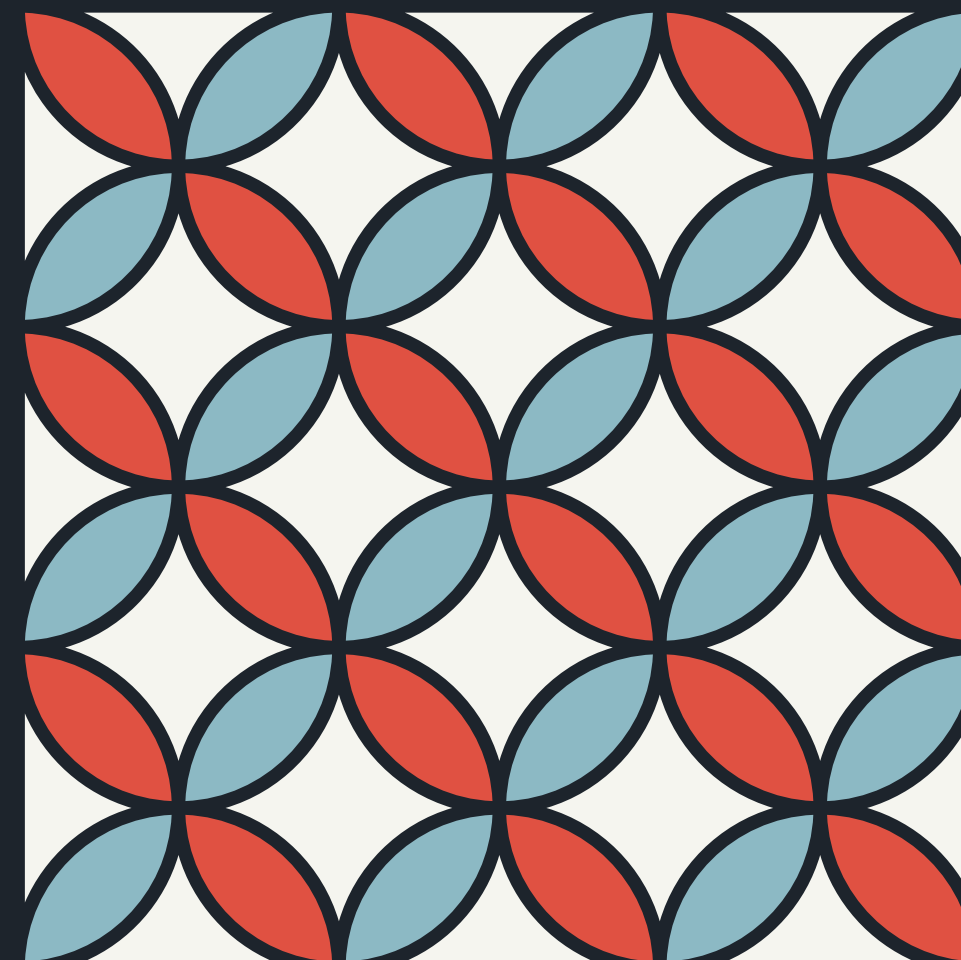
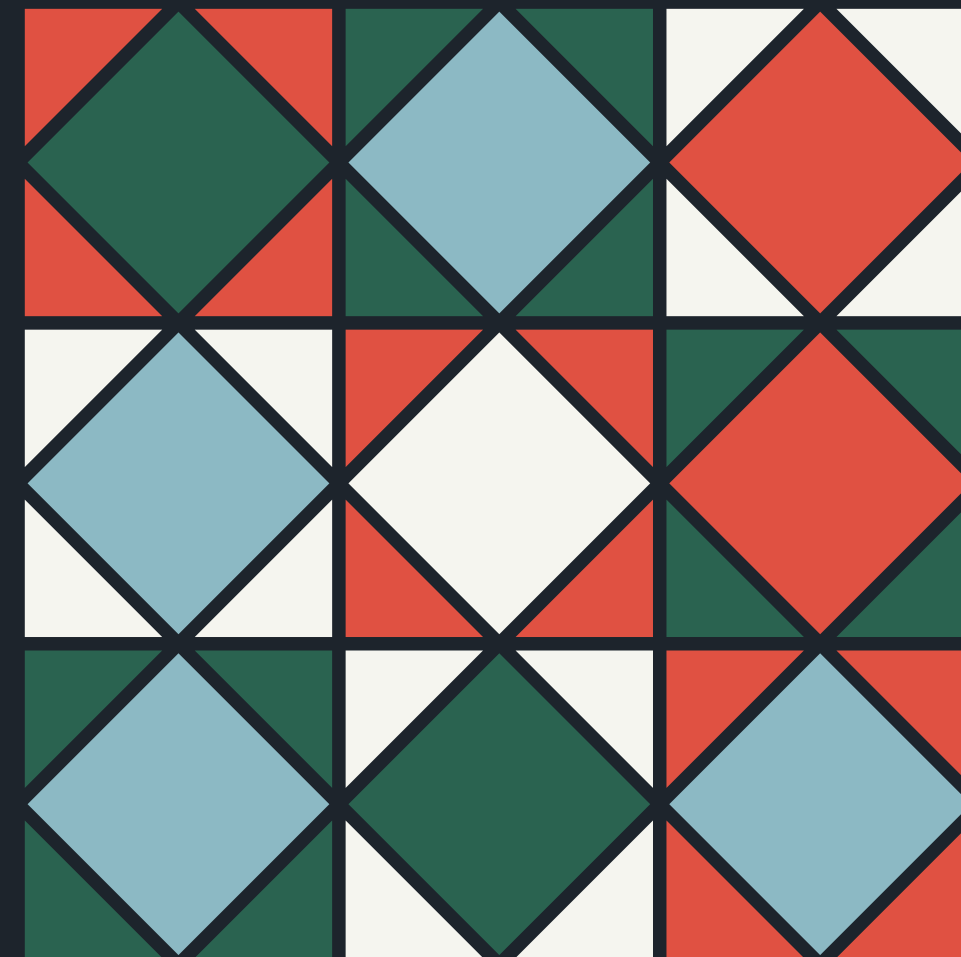
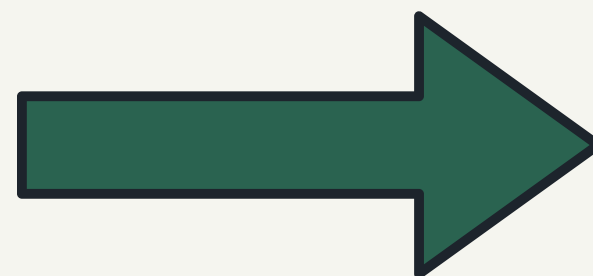
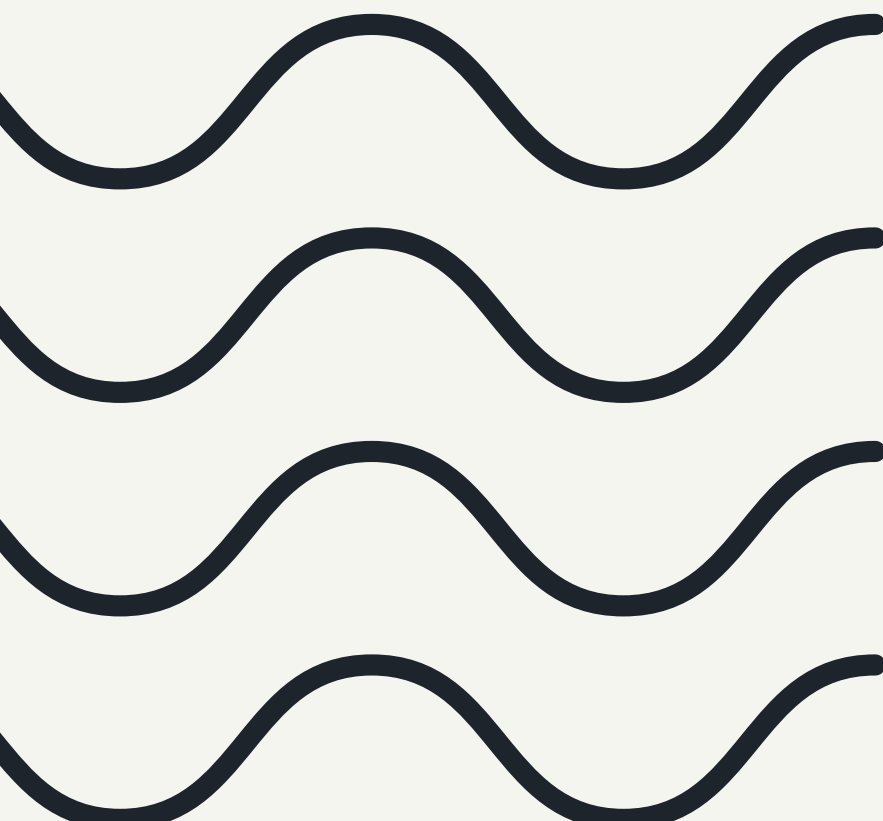


# CIFRADO POR BLOQUES

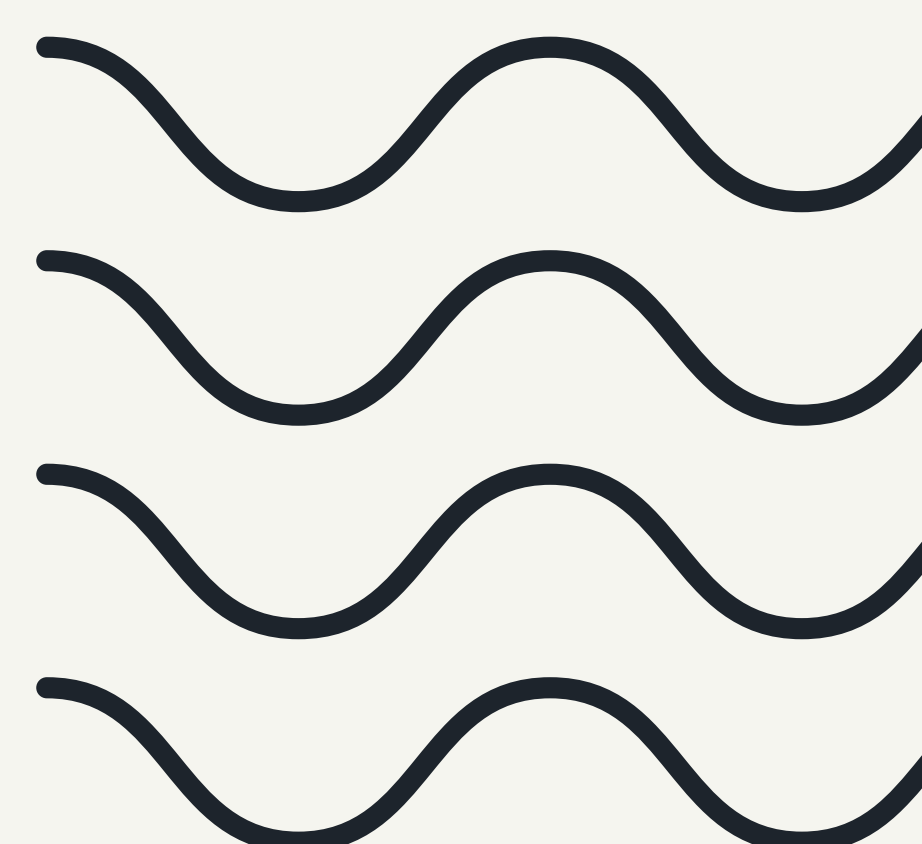
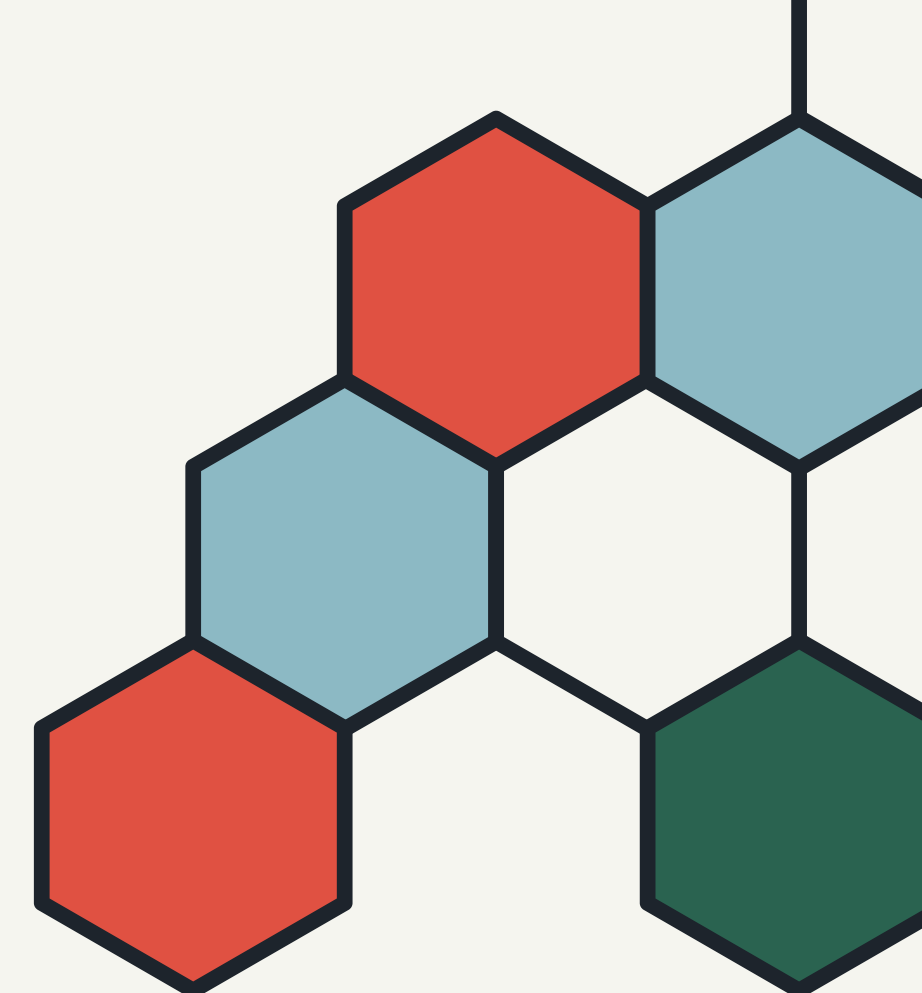
Sistemas operativos 2022-1





# Integrantes

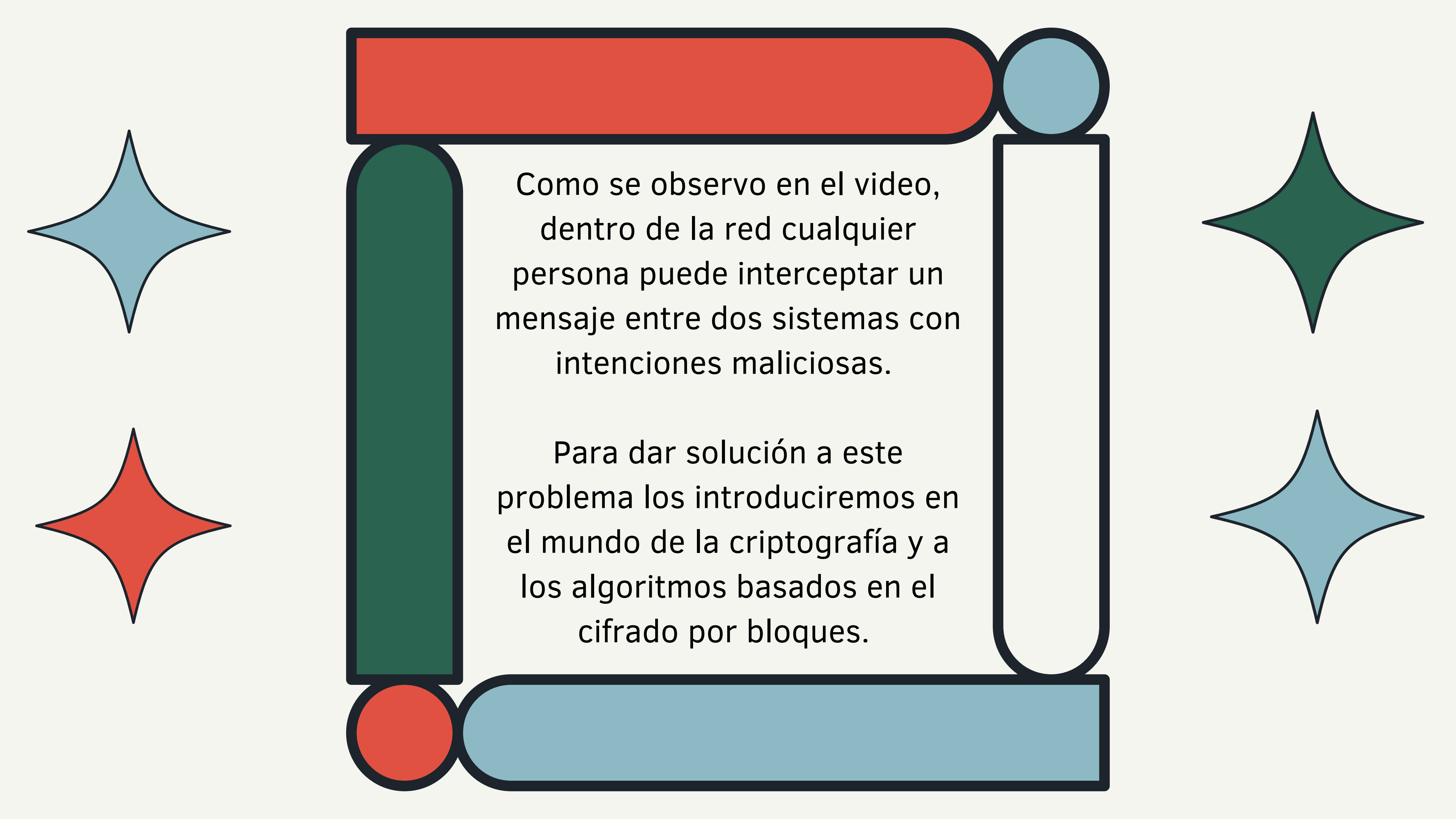
Tafolla Rosales Esteban  
Vazquez Sanchez Erick Alejandro



# INTRODUCCION



<https://youtu.be/NQVjic6Ekyg>



Como se observo en el video,  
dentro de la red cualquier  
persona puede interceptar un  
mensaje entre dos sistemas con  
intenciones maliciosas.

Para dar solución a este  
problema los introduciremos en  
el mundo de la criptografía y a  
los algoritmos basados en el  
cifrado por bloques.

# ¿Qué es la criptografía?



La criptografía es lo que permite que un sistema se olvide por completo de confiar en una red



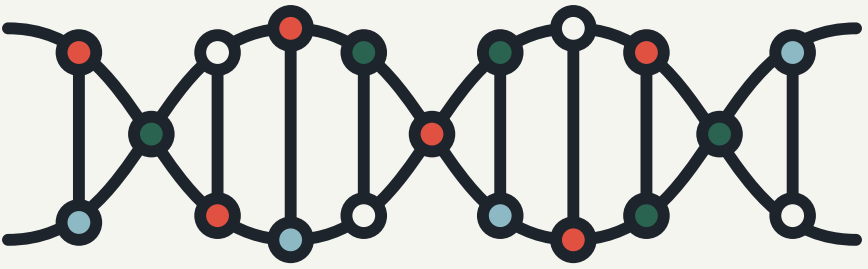
La criptografía permite cifrar un mensaje, con una sola llave que permite conocer el contenido original.

ABe → DeH

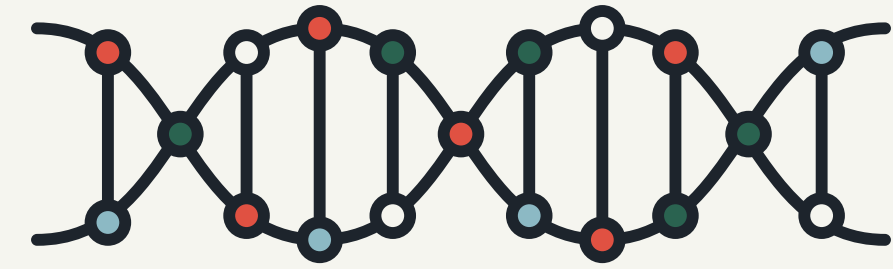
🔑 = 3







# ALGORITMOS DE CIFRADO



Son los encargados de codificar un mensaje e intercambiar la llave empleada entre un sistema y otro para que los mensajes compartidos mediante una red no segura no puedan ser descifrados por ningún atacante.

Un algoritmo de cifrado está compuesto por 3 propiedades principales:

- una llave
- una función que genera un mensaje cifrado
- una función que descifra un mensaje



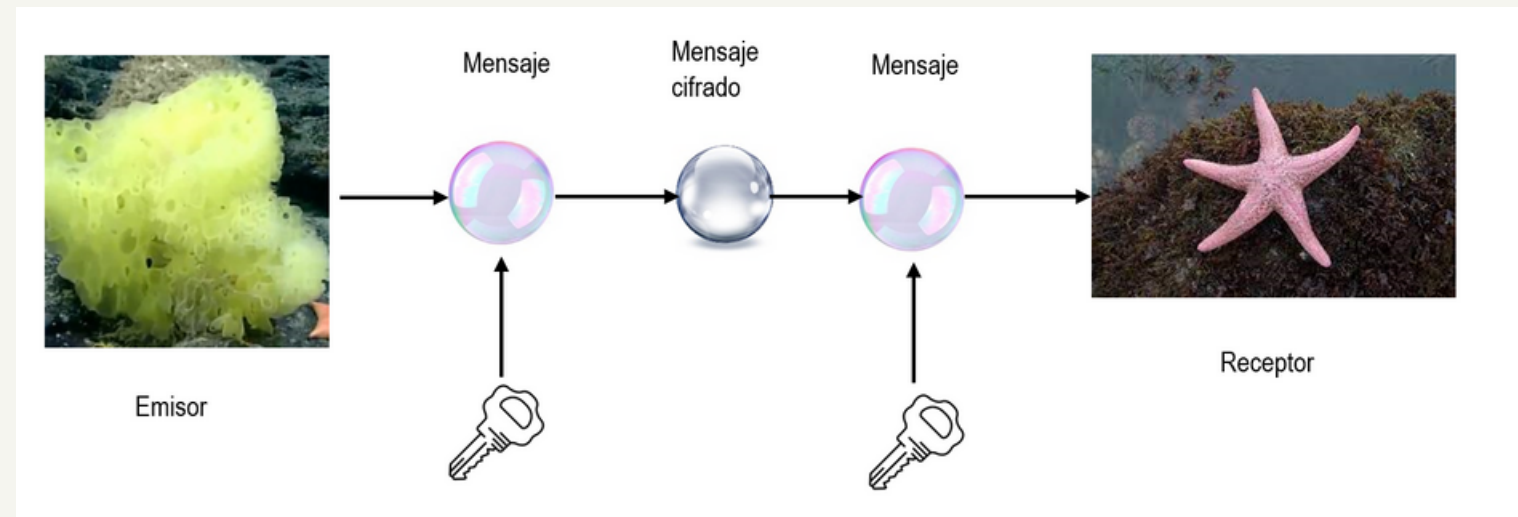
# ● TIPOS DE ● ALGORITMOS ● DE CIFRADO



Dentro de los algoritmos de cifrado encontramos dos tipos, simétricos y asimétricos, sin embargo profundizaremos en los algoritmos simétricos debido a que son los utilizados en el cifrado por bloques

## ALGORITMOS SIMÉTRICOS

Utilizan la misma llave para el cifrado y descifrado.



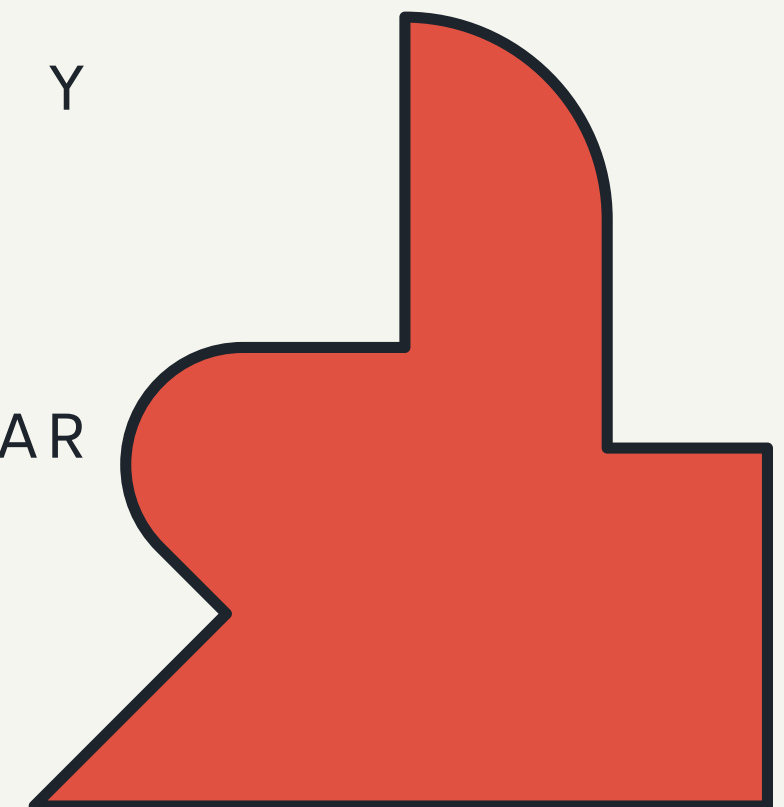
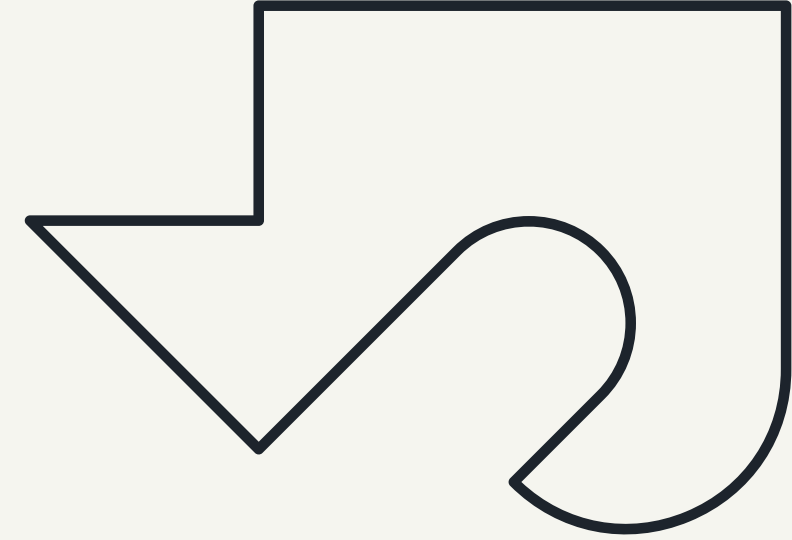


# CIFRADO POR BLOQUES

ALGORITMOS DE CIFRADO SIMÉTRICOS DONDE LA INFORMACIÓN SE DIVIDE EN GRUPOS DE LONGITUD ESTÁTICA LLAMADOS BLOQUES.

PARA HACER UN CIFRADO POR BLOQUES EFECTIVA, SE DEBEN CUMPLIR LOS SIGUIENTES REQUISITOS:

- EL TAMAÑO DE LA LLAVE DEBE SER LO SUFICIENTEMENTE GRANDE PARA QUE EL PODER COMPUTACIONAL NECESARIO PARA ATACAR Y ROMPERLA SEA RIDÍCULO.
- DE PREFERENCIA CADA ENTRADA DEBE DE DAR UNA SALIDA DISTINTA.







# DES

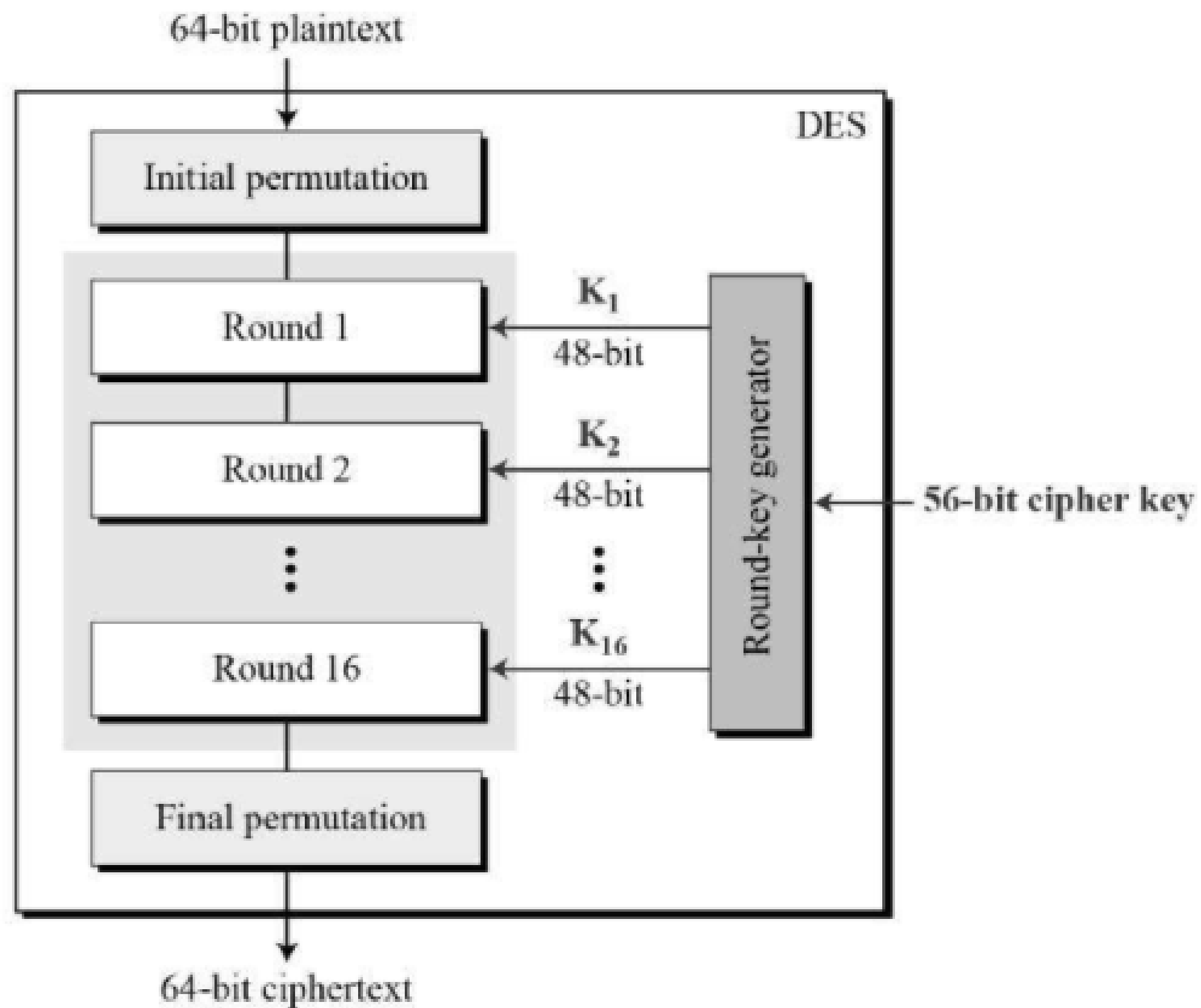
DATA-ENCRYPTION  
STANDARD

DES es un algoritmo que implementa el cifrado por bloques.



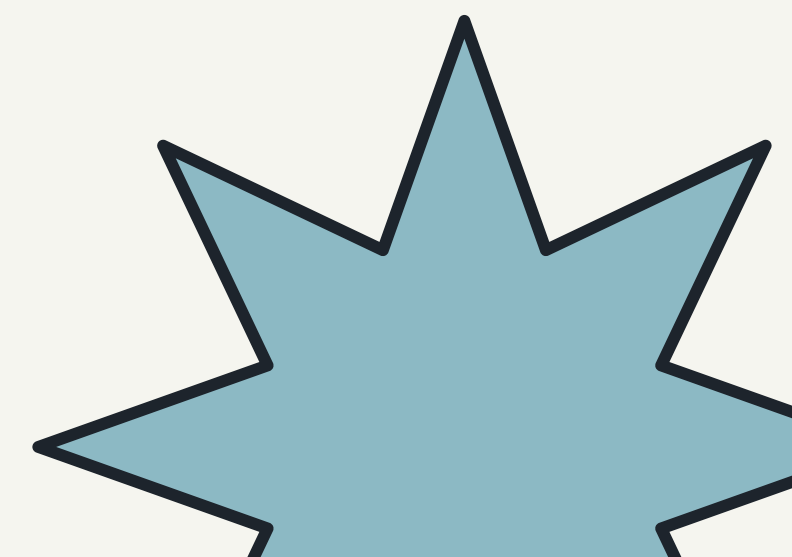
De manera general, este algoritmo está basado en las rondas de feistel y funciona tomando un valor de 64 bits del mensaje original, y una llave de 56 bits para cifrar ese bloque.





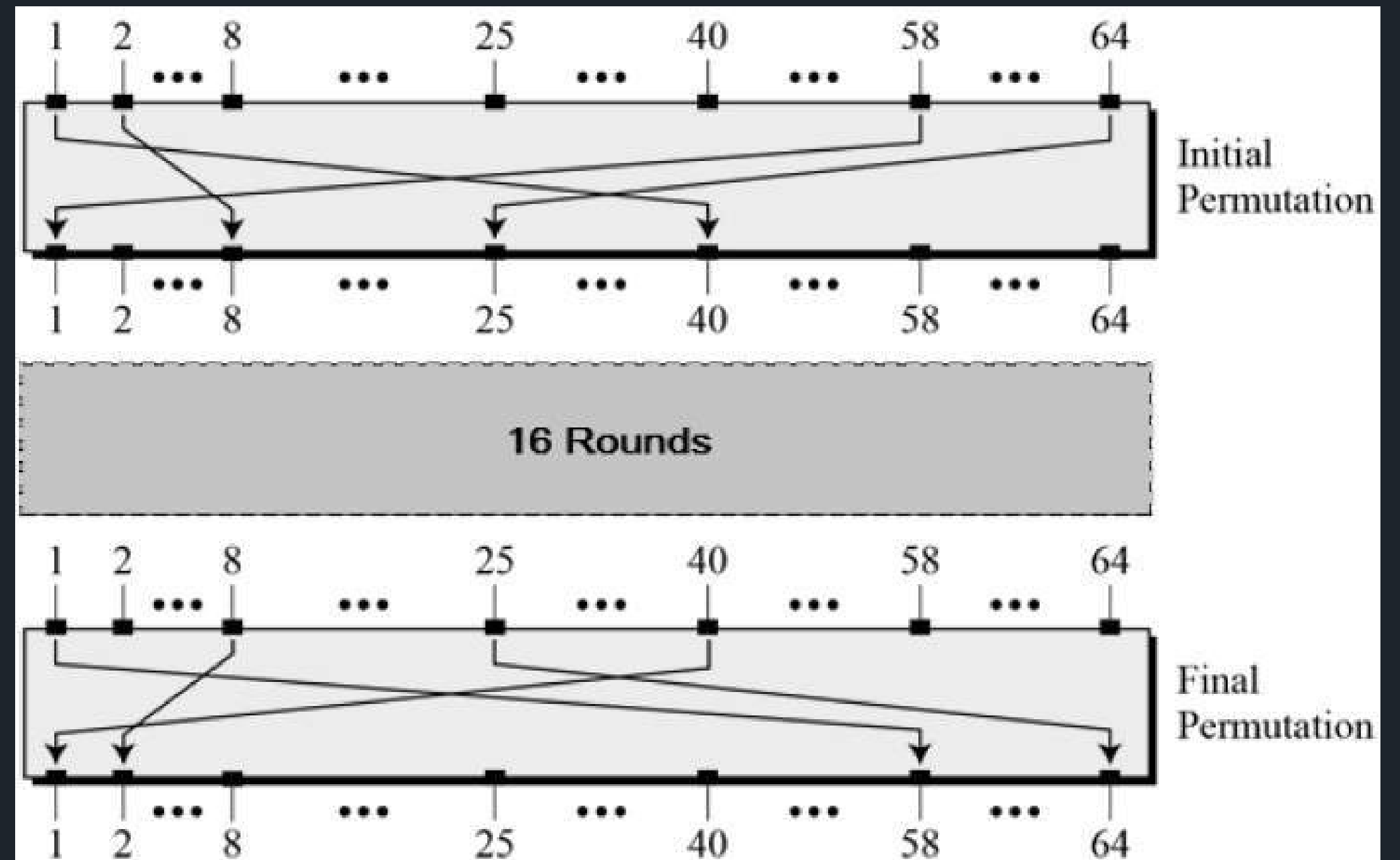
## ESTRUCTURA DE DES

En el diagrama podemos observar la estructura del algoritmo, en donde podemos ver que se conforma por 16 rondas feistel, las cuales generaran el mensaje cifrado

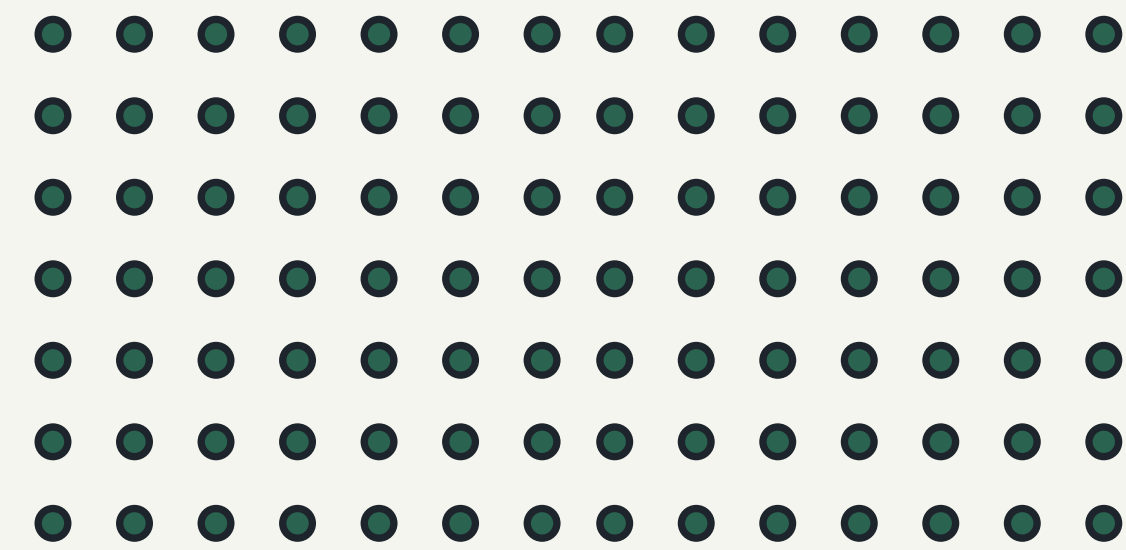


# PERMUTACION INICIAL Y FINAL

Estas permutaciones obtienen de una entrada una salida desplazando x valores los bits.



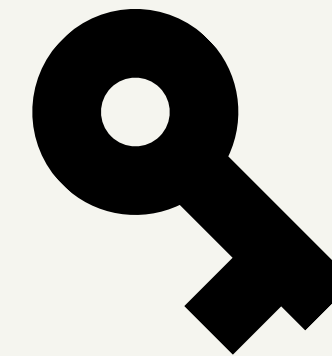
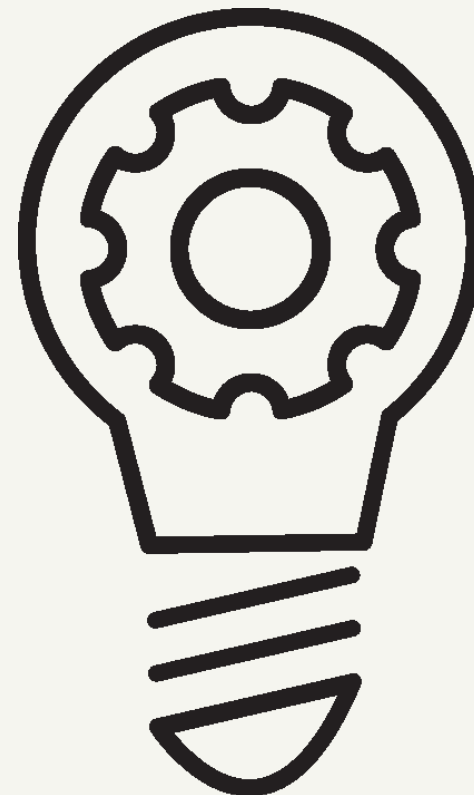
# Generador de llaves



Partiendo de la clave de 56 bits del comienzo, en cada una de las 16 rondas se generará una llave de 48 bits.



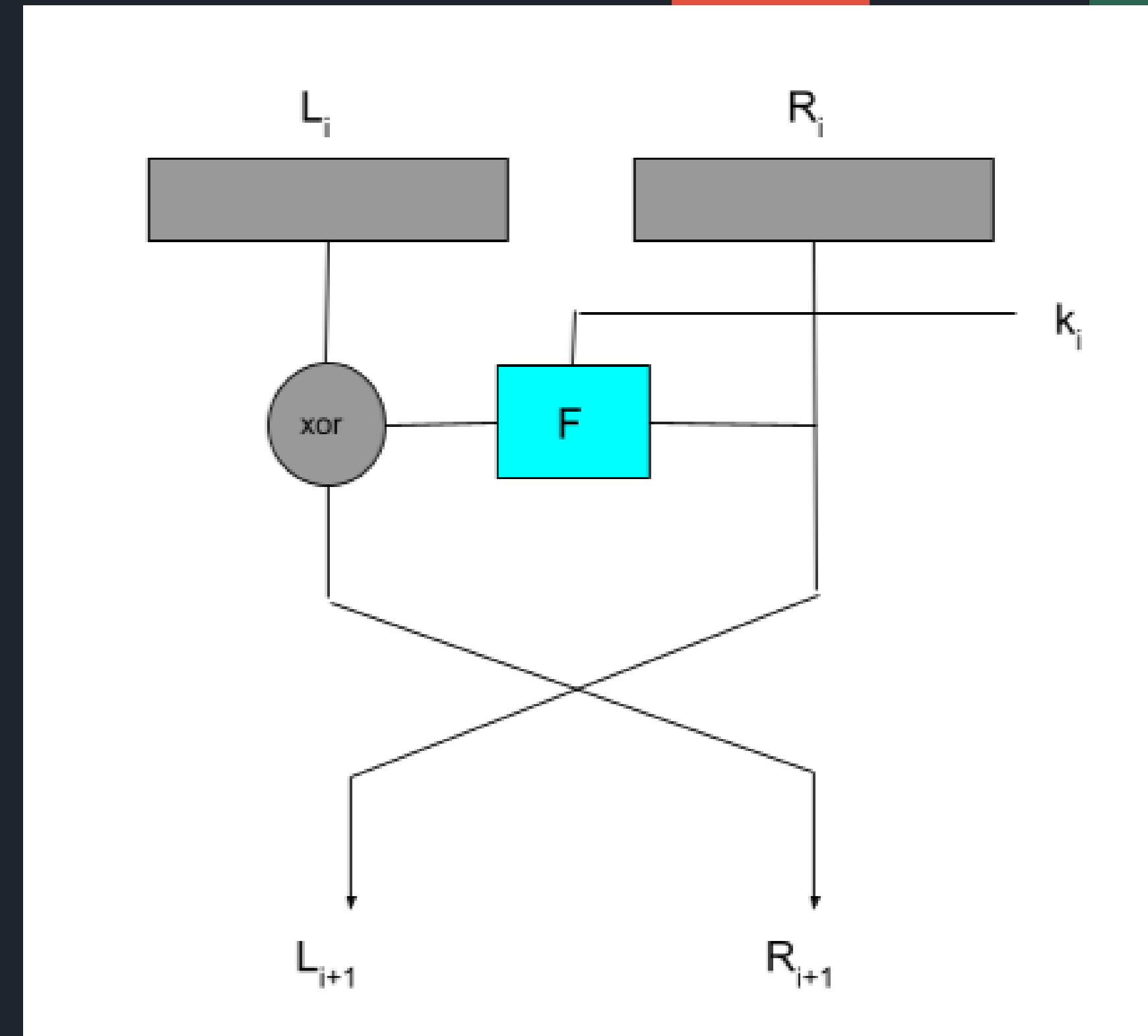
llave 56 bits



llave 48 bits

# Rondas Feistel

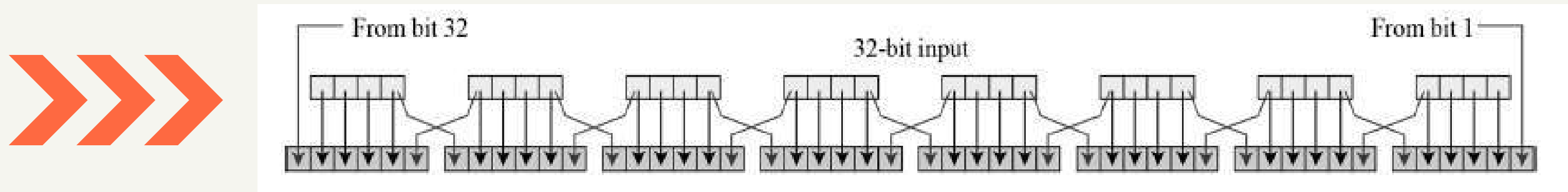
Acorde al diagrama, en las rondas Feistel se recibe como entrada dos bloques de 32 bits ( $L_i$  y  $R_i$ ), el bloque derecho es procesado mediante una función  $F$  y la salida de esta función se combina mediante una operación lógica, xor, con el bloque izquierdo. Por último, se intercambian los resultados obtenidos, el bloque derecho pasa al izquierdo y viceversa, dando la entrada a una nueva ronda.



# Función Feistel

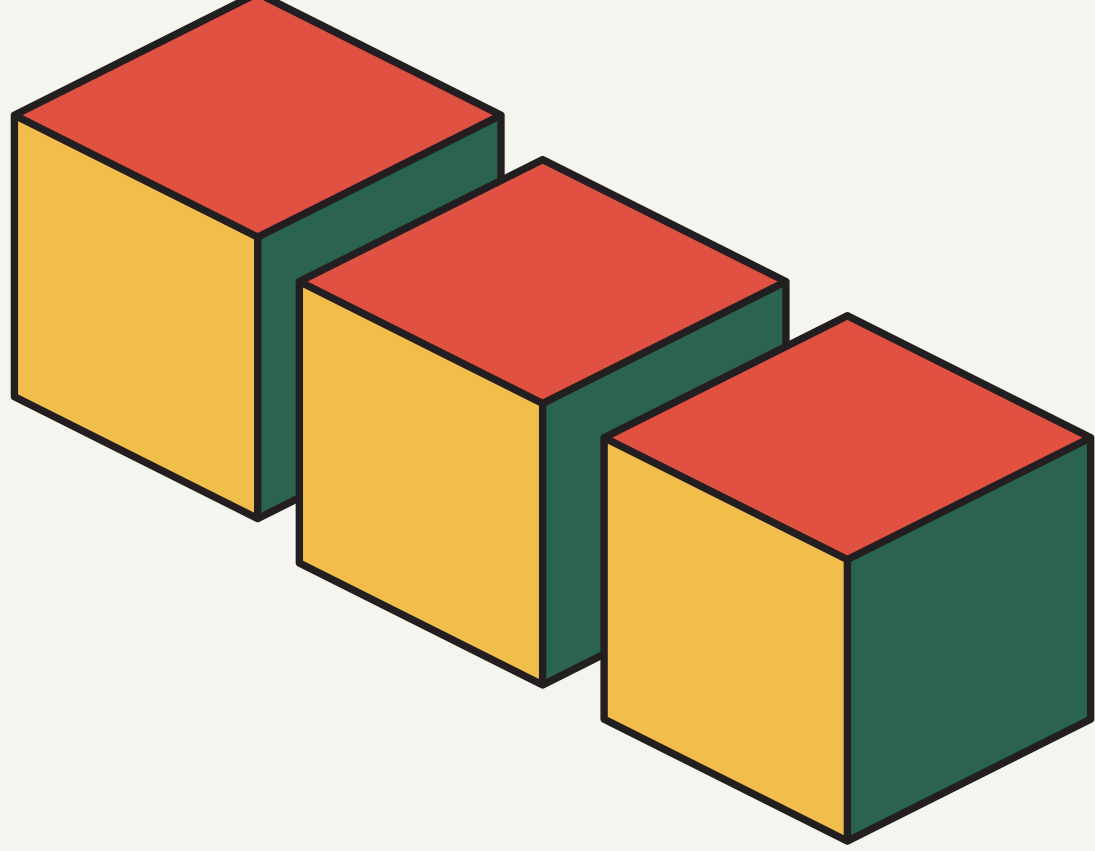
Dentro de la función Feistel se realizan una serie de operaciones para cifrar un bloque de 32 bits junto con una llave de 48 bits.

Para esto primero se realiza una permutación de expansión que hace que el bloque de 32 bits se expanda a 48 bits, esta es una operación estándar del algoritmo DES y lo que se hace es repetir algunos bits para rellenar los espacios faltantes.



Después de esto se realiza una operación lógica, xor, combinando la llave y el bloque, y por último, se realizará la última permutación dentro de la función para convertir la salida de 48 bits en una de 32 bits.





## Triple DES

En la actualidad el algoritmo DES no es un método seguro para el cifrado de información. Debido a este problema Triple DES fue elegido para suplantar al algoritmo DES.

Este algoritmo consiste en realizar 3 veces el cifrado de la información mediante DES, obteniendo una llave de 168 bits y haciéndolo mucho más seguro. Sin embargo, no entraremos en detalle con este algoritmo.

# AES (ADVANCED ENCRYPTION STANDARD)



## ORIGEN

Nace de la búsqueda de un nuevo algoritmo de cifrado para sustituir a DES

## TAMAÑO DE LLAVES

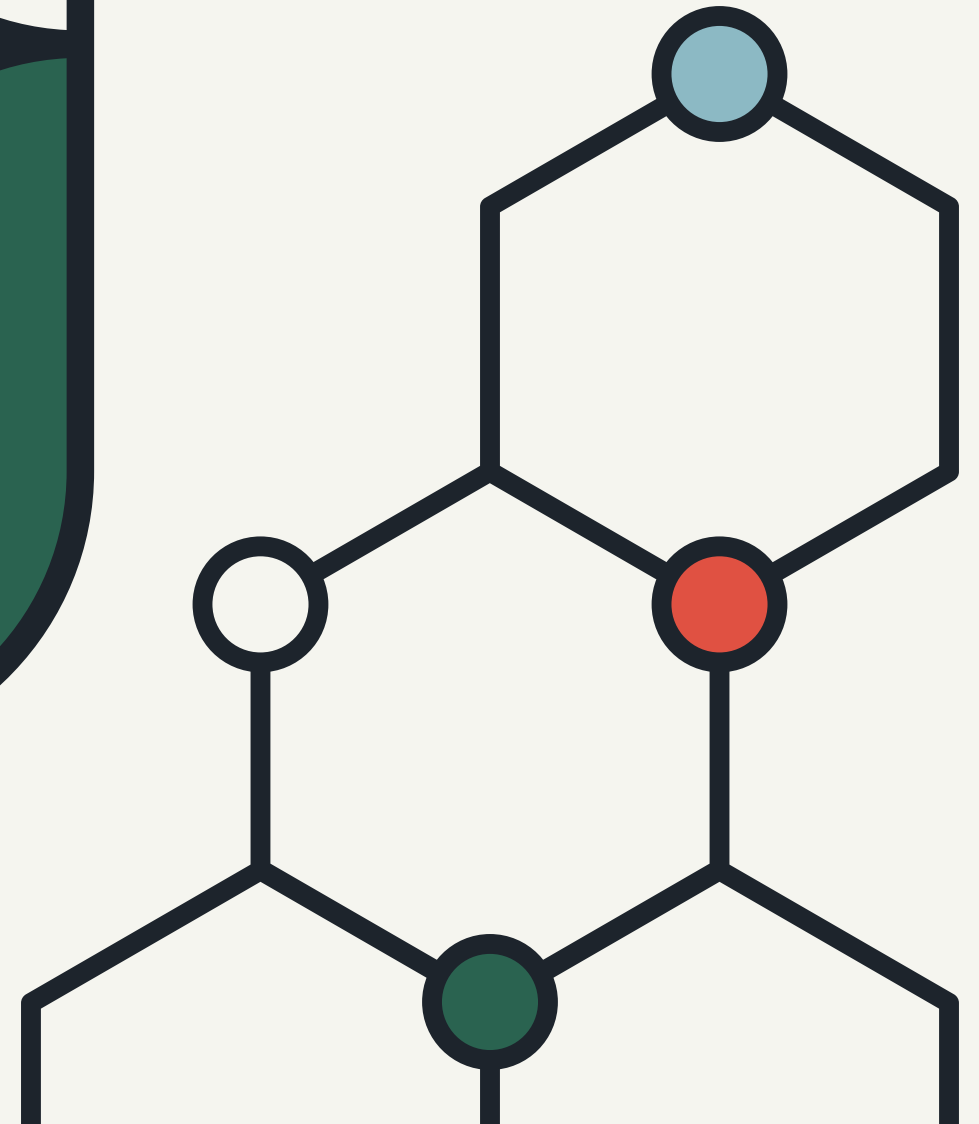
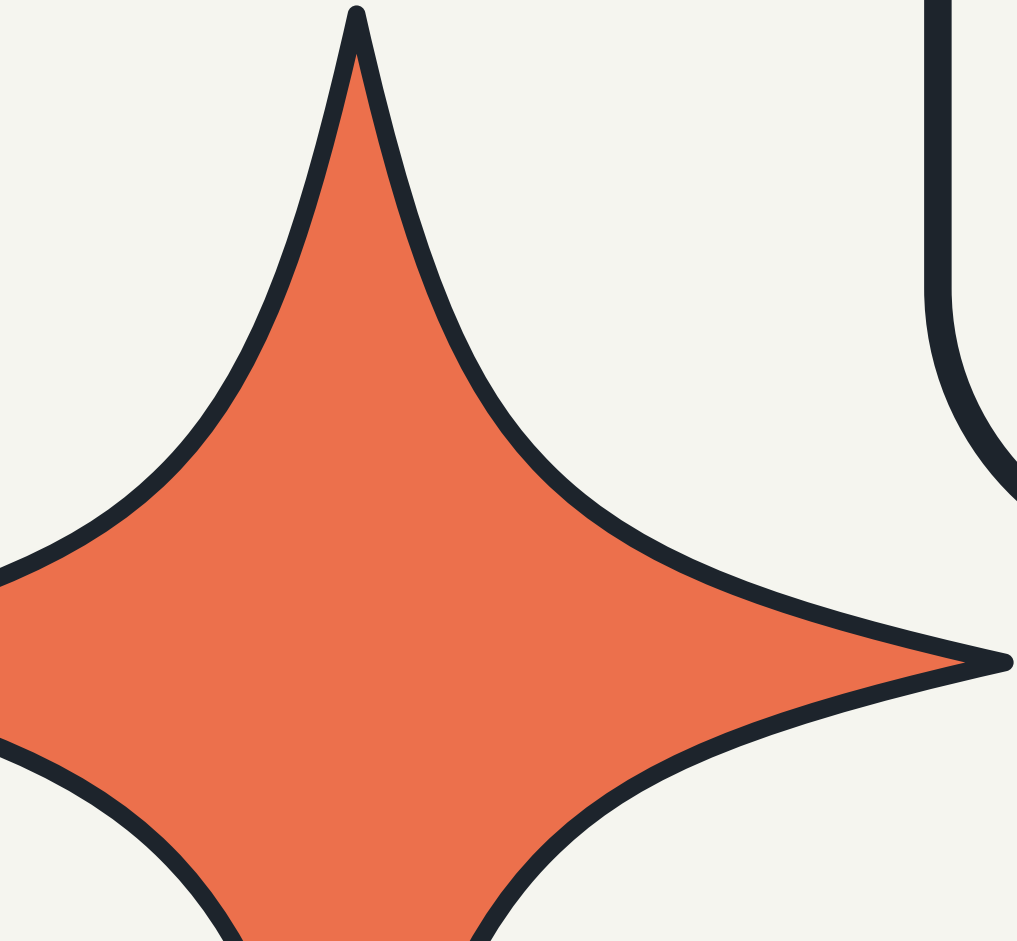
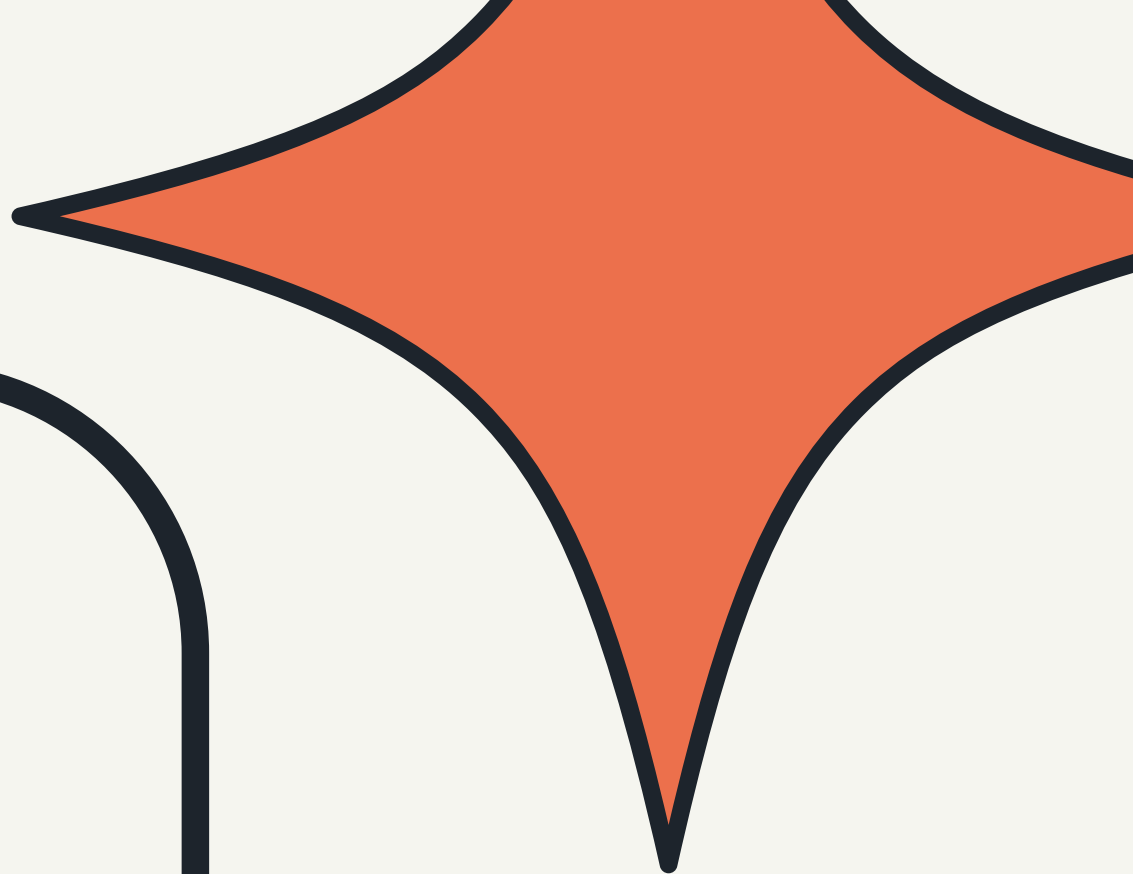
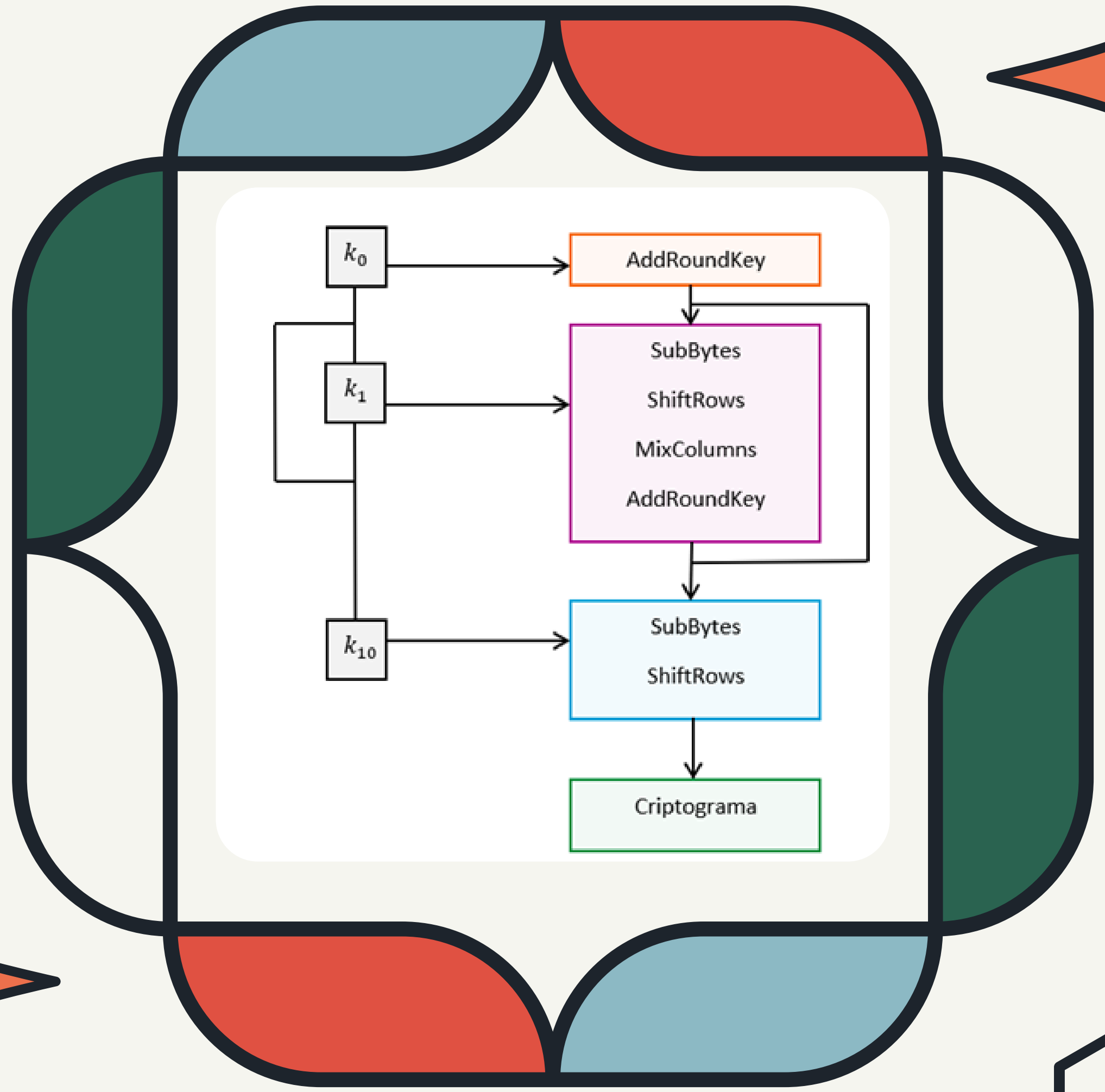
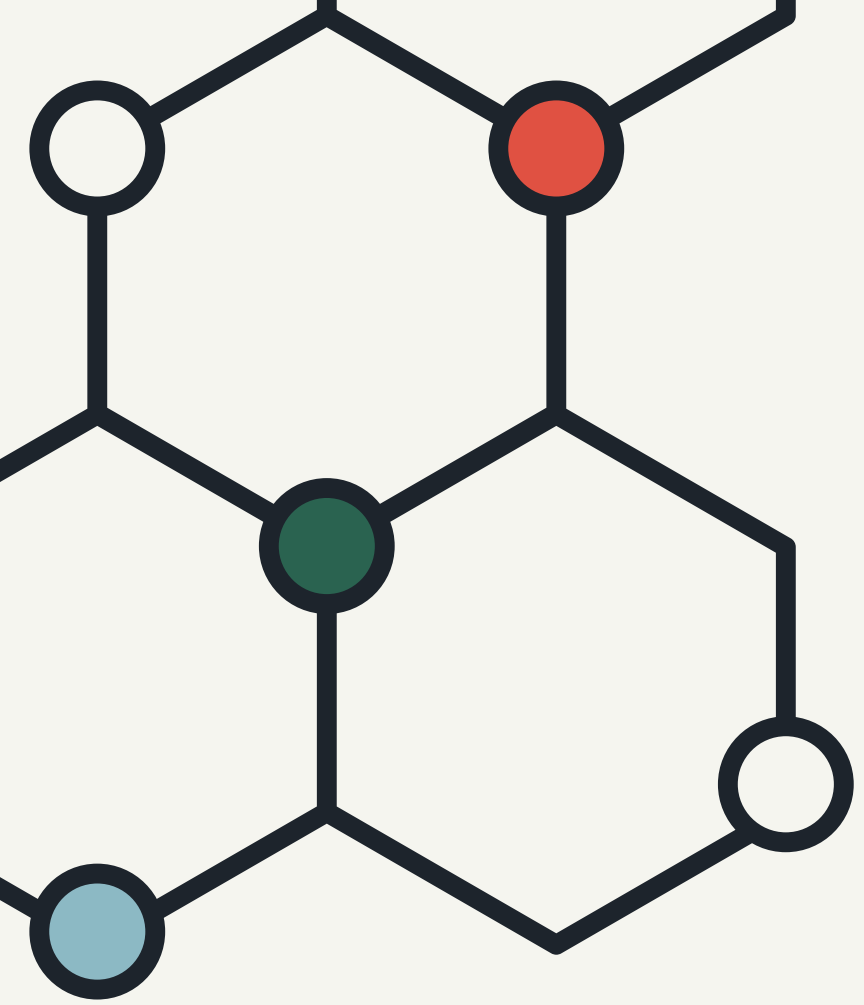
Tiene llaves de longitud de 128,192 o 256 bits.

## TAMAÑO DE BLOQUES

Implementa el cifrado por bloques del tamaño de 128 bits

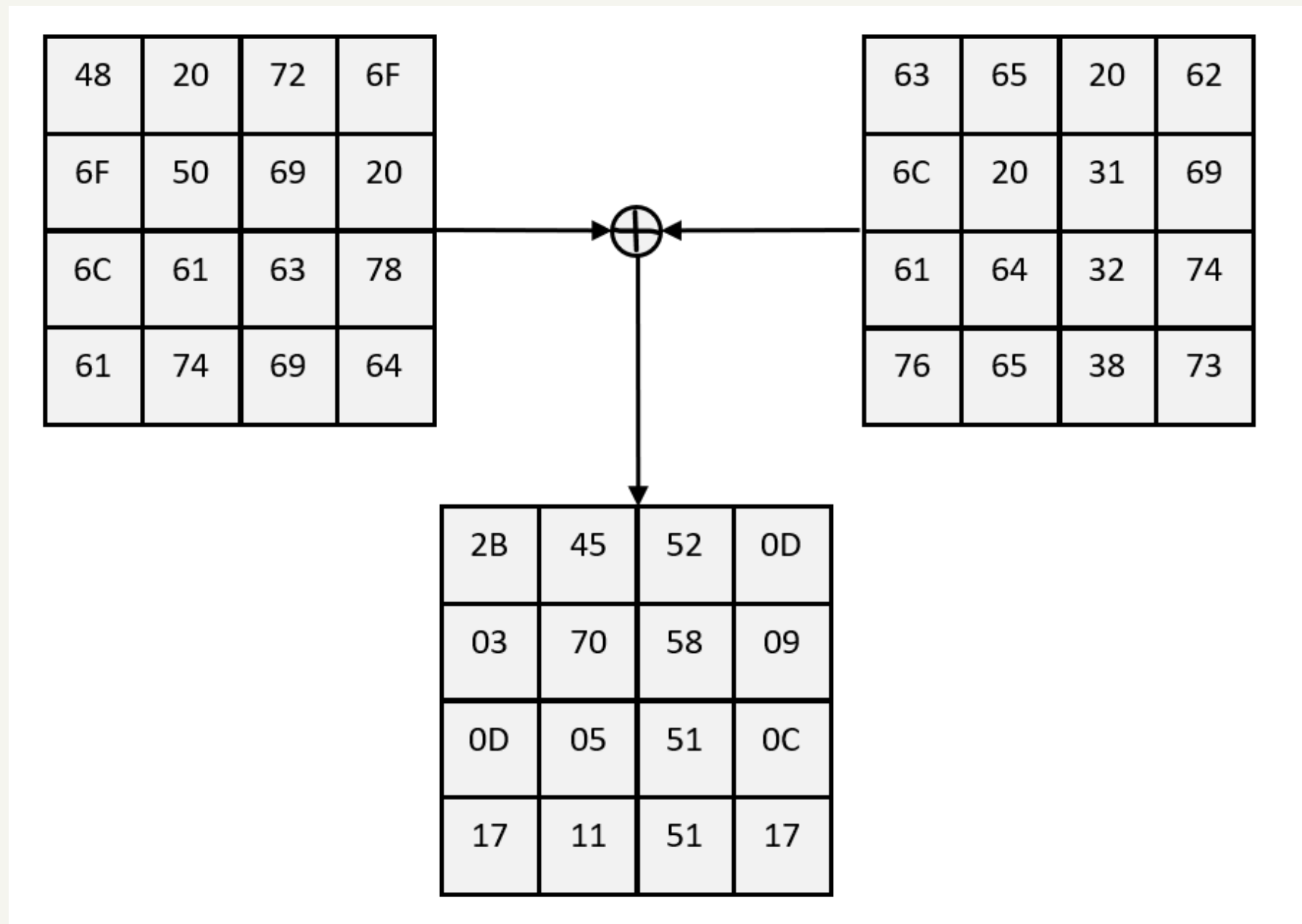
## NÚMERO DE VUELTAS

- 128 bits se hacen 10 vueltas al algoritmo
- 192 bits se hacen 12 vueltas al algoritmo
- 256 bits se hacen 14 vueltas al algoritmo



# ADDITIONAL KEY

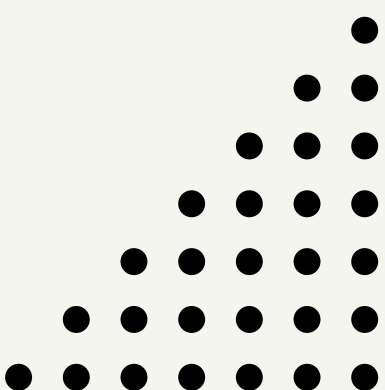
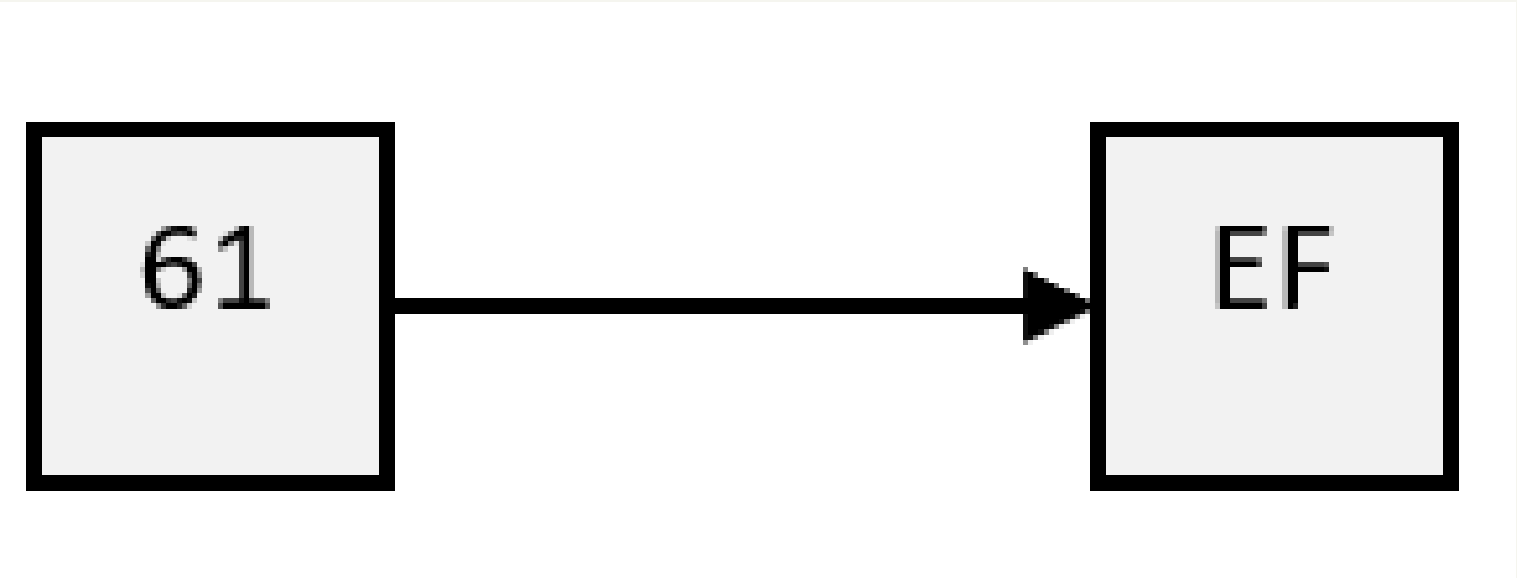
SE HACE UN XOR CON LA MATRIZ DE LA LLAVE Y LA MATRIZ DE NUESTRO MENSAJE QUE DESEAMOS CIFRAR.



# SUBBYTES

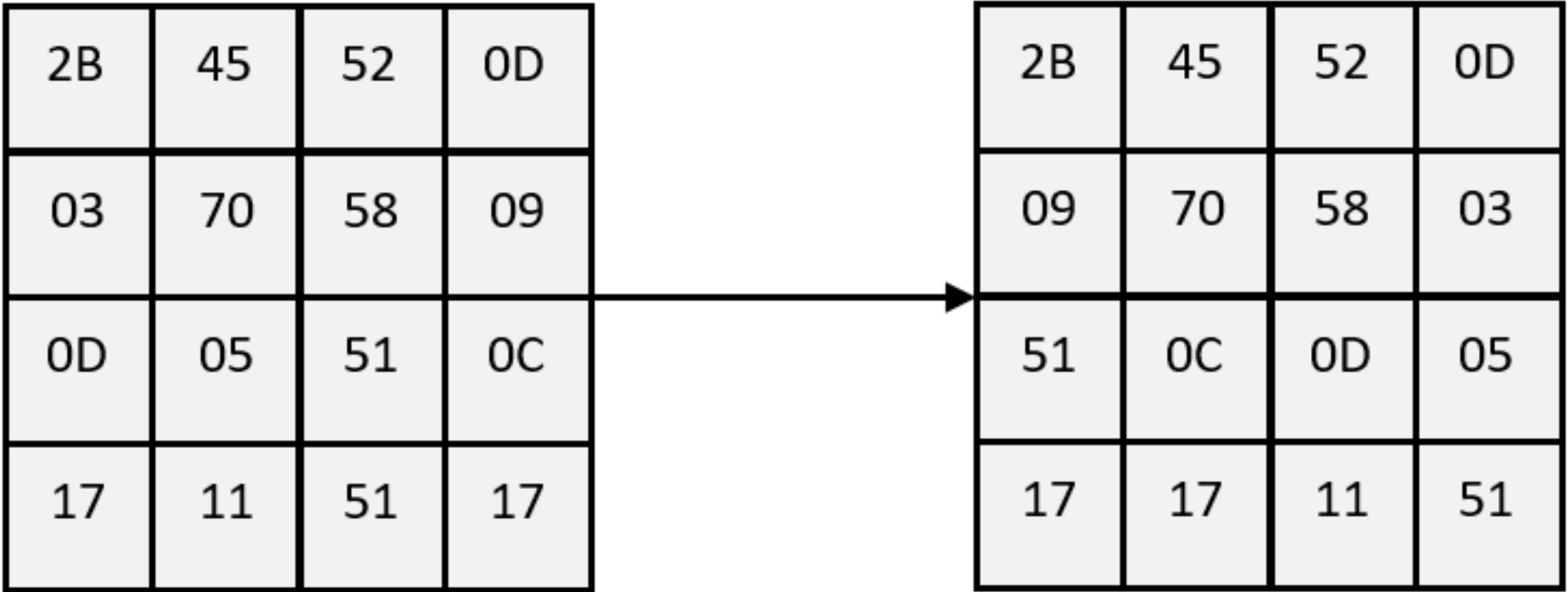
SE REALIZA UNA SUSTITUCIÓN DE LOS ELEMENTOS DE LA MATRIZ POR OTRA DE UNA TABLA DE BÚSQUEDA.

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



# SHIFTRROWS

EJECUTA PERMUTACIONES DE LAS FILAS DEL ESTADO  
DONDE EL PRIMER ELEMENTO NO ROTA NINGUNO, EL  
SEGUNDO UNO, EL TERCERO DOS Y EL CUARTO TRES.





# MIXCOLUMNS

OPERA LAS COLUMNAS CON UNA TRANSFORMACIÓN LINEAL.

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

$\times$

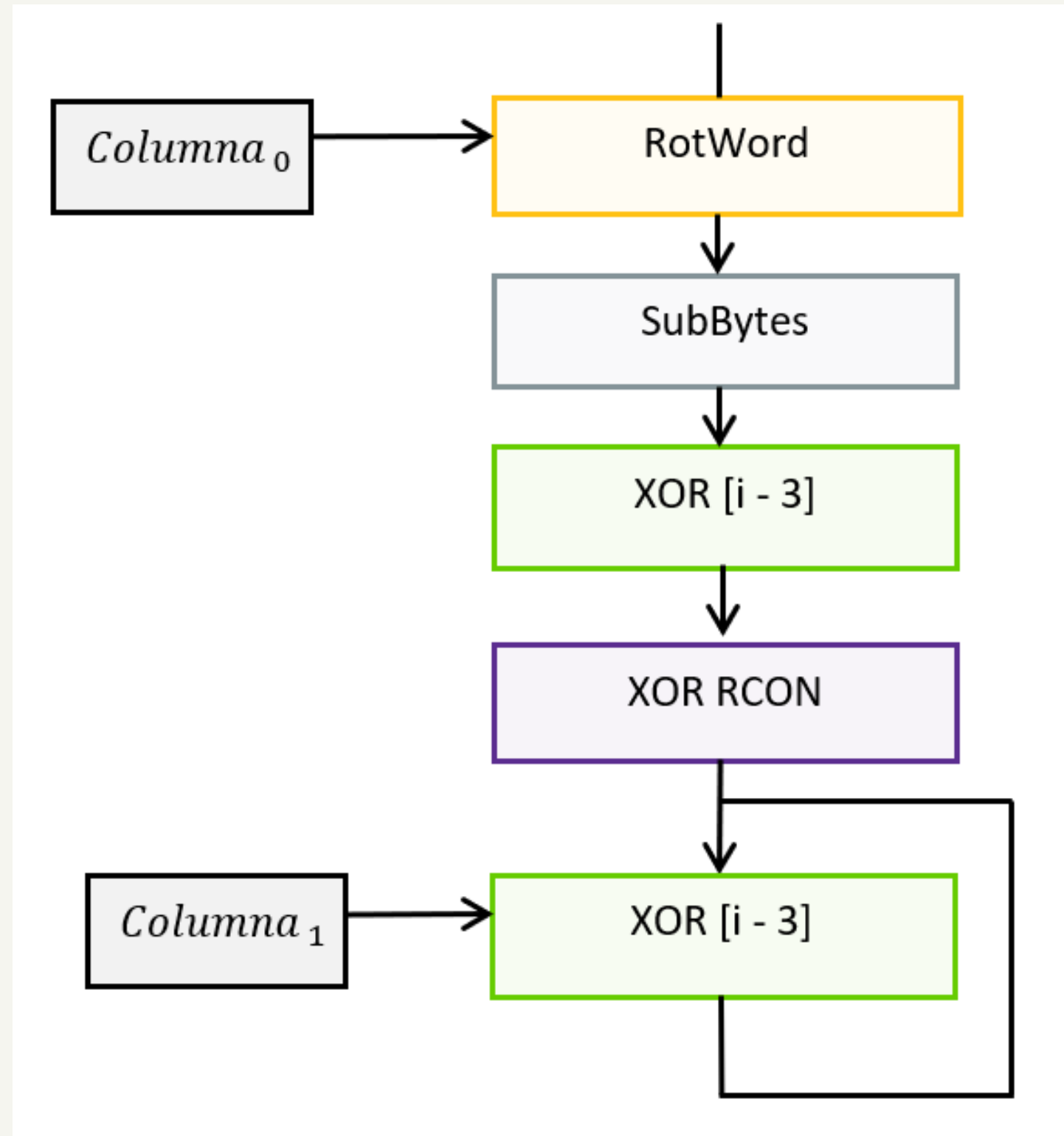
2B
09
51
17

$=$

98
EB
AE
9D



# CALCULO DE LAS LLAVES

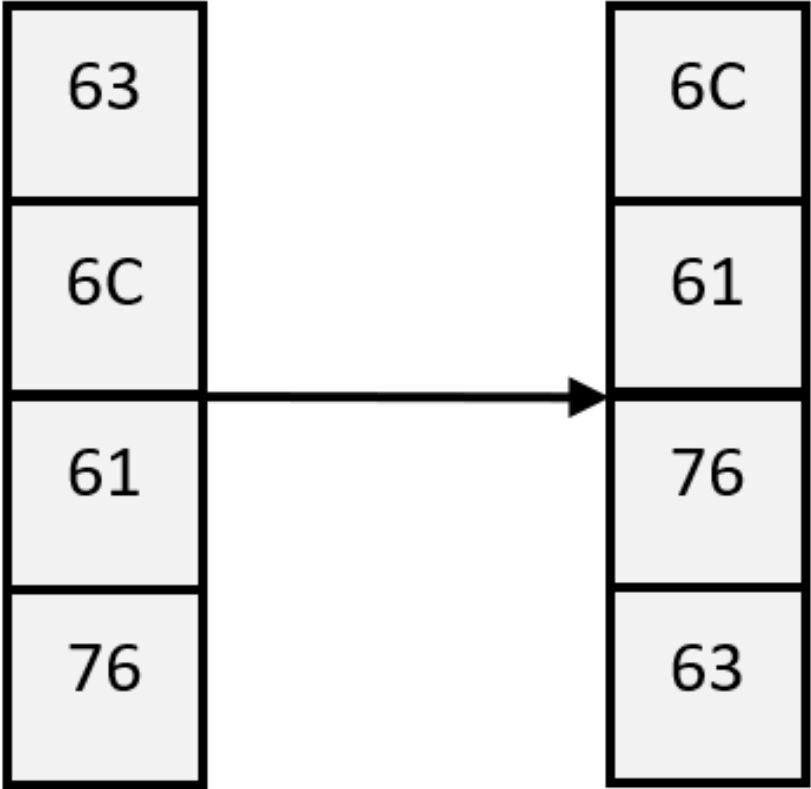


# ROTWORD

MUEVE EL PRIMER ELEMENTO DE LA ÚLTIMA COLUMNA  
AL FINAL DE LA COLUMNA



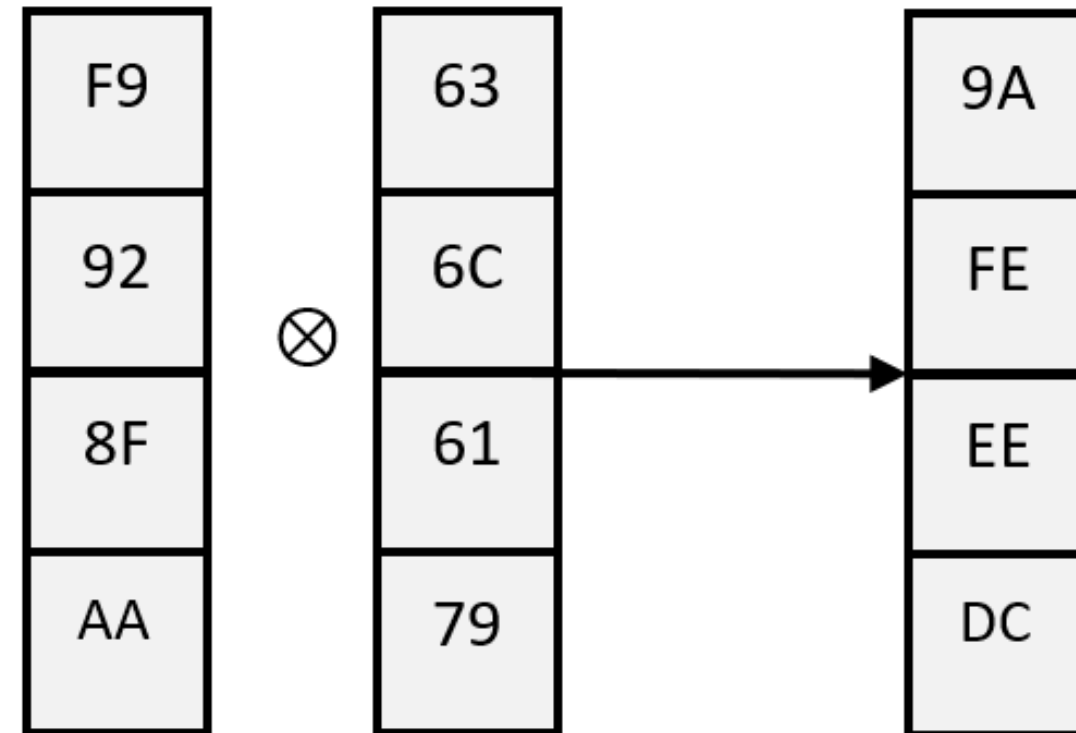
63	65	20	62
6C	20	31	69
61	64	32	74
76	65	38	73



# XOR [I-3]

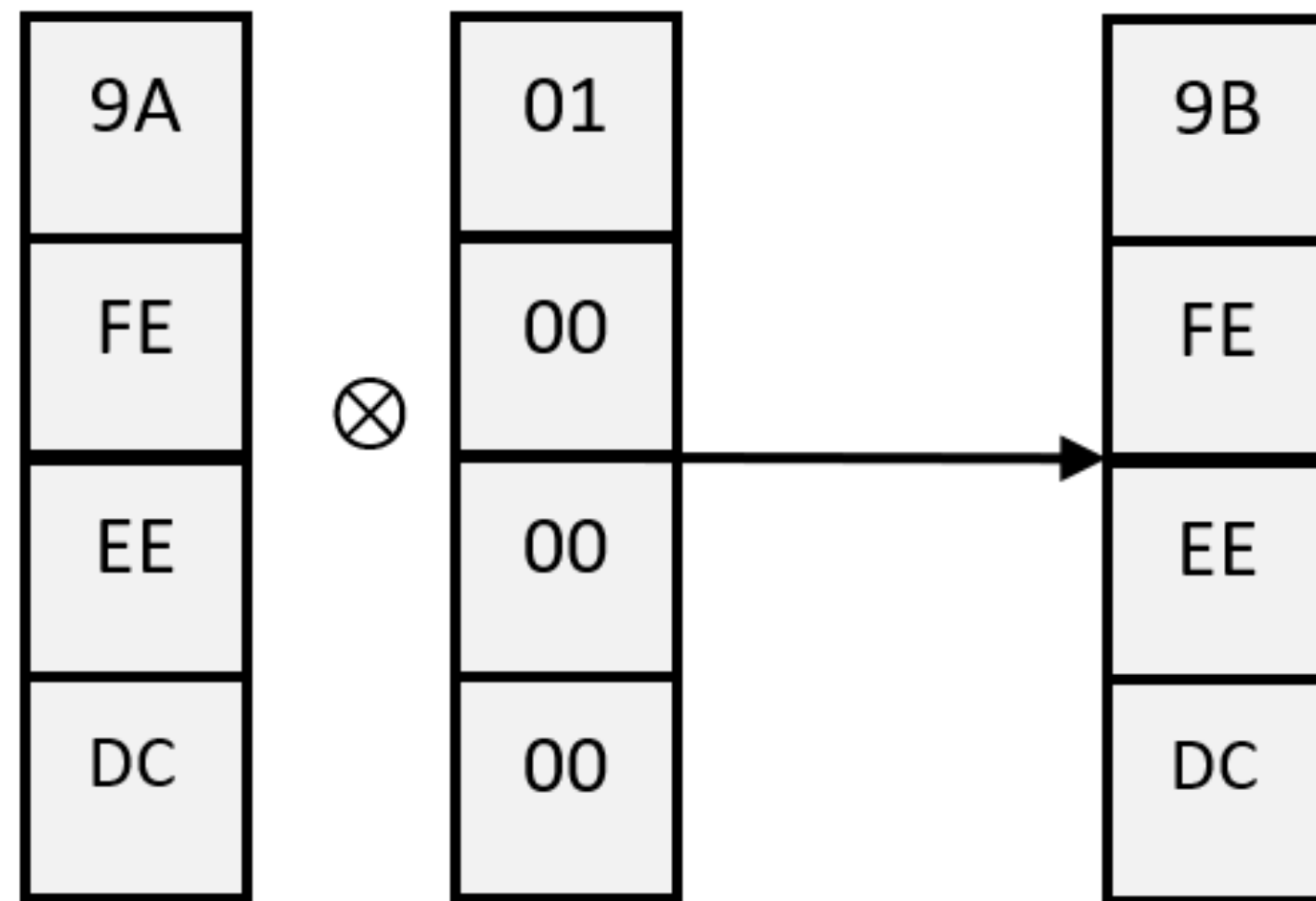
SE LE APLICA XOR CON LA ÚLTIMA COLUMNA DE LA  
MATRIZ Y LA COLUMNA QUE SE ENCUENTRA TRES  
POSICIONES DETRÁS

63	65	20	62
6C	20	31	69
61	64	32	74
76	65	38	73



# XOR RCON

A LA COLUMNA SE LE APLICA UN XOR CON EL VECTOR RCON EL CUAL ES DIFERENTE PARA CADA VUELTA DE LA LLAVE.



63	65	20	62	9B
6C	20	31	69	FE
61	64	32	74	EE
76	65	38	73	DC

# Conclusiones

- La criptografía nos protege en caso de nuestro mensaje sea interceptado antes de llegar a su destino
- Dentro del cifrado por bloques la diferencia entre algoritmos dependerá del tamaño de la llave.
- Al final descubrimos que el cifrado por bloques no es mas que una selección de bloques de un tamaño fijo para cifrar la información de una manera mas rápida, por lo que la complejidad radica en las implementaciones que le podemos dar a estos algoritmos, como se da el caso en AES y DES.