

# Criptografía de Llave Privada

Introducción a la Criptografía y a la Seguridad de la Información

Iván Castellanos

Departamento de ingeniería de sistemas e industrial  
Universidad Nacional de Colombia

19 de septiembre de 2019

# Notación

- $A$  es el *alfabeto*, eg.  $A = \{0, 1\}$
- $M$  es el espacio de posibles mensajes sobre  $A$ ,  $M \subseteq A^*$
- $m \in M$  es un texto limpio (*plaintext*) o mensaje
- $C$  es el espacio de posibles mensajes cifrados
- $K$  es el espacio de posibles llaves
- $k_e \in K, k_d \in K$  son llaves de cifrado y descifrado respectivamente
- $E_{k_e} : M \rightarrow C$  es la función de cifrado
- $D_{k_d} : C \rightarrow M$  es la función de descifrado
- $c = E_{k_e}(m) \in C$  es un texto cifrado (*ciphertext*)
- Aplicar  $E_{k_e}$  (o  $D_{k_d}$ ) es llamado proceso de cifrado (o descifrado).

# Correctitud

Un sistema de cifrado consiste en un conjunto  $\{E_{k_e} : k_e \in K\}$  y  $\{D_{k_d} : k_d \in K\}$  con la propiedad de correctitud

## Definición (Propiedad de correctitud)

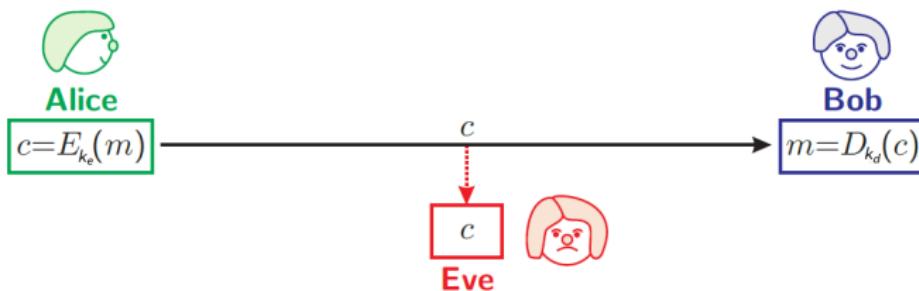
$$\forall k_e \in K, \exists! k_d \in K \text{ tal que } D_{k_d} = E_{k_e}^{-1}$$

## Nota

Principalmente verificaremos que  $\forall m \in M, D_{k_d}(E_{k_e}(m))$

## Sistemas de cifrado

- Para construir un sistema de cifrado debemos definir el alfabeto, los espacios de textos limpios y cifrados, el espacio de las llaves y las funciones de cifrado y descifrado

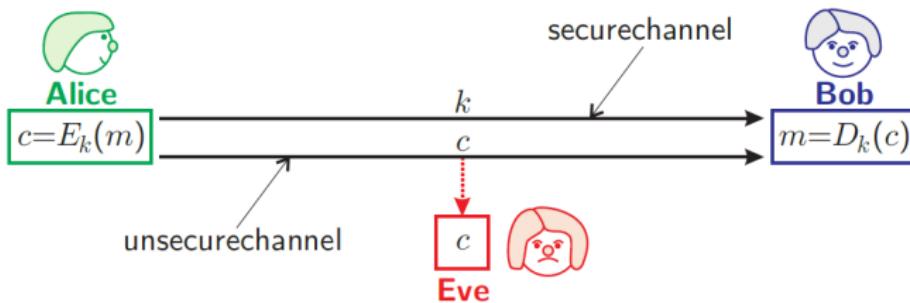


## Nota

Lo otro que se busca de un sistema de cifrado es que sea *seguro*

## Definición

Un sistema de *cifrado de llave privada* usa la misma llave para la función de cifrado y descifrado, es decir,  $k_e = k_d = k$ .



Nota

Estos sistemas también se conocen como de *cifrado de llave simétrica*

# One-Time Pad

El One-Time Pad es un sistema de cifrado definido de la siguiente manera.

- $A = \{0,1\}$
- $M = C = K = \{0,1\}^n$
- Sea  $m \in M$  y  $k \in K$ ,  $|k| = |m| = n$
- $E_k(x) = D_k(x) = x \oplus k$ , donde  $\oplus$  es la operación lógica XOR

## Nota

$$0 \oplus 0 = 0$$

$$0 \oplus 1 = 1$$

$$1 \oplus 0 = 1$$

$$1 \oplus 1 = 0$$

# One-Time Pad

El One-Time Pad es un sistema de cifrado definido de la siguiente manera.

- $A = \{0,1\}$
- $M = C = K = \{0,1\}^n$
- Sea  $m \in M$  y  $k \in K$ ,  $|k| = |m| = n$
- $E_k(x) = D_k(x) = x \oplus k$ , donde  $\oplus$  es la operación lógica XOR

## Nota

$$0 \oplus 0 = 0$$

$$0 \oplus 1 = 1$$

$$1 \oplus 0 = 1$$

$$1 \oplus 1 = 0$$

## Ejercicio

Sean  $x_1 = "Al"$  y  $x_2 = "Ma"$ . ¿Cuál sería el valor de  $y$  de modo que  $x_1 \oplus y = x_2$ ? cada carácter de la cadena codifíquelo como una cadena binaria de 7 bits utilizando su representación en ASCII.

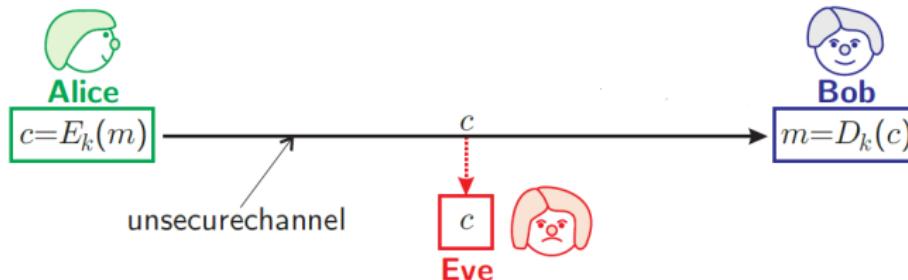
# Seguridad de cifrado

Un sistema de cifrado es *perfectamente seguro* si el texto cifrado no le da al adversario ninguna *información* sobre el texto limpio.

## Definición (Seguridad perfecta)

Formalmente un sistema es perfectamente seguro si

$$\forall m^* \in M, P(m = m^* | E_k(m) = c) = P(m = m^*)$$



## Nota

El One-Time Pad es un sistema *perfectamente seguro*

# Seguridad de cifrado

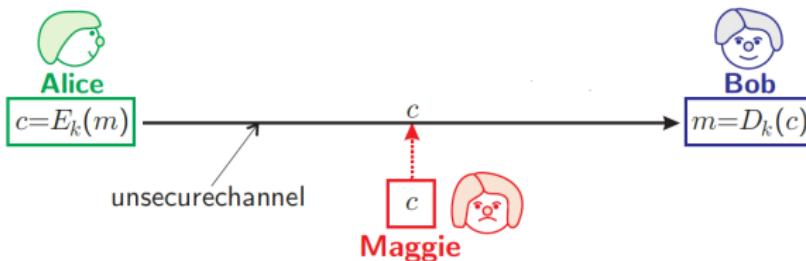
La idea de seguridad en un sistema de cifrado está en la capacidad del cifrado de esconder las propiedades estadísticas del espacio de mensajes y de llaves

- *Confusión*: La relación entre el texto cifrado y la llave debe ser lo mas compleja posible
- *Difusión*: La distribución de los grupos de caracteres del texto limpio debe ser distribuida en mas grandes estructuras del texto cifrado

## Nota

El criptoanalista busca cualquier propiedad estadística en el texto cifrado que le ayude a romper la llave o el mensaje

# Maleabilidad



## Definición (Maleabilidad)

Un sistema es *maleable* (*malleable*) si al modificar el mensaje cifrado se controla la modificación del mensaje descifrado

## Nota

El One-Time Pad es maleable

## Ejemplo

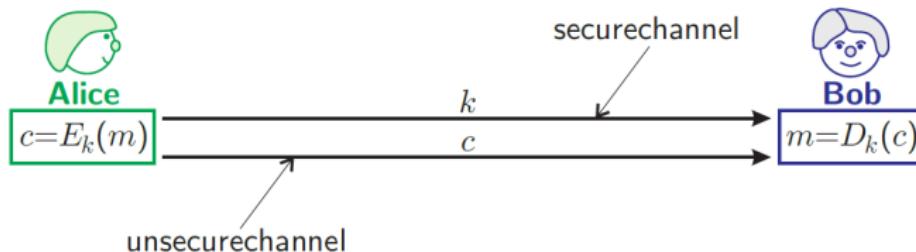
$m = \text{"Transferir a Alice."}$ ,  $p = \text{"Transferir a Maggie"}$ , si Maggie modifica  $c$  por  $c' = c \oplus m \oplus p$  el mensaje que recibiría Bob sería  $p$

# Impracticidad

- Note que fijar una llave del OTP (utilizarla para multiples mensajes) sería vulnerable a ataques

## Ejemplo

Sea  $c_1 = E_k(m_1)$  y  $c_2 = E_k(m_2)$ ,  $c_1 \oplus c_2 = m_1 \oplus m_2$



- Un sistema de cifrado es *impráctico* si  $|K| \geq |M|$
- El One-Time Pad es *impráctico*, pues  $|M| = |K|$

# Impracticidad

## Teorema (Shannon)

*Todo sistema de cifrado perfectamente seguro es impráctico*

Demostración.

Por contradicción

Corolario

*Ningún sistema de cifrado práctico es perfectamente seguro*

Nota

Todos los demás métodos de cifrado que se verán en el curso en teoría se pueden romper, sin embargo, varios son imposibles (hasta ahora) de romperlos en la práctica.

# Cifrado por bloques

## Definición

Un sistema de cifrado se dice que es un *cifrado por bloques (block cipher)* si parte el texto limpio en bloques de tamaño fijo  $t$  y cifra un bloque a la vez.

Existen 3 clases de cifrado por bloques:

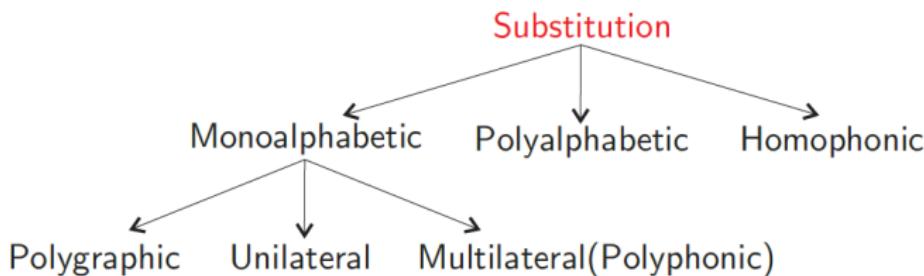
- ① *cifrado por sustitución*: reemplaza bloques de simbolos por otros simbolos o bloques de simbolos
- ② *cifrado por transposición*: permuta simbolos en un bloque
- ③ *cifrado por producto*: es una composición de cifrados pos sustitución y transposición

# Cifrado por sustitución

## Definición

Un sistema de *cifrado por sustitución* reemplaza cada bloque de simbolos con otro simbolo de cifrado

- Para el descifrado se realiza la sustitución inversa
- Hay una gran clasificación de los sistemas de cifrado por sustitución



# Sustitucion monoalfabética

La idea principal de estos sistemas de cifrado es el uso de una sustitución fija sobre todo el mensaje.

Existen 3 tipos de cifrados monoalfabéticos:

- *unilateral*: cada bloque es de sustutición es de un carácter.
- *multilateral*: en el cifrado hay mas caracteres que en el texto plano.
- *poligráfico*: cada bloque de texto limpio consiste en más de un carácter.

# Cifrado César (Unilateral)

- ①  $A = \{'A', 'B', \dots, 'Z'\}$
- ②  $M = C = A^+$
- ③  $k \in \{0, 1, \dots, 25\}$
- ④ El cifrado sustituye cada letra del alfabeto por otra que se encuentre  $k$  posiciones mas adelante (considerando que adelante de la ' $Z$ ' está la ' $A$ ')
- ⑤ El descifrado corresponde a la sustitucion inversa

## Nota

Este sistema de cifrado viene de los años 60 A.C. por el militar romano Julio César

# Cifrado César (Unilateral)

## Ejemplo

- $m = \text{HOLA MUNDO}$
- $k = 3$
- $c = E_3(m) = \text{KROD PXQGR}$

# Cifrado Rot13 (Unilateral)

## Nota

El cifrador César también es conocido como ROTN donde N es el valor de la llave (el corrimiento)

- El sistema de cifrado ROT13 es un caso particular del cifrado César, donde se toman las letras corridas 13 posiciones
- Es muy común en foros online y en cultura popular

## Ejemplo

ant → nag, bar → one, barf → ones, be ← or, envy → rail, flap → sync, fur → she, gel → try

# Cifrado de Puntos (Unilateral)

Símbolos en el texto limpio serán reemplazados por cuadrados con algunos lados y puntos con las siguiente reglas:

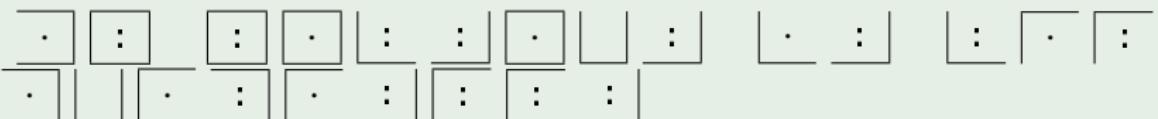
|     |     |     |
|-----|-----|-----|
| A : | B : | C : |
| D : | E : | F : |
| G : | H : | I : |

|     |     |     |
|-----|-----|-----|
| J . | K . | L . |
| M . | N . | O . |
| P . | Q . | R . |

|   |   |   |
|---|---|---|
| S | T | U |
| V | W | X |
| Y | Z |   |

## Ejemplo

ME ENCANTA LA CRIPTOGRAFIA



# Cifrado Porta (Poligráfico)

- Creado por Giovanni Battista della Porta en 1563
- Basado en la siguiente tabla (llave):

| A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | V | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ♀ | ¤ | Y | ♀ | △ | ¤ | □ | ♂ | × | ♂ | ♀ | × | ■ | ▀ | ▀ | ♂ | ○ | ▼ | ♀ | A |
| ♂ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | B |
| ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | C |
| ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | D |
| ♀ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | E |
| ♂ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | F |
| ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | G |
| ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | H |
| ♀ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | I |
| ♂ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | L |
| ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | M |
| ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | N |
| ♀ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | O |
| ♂ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | P |
| ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | Q |
| ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | R |
| ♀ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | S |
| ♂ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | T |
| ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | V |
| ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | ¤ | Z |

# Cifrado Playfair

- Creado por Sir Charles Wheatstone y popularizado por Baron Lyon Playfair en 1854
- La clave es una palabra de 5 letras diferentes
- La posiciona como la primera fila de una matriz de  $5 \times 5$
- Llena el resto de la matriz con las demás letras del alfabeto

## Ejemplo

IVANC

BDEFG

HKLMO

PQRST

UWXYZ

## Nota

En la matriz ignoramos la J  
(también podemos asumir que es igual que la I)

# Cifrado Playfair

- Tomamos bloques de 2 letras en el texto plano
- Si algun bloque tiene letras iguales lo sepáramos con una letra diferente, X por ejemplo
- Si en el ultimo bloque queda solo 1 letra le agregamos una letra diferente, X por ejemplo

Para encriptar un bloque:

- Si ambas letras están en la misma fila tomamos la letra a la derecha en la matriz
- Si ambas letras están en la misma columna tomamos la letra debajo en la matriz
- Tomamos las letras en la intersección de la misma fila y la otra columna

# Cifrado Playfair

## Ejemplo

Cifrar "THIS IS AN INTERESTING BIG MESSAGE"

TH IS IS AN IN TE RE ST IN GB IG ME SX SA GE

$$\text{TH} = \text{PO}$$

$$\text{IN} = \text{VC}$$

$$\text{ER} = \text{LX}$$

I V A N C

I V A N C

I V A N C

I V A N C

B D E F G

B D E F G

B D E F G

B D E F G

H K L M O

H K L M O

H K L M O

H K L M O

P Q R S T

P Q R S T

P Q R S T

P Q R S T

U W X Y Z

U W X Y Z

U W X Y Z

U W X Y Z

c = PO NP NP NC VC RG XL TP VC BD CB LF RY RN BF

# Cifrado Playfair

## Ejemplo

Cifrar "THIS IS AN INTERESTING BIG MESSAGE"

TH IS IS AN IN TE RE ST IN GB IG ME SX SA GE

$$\text{TH} = \text{PO}$$

$$\text{IN} = \text{VC}$$

$$\text{ER} = \text{LX}$$

I V A N C

I V A N C

I V A N C

I V A N C

B D E F G

B D E F G

B D E F G

B D E F G

H K L M O

H K L M O

H K L M O

H K L M O

P Q R S T

P Q R S T

P Q R S T

P Q R S T

U W X Y Z

U W X Y Z

U W X Y Z

U W X Y Z

c = PO NP NP NC VC RG XL TP VC BD CB LF RY RN BF

## Ejercicio

Con la misma clave descifrar UV PO ET LE PQ KZ LX GT LF TF  
XL CR XL TQ MC PN HB HA SZ

# Cifrado de basura en medio

- En el cifrado de basura en medio el mensaje se escribe en diferentes posiciones determinadas por la llave.
- Despues de esto llenamos las posiciones vacias con letras de modo que el mensaje luzca con un contenido muy distinto

## Ejemplo

I LOVE YOU  
I HAVE YOU  
DEEP UNDER  
MY SKIN MY  
LOVE LASTS  
FOREVER IN  
HYPERSPACE

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

|   |      |     |   |   |   |   |   |   |   |  |  |  |  |  |
|---|------|-----|---|---|---|---|---|---|---|--|--|--|--|--|
| I | LOVE | YOU |   |   |   |   |   |   |   |  |  |  |  |  |
| I | HAVE | YO  | U |   |   |   |   |   |   |  |  |  |  |  |
| D | E    | E   | P | U | N | D | E | R |   |  |  |  |  |  |
| M | Y    | S   | K | I | N | M | Y |   |   |  |  |  |  |  |
| L | O    | V   | E | L | A | S | T | S |   |  |  |  |  |  |
| F | O    | R   | E | V | E | R | Y | E |   |  |  |  |  |  |
| H | Y    | P   | E | R | S | P | A | C | E |  |  |  |  |  |

# Cifrado de basura en medio

- En el cifrado de basura en medio el mensaje se escribe en diferentes posiciones determinadas por la llave.
- Después de esto llenamos las posiciones vacías con letras de modo que el mensaje luzca con un contenido muy distinto

## Ejemplo

I LOVE YOU  
I HAVE YOU  
DEEP UNDER  
MY SKIN MY  
LOVE LASTS  
FOREVER IN  
HYPERSPACE

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

|            |       |     |            |   |   |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|------------|-------|-----|------------|---|---|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
| I          | LOVE  | YOU |            |   |   |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| I          | HAVE  | YOU | O          |   |   |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| DEEP       | UNDER |     | U          |   |   |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| MY         | SKIN  | MY  | KI         |   |   |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| LOVE       | LASTS |     | LASTS      |   |   |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| FOREVER    | IN    |     | FOREVER    |   |   |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| HYPERSPACE |       |     | HYPERSPACE | C | E |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

## Ejercicio

De algún ejemplo creativo de basura en medio



# Sustitucion polialfabética

- El mayor problema de la sustitución monoalfabética es que no tienen la propiedad de *difusión*

## Nota

Con análisis de frecuencias se pueden romper fácilmente los cifrados monoalfabéticos vistos

- Los sistemas de sustitución polialfabética cifran cada simbolo o grupo de simbolos en diferentes simbolos en lugar de uno solo

# Cifrado Vigènere

- Creado por Blaise de Vigenere, Siglo XVI. Al igual que el cifrado César se cifra cada letra a partir de un corrimiento.
- El valor del corrimiento no será fijo para todo el mensaje, sino que utilizará una palabra clave
- La clave se repetirá a lo largo del texto a cifrar y el corrimiento dependerá de la letra ('A' = 0, 'B' = 1, ..., 'Z' = 25)

## Ejemplo

Cifrar "EL CURSO DE CRIPTOGRAFIA ME ENCANTA",  
utilizando la llave = "UNAL"

mensaje = ELCURSODECRIPTOGRAFIAMEENCANTA

llave = UNALUNALUNALUNALUNALUNALUNALUN

cifrado = YYCFLFOOYPRTJGORLNFTUZEHPAYNN

# Cifrado Vigènere

## Nota

Este sistema de cifrado es la idea básica de la maquina Enigma.

## Nota

Por 300 años este cifrado fue considerado irrompible hasta 1863 donde la milicia encontró un método para determinar la longitud de la llave, de ahí se puede utilizar frecuencia de análisis.

# Cifrado Vigènere

## Nota

Este sistema de cifrado es la idea básica de la maquina Enigma.

## Nota

Por 300 años este cifrado fue considerado irrompible hasta 1863 donde la milicia encontró un método para determinar la longitud de la llave, de ahí se puede utilizar frecuencia de análisis.

## Ejercicio

Descifre "GJBTJIKQMHYOEZT" utilizando como llave "CRIPTO"

# Cifrado Hill

- Cada elemento del alfabeto es numerado desde 0 hasta  $n - 1$  ( $n = |A|$ ).
- $M = C = (\mathbb{Z}_n)^t$  donde  $t$  es el tamaño del bloque.
- Ciframos a partir de  $t$  combinaciones lineales de los elementos.

## Ejemplo

Si  $t = 2$ , podemos tomar un bloque de texto limpio  $m = (m_1, m_2)$ , el texto cifrado podría ser por ejemplo  $c = (11m_1 + 3m_2, 8m_1 + 7m_2)$ . Podriamos escribir  $\begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} 11 & 3 \\ 8 & 7 \end{pmatrix} \begin{pmatrix} m_1 \\ m_2 \end{pmatrix}$

# Cifrado Hill

- En general la llave será una matriz  $K \in (\mathbb{Z}_n)^{t \times t}$
- La función de cifrado sería  $E_K(m) = K \cdot m$ ,  $m$  es un vector columna
- Estudiantes familiarizados con el álgebra lineal se darán cuenta que para descifrar utilizaremos  $K^{-1}$  la inversa de  $K$

## Nota

La inversa de una matriz  $A$  (si existe) es una matriz  $A^{-1}$  tal que  $AA^{-1} = A^{-1}A = I$ , donde  $I$  es la matriz identidad (una matriz con 1's en la diagonal y 0's en las demás posiciones)

# Cifrado Hill

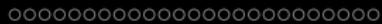
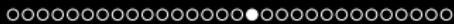
- En general la llave será una matriz  $K \in (\mathbb{Z}_n)^{t \times t}$
- La función de cifrado sería  $E_K(m) = K \cdot m$ ,  $m$  es un vector columna
- Estudiantes familiarizados con el álgebra lineal se darán cuenta que para descifrar utilizaremos  $K^{-1}$  la inversa de  $K$

## Nota

La inversa de una matriz  $A$  (si existe) es una matriz  $A^{-1}$  tal que  $AA^{-1} = A^{-1}A = I$ , donde  $I$  es la matriz identidad (una matriz con 1's en la diagonal y 0's en las demás posiciones)

## Ejercicio

Tomando el alfabeto de letras inglesas ( $n = 26$ ) y  $K = \begin{pmatrix} 7 & 3 \\ 8 & 11 \end{pmatrix}$  como la matriz de cifrado, calcule la matriz de descifrado



# Cifrado Hill

## Ejemplo

Sea  $A = 'A', 'B', \dots, 'Z' \equiv \mathbb{Z}_{26}$  donde  $'A' = 0, 'B' = 1, \dots, 'Z' = 25$ .

Encriptar "HELP" usando  $K = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}$

HE = (7, 4), LP = (11, 15)

$$\begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} \begin{pmatrix} 7 \\ 4 \end{pmatrix} = \begin{pmatrix} 7 \\ 8 \end{pmatrix} \pmod{26} \text{ y } \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} \begin{pmatrix} 11 \\ 15 \end{pmatrix} = \begin{pmatrix} 0 \\ 19 \end{pmatrix} \pmod{26}$$

Luego c = HIAT

# Cifrado Hill

## Ejemplo

Sea  $A = 'A', 'B', \dots, 'Z' \equiv \mathbb{Z}_{26}$  donde ' $A' = 0, 'B' = 1, \dots, 'Z' = 25$ .

Encriptar "HELP" usando  $K = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}$

$HE = (7, 4)$ ,  $LP = (11, 15)$

$$\begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} \begin{pmatrix} 7 \\ 4 \end{pmatrix} = \begin{pmatrix} 7 \\ 8 \end{pmatrix} \pmod{26} \text{ y } \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} \begin{pmatrix} 11 \\ 15 \end{pmatrix} = \begin{pmatrix} 0 \\ 19 \end{pmatrix} \pmod{26}$$

Luego  $c = HIAT$

## Ejercicio

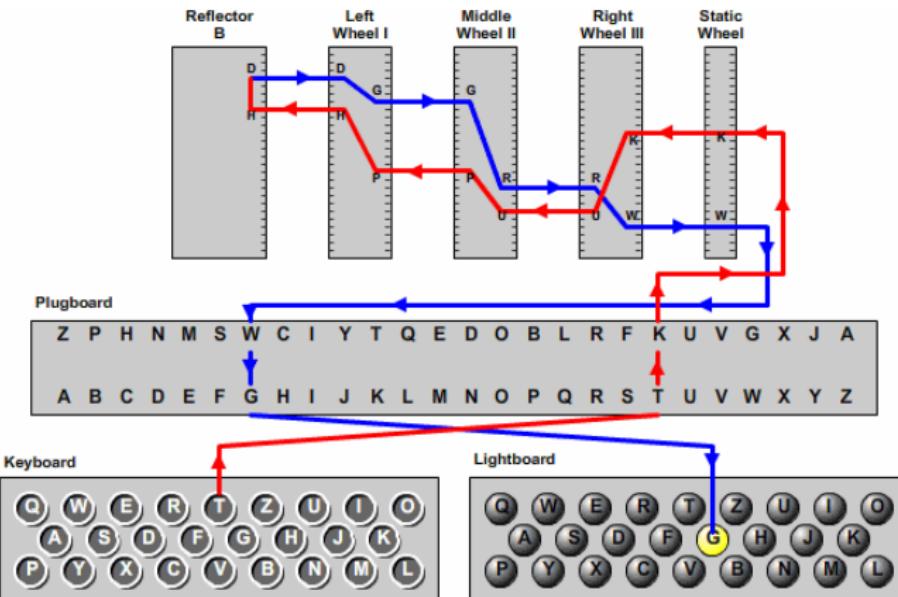
Con el alfabeto anterior encripte  $m = "EL CIFRADO DE HILL ES$

DIFÍCIL"

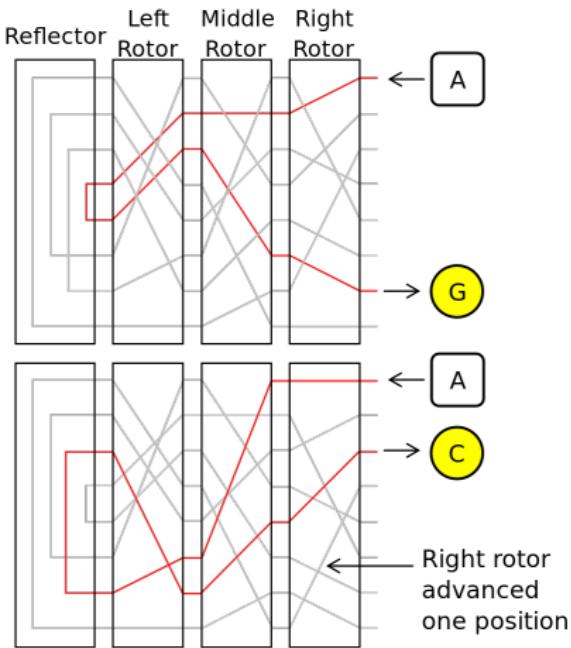
(quitando los espacios) con  $t = 3$  y  $K = \begin{pmatrix} 20 & 7 & 23 \\ 23 & 13 & 3 \\ 7 & 23 & 6 \end{pmatrix}$

# Cifrado Enigma

- Las máquinas Enigma fueron una familia de máquinas cifrados que funcionaban con ruedas codificadoras utilizadas en la II guerra mundial



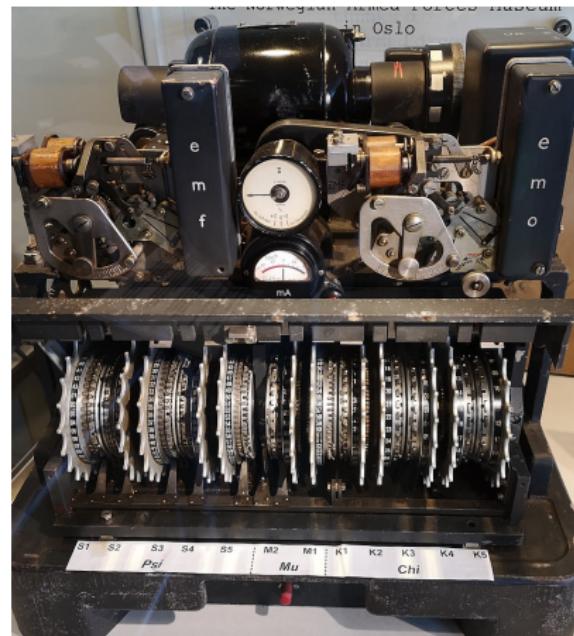
# Cifrado Enigma



- Los rotores internamente manejan una configuración *ringstellung* correspondiente a una permutación del alfabeto
- Las posiciones iniciales del rotor se configuran de manera externa (*grundstellung*)
- Al ingresar una letra alguna de las ruedas se corre
- El *grundstellung* era enviado 2 veces (6 caracteres), esto dió pie a vulnerabilidades del cifrado

# Cifrado Lorenz

- Otra máquina de cifrado utilizada en la guerra fue la de *cifrado Lorenz*
- Esta máquina tiene ruedas de varios tamaños que rotan para generar llaves binarias
- Para que funcione se deben tener ambas máquinas con la misma configuración inicial
- Calcula el XOR entre el mensaje y la llave
- Se pudo realizar criptoanálisis cuando 2 mensajes fueron enviados con la misma llave



# Cifrado Homofónico

- Los cifrados de sustitución homofónicos pueden cifrar cada elemento del alfabeto en diferentes letras
- Tipicamente el alfabeto de los textos cifrados es mas grande que el de los textos limpios
- La sustitución se basa en la frecuencia de los elementos en el espacio de mensajes
- cuando tenemos varias opciones de escogencia para el cifrado de una letra lo podemos hacer de manera uniformemente aleatoria

## Nota

La idea de este cifrado es aplanar la frecuencia de aparición de cada letra

# Cifrado Homofónico

## Ejemplo

Cifrar el mensaje en inglés "STATISTICS ARE COMPLEX"

| A  | B  | C  | D  | E  | F  | G  | H  | I  | J  | K  | L  | M  | N  | O  | P  | Q  | R  | S  | T  | U  | V  | W  | X  | Y  | Z |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|---|
| 3  | 10 | 20 | 26 | 9  | 2  | 17 | 44 | 18 | 14 | 37 | 7  | 12 | 28 | 40 | 0  | 22 | 4  | 34 | 8  | 43 | 25 | 13 | 41 | 1  | 5 |
| 6  | 29 | 45 | 35 | 11 | 59 | 32 | 48 | 38 |    |    | 21 | 39 | 33 | 46 | 31 |    | 15 | 62 | 19 | 52 |    | 30 |    | 47 |   |
| 24 |    | 73 | 55 | 16 |    |    | 53 | 51 |    |    | 36 |    | 58 | 60 | 67 |    | 42 | 65 | 49 | 69 |    |    |    |    |   |
| 56 |    |    | 61 | 23 |    |    | 66 | 63 |    |    | 57 |    | 64 | 84 |    |    | 54 | 74 | 70 |    |    |    |    |    |   |
| 68 |    |    |    | 27 |    |    | 77 | 72 |    |    |    |    | 81 | 93 |    |    | 75 | 79 | 71 |    |    |    |    |    |   |
| 76 |    |    |    |    | 50 |    |    | 80 | 92 |    |    |    | 89 | 96 |    |    | 85 | 91 | 82 |    |    |    |    |    |   |
| 83 |    |    |    |    | 78 |    |    |    |    |    |    |    | 99 |    |    |    |    |    |    | 88 |    |    |    |    |   |
| 86 |    |    |    |    | 87 |    |    |    |    |    |    |    |    |    |    |    |    |    |    | 95 |    |    |    |    |   |
|    |    |    |    |    | 90 |    |    |    |    |    |    |    |    |    |    |    |    |    |    | 98 |    |    |    |    |   |
|    |    |    |    |    | 94 |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |   |
|    |    |    |    |    | 97 |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |   |

$$c = 79 \ 19 \ 56 \ 98 \ 51 \ 91 \ 71 \ 18 \ 45 \ 34 \ 3 \ 15 \ 50 \ 20 \ 96 \ 39 \ 67 \ 7 \ 87 \ 41$$

# Cifrado Homofónico

## Ejemplo

Cifrar el mensaje en inglés "STATISTICS ARE COMPLEX"

| A         | B  | C  | D  | E         | F  | G  | H  | I  | J  | K  | L  | M  | N  | O  | P  | Q  | R  | S  | T  | U         | V  | W  | X  | Y  | Z |  |
|-----------|----|----|----|-----------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|-----------|----|----|----|----|---|--|
| 3         | 10 | 20 | 26 | 9         | 2  | 17 | 44 | 18 | 14 | 37 | 7  | 12 | 28 | 40 | 0  | 22 | 4  | 34 | 8  | 43        | 25 | 13 | 41 | 1  | 5 |  |
| 6         | 29 | 45 | 35 | 11        | 59 | 32 | 48 | 38 |    |    | 21 | 39 | 33 | 46 | 31 |    | 15 | 62 | 19 | 52        |    | 30 |    | 47 |   |  |
| 24        |    | 73 | 55 | 16        |    |    | 53 | 51 |    |    | 36 |    | 58 | 60 | 67 |    | 42 | 65 | 49 | 69        |    |    |    |    |   |  |
| <u>56</u> |    | 61 | 23 |           |    | 66 | 63 |    |    | 57 |    | 64 | 84 |    |    | 54 | 74 | 70 |    |           |    |    |    |    |   |  |
| 68        |    |    | 27 |           |    | 77 | 72 |    |    |    |    | 81 | 93 |    |    | 75 | 79 | 71 |    |           |    |    |    |    |   |  |
| 76        |    |    |    | 50        |    |    | 80 | 92 |    |    |    | 89 | 96 |    |    | 85 | 91 | 82 |    |           |    |    |    |    |   |  |
| 83        |    |    |    | 78        |    |    |    |    |    |    |    | 99 |    |    |    |    |    |    |    | 88        |    |    |    |    |   |  |
| 86        |    |    |    | <u>87</u> |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    | 95        |    |    |    |    |   |  |
|           |    |    |    | 90        |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    | <u>98</u> |    |    |    |    |   |  |
|           |    |    |    | 94        |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |           |    |    |    |    |   |  |
|           |    |    |    | 97        |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |           |    |    |    |    |   |  |

$$c = 79 \ 19 \ 56 \ 98 \ 51 \ 91 \ 71 \ 18 \ 45 \ 34 \ 3 \ 15 \ 50 \ 20 \ 96 \ 39 \ 67 \ 7 \ 87 \ 41$$

## Ejercicio

Descifrar 29 63 32 4 76 39 74 56 15 90 82 54 60 43 10 36 9





# Cifrado por transposición

## Definición (Cifrado por transposición)

Un sistema de cifrado por transposición es aquel que cambia la posición de las letras a lo largo del mensaje

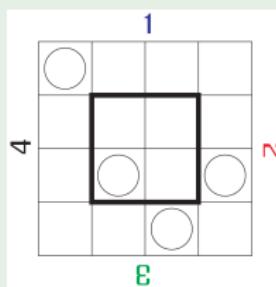
- Cambiando las posiciones de los elementos en el texto se disipan propiedades estadísticas dependientes de la posición

# Cifrado de grilla giratoria

- Utilizada por Alemania en la primera guerra mundial
- Utiliza un cuadrado con hoyos tal que cada celda aparece una vez en las rotaciones
- El resultado nos da una permutación de los elementos del texto original

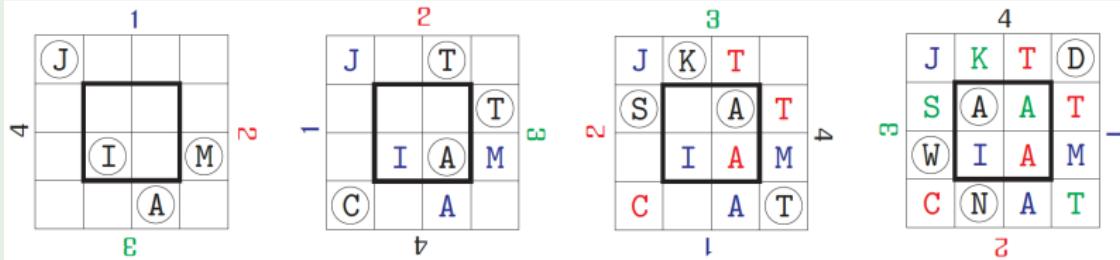
## Ejemplo

Cifrar JIM ATTACKS AT DAWN utilizando la siguiente grilla  $4 \times 4$



# Cifrado de grilla giratoria

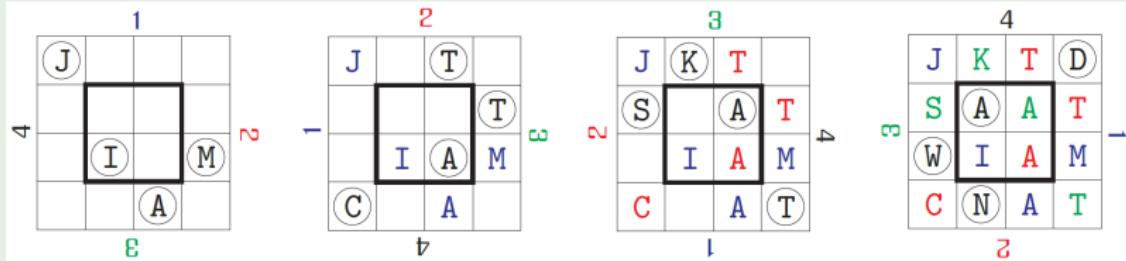
## Ejemplo



JIMA TTAC KSAT DAWN  
JKTD SAAT WIAM CNAT

# Cifrado de grilla giratoria

## Ejemplo



JIMA TTAC KSAT DAWN  
JKTD SAAT WIAM CNAT

## Ejercicio

¿Cuántos textos limpios diferentes pueden corresponder al siguiente texto cifrado ALEA BXCH GSNT KORP?

# Cifrado por producto

## Definición (Cifrado por producto)

Un sistema de cifrado por producto corresponde a una composición de un cifrado por sustitución y uno de transposición.

- Componer 2 sustituciones crea una sustitución mas compleja
- Componer 2 transposiciones crea una transposición mas compleja
- Componer una sustitución con una transposición crea un cifrado mas complejo en general

## Nota

Componiendo estos cifrados apuntamos a tener *confusión* (sustitución) y *difusión* (transposición)

# Cifrado de Feistel

- Creado por Feistel para IBM, 1971
- Utiliza permutaciones en bloques grandes y sustitución en pequeños bloques
- No utiliza llave (seguridad por oscuridad)
- Fue implementado en hardware, los chips de permutación se llamaron **P-Boxes** y los de sustitución **S-Boxes**.

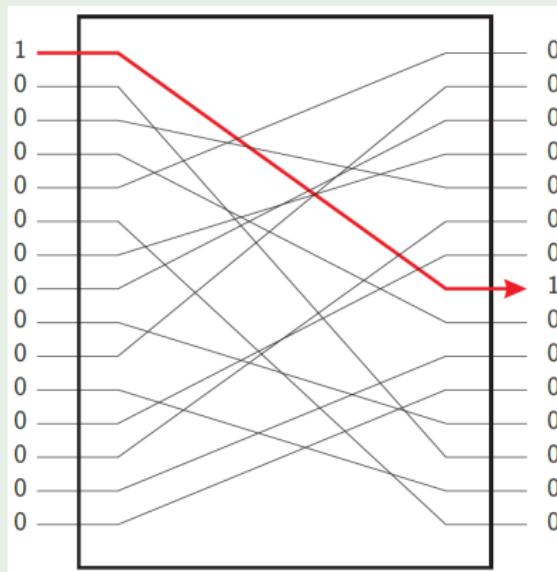
## Nota

Originalmente lo llamaron "Demonstration Cipher", abreviado "Demon" que llevó a que este cifrado también se conozca como "Lucifer".

# P-Box

Una caja de permutación (*P-Box*) es un componente que permuta los bits de su entrada

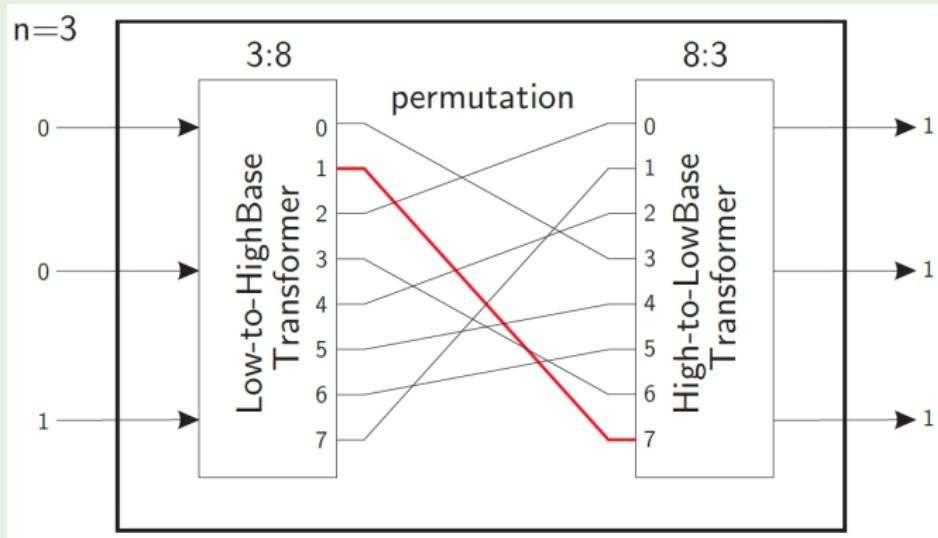
## Ejemplo



# S-Box

Una caja de sustitución (*S-Box*) es un componente que codifica un número de  $n$  bits a otro número de  $n$  bits.

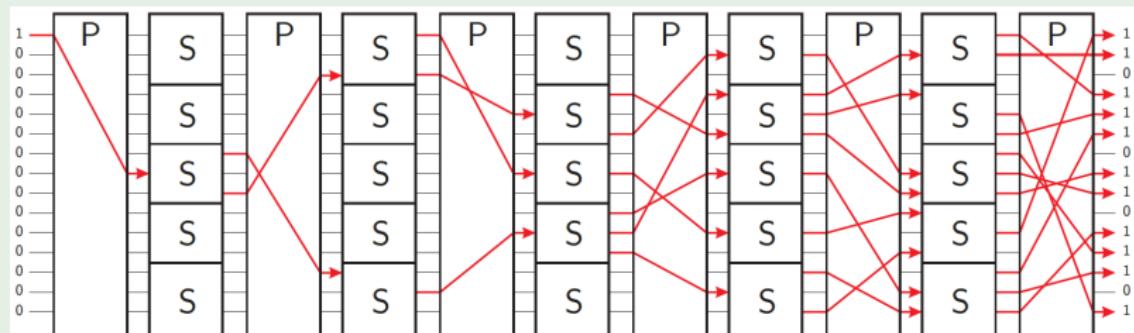
## Ejemplo



# Cifrado de Feistel

El cifrado Lucifer simplemente consistía en la concatenación de varios P-Boxes y S-Boxes de manera alternada

## Ejemplo



## Nota

Esta fue la inspiración para el cifrado *DES*

# Data Encryption Standard (DES)

- El Estándar de Cifrado de Datos (Data Encryption Standard) es un cifrado por bloques inventado por IBM en los 70s
- $M = C = \{0,1\}^{64}, K = \{0,1\}^{56}$
- En su momento se creía que el *DES* era imposible de romper a fuerza bruta tratando las  $72,057,594,037,927,936 \approx 7 * 10^{16}$  posibles llaves.

## Nota

En 1998 el Electronic Frontier Foundation (EFF) construyó una máquina que puede *crackear* el DES por fuerza bruta, gasta aproximadamente 4.5 días

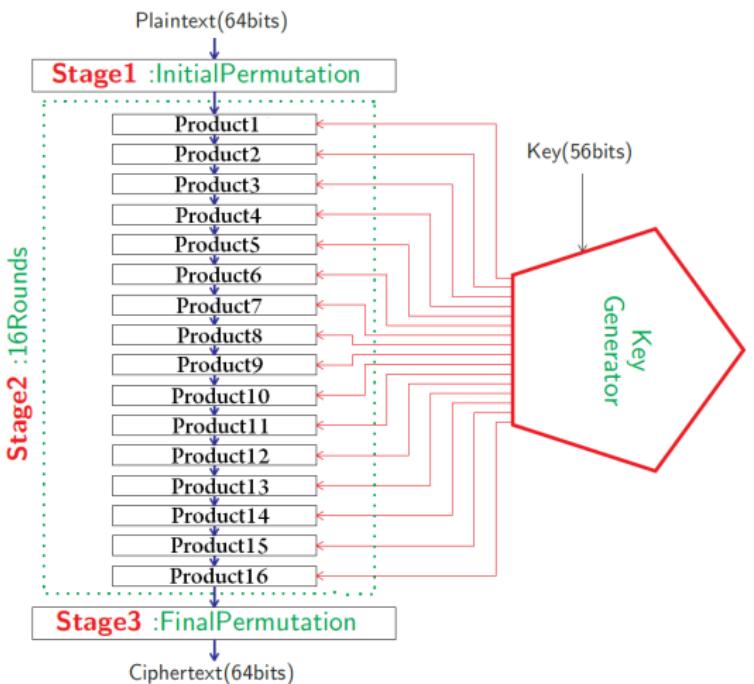
## Nota

El DES dejó ser un estándar en 2004, fue reemplazado por el AES

# Pasos del algoritmo DES

El algoritmo tiene 3 etapas:

- ① Permutación inicial
- ② 16 rondas
- ③ Permutación final



# Generador de llaves

A partir de la llave inicial de 56 bits se crean 16 subllaves de 48 bits

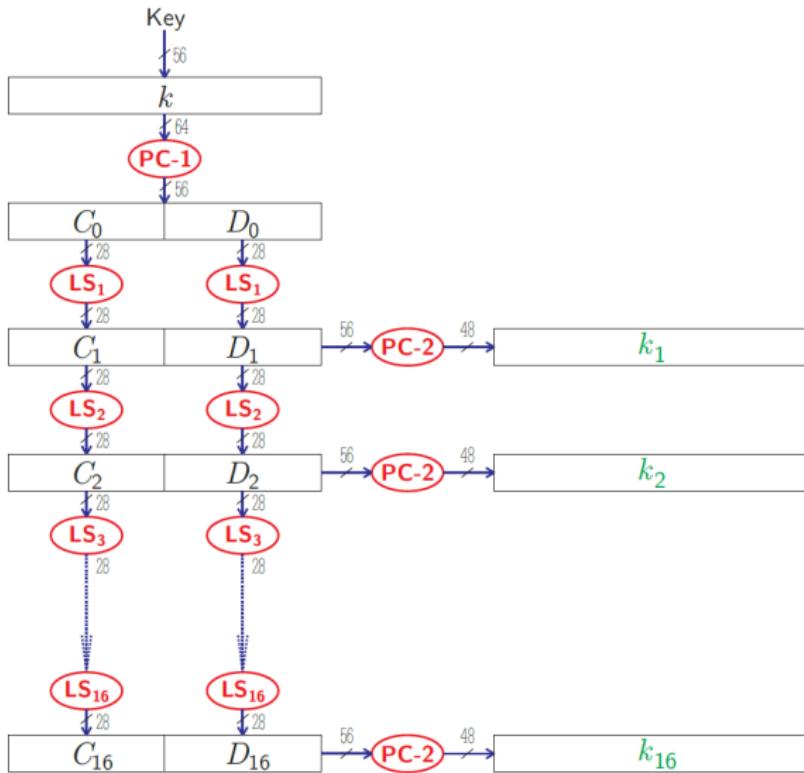
- Primero el generador recibe una cadena  $k$  de 64 bits (8 bytes)
- En cada byte 7 bits hacen parte de la llave y el otro es un *bit de paridad*
- Se computa  $k_0 = \text{PC-1}(k) = C_0 D_0$ , donde  $|C_0| = |D_0| = 28$
- Para  $i = 1, \dots, 16$  se calcula:  
 $C_i = LS_i(C_{i-1}), D_i = LS_i(D_{i-1}), k_i = \text{PC-2}(C_i D_i)$   
donde  $LS_i$  es un *corrimiento cíclico de bits* (a la izquierda) de 1 posición para  $i = 1, 2, 9, 16$  o 2 posiciones en caso contrario
- PC-1 y PC-2 son P-Boxes.

## Nota

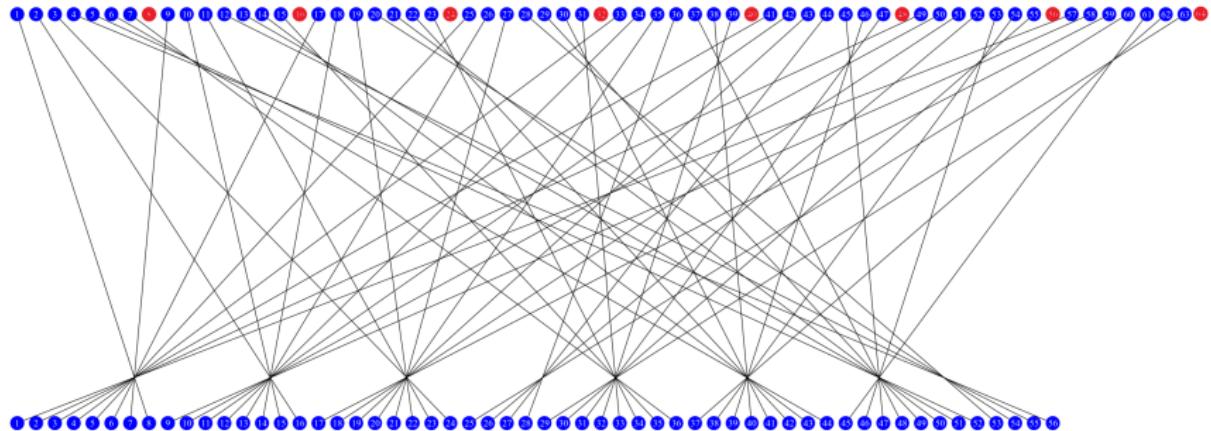
El bit de paridad se usa para verificar que la correctitud de la información, la idea es asegurar que cada byte siempre tenga una cantidad impar de 1's



# Generador de llaves

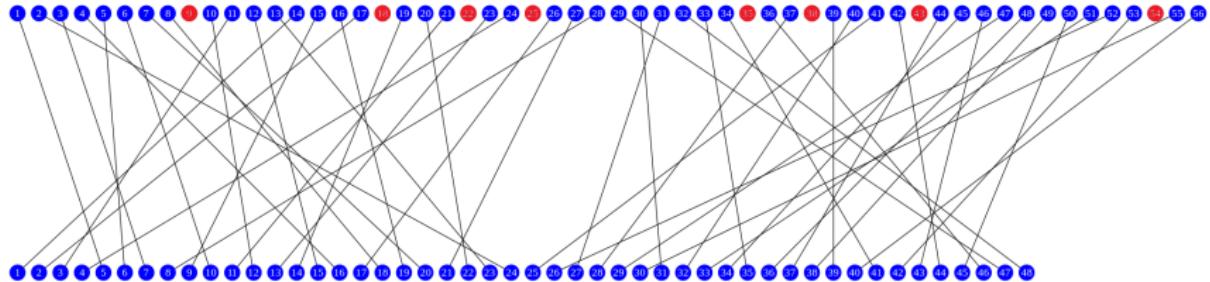


# Permuted Choice 1 (PC-1)



La permutación es la siguiente: 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

# Permuted Choice 2 (PC-2)



La permutación es la siguiente: 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

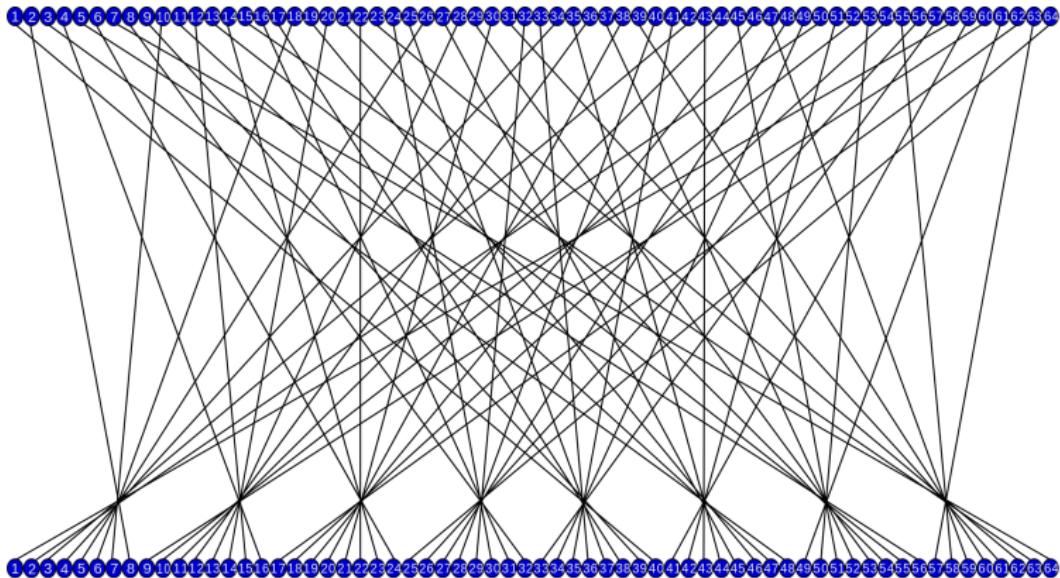
# Permutaciones inicial y final

- En la primera etapa del DES a partir de un texto limpio  $m$  una cadena de bits  $m_0$  se construye permutando los bits con la P-Box IP (*Initial Permutation*)
- Escribimos  $m_0 = \text{IP}(x) = L_0 R_0$ , donde  $|L_0| = |R_0| = 32$
- En la última etapa del DES hacemos la permutación inversa a la inicial, es decir,  $\text{IP}^{-1}$ .
- Al final  $c = \text{IP}^{-1}(R_{16} L_{16})$

## Nota

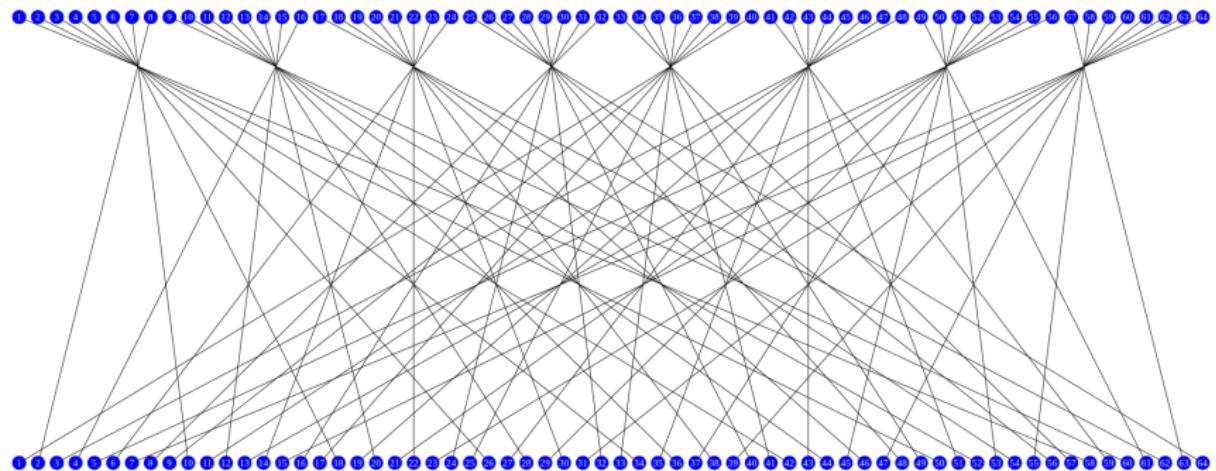
Si el bloque es mas corto de 64 bits se debe completar con 0's

# Permutación inicial (IP)



La permutación es la siguiente: 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

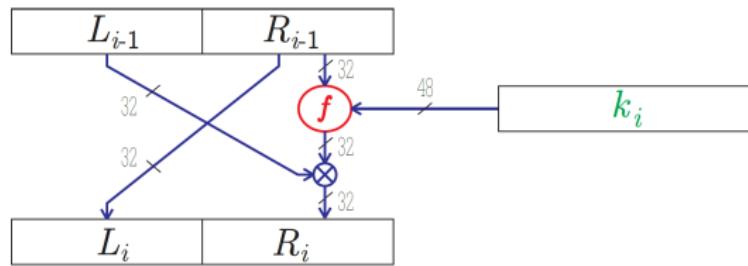
## Permutación final ( $IP^{-1}$ )



La permutación es la siguiente: 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

## 16 rondas

- Despues de la permutación inicial se realizan 16 rondas de cifrados producto
- Para  $i = 1, \dots, 16$  computamos  $L_i, R_i$  de la siguiente forma:  
$$L_i = R_{i-1}, R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$$
- $f$  es la función interna del DES que compone cifrados usando las subllaves  $k_1, \dots, k_{16}$



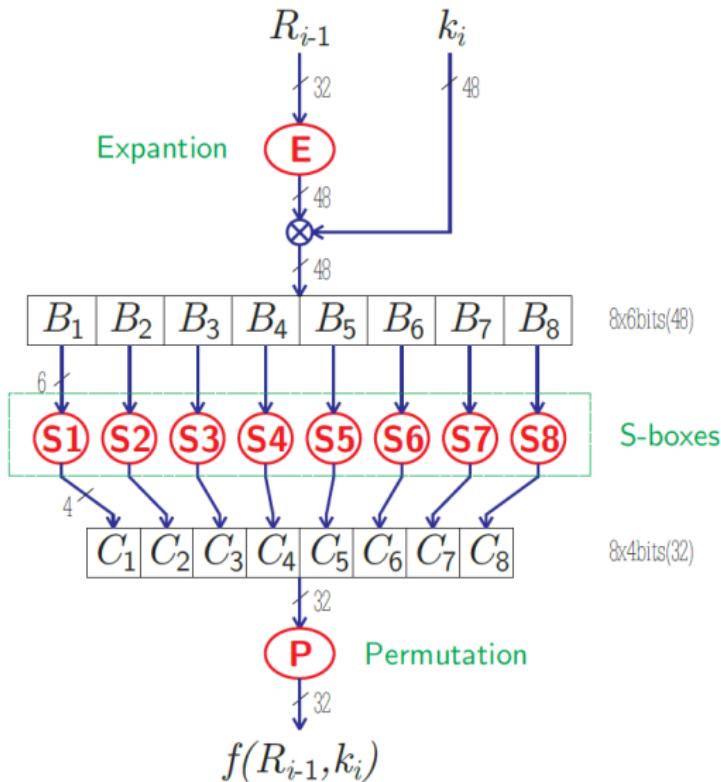
# Función F

- La función F creada por Feistel se derivó de Lucifer y hace parte de las rondas del DES
- Toma como entrada  $R_{i-1}$  y  $k_i$  y produce una salida de 32 bits

Los pasos son los siguientes:

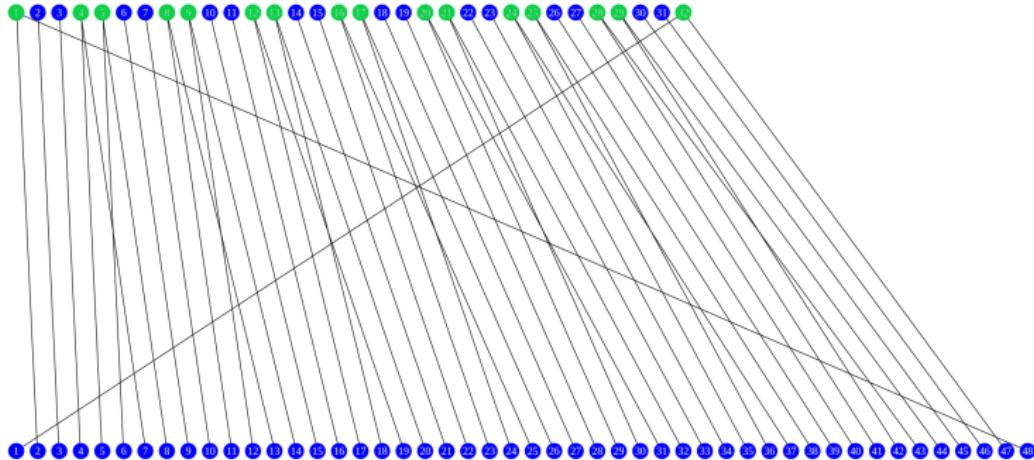
- ①  $R_{i-1}$  es expandido a una cadena de bits de tamaño 48 con una función fija  $E$
- ② Se computa  $B = E(R_{i-1}) \oplus k_i$ ,  $B = B_1B_2B_3B_4B_5B_6B_7B_8$ , donde cada bloque  $B_j$  es de 6 bits
- ③ Computamos  $C_j = S_j(B_j)$  a cada bloque.  $S_j$  son S-Boxes
- ④ La cadena de bits  $C = C_1C_2C_3C_4C_5C_6C_7C_8$  la permutamos a través de una P-Box P

## Función F



## Expansión E

- La función de expansión es una P-Box en la que varios de los bits de entrada se duplican



La permutación es la siguiente: 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

# Sustituciones $S_j$

- Para cada  $B_j = b_1 b_2 b_3 b_4 b_5 b_6$  las S-Boxes  $S_j$  corresponden a tablas de tamaño  $4 \times 16$  donde  $b_1 b_6$  es el numero de la fila y  $b_2 b_3 b_4 b_5$  es el de la columna
- Los valores de la tabla van de 0 a 15

|          |    | <i>c</i> |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
|----------|----|----------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
|          |    | 00       | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 |
| <i>r</i> | 00 | 14       | 04 | 13 | 01 | 02 | 15 | 11 | 08 | 03 | 10 | 06 | 12 | 05 | 09 | 00 | 07 |
|          | 01 | 00       | 15 | 07 | 04 | 14 | 02 | 13 | 01 | 10 | 06 | 12 | 11 | 09 | 05 | 03 | 08 |
|          | 02 | 04       | 01 | 14 | 08 | 13 | 06 | 02 | 11 | 15 | 12 | 09 | 07 | 03 | 10 | 05 | 00 |
|          | 03 | 15       | 12 | 08 | 02 | 04 | 09 | 01 | 07 | 05 | 11 | 03 | 14 | 10 | 00 | 06 | 13 |

$$B = b_1 b_2 b_3 b_4 b_5 b_6$$

$$r = b_1 b_6 \in [0, \dots, 3]$$

$$c = b_2 b_3 b_4 b_5 \in [0, \dots, 15]$$

# Sustituciones $S_j$

- Para cada  $B_j = b_1 b_2 b_3 b_4 b_5 b_6$  las S-Boxes  $S_j$  corresponden a tablas de tamaño  $4 \times 16$  donde  $b_1 b_6$  es el numero de la fila y  $b_2 b_3 b_4 b_5$  es el de la columna
- Los valores de la tabla van de 0 a 15

|          |    | <i>c</i> |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
|----------|----|----------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
|          |    | 00       | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 |
| <i>r</i> | 00 | 14       | 04 | 13 | 01 | 02 | 15 | 11 | 08 | 03 | 10 | 06 | 12 | 05 | 09 | 00 | 07 |
|          | 01 | 00       | 15 | 07 | 04 | 14 | 02 | 13 | 01 | 10 | 06 | 12 | 11 | 09 | 05 | 03 | 08 |
|          | 02 | 04       | 01 | 14 | 08 | 13 | 06 | 02 | 11 | 15 | 12 | 09 | 07 | 03 | 10 | 05 | 00 |
|          | 03 | 15       | 12 | 08 | 02 | 04 | 09 | 01 | 07 | 05 | 11 | 03 | 14 | 10 | 00 | 06 | 13 |

$$B = b_1 b_2 b_3 b_4 b_5 b_6$$

$$r = b_1 b_6 \in [0, \dots, 3]$$

$$c = b_2 b_3 b_4 b_5 \in [0, \dots, 15]$$

## Ejercicio

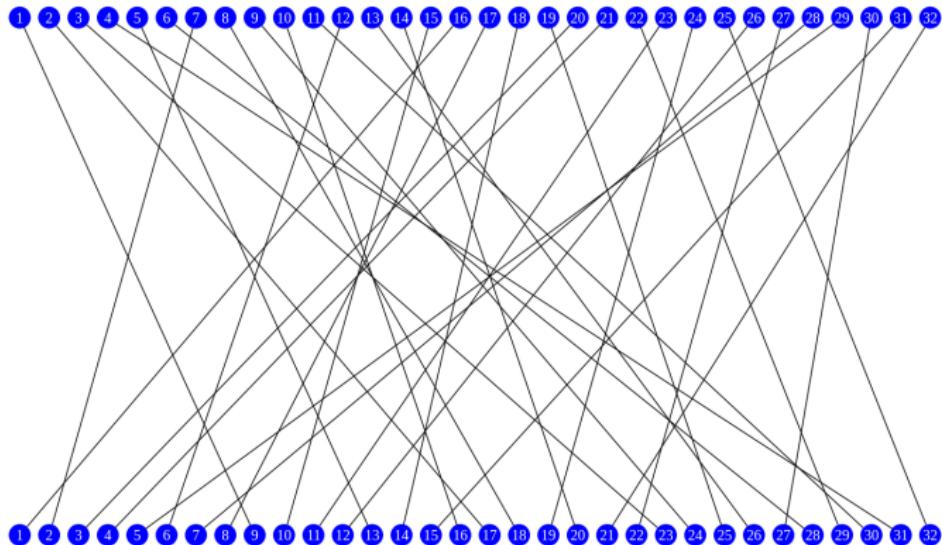
Calcular  $S_3(35)$

# Sustituciones S<sub>j</sub>

|   |    | c  |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
|---|----|--|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
|   |    | S1 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| r | 00 | 14   | 04 | 13 | 01 | 02 | 15 | 11 | 08 | 03 | 10 | 06 | 12 | 05 | 09 | 00 | 07 |
|   | 01 | 00   | 15 | 07 | 04 | 14 | 02 | 13 | 01 | 10 | 06 | 12 | 11 | 09 | 05 | 03 | 08 |
|   | 02 | 04   | 01 | 14 | 08 | 13 | 06 | 02 | 11 | 15 | 12 | 09 | 07 | 03 | 10 | 05 | 00 |
|   | 03 | 15   | 12 | 08 | 02 | 04 | 09 | 01 | 07 | 05 | 11 | 03 | 14 | 10 | 00 | 06 | 13 |
|   |    | S2 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| r | 00 | 15   | 01 | 08 | 14 | 06 | 11 | 03 | 04 | 09 | 07 | 02 | 13 | 12 | 00 | 05 | 10 |
|   | 01 | 03   | 13 | 04 | 07 | 15 | 02 | 08 | 14 | 12 | 00 | 01 | 10 | 06 | 09 | 11 | 05 |
|   | 02 | 00   | 14 | 07 | 11 | 10 | 04 | 13 | 01 | 05 | 08 | 12 | 06 | 09 | 03 | 02 | 15 |
|   | 03 | 13   | 08 | 10 | 01 | 03 | 15 | 04 | 02 | 11 | 06 | 07 | 12 | 00 | 05 | 14 | 09 |
|   |    | S3 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| r | 00 | 10   | 00 | 09 | 14 | 06 | 03 | 15 | 05 | 01 | 13 | 12 | 07 | 11 | 04 | 02 | 08 |
|   | 01 | 13   | 07 | 00 | 09 | 03 | 04 | 06 | 10 | 02 | 08 | 05 | 14 | 12 | 11 | 15 | 01 |
|   | 02 | 13   | 06 | 04 | 09 | 08 | 15 | 03 | 00 | 11 | 01 | 02 | 12 | 05 | 10 | 14 | 07 |
|   | 03 | 01   | 10 | 13 | 00 | 06 | 09 | 08 | 07 | 04 | 15 | 14 | 03 | 11 | 05 | 02 | 12 |
|   |    | S4 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| r | 00 | 07   | 13 | 14 | 03 | 00 | 06 | 09 | 10 | 01 | 02 | 08 | 05 | 11 | 12 | 04 | 15 |
|   | 01 | 13   | 08 | 11 | 05 | 06 | 15 | 00 | 03 | 04 | 07 | 02 | 12 | 01 | 10 | 14 | 09 |
|   | 02 | 10   | 06 | 09 | 00 | 12 | 11 | 07 | 13 | 15 | 01 | 03 | 14 | 05 | 02 | 08 | 04 |
|   | 03 | 03   | 15 | 00 | 06 | 10 | 01 | 13 | 08 | 09 | 04 | 05 | 11 | 12 | 07 | 02 | 14 |

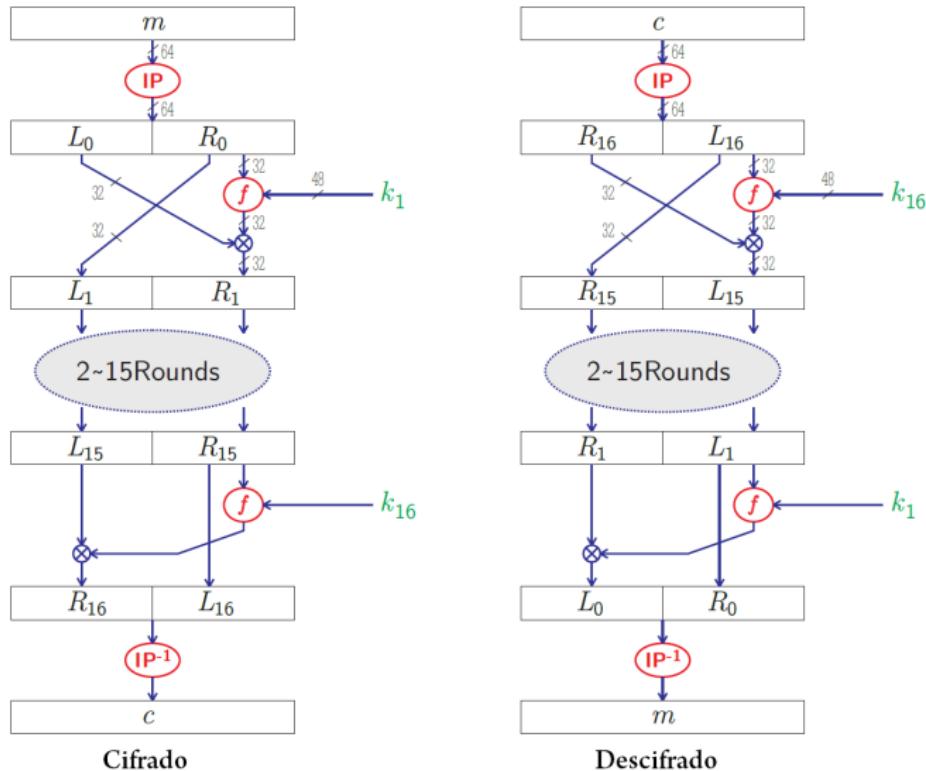
|    |    | c  |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
|----|----|--|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
|    |    | S5 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 00 | 02 | 12   | 04 | 01 | 07 | 10 | 11 | 06 | 08 | 05 | 03 | 15 | 13 | 00 | 14 | 09 |
| 01 | 14 | 11   | 02 | 12 | 04 | 07 | 13 | 01 | 05 | 00 | 15 | 10 | 03 | 09 | 08 | 06 |
| 02 | 04 | 02   | 01 | 11 | 10 | 13 | 07 | 08 | 15 | 09 | 12 | 05 | 06 | 03 | 00 | 14 |
| 03 | 11 | 08   | 12 | 07 | 01 | 14 | 02 | 13 | 06 | 15 | 00 | 09 | 10 | 04 | 05 | 03 |
|    |    | S6 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 00 | 12 | 01   | 10 | 15 | 09 | 02 | 06 | 08 | 00 | 13 | 03 | 04 | 14 | 07 | 05 | 11 |
| 01 | 10 | 15   | 04 | 02 | 07 | 12 | 09 | 05 | 06 | 01 | 13 | 14 | 00 | 11 | 03 | 08 |
| 02 | 09 | 14   | 15 | 05 | 02 | 08 | 12 | 03 | 07 | 00 | 04 | 10 | 01 | 13 | 11 | 06 |
| 03 | 04 | 03   | 02 | 12 | 09 | 05 | 15 | 10 | 11 | 14 | 01 | 07 | 06 | 00 | 08 | 13 |
|    |    | S7 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 00 | 04 | 11   | 02 | 14 | 15 | 00 | 08 | 13 | 03 | 12 | 09 | 07 | 05 | 10 | 06 | 01 |
| 01 | 13 | 00   | 11 | 07 | 04 | 09 | 01 | 10 | 14 | 03 | 05 | 12 | 02 | 15 | 08 | 06 |
| 02 | 01 | 04   | 11 | 13 | 12 | 03 | 07 | 14 | 10 | 15 | 06 | 08 | 00 | 05 | 09 | 02 |
| 03 | 06 | 11   | 13 | 08 | 01 | 04 | 10 | 07 | 09 | 05 | 00 | 15 | 14 | 02 | 03 | 12 |
|    |    | S8 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 00 | 13 | 02   | 08 | 04 | 06 | 15 | 11 | 01 | 10 | 09 | 03 | 14 | 05 | 00 | 12 | 07 |
| 01 | 01 | 15   | 13 | 08 | 10 | 03 | 07 | 04 | 12 | 05 | 06 | 11 | 00 | 14 | 09 | 02 |
| 02 | 07 | 11   | 04 | 01 | 09 | 12 | 14 | 02 | 00 | 06 | 10 | 13 | 15 | 03 | 05 | 08 |
| 03 | 02 | 01   | 14 | 07 | 04 | 10 | 08 | 13 | 15 | 12 | 09 | 00 | 03 | 05 | 06 | 11 |

# Permutación P



La permutación es la siguiente: 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

# DES



# Ejemplo DES

## Ejemplo

Sea  $m = 0123456789ABCDEF$  y  $k = 133457799BBCDFF1$  ambos en base hexadecimal,  $k$  incluye los bits de paridad

Primero creamos las 16 subllaves:

$k = 00010011\ 00110100\ 01010111\ 01111001\ 10011011\ 10111100\ 11011111$   
 $11110001$

Computamos  $k' = \text{PC-1}(k)$

$k = 1111000\ 0110011\ 0010101\ 0101111\ 0101010\ 1011001\ 1001111\ 0001111$

Ahora partimos  $k$  en dos mitades  $C_0$  y  $D_0$

$C_0 = 1111000\ 0110011\ 0010101\ 0101111$   $D_0 = 0101010\ 1011001\ 1001111\ 0001111$

# Ejemplo DES

## Ejemplo

Calculamos  $C_i = LS_i(C_{i-1}), D_i = LS_i(D_{i-1})$  para  $i = 1, \dots, 16$

$$C_1 = 1110000110011001010101011111, D_1 = 1010101011001100111100011110$$

$$C_2 = 1100001100110010101010111111, D_2 = 0101010110011001111000111101$$

$$C_3 = 0000110011001010101011111111, D_3 = 0101011001100111100011110101$$

$$C_4 = 001100110010101010111111100, D_4 = 0101100110011110001111010101$$

$$C_5 = 1100110010101010111111110000, D_5 = 0110011001111000111101010101$$

$$C_6 = 0011001010101011111111000011, D_6 = 1001100111100011110101010101$$

$$C_7 = 1100101010101111111100001100, D_7 = 0110011110001111010101010110$$

$$C_8 = 0010101010111111110000110011, D_8 = 1001111000111101010101011001$$

$$C_9 = 01010101011111111100001100110, D_9 = 0011110001111010101010110011$$

$$C_{10} = 01010101111111110000110011001, D_{10} = 1111000111101010101011001100$$

$$C_{11} = 0101011111111000011001100101, D_{11} = 1100011110101010101100110011$$

$$C_{12} = 01011111111100001100110010101, D_{12} = 0001111010101010110011001111$$

$$C_{13} = 01111111110000110011001010101, D_{13} = 0111101010101011001100111100$$

$$C_{14} = 1111111000011001100101010101, D_{14} = 1110101010101100110011110001$$

$$C_{15} = 1111100001100110010101010111, D_{15} = 101010101100110011110001111$$

$$C_{16} = 1111000011001100101010101111, D_{16} = 0101010101100110011110001111$$

# Ejemplo DES

## Ejemplo

Calculamos  $k_i = \text{PC-2}(C_i D_i)$  para  $i = 1, \dots, 16$

$k_1 = 0001101100000010111011111111000111000001110010$   
 $k_2 = 01110011010111011011001110110111100100111100101$   
 $k_3 = 0101010111111001000101001000010110011110011001$   
 $k_4 = 0111001010101110101101101110011010100011101$   
 $k_5 = 011111001110110000000111111010110101001110101000$   
 $k_6 = 011000111010010100111110010100000111101100101111$   
 $k_7 = 11101100100001001011011111101100001100010111100$   
 $k_8 = 11110111100010100011101011000001001110111111011$   
 $k_9 = 111000001101101111101011111011011110011110000001$   
 $k_{10} = 101100011111001101000111101110100100011001001111$   
 $k_{11} = 00100001010111111010011110111101101001110000110$   
 $k_{12} = 011101010111000111110101100101000110011111101001$   
 $k_{13} = 100101111100010111010001111110101011101001000001$   
 $k_{14} = 01011111010000111011011111100101110011100111010$   
 $k_{15} = 101111111001000110011010011111010011111100001010$   
 $k_{16} = 11001011001111011000101100001110000101111110101$

# Ejemplo DES

## Ejemplo

Comenzamos la codificación del mensaje

$$m = 0000000100100011010001010110011110001001101010111100110111101111$$

Calculamos  $m' = \text{IP}(m)$

$$m' = 1100110000000000110011001111111110000101010101111000010101010$$

Ahora partimos  $m'$  en dos mitades  $L_0$  y  $R_0$

$$L_0 = 110011000000000011001100111111111$$

$$R_0 = 11110000101010101111000010101010$$

Luego hacemos las 16 rondas.

Para  $i = 1, \dots, 16$  calculamos  $L_i = R_{i-1}$ ,  $R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$

# Ejemplo DES

## Ejemplo

Para  $i = 1$  tenemos:

$$L_1 = R_0 = 11110000101010101111000010101010$$

$$R_1 = L_0 \oplus f(R_0, k_1)$$

Para calcular  $f(R_0, k_1)$  debemos calcular  $E(R_0)$

$$E(R_0) = 0111101000010101010101011110100001010101010101$$

Calculamos  $B = E(R_0) \oplus k_1$

$$B = E(R_0) \oplus k_1 = 011000\ 010001\ 011110\ 111010\ 100001\ 100110\ 010100\ 100111$$

Partimos  $B$  en 8 bloques de 6 bits,  $B = B_1 B_2 B_3 B_4 B_5 B_6 B_7 B_8$

Calculamos  $S = S_1(B_1)S_2(B_2)S_3(B_3)S_4(B_4)S_5(B_5)S_6(B_6)S_7(B_7)S_8(B_8)$

$$S = 0010\ 0011\ 0100\ 1010\ 1010\ 1001\ 1011\ 1011$$

# Ejemplo DES

## Ejemplo

Para terminar el calculo de  $f$  calculamos  $P(S)$

$$f(R_0, k_1) = p(S) = 001000110100101010100110111011$$

$$R_1 = L_0 \oplus f(R_0, k_1) = 11101111010010100110010101000100$$

Luego al finalizar la primera ronda tenemos

$$L_1 = 11110000101010101111000010101010$$

$$R_1 = 11101111010010100110010101000100$$

Realizamos este proceso 15 veces más para  $i = 2, \dots, 16$

# Ejemplo DES

## Ejemplo

|   |   |
|---|---|
| $L_2 = 11101111010010100110010101000100$    | $R_2 = 11001100000000010111011100001001$    |
| $L_3 = 11001100000000010111011100001001$    | $R_3 = 1010001001011100000010111110100$     |
| $L_4 = 1010001001011100000010111110100$     | $R_4 = 01110111001000100000000001000101$    |
| $L_5 = 01110111001000100000000001000101$    | $R_5 = 10001010010011111010011000110111$    |
| $L_6 = 10001010010011111010011000110111$    | $R_6 = 11101001011001111100110101101001$    |
| $L_7 = 11101001011001111100110101101001$    | $R_7 = 00000110010010101011101000010000$    |
| $L_8 = 00000110010010101011101000010000$    | $R_8 = 11010101011010010100101110010000$    |
| $L_9 = 11010101011010010100101110010000$    | $R_9 = 00100100011111001100011001111010$    |
| $L_{10} = 00100100011111001100011001111010$ | $R_{10} = 1011011111010101110101110110010$  |
| $L_{11} = 10110111110101011101011110110010$ | $R_{11} = 11000101011110000011110001111000$ |
| $L_{12} = 11000101011110000011110001111000$ | $R_{12} = 01110101101111010001100001011000$ |
| $L_{13} = 01110101101111010001100001011000$ | $R_{13} = 000110001100001100010101011010$   |
| $L_{14} = 00011000110000110001010101011010$ | $R_{14} = 11000010100011001001011000001101$ |
| $L_{15} = 11000010100011001001011000001101$ | $R_{15} = 01000011010000100011001000110100$ |
| $L_{16} = 01000011010000100011001000110100$ | $R_{16} = 00001010010011001101100110010101$ |

# Ejemplo DES

## Ejemplo

Finalmente  $c = P^{-1}(R_{16}L_{16})$

$c = 1000010111101000000100110101010000001111000010101011010000000101$

El cual en hexadecimal es 85E813540F0AB405

Luego  $m = 0123456789ABCDEF$  cifrado usando DES con  $k = 133457799BBCDFF1$  es  $c = 85E813540F0AB405$

# Advanced Encryption Standard (AES)

- El Estándar de Cifrado Avanzado (Advanced Encryption Standard) es un cifrado por bloques inventado por Joan Daemen y Vincent Rijmen en 1997
- AES procesa bloques de 128 bits con una llave que puede ser de 128, 192 o 256 bits.
- El gobierno de Estados Unidos permite el AES-128 para cifrar información sensible y los AES-192 y AES-256 para información ultra secreta

# Advanced Encryption Standard (AES)

- En 1997 el NIST (National Institute Of Standards and Technology) de Estados Unidos lanzó la iniciativa AES y de 15 candidatos considerados el cifrado *Rijndael* fue seleccionado como el AES
- En 1999, el cifrado Rijndael era uno de los 5 potenciales reemplazos del DES. los otros cuatro eran:
  - *MARS* de IBM
  - *RC6* de RSA Security
  - *Serpent* de Anderson, Biham y Knudsen
  - *Twofish* de un equipo liderado por Bruce Schneier
- Rijndael fue seleccionado en 2001 despues de un extenso proceso de pruebas abierto al público

## Nota

El nombre del cifrado Rijndael viene de la composición de los apellidos de los autores (rij y dae)

## Parámetros del AES

## Definición (Palabra)

En el AES una *palabra* corresponde a una cadena de 32 bits

Se manejan los siguientes parámetros para el AES en diferentes longitudes de llaves:

| Variante | Tamaño Bloque | Tamaño Llave | # Rondas ( $N_r$ ) |
|----------|---------------|--------------|--------------------|
| AES-128  | 4 palabras    | 4 palabras   | 10 rondas          |
| AES-196  | 4 palabras    | 6 palabras   | 12 rondas          |
| AES-256  | 4 palabras    | 8 palabras   | 14 rondas          |

## Nota

## Vamos a estudiar el AES-128

# Estados

## Definición (Estado)

Un *estado* en el AES es un arreglo de 4 palabras, cada palabra la representamos como una columna con 4 bytes

## Ejemplo

Consideremos el mensaje: "AES es muy facil" y la llave  $k = 2B7E151628AED2A6ABF7158809CF4F3C$

message= 41455320 6573206d 75792066 6163696c

key= 2b7e1516 28aed2a6 abf71588 09cf4f3c

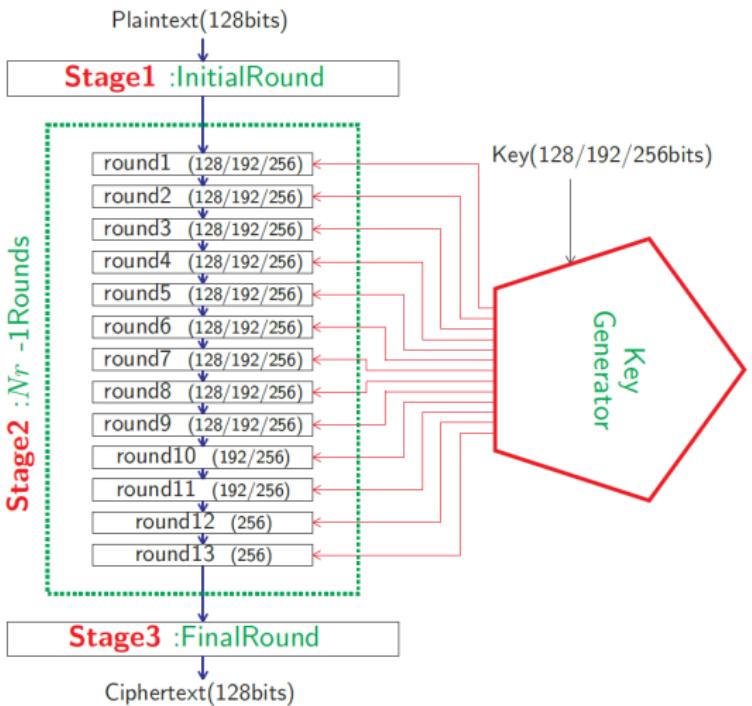
| state |
|-------|
| 41    |
| 45    |
| 53    |
| 20    |
| 6d    |
| 75    |
| 79    |
| 20    |
| 66    |
| 61    |
| 63    |
| 69    |
| 6c    |

key  
2b 28 ab 09  
7e ae f7 cf  
15 d2 15 4f  
16 a6 88 3c

# Pasos del Algoritmo de cifrado AES

El algoritmo tiene 3 etapas:

- ① Transformación ARK inicial
  - ②  $N_r - 1$  rondas con transformaciones  $SB$ ,  $SR$ ,  $MC$  y  $ARK$  en ese orden
  - ③ Ronda final con transformaciones  $SB$ ,  $SR$  y  $ARK$  en ese orden



# Pasos del Algoritmo de descifrado AES

El algoritmo de descifrado tiene 3 etapas:

- ① Ronda inicial con transformaciones  $ARK$ ,  $SB^{-1}$  y  $SR^{-1}$  en ese orden
- ②  $N_r - 1$  rondas con transformaciones  $ARK$ ,  $MC^{-1}$ ,  $SB^{-1}$ ,  $SR^{-1}$  en ese orden
- ③ Transformación final  $ARK$

## Nota

A diferencia del DES en el AES el algoritmo y la implementación del descifrado varía al del cifrado

# Generación de llaves

En el AES debemos crear  $N_r$  subllaves (10 para AES-128) de la siguiente manera:

- ① Almacenamos la llave en una matriz  $W$  de tamaño  $4 \times 4$ ,  
 $W = [W_0, W_1, W_2, W_3]$  donde  $W_i$  es la  $i$ -ésima palabra de la llave para  $i = 0, 1, 2, 3$
- ② Expandemos la matriz agregando 40 columnas adicionales  $W_i$  para  $i = 4, \dots, 43$  de manera recursiva:

$$W_i = \begin{cases} W_{i-4} \oplus T_{\frac{i}{4}}(W_{i-1}) & \text{si } i \equiv 0 \pmod{4} \\ W_{i-4} \oplus W_{i-1} & \text{en otro caso} \end{cases}$$

donde  $T_j$  es una transformación para la ronda  $j$  (En la ronda  $j$  se transforma la columna  $4j$ )

- ③ La subllave de la ronda  $i$  corresponde a  
 $W_{4i}, W_{4i+1}, W_{4i+2}, W_{4i+3}$

## Transformación T

Sea  $X$  una palabra,  $T_i(X)$  es la siguiente transformación:

- ① Sean  $X_0, X_1, X_2, X_3$  los bytes de  $X$ , corremos los elementos de manera cíclica para obtener  $X_1, X_2, X_3, X_0$
- ② Reemplazamos cada uno de estos bytes con la transformación  $SB$  obteniendo  $Y_1, Y_2, Y_3, Y_0$  donde  $Y_j = SB(X_j)$  para  $j = 0, 1, 2, 3$
- ③ Finalmente computamos la constante de la ronda  $r_i = 00000010^{i-1} \in GF(2^8)$
- ④  $T_i(x) = (Y_1 \oplus r_i, Y_2, Y_3, Y_0)$

### Nota

$GF(2^8)$  es el campo finito de Galois de tamaño  $2^8$  (256)

# Transformación T

Sea  $X$  una palabra,  $T_i(X)$  es la siguiente transformación:

- ① Sean  $X_0, X_1, X_2, X_3$  los bytes de  $X$ , corremos los elementos de manera cíclica para obtener  $X_1, X_2, X_3, X_0$
- ② Reemplazamos cada uno de estos bytes con la transformación  $SB$  obteniendo  $Y_1, Y_2, Y_3, Y_0$  donde  $Y_j = SB(X_j)$  para  $j = 0, 1, 2, 3$
- ③ Finalmente computamos la constante de la ronda  $r_i = 00000010^{i-1} \in GF(2^8)$
- ④  $T_i(x) = (Y_1 \oplus r_i, Y_2, Y_3, Y_0)$

## Nota

$GF(2^8)$  es el campo finito de Galois de tamaño  $2^8$  (256)

## Ejercicio

¿Cuál es el valor de  $r_{10}$ ?

## Transformación SubBytes (SB)

- La transformación SB corresponde a una S-Box de bytes a bytes
  - Es una transformación biyectiva
  - Esto es isomorfo a una permutación de los elementos de  $GF(2^8)$

## Definición (Transformación SB)

Sea  $x \in GF(2^8)$ ,  $SB(x) = AF(INV(x))$ , donde  $INV(0) = 0$  e  $INV(x)$  es el inverso multiplicativo de  $x$  para  $x \neq 0$ .  
 $AF(y)$  es una transformación afín de  $y$  sobre  $GF(2)$

## Nota

La idea con esta transformación es tener alta confusión debido a la no-linealidad de las operaciones

# Transformación SubBytes (SB)

- Para calcular SB podemos revisar la siguiente tabla, donde las filas corresponden a la porción de 4 bits mas significativas del byte y las columnas a la porción de 4 bits menos significativa

|   | 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 |

# Ejemplo SB

## Ejemplo

|   | 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 | c6 | b3 | 29 | e3 | 2f | 84 |
| 5 | 53 | d1 | 00 | ed | 20 | fc | b1 | 5b | 6a | cb | b4 | 39 | 4a | 4c | 58 | cf |
| 6 | 40 | c1 | a0 | fb | 40 | 4d | 00 | 05 | 10 | 14 | 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 | 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 |

6a 4dde68  
3bdd8eac  
46f23526  
36abee50

02 e31d45  
e2c11991  
5a8996f7  
051f2853

# Ejemplo generador de llaves

## Ejemplo

Calcular las subllaves para  $k = 2b\ 7e\ 15\ 16\ 28\ ae\ d2\ a6\ ab\ f7\ 15\ 88\ 09\ cf\ 4f\ 3c$

| $i$ | $W_{i-1}$ | RotWord() | SB()     | $r_i/4$  | $\textcircled{1} \oplus \textcircled{2}$ | $W_{i-4}$ | $W_i$     |
|-----|-----------|-----------|----------|----------|--|-----------|-----------|
| 0   |           |           |          |          |  |           | 2b7e1516  |
| 1   |           |           |          |          |  |           | 28aed2a6  |
| 2   |           |           |          |          |  |           | abf71588  |
| 3   |           |           |          |          |  |           | 09cf4f3c  |
| 4   | 09cf4f3c  | cf4f3c09  | 8a84eb01 | 01000000 | 8b84eb01                                 | 2b7e1516  | a0fafef17 |
| 5   | a0fafef17 |           |          |          |  | 28aed2a6  | 88542cb1  |
| 6   | 88542cb1  |           |          |          |  | abf71588  | 23a33939  |
| 7   | 23a33939  |           |          |          |  | 09cf4f3c  | 2a6c7605  |
| 8   | 2a6c7605  | 6c76052a  | 50386be5 | 02000000 | 52386be5                                 | a0fafef17 | f2c295f2  |
| 9   | f2c295f2  |           |          |          |  | 88542cb1  | 7a96b943  |
| 10  | 7a96b943  |           |          |          |  | 23a33939  | 5935807a  |
| 11  | 5935807a  |           |          |          |  | 2a6c7605  | 7359f67f  |
| 12  | 7359f67f  | 59f67f73  | cb42d28f | 04000000 | cf42d28f                                 | f2c295f2  | 3d80477d  |
| 13  | 3d80477d  |           |          |          |  | 7a96b943  | 4716fe3e  |
| 14  | 4716fe3e  |           |          |          |  | 5935807a  | 1e237e44  |
| 15  | 1e237e44  |           |          |          |  | 7359f67f  | 6d7a883b  |

key  
2b 28 ab 09  
7e ae f7 cf  
15 d2 15 4f  
16 a6 88 3c

roundkey1  
a0 88 23 2a  
fa 54 a3 6c  
fe 2c 39 76  
17 b1 39 05

roundkey2  
f2 7a 59 73  
c2 96 35 59  
95 b9 80 f6  
f2 43 7a 7f

roundkey3  
3d 47 1e 6d  
80 16 23 7a  
47 fe 7e 88  
7d 3e 44 3b

# Ejemplo generador de llaves

## Ejemplo

| $i$ | $W_{i-1}$ | RotWord() | SB()     | $r_i/4$  | $\textcircled{1} \oplus \textcircled{2}$ | $W_{i-4}$                                    | $W_i$  |
|-----|-----------|-----------|----------|----------|--|--|--|
| 16  | 6d7a883b  | 7a883b6d  | dac4e23c | 08000000 | d2c4e23c                                 | 3d80477d<br>4716fe3e<br>1e237e44<br>6d7a883b | ef44a541<br>a8525b7f<br>b671253b<br>db0bad00 |
| 17  | ef44a541  |           |          |          |  |  |  |
| 18  | a8525b7f  |           |          |          |  |  |  |
| 19  | b671253b  |           |          |          |  |  |  |
| 20  | db0bad00  | 0bad00db  | 2b9563b9 | 10000000 | 3b9563b9                                 | ef44a541<br>a8525b7f<br>b671253b<br>db0bad00 | d4d1c6f8<br>7c839d87<br>caf2b8bc<br>11f915bc |
| 21  | d4d1c6f8  |           |          |          |  |  |  |
| 22  | 7c839d87  |           |          |          |  |  |  |
| 23  | caf2b8bc  |           |          |          |  |  |  |
| 24  | 11f915bc  | f915bc11  | 99596582 | 20000000 | b9596582                                 | d4d1c6f8<br>7c839d87<br>caf2b8bc<br>11f915bc | 6d88a37a<br>110b3efd<br>dbf98641<br>ca0093fd |
| 25  | 6d88a37a  |           |          |          |  |  |  |
| 26  | 110b3efd  |           |          |          |  |  |  |
| 27  | dbf98641  |           |          |          |  |  |  |
| 28  | ca0093fd  | 0093fdca  | 63dc5474 | 40000000 | 23dc5474                                 | 6d88a37a<br>110b3efd<br>dbf98641<br>ca0093fd | 4e54f70e<br>5f5fc9f3<br>84a64fb2<br>4ea6dc4f |
| 29  | 4e54f70e  |           |          |          |  |  |  |
| 30  | 5f5fc9f3  |           |          |          |  |  |  |
| 31  | 84a64fb2  |           |          |          |  |  |  |

roundkey4

ef a8 b6 db  
44 52 71 0b  
a5 5b 25 ad  
41 7f 3b 00

roundkey5

d4 7c ca 11  
d1 83 f2 f9  
c6 9d b8 15  
f8 87 bc bc

roundkey6

6d 11 db ca  
88 0b f9 00  
a3 3e 86 93  
7a fd 41 fd

roundkey7

4e 5f 84 4e  
54 5f a6 a6  
f7 c9 4f dc  
0e f3 b2 4f

# Ejemplo generador de llaves

## Ejemplo

| <i>i</i> | $W_{i-1}$ | RotWord() | SB()     | $r_{i/4}$ | $① + ②$  | $W_{i-4}$                                    | $③ \oplus ④$                                 |
|----------|-----------|-----------|----------|-----------|----------|--|--|
| 32       | 4ea6dc4f  | a6dc4f4e  | 2486842f | 80000000  | a486842f | 4e54f70e<br>5f5fc9f3<br>84a64fb2<br>4ea6dc4f | ead27321<br>b58dbad2<br>312bf560<br>7f8d292f |
| 33       | ead27321  |           |          |           |          |  |  |
| 34       | b58dbad2  |           |          |           |          |  |  |
| 35       | 312bf560  |           |          |           |          |  |  |
| 36       | 7f8d292f  | 8d292f7f  | 5da515d2 | 1B000000  | 46a515d2 | ead27321<br>b58dbad2<br>312bf560<br>7f8d292f | ac7766f3<br>19fadcc1<br>28d12941<br>575c006e |
| 37       | ac7766f3  |           |          |           |          |  |  |
| 38       | 19fadcc1  |           |          |           |          |  |  |
| 39       | 28d12941  |           |          |           |          |  |  |
| 40       | 575c006e  | 5c006e57  | 4a639f5b | 36000000  | 7c639f5b | ac7766f3<br>19fadcc1<br>28d12941<br>575c006e | d014f9a8<br>c9ee2589<br>e13f0cc8<br>b6630ca6 |
| 41       | d014f9a8  |           |          |           |          |  |  |
| 42       | c9ee2589  |           |          |           |          |  |  |
| 43       | e13f0cc8  |           |          |           |          |  |  |

roundkey8  
 ea b5 31 7f  
 d2 8d 2b 8d  
 73 ba f5 29  
 21 d2 60 2f

roundkey9  
 ac 19 28 57  
 77 fa d1 5c  
 66 dc 29 00  
 f3 21 41 6e

roundkey10  
 d0 c9 e1 b6  
 14 ee 3f 63  
 f9 25 0c 0c  
 a8 89 c8 a6

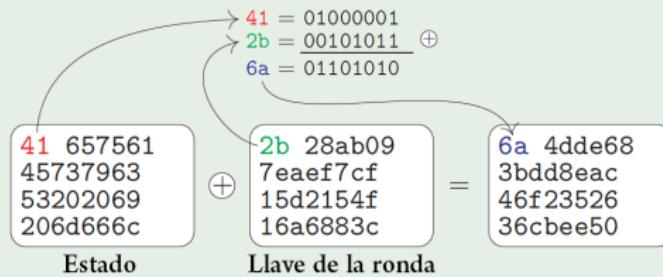
|   |  |  |  |  |  |
|---|--|--|--|--|--|
| key<br>2b 28 ab 09<br>7e ae f7 cf<br>15 d2 15 4f<br>16 a6 88 3c | a0 88 23 2a<br>fa 54 a3 6c<br>fe 2c 39 76<br>17 b1 39 05 | f2 7a 59 73<br>c2 96 35 59<br>95 b9 80 f6<br>f2 43 7a 7f | 3d 47 1e 6d<br>80 16 23 7a<br>47 fe 7e 88<br>7d 3e 44 3b | ef a8 b6 db<br>44 52 71 0b<br>a5 5b 25 ad<br>41 7f 3b 00 | d4 7c ca 11<br>d1 83 f2 f9<br>c6 9d b8 15<br>f8 87 bc bc |
|   | 6d 11 db ca<br>88 0b f9 00<br>a3 3e 86 93<br>7a fd 41 fd | 4e 5f 84 4e<br>54 5f a6 a6<br>f7 c9 4f dc<br>0e f3 b2 4f | ea b5 31 7f<br>d2 8d 2b 8d<br>73 ba f5 29<br>21 d2 60 2f | ac 19 28 57<br>77 fa d1 5c<br>66 dc 29 00<br>f3 21 41 6e | d0 c9 e1 b6<br>14 ee 3f 63<br>f9 25 0c 0c<br>a8 89 c8 a6 |



# Transformación AddRoundKey (ARK)

- Consiste en un simple XOR entre la llave de la ronda correspondiente, en la transformación ARK inicial utilizamos la llave original

## Ejemplo



## Nota

La idea es hacer al algoritmo altamente dependiente de la llave. Este proceso de hacer XOR con la llave se le llama *blanqueo* (*whitehing*)



# Transformación ShiftRow (SR)

Las 4 filas del estado se corren ciclicamente a la izquierda de la siguiente manera:

- ① Fila 0 no se corre
- ② Fila 1 se corre 1 posición
- ③ Fila 2 se corre 2 posiciones
- ④ Fila 3 se corre 3 posiciones

## Ejemplo



## Nota

La idea es hacer aumentar la difusión a través de una operación lineal

# Transformación MixColumns (MC)

- La transformación MC corresponde a una multiplicación de matrices en  $GF(2^8)$

$$\bullet \text{MC}(X) = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \cdot X$$

## Ejemplo

|    |    |    |    |
|----|----|----|----|
| 02 | 03 | 01 | 01 |
| 01 | 02 | 03 | 01 |
| 01 | 01 | 02 | 03 |
| 03 | 01 | 01 | 02 |

 $\bullet$ 

|    |    |    |    |
|----|----|----|----|
| 02 | e3 | 1d | 45 |
| c1 | 19 | 91 | e2 |
| 96 | f7 | 5a | 89 |
| 53 | 05 | 1f | 28 |

 $=$ 

|    |    |    |    |
|----|----|----|----|
| 99 | 04 | d7 | 16 |
| 69 | d6 | d5 | 32 |
| 01 | 00 | 19 | d6 |
| f7 | da | d2 | f4 |

# Multiplicación en $GF(2^8)$

La multiplicación en  $GF(2^8)$  se puede implementar utilizando las tablas E (exponencial) y L (logarítmica)

- ① Queremos calcular  $x * y$ ,  $x, y \in GF(2^8)$
- ②  $x * y = 3^{\log_3(x) + \log_3(y)} = E(L(x) + L(y))$
- ③ En caso que  $L(x) + L(y)$  sea mayor a 255 tomamos módulo 255

## Nota

Mas adelante veremos el funcionamiento de las operaciones en campos finitos

# Tabla L

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

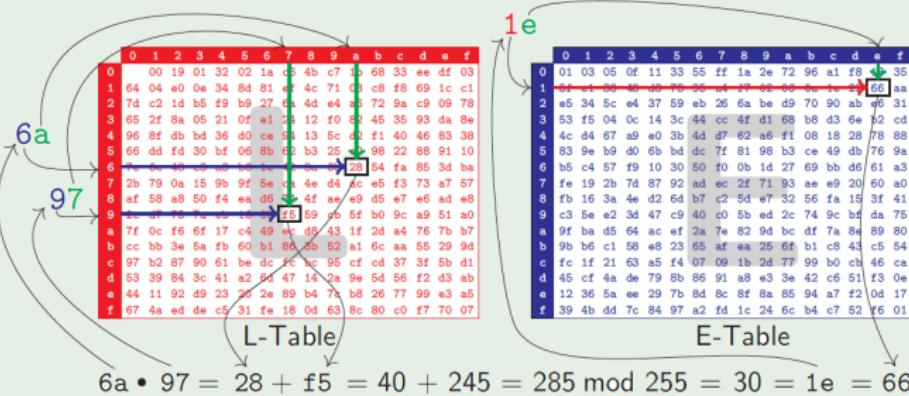
## Tabla E

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

# Ejemplo multiplicación en $GF(2^8)$

Para buscar en las tablas E y L los 4 bits más significativos corresponden a la fila y los 4 bits menos significativos a la columna

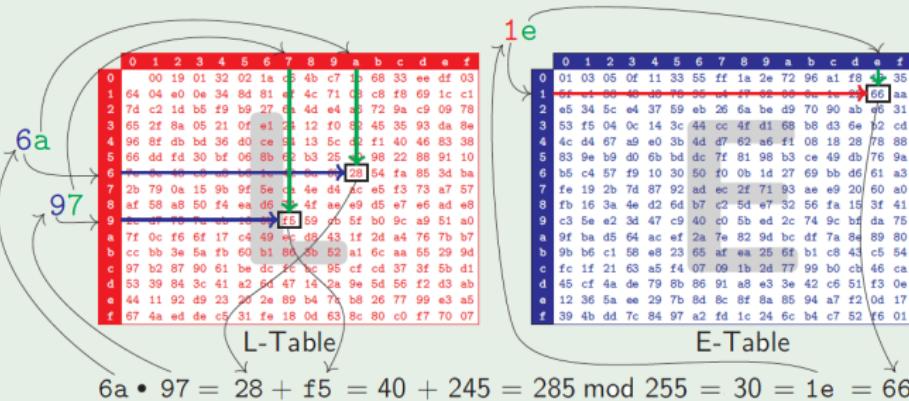
## Ejemplo



# Ejemplo multiplicación en $GF(2^8)$

Para buscar en las tablas E y L los 4 bits más significativos corresponden a la fila y los 4 bits menos significativos a la columna

## Ejemplo



## Ejercicio

Calcular los valores  $r_1, r_2, r_3, r_4, r_5, r_6, r_7, r_8, r_9, r_{10}$

# Transformaciones Inversas ( $SB^{-1}$ , $SR^{-1}$ , $MC^{-1}$ )

- Para el descifrado se necesitan las transformaciones inversas a las vistas
- $SB^{-1}(x) = \text{INV}(\text{AF}^{-1}(x))$  donde  $\text{AF}^{-1}$  es la transformación afín inversa a la utilizada en SB
- $SR^{-1}$  se obtiene haciendo los corrimientos a la derecha en lugar de a la izquierda
- $MC^{-1}$  se obtiene multiplicando a la matriz inversa a la utilizada en MC

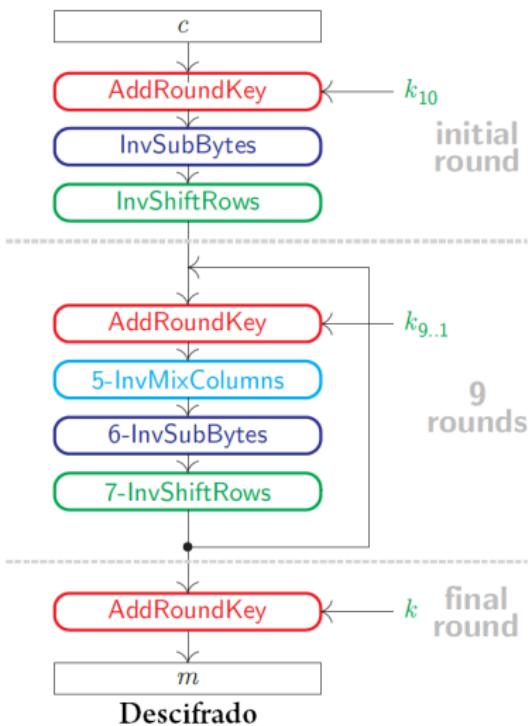
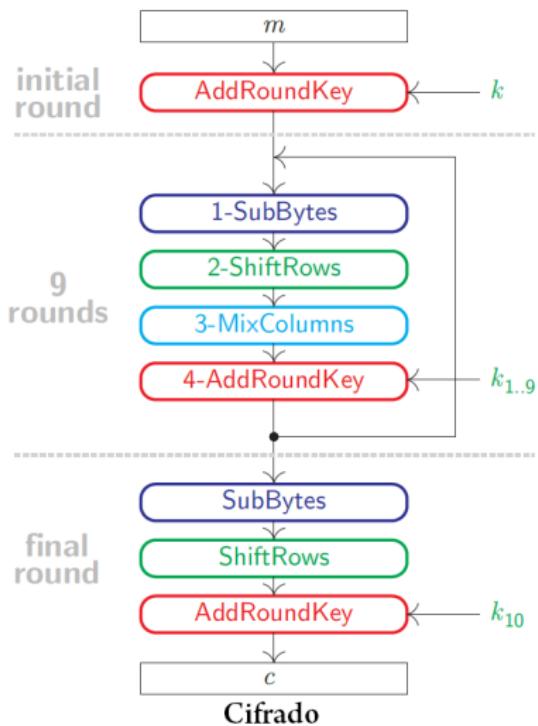
$$MC^{-1}(X) = \begin{pmatrix} 0e & 0b & 0d & 09 \\ 09 & 0e & 0b & 0d \\ 0d & 09 & 0e & 0b \\ 0b & 0d & 09 & 0e \end{pmatrix} \cdot X$$

# Transformación InvSubBytes ( $SB^{-1}$ )

- Para calcular  $SB^{-1}$  podemos revisar la siguiente tabla, donde las filas corresponden a la porción de 4 bits más significativas del byte y las columnas a la porción de 4 bits menos significativa

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

## AES



# Criptoanálisis AES

La dificultad de romper el AES es lo que lo ha hecho un cifrado popular entre muchos sistemas informáticos

## Nota

Actualmente el criptoanálisis sobre AES ha logrado reducir el espacio de búsqueda en un factor de casi 4, es decir, en el AES-128 esto es a posibles  $2^{126,1}$  llaves, con la computación actual esto es inviable de romper

# Ejemplo AES

## Ejemplo

Cifrar  $m = 41\ 45\ 53\ 20\ 65\ 73\ 20\ 6d\ 75\ 79\ 20\ 66\ 61\ 63\ 69\ 6c$  usando  $k = 2b\ 7e\ 15\ 16\ 28\ ae\ d2\ a6\ ab\ f7\ 15\ 88\ 09\ cf\ 4f\ 3c$ , donde  $m$  y  $k$  están en hexadecimal

Primero creamos las 10 subllaves

| key         |
|-------------|
| 2b 28 ab 09 |
| 7e ae f7 cf |
| 15 d2 15 4f |
| 16 a6 88 3c |

| subkey1     |
|-------------|
| a0 88 23 2a |
| fa 54 a3 6c |
| fe 2c 39 76 |
| 17 b1 39 05 |

| subkey2     |
|-------------|
| f2 7a 59 73 |
| c2 96 35 59 |
| 95 b9 80 f6 |
| f2 43 7a 7f |

| subkey3     |
|-------------|
| 3d 47 1e 6d |
| 80 16 23 7a |
| 47 fe 7e 88 |
| 7d 3e 44 3b |

| subkey4     |
|-------------|
| ef a8 b6 db |
| 44 52 71 0b |
| a5 5b 25 ad |
| 41 7f 3b 00 |

| subkey5     |
|-------------|
| d4 7c ca 11 |
| d1 83 f2 f9 |
| c6 9d b8 15 |
| f8 87 bc bc |

| subkey6     |
|-------------|
| 6d 11 db ca |
| 88 0b f9 00 |
| a3 3e 86 93 |
| 7a fd 41 fd |

| subkey7     |
|-------------|
| 4e 5f 84 4e |
| 54 5f a6 a6 |
| f7 c9 4f dc |
| 0e f3 b2 4f |

| subkey8     |
|-------------|
| ea b5 31 7f |
| d2 8d 2b 8d |
| 73 ba f5 29 |
| 21 d2 60 2f |

| subkey9     |
|-------------|
| ac 19 28 57 |
| 77 fa d1 5c |
| 66 dc 29 00 |
| f3 21 41 6e |

| subkey10    |
|-------------|
| d0 c9 e1 b6 |
| 14 ee 3f 63 |
| f9 25 0c 0c |
| a8 89 c8 a6 |

# Ejemplo AES

## Ejemplo

Despues comenzamos con el cifrado del mensaje

| round | ARK(④, ⑤)  | SB(①)  | SR(②)  | MC(③)  | roundkey   |
|-------|--|--|--|--|--|
| input | 41 65 75 61<br>45 73 79 63<br>53 20 20 69<br>20 6d 66 6c |  |  |  | 2b 28 ab 09<br>7e ae f7 cf<br>15 d2 15 4f<br>16 a6 88 3c |
| 1     | 6a 4d de 68<br>3b dd 8e ac<br>46 f2 35 26<br>36 cb ee 50 | 02 e3 1d 45<br>e2 c1 19 91<br>5a 89 96 f7<br>05 1f 28 53 | 02 e3 1d 45<br>c1 19 91 e2<br>96 f7 5a 89<br>53 05 1f 28 | 99 04 d7 16<br>69 d6 d5 32<br>01 00 19 d6<br>f7 da d2 f4 | a0 88 23 2a<br>fa 54 a3 6c<br>fe 2c 39 76<br>17 b1 39 05 |
| 2     | 39 8c f4 3c<br>93 82 76 5e<br>ff 2c 20 a0<br>e0 6b eb f1 | 12 64 bf eb<br>dc 13 38 58<br>16 71 b7 e0<br>e1 7f e9 a1 | 12 64 bf eb<br>13 38 58 dc<br>b7 e0 16 71<br>a1 e1 7f e9 | 07 81 e4 2a<br>57 ce 4a 32<br>8c bf 4a f5<br>cb ad 6a 42 | f2 7a 59 73<br>c2 96 35 59<br>95 b9 80 f6<br>f2 43 7a 7f |
| 3     | f5 fb bd 59<br>95 58 7f 6b<br>19 06 ca 03<br>39 ee 10 3d | e6 0f 7a cb<br>2a 6a d2 7f<br>d4 6f 74 7b<br>12 28 ca 27 | e6 0f 7a cb<br>6a d2 7f 2a<br>74 7b d4 6f<br>27 12 28 ca | 3a 1a 89 56<br>89 2f cb e4<br>0d 1d ce 7a<br>61 9c 75 8c | 3d 47 1e 6d<br>80 16 23 7a<br>47 fe 7e 88<br>7d 3e 44 3b |

# Ejemplo AES

## Ejemplo

| round | ARK(④, ⑤)  | SB(①)  | SR(②)  | MC(③)  | roundkey   |
|-------|--|--|--|--|--|
| 4     | 07 5d 97 3b<br>09 39 e8 9e<br>4a e3 b0 f2<br>1c a2 31 b7 | c5 4c 88 e2<br>01 12 9b 0b<br>d6 11 e7 89<br>9c 3a c7 a9 | c5 4c 88 e2<br>12 9b 0b 01<br>e7 89 d6 11<br>a9 9c 3a c7 | e9 3b fa 0a<br>7a 7d c5 14<br>e2 61 7a 93<br>e8 e5 2a b8 | ef a8 b6 db<br>44 52 71 0b<br>a5 5b 25 ad<br>41 7f 3b 00 |
| 5     | 06 93 4c d1<br>3e 2f b4 1f<br>47 3a 5f 3e<br>a9 9a 11 b8 | 6f dc 29 3e<br>b2 15 8d c0<br>a0 80 cf b2<br>d3 b8 82 6c | 6f dc 29 3e<br>15 8d c0 b2<br>cf b2 a0 80<br>6c d3 b8 82 | 42 4e 11 b3<br>63 c3 f1 58<br>4b 40 61 0a<br>b3 fd 70 6f | d4 7c ca 11<br>d1 83 f2 f9<br>c6 9d b8 15<br>f8 87 bc bc |
| 6     | 96 32 db a2<br>b2 40 03 a1<br>8d dd d9 1f<br>4b 7a cc d3 | 90 23 b9 3a<br>37 09 7b 32<br>5d c1 35 c0<br>b3 da 4b 66 | 90 23 b9 3a<br>09 7b 32 37<br>35 c0 5d c1<br>66 b3 da 4b | 73 b8 b8 a7<br>bb 3d e0 47<br>59 0d 44 49<br>5b a3 10 2e | 6d 11 db ca<br>88 0b f9 00<br>a3 3e 86 93<br>7a fd 41 fd |
| 7     | 1e a9 63 6d<br>33 36 19 47<br>fa 33 c2 da<br>21 5e 51 d3 | 72 d3 fb 3c<br>c3 05 d4 a0<br>2d c3 25 57<br>fd 58 d1 66 | 72 d3 fb 3c<br>05 d4 a0 c3<br>25 57 2d c3<br>66 fd 58 d1 | a8 70 63 34<br>71 64 8f 2e<br>97 b5 e9 0a<br>7a 0c 2b fd | 4e 5f 84 4e<br>54 5f a6 a6<br>f7 c9 4f dc<br>0e f3 b2 4f |

# Ejemplo AES

## Ejemplo

| round  | ARK(④, ⑤)  | SB(①)  | SR(②)  | MC(③)  | roundkey   |
|--------|--|--|--|--|--|
| 8      | e6 2f e7 7a<br>25 3b 29 88<br>60 7c a6 d6<br>74 ff 99 b2 | 8e 15 94 da<br>3f e2 a5 c4<br>d0 10 24 f6<br>92 16 ee 37 | 8e 15 94 da<br>e2 a5 c4 3f<br>24 f6 d0 10<br>37 92 16 ee | 29 ba a2 10<br>0a d7 7a 7a<br>7d ea d1 ec<br>21 53 9f 9d | ea b5 31 7f<br>d2 8d 2b 8d<br>73 ba f5 29<br>21 d2 60 2f |
| 9      | c3 0f 93 6f<br>d8 5a 51 f7<br>0e 50 24 c5<br>00 81 ff b2 | 2e 76 dc a8<br>61 be d1 68<br>ab 53 36 a6<br>63 0c 16 37 | 2e 76 dc a8<br>be d1 68 61<br>36 a6 ab 53<br>37 63 0c 16 | 84 41 bc ad<br>24 5d e6 89<br>a5 55 ed 55<br>94 2b a4 fd | ac 19 28 57<br>77 fa d1 5c<br>66 dc 29 00<br>f3 21 41 6e |
| 10     | 28 58 94 fa<br>53 a7 37 d5<br>c3 89 c4 55<br>67 0a e5 93 | 34 6a 22 2d<br>ed 5c 9a 03<br>2e a7 1c fc<br>85 67 d9 dc | 34 6a 22 2d<br>5c 9a 03 ed<br>1c fc 2e a7<br>dc 85 67 d9 |  | d0 c9 e1 b6<br>14 ee 3f 63<br>f9 25 0c 0c<br>a8 89 c8 a6 |
| output | e4 a3 c3 9b<br>48 74 3c 8e<br>e5 d9 22 ab<br>74 0c af 7f |  |  |  |  |

El texto cifrado es  $c = e4\ 48\ e5\ 74\ a3\ 74\ d9\ 0c\ c3\ 3c\ 22\ af\ 9b\ 8e\ ab\ 7f$