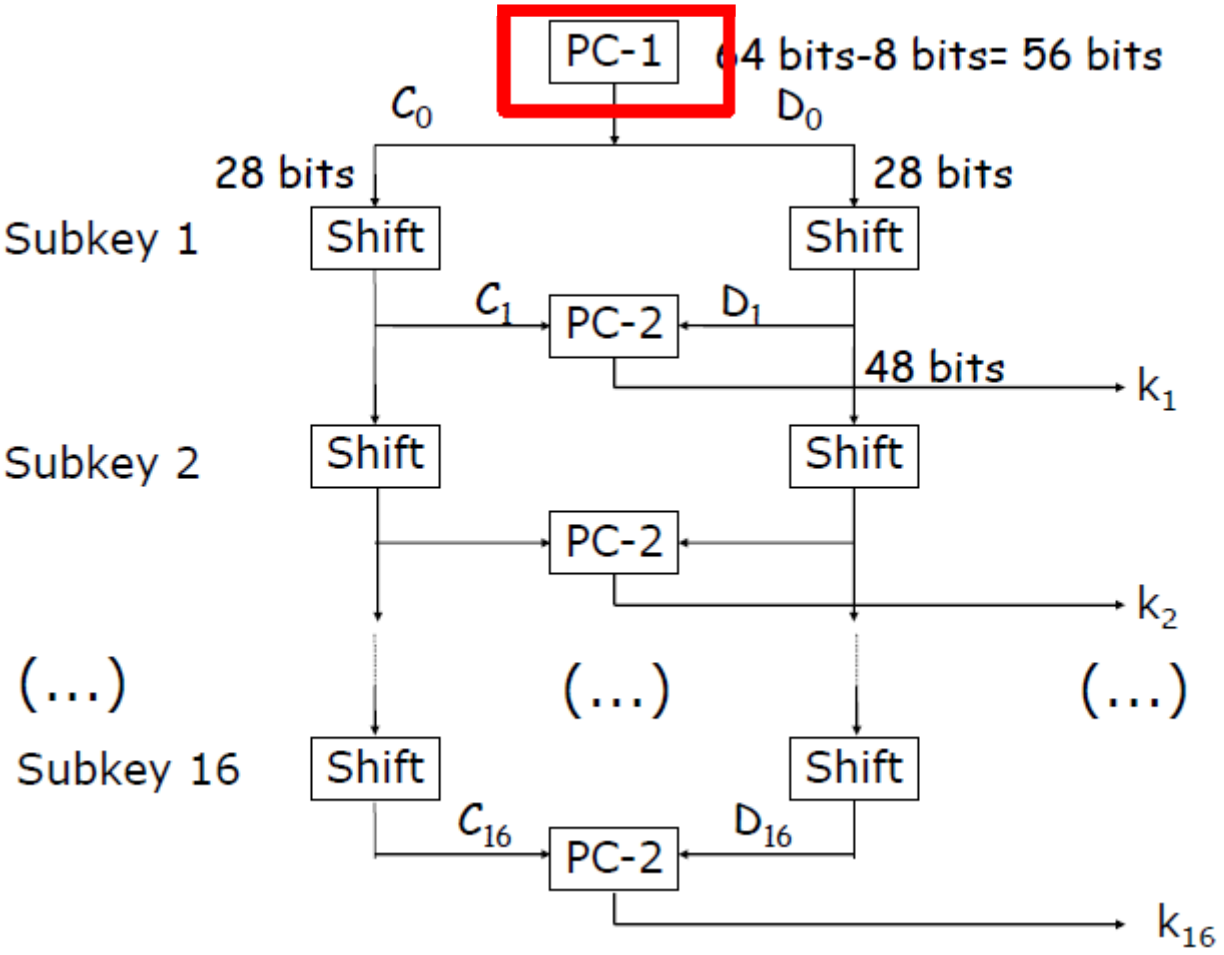
DES: Permutation PC-1

- From 64 bits to 56 bits

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

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

DES: "Situational map" – internal keys



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

DES: Permutation PC-1

- Division in two halves, C_0 y D_0

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

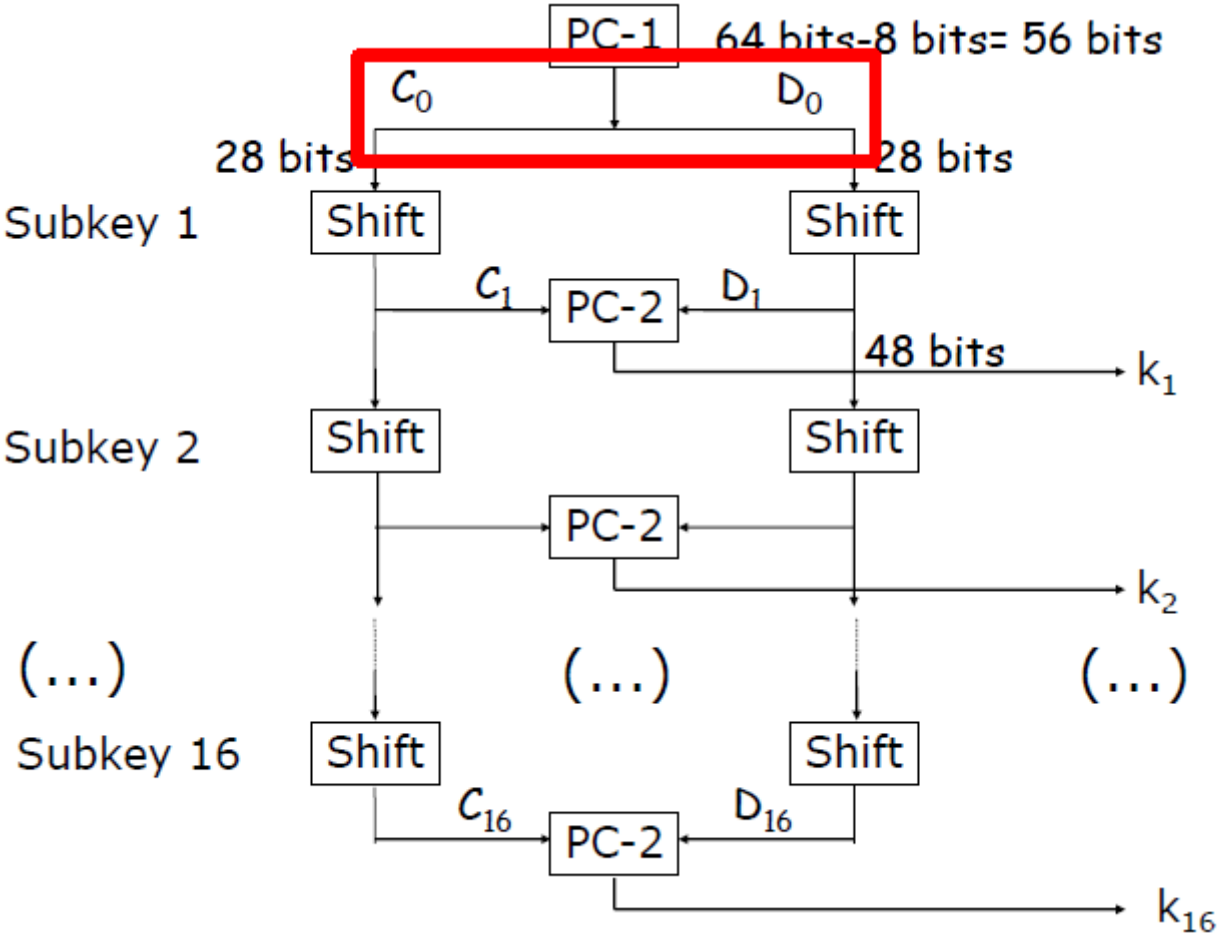
Block C_0

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

Block D_0

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

DES: "Situational map" – internal keys



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

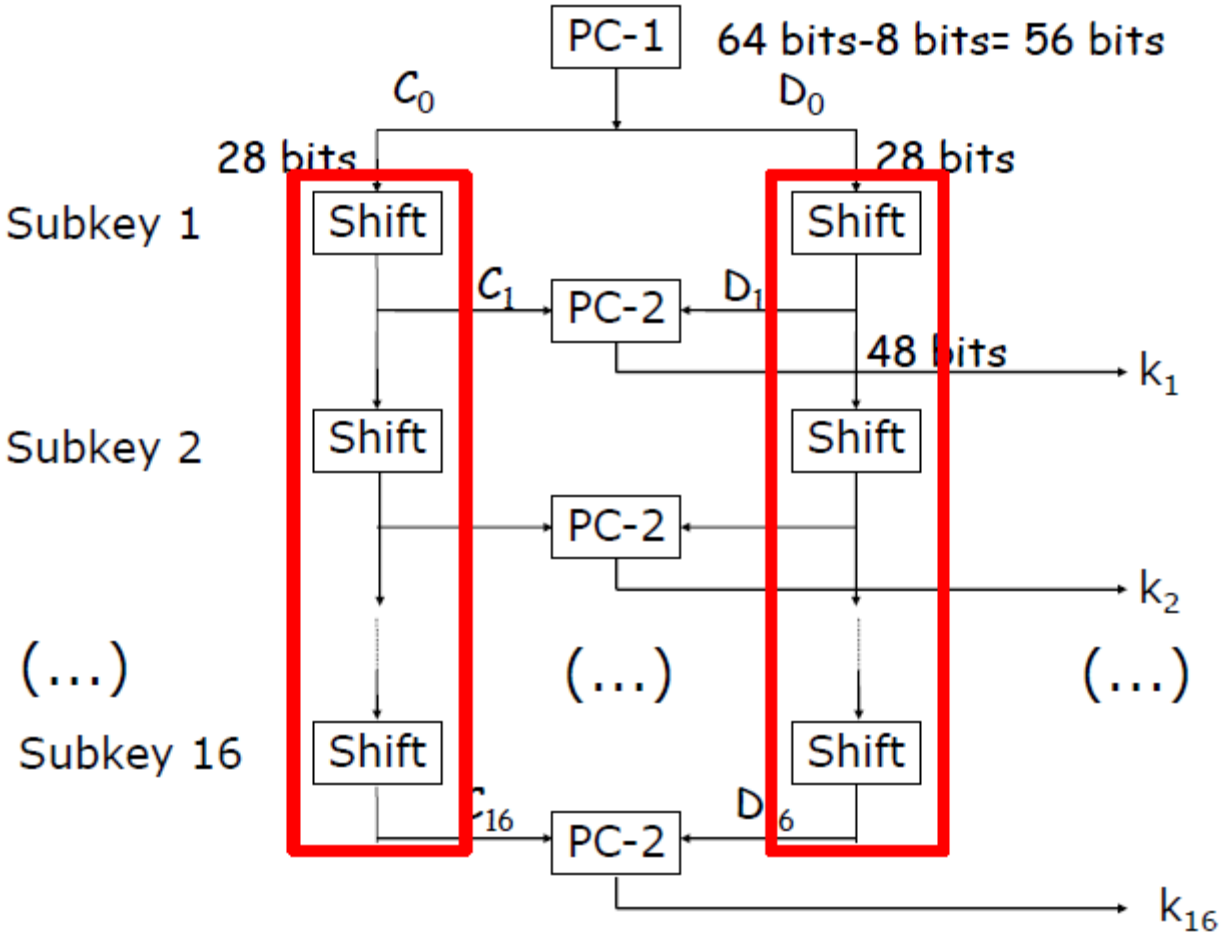
DES: Shift

- Left circular shift within each of the halves

Subkey nº	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

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

DES: "Situational map" – internal keys



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

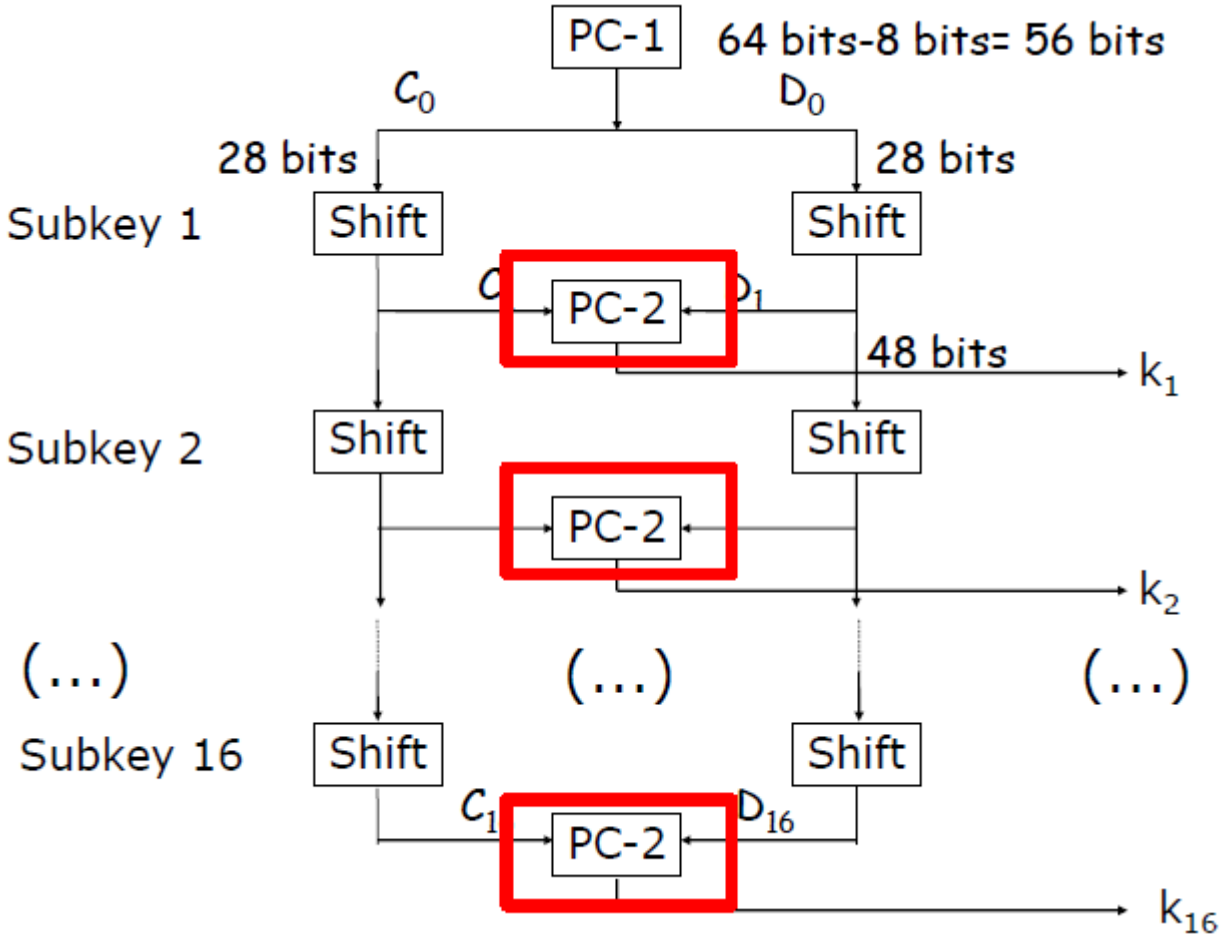
DES: Permutation PC-2

- From 56 bits to 48 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

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

DES: "Situational map" – internal keys



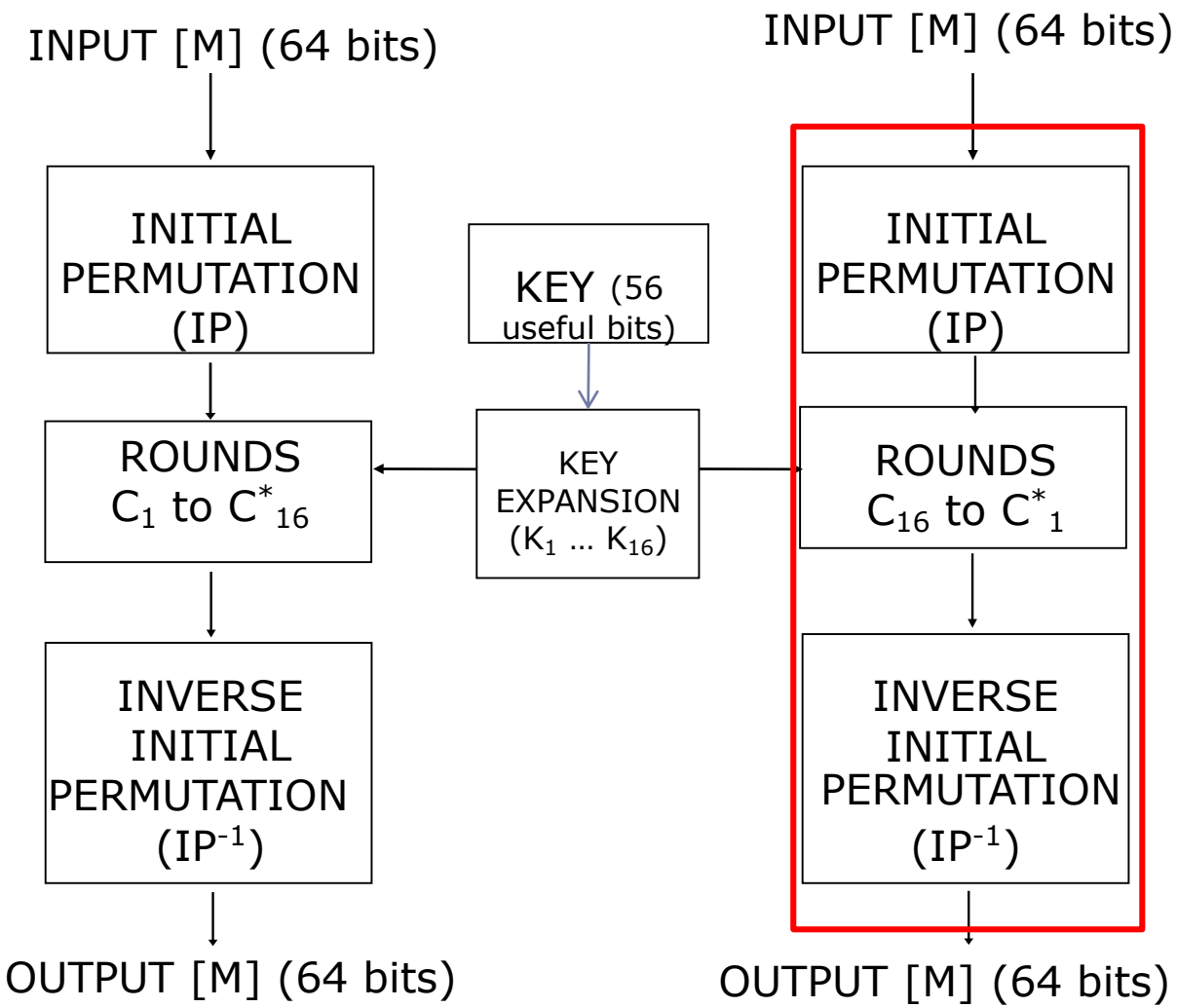
Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

OUTLINE

- (…)
  - Data Encryption Standard (DES)
    - Encryption
    - Key expansion
    - Decryption
    - Triple DES
    - Security
  - AES
  - (…)

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

DES: "Situational map"



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

DES: Decryption

- Same algorithms but with 2 changes
  - Internal keys used in inverse order
- The key expansion algorithm is the same, but it should be computed "going up" instead of "going down"
  - After PC-1: $C_0=C_{16}$ and $D_0=D_{16}$
  - Swift to C_i and D_i should be "right swifts"

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

OUTLINE

- (…)
  - Data Encryption Standard (DES)
    - Encryption
    - Key expansion
    - Decryption
    - Triple DES
    - Security
  - AES
  - (…)

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

Triple DES (TDES)

- 3 DES con 2 claves => clave de 112 bit
  - $C = E(k_1, D(k_2, E(k_1,M)))$
  - Compatibility with simple DES if $k_1=k_2$
- 3 DES con 3 claves => clave de 112 bit
  - $C = E(k_3, D(k_2, E(k_1,M)))$
- Cost of the meet in the middle attack 2^{112}

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

OUTLINE

- (…)
  - Data Encryption Standard (DES)
    - Encryption
    - Key expansion
    - Decryption
    - Triple DES
    - Security
  - AES
  - (…)

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

Security

- Attacks to DES
  - Frute force
    - Broken in less than one day

    http://www.sciengines.com/company/news-a-events/74-des-in-1-day.html
  - Differential cryptoanalysis (Biham and Shamir)
    - 2^{47} chosen plaintexts needed. Effort on 2^{47} encryptions
    - Lucifer was vulnerable but DES is not
  - Linear Cryptanalysis (Matsui)
    - 2^{43} knownplaintexts needed
- Attack to Triple DES
  - Meet-in-the-middle attack
    - Reduces the effort to an order of 256

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

OUTLINE

- 5. Symmetric encryption: Block ciphers
  - Modern encryption
  - Block ciphers
    - Introduction
    - Feistel scheme
    - Operation modes
    - Block ciphers: advantages and disadvantages
    - DES
    - AES

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

Advanced Standard Encryption (AES)

- **A**dvanced **E**ncryption **S**tandard
- Standard for symmetric encryption (block cipher)
- NIST contest to substitute DES
  - Government communications
  - Bank transfers
  - Electronic commerce
  - Etc.

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

Advanced Standard Encryption (AES)

- At least as secure as 3DES but faster in SW
- Symmetric block cipher
- Block size: 128 (16 bytes)
- Key sizes: 128, 192, 296

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

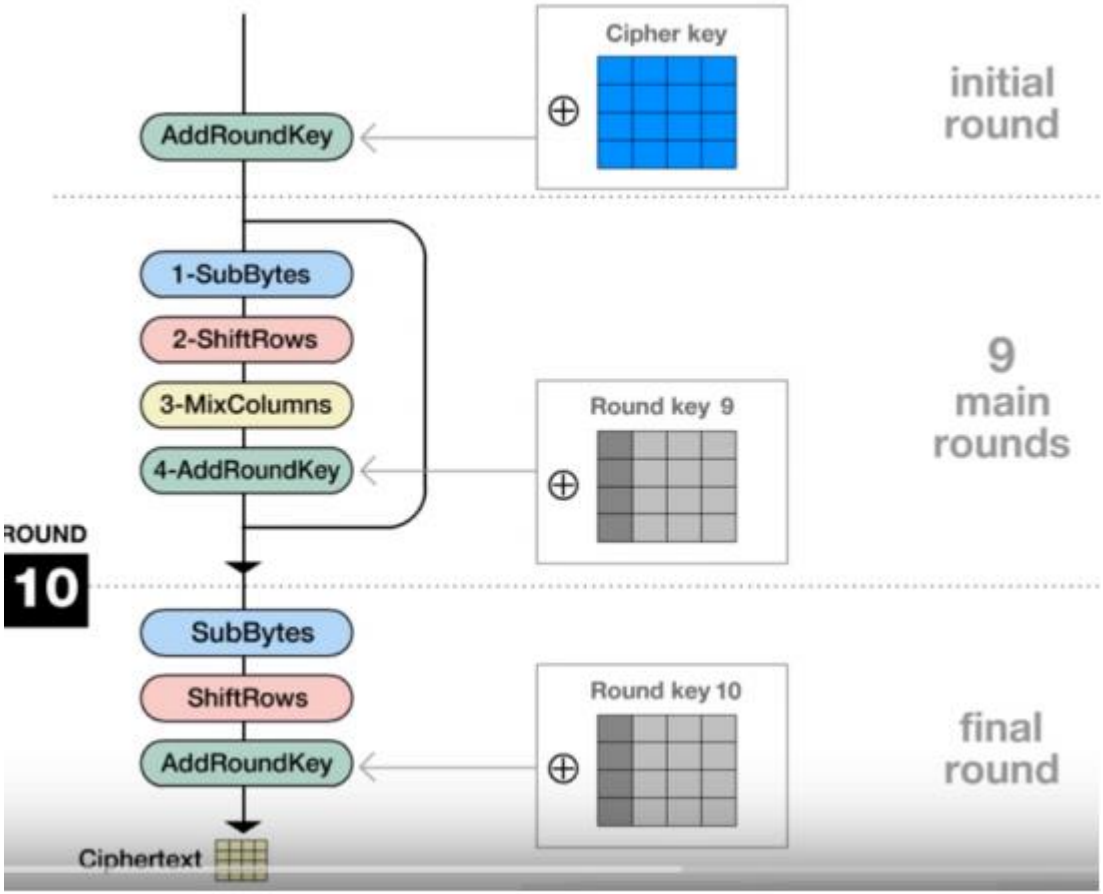
AES: Evaluation criteria

Security	Cost	Features
• Compared to the other proposals • Output indistinguishable from a random permutation • Sound Mathematical foundations • Resistance against known cryptanalitical attacks	• No royalties • Efficiency – both in HW and SW • Memory requirements	• Flexibility Able to manage different block and key sizes • Simplicity

AES: Winner features

- Operates on blocks of 16 bytes (128 bits)
- Accepts 3 key sizes 128, 192, 256 bits
- Substitución-permutation network (not a Feistel network)
- Fast in SW and HW, easy to implement and low memory requirements
- Based on 4 reversable functions, applied n rounds
- State matrix evolution

AES scheme



Author: Enrique Zabala
http://www.formaestudio.com/rijndaelinspector/

- Encryption functions (from the top to the bottom):
  - *AddRoundKey*
  - *ByteSub*
  - *ShiftRow*
  - *MixColumns*
- Decryption functions (from the bottom to the top):
  - *InvAddRoundKey*
  - *InvByteSub*
  - *InvShiftRow*
  - *InvMixColumns*

AES: key bytes and states

- Key bytes and state bytes are placed in rectangular arrays

k 0,0	k 0,1	k 0,2	k 0,3	k 0,4	k 0,5	k 0,6	k 0,7
k 1,0	k 1,1	k 1,2	k 1,3	k 1,4	k 1,5	k 1,6	k 1,7
k 2,0	k 2,1	k 2,2	k 2,3	k 2,4	k 2,5	k 2,6	k 2,7
k 3,0	k 3,1	k 3,2	k 3,3	k 3,4	k 3,5	k 3,6	k 3,7

Key sizes:
16, 24 or 32 bytes

Variable block size:
16, 24 or 32 bytes
AES: 16 bytes

a 0,0	a 0,1	a 0,2	a 0,3	a 0,4	a 0,5	a 0,6	a 0,7
a 1,0	a 1,1	a 1,2	a 1,3	a 1,4	a 1,5	a 1,6	a 1,7
a 2,0	a 2,1	a 2,2	a 2,3	a 2,4	a 2,5	a 2,6	a 2,7
a 3,0	a 3,1	a 3,2	a 3,3	a 3,4	a 3,5	a 3,6	a 3,7

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

RINDAEL algorithm

```
Rijndael(State, Key) {
    KeyExpansion( Key, ExpandedKey );
    AddRoundKey( State, ExpandedKey );
    for (i=1; i<10; i++)
      Round(State, ExpandedKey+4);
    FinalRound(State,ExpandedKey+4X10);
}
```

```
Round(State, RoundKey) {
    ByteSub(State);
    ShiftRow(State);
    MixColumn(State);
    AddRoundKey(State,
    RoundKey);
}
```

State	-- array of 4 words (de 32 bits)
No. of Rounds	-- 9 rounds
KeyExpansion	-- XOR of the keywords, S-box lookups, rotation of bytes intra-word
AddRoundKey	-- bitwise-XOR with the keywords
FinalRound	-- similar to a Round but without MixColumn

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

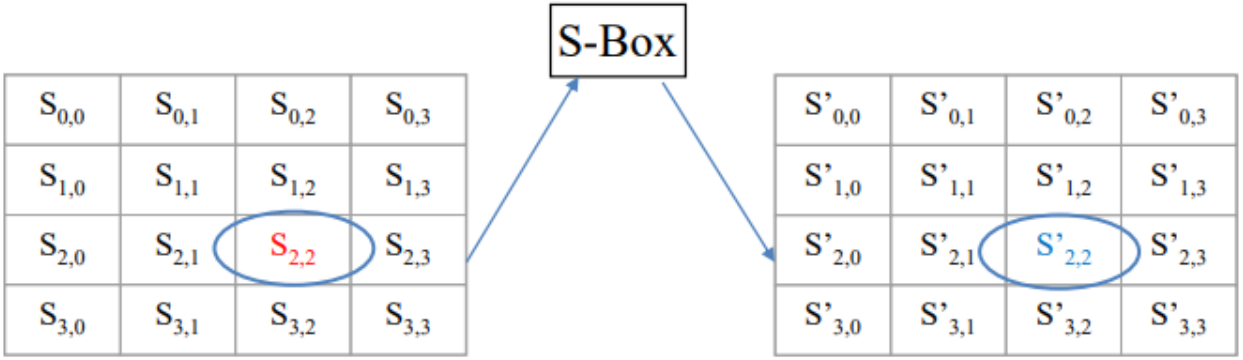
AES: Operation with bytes

- Additions and multiplications: Galois field GF(2^8) with 8 bits
- The following polynomial is used:

$$p(x) = x^8 + x^4 + x^3 + x + 1.$$

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

AES: SubByte function



$$\begin{pmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{pmatrix} = \begin{pmatrix} 1&0&0&0&1&1&1&1 \\ 1&1&0&0&0&1&1&1 \\ 1&1&1&0&0&0&1&1 \\ 1&1&1&1&0&0&0&1 \\ 1&1&1&1&1&0&0&0 \\ 0&1&1&1&1&1&0&0 \\ 0&0&1&1&1&1&1&0 \\ 0&0&0&1&1&1&1&1 \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

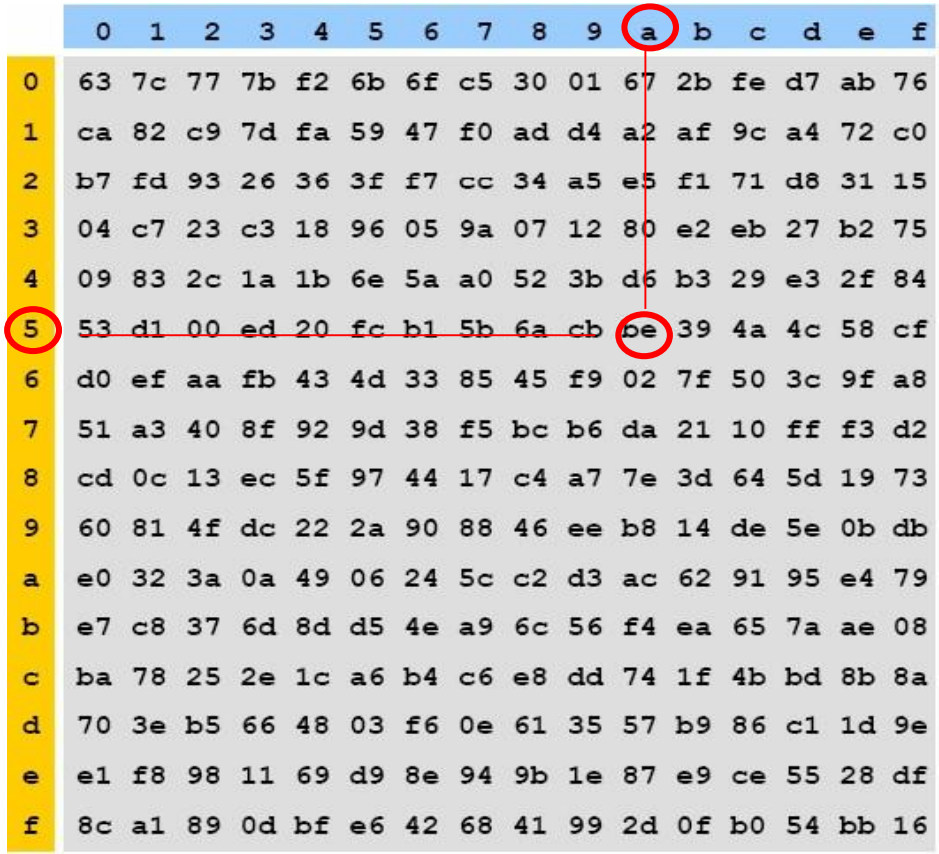
Value $\{63\}_{16}$ or $\{01100011\}_2$

Inverse of the input

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

AES: SubByte table

- The inverse of the input can be also computed through this table
- 5a => be



	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

AES: SubByte example

- Calculus of SubByte(5a)

5a = 01011010 = $x^6 + x^4 + x^3 + x + 1$

inv (5A) = 22 = 00100010

$$\begin{pmatrix} 1&0&0&0&1&1&1&1 \\ 1&1&0&0&0&1&1&1 \\ 1&1&1&0&0&0&1&1 \\ 1&1&1&1&0&0&0&1 \\ 1&1&1&1&1&0&0&0 \\ 0&1&1&1&1&1&0&0 \\ 0&0&1&1&1&1&1&0 \\ 0&0&0&1&1&1&1&1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

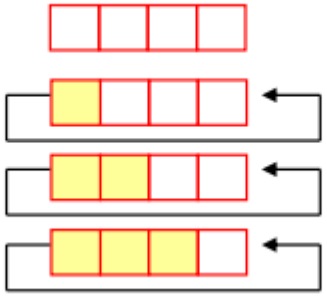
- Once operations are performed, the result is: 1011 1110 = be (the same as using the table)

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

AES: Shiftrows function

- Row 0 => no swift
- Row 1 => Swift 1 byte
- Row 2 => Swift 2 bytes
- Row 3 => Swift 3 bytes

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$



$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,1}$	$S_{1,2}$	$S_{1,3}$	$S_{1,0}$
$S_{2,2}$	$S_{2,3}$	$S_{2,0}$	$S_{2,1}$
$S_{3,3}$	$S_{3,0}$	$S_{3,1}$	$S_{3,2}$

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

AES: Mixcolumns function

- We work in GF(28). Polynomial $p(x) = x^8 + x^4 + x^3 + x + 1$.
- Remember: {03} = x + 1, {02} = x, {01} = 1.

$$\begin{pmatrix} S'_{0,C} \\ S'_{1,C} \\ S'_{2,C} \\ S'_{3,C} \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} S_{0,C} \\ S_{1,C} \\ S_{2,C} \\ S_{3,C} \end{pmatrix}$$

- Operations over each column:

$$S'_{0,C} = (\{02\} \bullet S_{0,C}) \oplus (\{03\} \bullet S_{1,C}) \oplus S_{2,C} \oplus S_{3,C}$$
$$S'_{1,C} = S_{0,C} \oplus (\{02\} \bullet S_{1,C}) \oplus (\{03\} \bullet S_{2,C}) \oplus S_{3,C}$$
$$S'_{2,C} = S_{0,C} \oplus S_{1,C} \oplus (\{02\} \bullet S_{2,C}) \oplus (\{03\} \bullet S_{3,C})$$
$$S'_{3,C} = (\{03\} \bullet S_{0,C}) \oplus S_{1,C} \oplus S_{2,C} \oplus (\{02\} \bullet S_{3,C})$$

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

AES: Mixcolumns example

- We assume this is the intermediate state

e1	a8	63	0d
fb	18	f4	c8
96	5b	73	11
7c	a0	e6	fd

- The first byte of the state matrix ($S'_{0,0}$) is:

$$S'_{0,0} = \{02\}S_{0,0} \oplus \{03\}S_{1,0} \oplus S_{2,0} \oplus S_{3,0}\,;\; S'_{0,0} = \{02\}e1 \oplus \{03\}fb \oplus 96 \oplus 7c$$

$$\{02\}e1 = x(x^7 + x^6 + x^5 + 1) = x^8 + x^7 + x^6 + x\,;$$

$$\{02\}e1 = (x^8 + x^7 + x^6 + x) \bmod (x^8 + x^4 + x^3 + x + 1) = d9$$

$$\{03\}fb = (x + 1)(x^7 + x^6 + x^5 + x^4 + x^3 + x + 1)$$

$$\{03\}fb = x^8 + x^3 + x^2 + 1$$

$$\{03\}fb = (x^8 + x^3 + x^2 + 1) \bmod (x^8 + x^4 + x^3 + x + 1) = 16$$

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

AES: Mixcolumns example

- The first byte of the state matrix ($S'_{0,0}$) is:

$$S'_{0,0} = \{02\}S_{0,0} \oplus \{03\}S_{1,0} \oplus S_{2,0} \oplus S_{3,0}\,;\; S'_{0,0} = \{02\}e1 \oplus \{03\}fb \oplus 96 \oplus 7c$$

$$\{02\}e1 = (0000\ 0010)(1110\ 0001) = (1\ 1100\ 0010);$$

$$\{02\}e1 = (1\ 1100\ 0010) \oplus (1\ 0001\ 1011) = (1101\ 1000) = d9$$

$$\{03\}fb = (0000\ 0011)\ (1111\ 1011) = (0000\ 0010)\ (1111\ 1011) \oplus (1111\ 1011)$$

$$\{02\}fb = (0000\ 0010)\ (1111\ 1011) = (1\ 1111\ 0110)$$

$$\{02\}fb = (1\ 1111\ 0110) \oplus (1\ 0001\ 1011) = (1110\ 1101)$$

$$\{03\}fb = (1110\ 1101) \oplus (1111\ 1011) = (0001\ 0110) = 16$$

$$S'_{0,0} = d9 \oplus 16 \oplus 96 \oplus 7c$$

Then: $S'_{0,0} = 25$

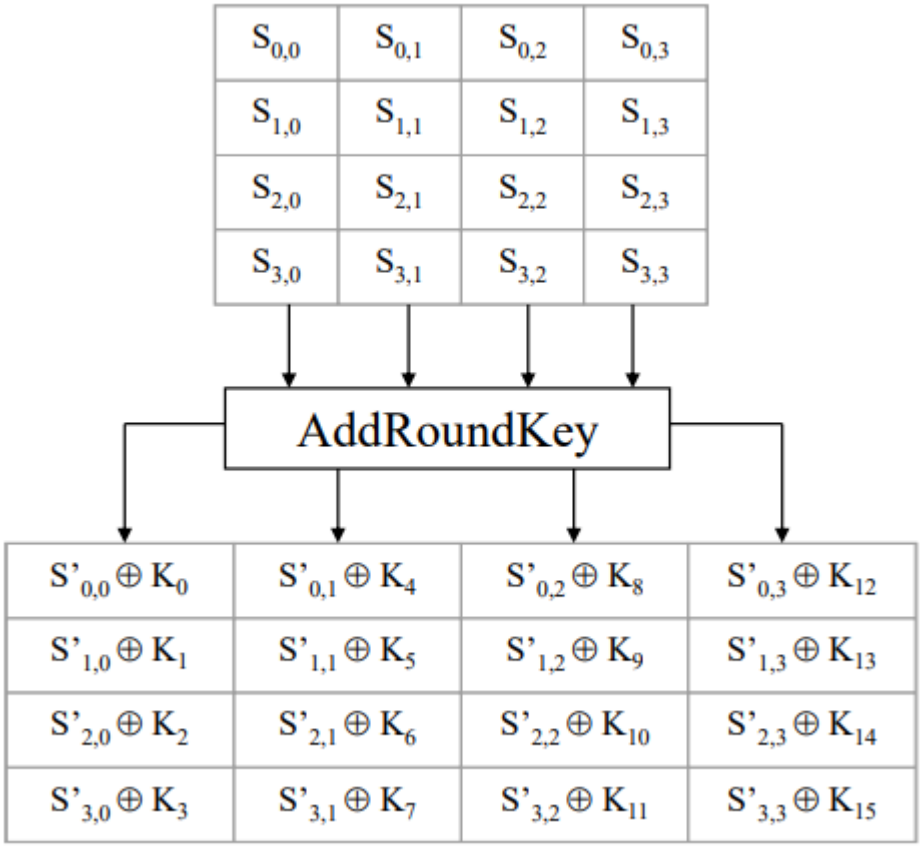
Similar calculations are computed until byte $S'_{4,4}$

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

AES: AddRoundKey functin

AddRoundKey, XOR between the State and the round subkey.

Goal – round function does not depend on the key



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

CRYPTOGRAPHY AND COMPUTER SECURITY

COSEC

uc3m | Universidad Carlos III de Madrid