PROYECTO INVESTIGACION
ÁLGEBRA ABSTRACTA

Eliazar Kenyi Arpasi Llanos
Miguel Motta Vilca
Alan Javier Monroy Bernedo

2020

“Los alumnos declaran haber realizado el presente trabajo de acuerdo a las normas de la Universidad Católica San Pablo”

FIRMA

Miguel Alberto Motta Vilca , Alan Javier Monroy Bernedo , Eliazar Kenyi Arpasi Llanos

Índice

1. César

Llamado también cifrado por desplazamiento, es uno de los métodos criptograficos más antiguos y conocidos, así como un ejemplo perfecto de un cifrado monoalfabético. Consiste en el desplazamiento de los caracteres del mensaje dentro del alfabeto utilizado.

1.1. Historia

El cifrado le debe su nombre al emperador romano Julio César, quien lo usó con el objetivo de proteger los mensajes que intercambiaba con sus generales. Originalmente se desplazaban 3 caracteres a la derecha(Figura 1) aunque la implementación de hoy en día es más flexible en este aspecto, como ya se verá en el siguiente apartado.

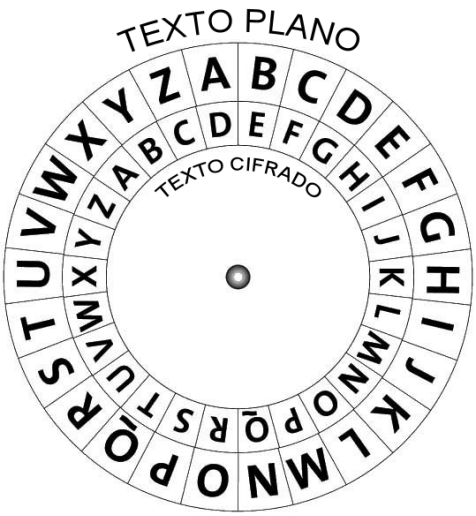


Figura 1: Cifrado César original con un desplazamiento de 3

Es necesario observar que, si bien este el primer cifrado por sustitución del que se tiene registros oficiales, provenientes de Suetonio [1], se conocen otros cifrados del mismo tipo que le preceden por siglos.

En aquel entonces, el cifrado era bastante efectivo debido a que las tropas enemigas del Cesar, no sabían leer en su mayoria, por lo que un criptoanalisis de su parte es bastante improbable.

1.2. Funcionamiento

El cifrado actualmente consiste en el desplazamiento de un determinado numero llamado clave de los caracteres en el mensaje a lo largo de un abecedario. Para el descifrado se realiza el desplazamiento en el sentido opuesto.

Cifrado

Para el cifrado de Cesar se puede usar aritmética modular [2], utilizando la posicion de cada letra en su alfabeto por medio de la siguiente función :

$$f(x) = (x + n) \mod N$$

Donde :

x = posición de la letra
n = número de posiciones a desplazar
N = tamaño del alfabeto

La cual se aplica a cada caracter en el mensaje a cifrar.

Descifrado

Tomando en cuenta el numero de posiciones ya desplazadas en los caracteres, se obtiene:

$$f(x) = (x - n) \mod N$$

Donde :

x = posición de la letra
n = número de posiciones a desplazar
N = tamaño del alfabeto

1.3. Criptoanálisis

El metodo dejó de ser efectivo hace miles de años, en parte por la difusión del mismo, que hoy en día es de los más enseñados en la introducción a la criptografía. Es por esto que no debe ser utilizado para cifrar un mensaje si se espera la mínima confidencialidad del mismo.

Este puede ser roto manualmente desplzando uno a uno los caracteres hasta que el mensaje cobre sentido, lo que tomaría en el peor de los casos un numero de intentos similar al número de caracteres con los que cuenta el alfabeto que se está utilizando.

Un método más eficaz en este caso, seria utilizar la frecuencia de las letras o palabras más utlizadas en el idioma de las partes para compararlo con las más utilizadas en el texto cifrado, una vez hecho esto. Sería cuestion de contar el número de desplazamientos y restarle este mismo número a todo el texto.

2. Hill

2.1. Historia

Lester S. Hill nació en el año 1891 y falleció en 1961, recibió una licenciatura de Columbia College (1911) y un doctorado de la Universidad de Yale (1926). También enseñó en la Universidad de Montana, la Universidad de Princeton, la Universidad de Maine, la Universidad de Yale y el Hunter College.

Una de sus contribuciones más notables estaba el cifrado Hill que lo desarrolló en el año 1929 que consiste en una sustitución poligrámica mediante la multiplicación de matrices ,uno de sus beneficios fue espacios de clave potencialmente enormes. También desarrolló métodos para detectar errores en números de código telegrafiados y escribió dos libros.

2.2. Funcionamiento

CIFRADO: $Y = K * X \mod N$
DESCIFRADO: $Y = K * X^{-1} \mod N$

Concepto de matriz inversa:

$$k * k^{-1} = k^{-1} * k = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$k^{-1} = \frac{adjK^t}{detk} \mod N$

$K \equiv k^{-1}$

Cifrado

Este consiste en un conjunto de ecuaciones:

$y_1 = kx_1 + kx_2 + kx_3 + kx_4 \mod 26$
$y_2 = kx_1 + kx_2 + kx_3 + kx_4 \mod 26$
$y_3 = kx_1 + kx_2 + kx_3 + kx_4 \mod 26$
$y_4 = kx_1 + kx_2 + kx_3 + kx_4 \mod 26$

x_i letras del texto en claro
y_i resultado de la cifra
k_{ij} (valores numéricos) clave aleatoria

Descifrado

$k^{-1} = \frac{adjK^t}{detk}$ mód N

La matriz K debe cumplir las siguientes condiciones:

$detk \neq 0$
factores det K $\neq$ foctores de N

3. Afin

Conocido también como cifrado de transformación afín o cifrado monoalfabético genérico , es un versión de una sola dimensión del cifrado de Hill.

3.1. Historia

3.2. Funcionamiento

Cifrado

$c_i = (a * m + b)$ mód n

Donde:

c_i : identifica el símbolo i del texto cifrado
a :constante de multiplicación
m_i :identifica el símbolo i del texto cifrado b : constante de desplazamiento
n : número de símbolos del alfabeto

Descifrado

$m = (c - b) * inv(a, n)$ mód n

Donde:

c : identifica el símbolo i del texto cifrado
a :constante de multiplicación
b : constante de desplazamiento
n : número de símbolos del alfabeto

4. Enigma

4.1. Historia

Era una máquina de rotores que permitía usarla tanto para cifrar como para descifrar mensajes su mayor uso se dio antes y en la segunda guerra mundial para la protección de mensajes para la organización en la guerra .

Fue patentada en 1918 por la empresa alemana Scherbius and Ritter, cofundada por Arthur Scherbius, quien había comprado la patente de un inventor neerlandés, y se puso a la venta en 1923 para un uso comercial.

La máquina enigma era de un uso muy practico y facil , la cual no duró mucho tiempo en la segunda guerra mundial para el cifrado de sus mensajes debido a que los servicios de inteligencia polacos quienes instruyeron a los franceses e inglese en el sistema de cifrado ,se logró descifrar los mensajes y este fue uno de las causas de haber podido concluir la segunda guerra mundial.

La máquina para el cifrado de enigma fue un dispositivo electromecánico , esta máquina estaba compuesta por un teclado similar a las máquinas de escribir y el corazón de maquina estaba de rotores entre sí .

4.2. Funcionamiento

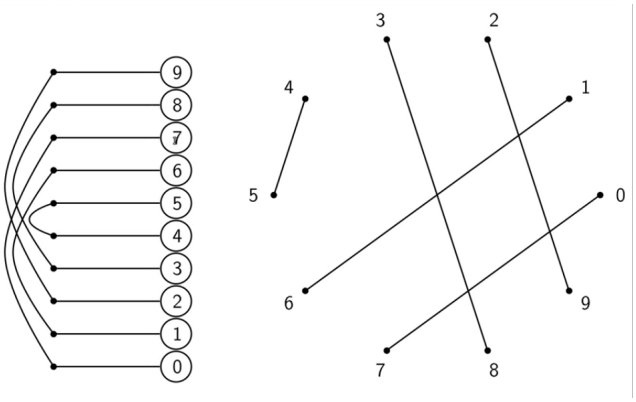


Figura 2: Reflector

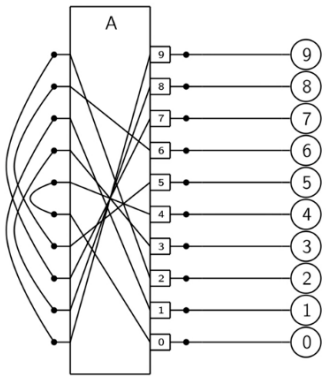


Figura 3: Reflector + Rotor

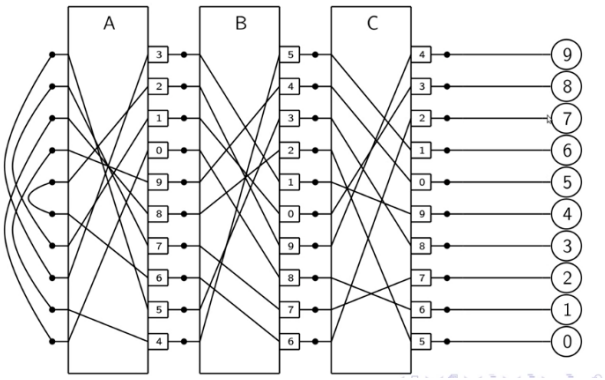


Figura 4: Tres reflectores + Rotor

5. Red de Feistel

Es un método simétrico de cifrado en bloque utilizado por algoritmos tales como DES (Data Ecryption Standard), Blowfish, CAST-128, entre otros.

5.1. Historia

El método fue nombrado por el criptógrafo alemán Horst Feistel, quien lo implementó por primera vez en la creación del algoritmo de cifrado Lucifer [4] para la IBM junto al matemático Don Coppersmith en 1971. El primero posteriormente implementó este método para el desarrollo del DES que fue utilizado como estándar FIPS en los Estados Unidos por su seguridad y facilidad de implementación de hardware.

Bastantes algoritmos de cifrados por bloque están basados en esta estructura, la cual fue estudiada junto a sus propiedades ampliamente por Michael Luby y Charles Rackoff [5] en los ochenta, quienes demostraron su seguridad.

5.2. Funcionamiento

Cifrado

Es un método simétrico iterativo de cifrado en bloque por rondas, lo que significa que, cifra el mensaje por bloques, generalmente 64 o 128 bits de manera repetitiva un numero especifico de veces (rondas) [3]. También se necesita de una función F y de un numero de llaves (k_i) igual al numero de rondas (n) que suele ser un numero par y mayor igual que 3. A partir de ahí realiza lo siguiente:

1. Divide el bloque de longitud N en dos bloques (R_0, L_0) de igual longitud $(N/2)$ (aunque hay excepciones, a esto se llama cifrado de Feistel desbalanceado).
2. La función F recibe los valores de R_0 y k_i, donde realiza una serie de operaciones.
3. El resultado es evaluado por la operación $\bigoplus$ (XOR) junto a L_0.
4. Se intercambia a $L_0 \bigoplus F(R0, k1)$ por R_0, que pasan a denominarse R_1 y L_1.
5. Se repite el proceso tantas rondas como llaves se tengan.
6. En la ultima ronda, ambos bloques intercambian una vez mas de lugar.

Este proceso se generaliza para la ronda n en la Figura 5.

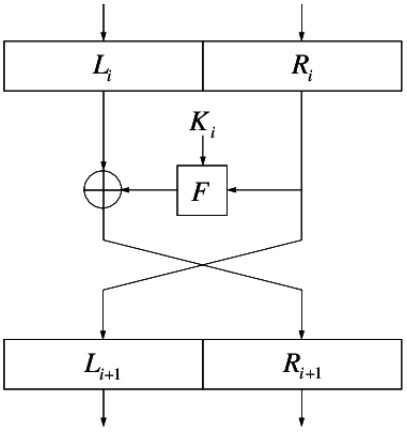


Figura 5: Ronda n de una red de Feistel

Descifrado

Una ventaja de este método es que la función F no necesita ser invertible puesto que al ingresar un texto ya cifrado e invirtiendo el orden de las claves se obtendrá como salida el texto original (Ver Figura 6). Esto debido a las propiedades del operador XOR, que se observan al aplicarlas sobre elementos ya cifrados:

Al aplicar el cifrado los bloques ya cifrados R_{n+1} y L_{n+1}:
Tomando en cuenta que: $R_{n+1} = L_n \bigoplus F(R_n, Kn)$

Luego:

$$R_{n+1} \bigoplus F(R_n, Kn) = L_n \bigoplus F(R_n, Kn) \bigoplus F(R_n, Kn)$$
$$R_{n+1} \bigoplus F(R_n, Kn) = L_n \bigoplus 0 \quad \text{... Inverso XOR } (a \bigoplus a = 0)$$
$$R_{n+1} \bigoplus F(R_n, Kn) = L_n \quad \text{... Elemento neutro } (a \bigoplus 0 = a)$$

L_{n+1} pasa como R_n

Así, los bloques pasaron a ser L_n y R_n.

Es gracias a esto que el receptor descifra el mensaje y su implementación en hardware es bastante sencilla.

5.3. Criptoanálisis

Al ser tan solo una estructura de cifrado su seguridad depende enormemente de su implementación, es así que la seguridad de los algoritmos que usan una red de Fesitel es bastante variable. Sin embargo, como ya se mencionó, los estudios de Luby y Rackoff señalan que la fortaleza del método radica en la función más que en el número de rondas. Añadir otros métodos tanto en la función como entre las mismas rondas ayudan también a dificultar el romper el cifrado.

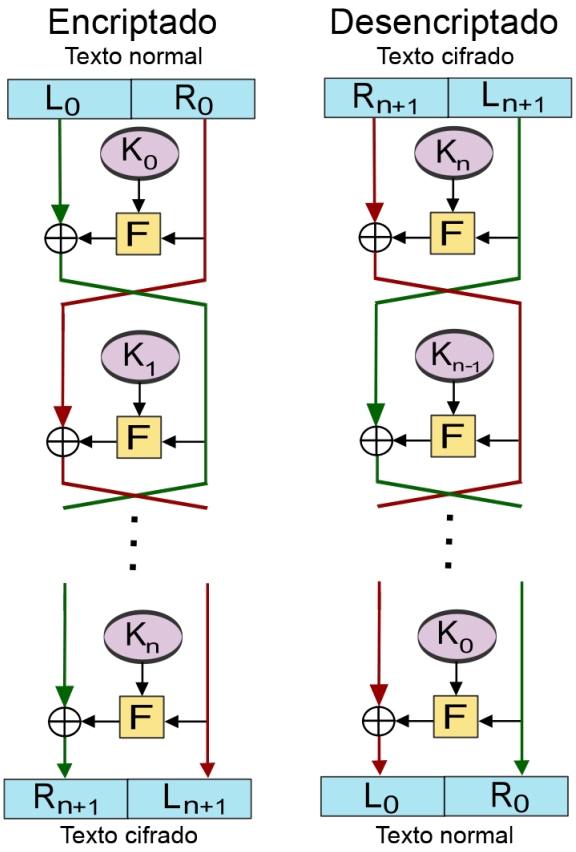


Figura 6: Esquema del cifrado y descifrado de una red de Feistel

6. DES

6.1. Historia

A comienzos de la década de los setenta el NBS (National Bureau of Standards) - ahora NIST (National Institute of Standards and Technology) tomó conciencia de la importancia de la seguridad informática en las operaciones comerciales de los EEUU, por lo que en 1973 decide solicitar propuestas para un nuevo estándar a usar para cifrar toda la información confidencial. Ante esto un equipo de científicos de IBM liderados por Horst Feistel desarrollo una modificación del algoritmo Lucifer.

Este algoritmo fue publicado en el Registro Federal en Marzo de 1975. Sin embargo el algoritmo fue duramente criticado por dos motivos: La inseguridad por el pequeño tamaño de las llaves (que lo dejaba expuesto a ataques por fuerza bruta) y la incertidumbre del control de la NSA sobre el algoritmo, particularmente las S-boxes, que se supone, permitían a la NSA descifrar los mensajes sin necesidad de las llaves.

Aun con la polémica, el algoritmo fue aprobado como parte del FIPS en 1977 y siguió así hasta 1998, cuando logró ser roto en 56 horas. Debido a esto y otros problemas de seguridad, el algoritmo fue optimizado y pasó a llamarse 3DES. Ya en 2004 es retirado oficialmente como estándar y es reemplazado por el AES.

6.2. Funcionamiento

DES es un algoritmo de cifrado por bloques que implementa una red de Feistel de 16 rondas(Ver Figuar 6), bloques de 64 bits y una clave también de 64 de los cuales son utilizados solo 56, puesto que los 8 restantes se encargan de encontrar errores, por medio de una comprobación de paridad. [7]

Como todo algoritmo por bloques, para trabajar con textos con un tamaño mayor a 64 bits este posee una variedad de modos de operación que permiten el cifrado por bloques y proporcionan confidencialidad y autenticidad al cifrado, en particular DES puede utilizar cuatro [6]:

1. ELECTRONIC CODEBOOK (ECB) MODE
2. CIPHER BLOCK CHAINING (CBC) MODE
3. CIPHER FEEDBACK (CFB) MODE
4. OUTPUT FEEDBACK (OFB) MODE

Para crear las 16 claves que necesita el algoritmo (puesto que consta de 16 rondas) se seleccionan los 56 bits efectivos de la clave original, se permutan una vez, se dividen en dos bloques y luego siguen una serie de desplazamientos y permutaciones prefijadas sucesivas (en particular una para la primera ronda y otra para las siguientes)de donde se les extrae 48 bits cada vez hasta obtener las 16 subclaves($k1, k2, k3, \ldots, k16$). Figura 7

Su función F utiliza S-boxes (Substitution Boxes) y una P-box (Permutation Box) las cuales son componentes que agregan confusión y difusión [8], respectivamente. Las primeras cambian un número de bits por otro distinto (de 8 a 6 en el caso del DES) por medio de una tabla según los bits externos e internos, la cual en el caso de DOS está prefijada. Figura 8

La función realiza lo siguiente. Graficado también en la Figura 9:

1. Expande el semi-bloque de 32 bits a 48 para que pueda operarse con la subclave mediante una permutación prefijada que además duplicada algunos bits.
2. Se aplica el operador XOR entre el semi-bloque expandido y la sub-clave ki

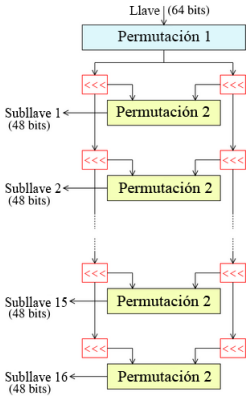


Figura 7: Creación de sub-llaves para el DES

S_4	x0000x	x0001x	x0010x	x0011x	x0100x	x0101x	x0110x	x0111x	x1000x	x1001x	x1010x	x1011x	x1100x	x1101x	x1110x	x1111x
0yyyy0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
0yyyy1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
1yyyy0	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
1yyyy1	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

Figura 8: Tabla que muestra la distribucion prefijada de la S-box 4 del DES

3. El resultado se divide en 8 bloques de 6 bits cada uno e ingresan a las 8 S-boxes$(s_1, s_2, ..., s_8)$ de la función, resultando en 8 bloques de 4 bits.

4. Estos bloques se jutan e ingresan a la P-box(P) y su salida es el resultado de la función

El algoritmo además de lo mencionado posee una Permutación Inicial (PI) y otra final (PF) la cual es la inversa de la primera, por lo que Regresa los bits a su posición original $(PF = PI - 1)$. Por lo que la estructura del algoritmo debería de verse así:

Nótese que a diferencia de una estructura Feistel convencional, esta no posee un intercambio al finalizar la última ronda.

6.3. Criptoanálisis

No es eficiente utilizar el algoritmo debido a que es posible quebrantarlo mediante un ataque por fuerza bruta debido al pequeño tamaño de su clave. Sin embargo al ser un estándar en el mundo de la criptografía, este es el algoritmo que cuenta con la mayor documentación respecto a su criptoanálisis.

Ahora bien, si el ataque por fuerza bruta es el más efectivo en la práctica. Existen otros ataques , tales como el Criptoanálisis Diferencial (DC por sus siglas en inglés) y

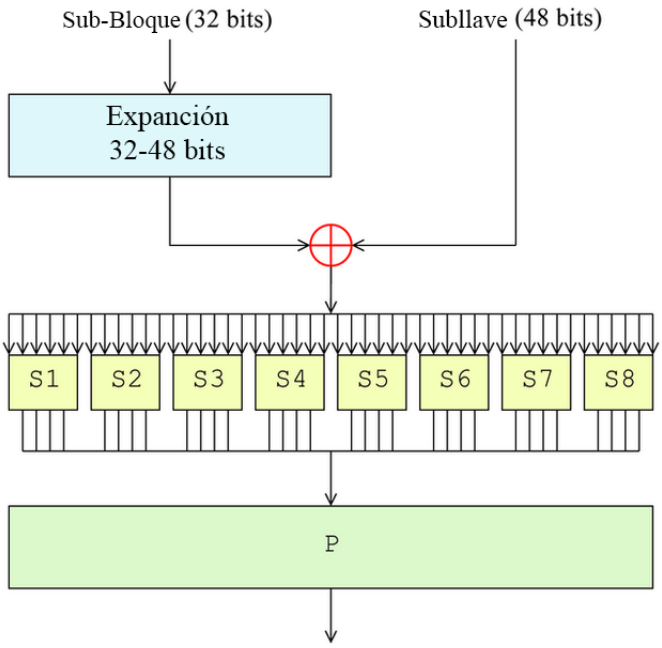


Figura 9: Función F de Feistel en DES

el Criptoanálisis Lineal (CL), los cuales si bien son menos complejos y en teoría, más rápidos, es imposible aplicarlos en la práctica. Con respecto al primero, las S-boxes fueron implementadas específicamente para proteger al DES de dicho ataque [9] [10].

Otro ataque conocido es el Ataque Davie, el cual fue creado para ser utilizado únicamente contra el DES, sin mejor aplicación práctica que los anteriores

7. Escítala

Considerado uno de los primeros sistemas criptográficos en la historia, utilizado por los antiguos espartanos, donde se emplea el método de transición para codificar los mensajes.

7.1. Historia

Escítala, del griego $\sigma\kappa\upsilon\tau\alpha\lambda\eta$ (skitáli), que significa vara o palo. Se señala que el primero en hablar de ella fue Apolonio de Rodas, quien la menciona como un criptograma utilizado por los generales espartanos y el primero en mencionar su funcionamiento detalladamente fue Plutarco allá por el siglo I a.C. en su obra la Vida de Lisandro.

Ahora bien, nuevos autores indican que son varios los que la mencionan antes [11], de ellos el primero fue el poeta Arquíloco en el siglo VII a.C. quien no men-

ciona nunca que hayan sido utilizadas solo por los espartanos o que fueran siquiera aparatos de cifrado, sino mas bien, representaciones tangibles de un mensaje cualquiera. Debido a estos hallazgos y a la inseguridad del método de cifrado que parece ser una utilidad secundaria, se concluye que la escítala fue un mero instrumento de mensajería. Aun así forman parte importante de la criptografía y su estudio es indispensable.

7.2. Funcionamiento

Su funcionamiento es detallado por Plutarco [12], que indica lo siguiente:

1. Se crean dos varas de madera con las mismas medidas (preferentemente del mismo diámetro) que se le entregan a cada una de las dos partes y un pergamino (de cuero generalmente) muy largo y bastante estrecho.

2. El pergamino es enrollado en una vara sin dejar espacio alguno y el mensaje es escrito en él. Figura 10.

3. Ahora el pergamino es enviado a la otra parte, donde al enrollarlo en la segunda vara, el mensaje cobrará sentido.

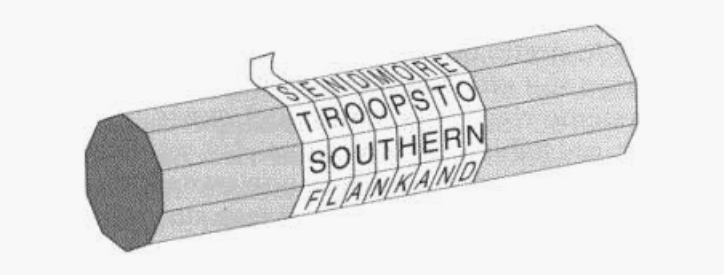


Figura 10: Representación de una escítala griega. (Notese que ambos, la vara y el pergamino, conforman juntos a la escítala

Este proceso es conocido como transposición en la criptografía, el cual consiste en alterar el orden de los elementos en el mensaje sin alterarlos a ellos mismos. En particular, se está utilizando una transposición sin llave, donde todo el mensaje se cifra de una forma predeterminada.

El sistema se puede explicar también por medio de matrices, donde el mensaje es puesto a a lo largo una matriz con un largo y ancho variables que dependen, en este caso, del diámetro de la vara. Si es que el mensaje es incapaz de llenar la matriz, se le completa con caracteres vacíos o algun otro caracter poco utilizado en el idioma en el que se este escribiendo. Los espacios pueden ser o no considerados, dependiendo de lo quieran ambas partes.

El mensaje cifrado resulta ser la transpuesta de dicha matriz dispuesta a lo largo, lo que indica que para el descifrado, tan solo habría que transponerla una vez mas hasta llegar a la original. Dado que esta es una función involutiva. El mensaje siempre se lee por filas en la matriz

En el siguiente ejemplo, se demuestra el cifrado y descifrado por medio de matrices.

Mensaje = MENSAJE SECRETO

$$A = \begin{bmatrix} M & E & N & S & A \\ J & E & S & E & C \\ R & E & T & O & X \end{bmatrix},\ A^T = \begin{bmatrix} M & J & R \\ E & E & E \\ N & S & T \\ S & E & O \\ A & C & X \end{bmatrix},\ (A^T)^T = A = \begin{bmatrix} M & E & N & S & A \\ J & E & S & E & C \\ R & E & T & O & X \end{bmatrix} \tag{7.1}$$

La matriz A contiene al mensaje: MENSAJE SECRETO, que pasa a denominarse: MENSAJESECRETOX.

La matriz A^T contiene al mensaje ya cifrado: MJREEENSTSEOACX.

Si se transpone la matriz que contiene al mensaje cifrado, dara como resultado: MENSAJESECRETOX, que viene a ser el mensaje original.

7.3. Criptoanálisis

Los métodos de transposición sin llave son bastante inseguros y no deben de ser utilizados si lo que se busca es un cifrar un mensaje de suma importancia. Tan solo basta con conocer el numero de columnas en los que el mensaje está dispuesto que al ser menor que el numero de caracteres en el mensaje, permite romper el cifrado con un ataque por fuerza bruta de manera bastante eficiente.

Es por esto que aquellos métodos de transposición que suceden al usado en la escítala usan un sistema de llaves que los hace más seguros permitiendo permutaciones más complicadas de descifrar a lo largo de distintos segmentos del bloque. Estos dos métodos (con y sin llave) pueden ser utilizados en conjunto para incrementar la seguridad.

8. Playfair

Es un cifrado de sustitución simétrico utilizado por las tropas inglesas durante la época victoriana el cual es considerado el primer cifrado digráfico (utilizando dos letras) de la historia.

8.1. Historia

El cifrado fue inventado en 1854 por Charles Wheatstone, científico e inventor inglés, entre cuyos inventos se encuentras el caleidoscopio, el estereoscopio y el puente de Wheatstone. Sin embargo, su nombre le fue atribuido al Baron Lyion Playfair, quien era amigo cercano del primero y también un científico reconocido, esto debido a que fue él y no Wheatstone quién presentó el cifrado y demostró su funcionamiento (aun cuando este lo nombró: "El nuevo cifrado simétrico de Wheatsonte") [13].

Como ya se mencionó, este fue el primer cifrado digráfico es ser creado, lo cual implica que cada carácter en el mensaje cifrado depende ya no de una, sino de dos letras, algo que para aquel entonces le proveía de un gran seguridad, claro que únicamente si no se conocía esta característica del método. Además que es bastante práctico manualmente, pues no se necesitan complementos adicionales cómo se verá más adelante.

Fue por estas características que fue adoptado por la Oficina de Guerra Inglesa para ser utilizado por el ejército británico. El barón Playfair sugirió utilizarlo por primera vez durante la Guerra de Crimea (1853 - 1856), sin embargo debido a que esta información es confidencial, los primeros reportes de su uso se dieron durante la primera guerra Boer unos 20 años después.

8.2. Funcionamiento

8.2.1. Cifrado

La clave es introducida en un cuadrado, (aunque originalmente podía ser un rectángulo [13], sin embargo se optó por la primera para evitar confusiones) de 5 x 5 caracteres donde irá nuestro alfabeto evitando repeticiones en los caracteres. Nótese que el tamaño del cuadrado permite un total de 25 letras para utilizar, por lo que se debe de combinar dos letras, lo que transformará el mensaje y puede que cause ciertas complicaciones [14].

En el caso del inglés se opta por la I y la J, mientras que en el español (que cuenta con 26), se pueden combinar la N con la Ñ y la V con la W. Por lo que tanto al cifrar como al descifrar se consideraran a ambos caracteres como el primero.

$I = I,\ J = I$

Posteriormente se procede a llenar el cuadrado con los caracteres restantes del alfabeto en orden. Se muestra un ejemplo en la Figura 11.

P	A	L	M	E
R	S	T	O	N
B	C	D	F	G
H	I/J	K	Q	U
V	W	X	Y	Z

Figura 11: Cuadrado resultante utilizando la clave PALMERSTON, la cual fue utilizada por Playfair durante su primera demostración

Luego, el mensaje a encriptar es dividido en pares, tomando en cuenta lo siguiente:

1. Si el par contiene caracteres repetidos, se introduce un carácter infrecuente como Q o X a fin de evitar confusiones (que puede llegar a ser peligroso si se usa en exceso), en el medio y se vuelve a dividir.

2. Si el número de caracteres en el mensaje es impar, se le añadirá otro (puede ser el mismo) carácter infrecuente al final.

Ejem:
ESTE MENSAJE ES SECRETO
ES TE ME NS AJ EX ES SE CR ET OX

Notese que el caracter repetido en "*ESSECRETO*"no es tomado en cuenta por pertenecer a dos pares diferentes.

Una vez dividido el mensaje, se pasa a encriptar cada dupla según los siguientes casos:

1. Si ambos caracteres se encuentran en la misma columna del cuadrado, cada uno toma el valor del caracter a su derecha (el primero de la columna si este resulta ser el último).

2. Si se encuentran en la misma fila, cada uno toma el valor del caracter debajo de este (el primero, si este resulta ser el último).

3. De no cumplirse los anteriores casos, cada caracter se intercambia con el que se encuentra en su misma fila y en la columna del otro caracter en el par.

8.2.2. Descifrado

El proceso de descifrado es el mismo, con la diferencia de que los caracteres que se combinaron pueden variar. Así el mensaje: "EL NIÑO SE LLAMA WALTER" tras cifrar y descifrarlo, pasar a ser: "EL NINO SE LLAMA VALTER" con las combinaciones recomendadas.

8.3. Criptoanálisis

Si bien es mucho más fuerte que una sustitución simple como en el caso de César, se cumple que cada par de letras en el texto llano tiene una y solamente una correspondencia con un par de letras en el texto codificado, lo que hace vulnerable al análisis de frecuencias aplicado a los pares de letras (aunque éste es algo más complicado que aplicado a los caracteres en solitario).

Ahora bien, se pueden utilizar otros métodos, tales como ataques a textos conocidos (siempre que se cuente con un texto suficientemente largo). Donde ciertas características del cifrado, tales como que los pares invertidos generan siempre pares cifrados invertidos, o la posición de los caracteres en el cuadrado que a partir de la clave tiene que estar en orden alfabético.

Los primeros registros de una solución general a Playfair son atribuidos al general americano Joseph Mauborgne, quien es co-inventor del cifrado de un solo uso (One-time pad).

9. Polybios

Alrededor del año 150 a. C. se encuentra tal vez el algoritmo de sustitución más antiguo del cual se tiene conocimiento y recibe el nombre de Polybios, nombre que se le dio en reconocimiento al historiador griego del mismo nombre y de quien se considera fue su creador.
El algoritmo Polybios utiliza como base de cifrado una tabla de sustitución como la que se muestra a continuación:

	A	B	C	D	E
A	A	B	C	D	E
B	F	G	H	I/J	K
C	L	M	N	O	P
D	Q	R	S	T	U
E	V	W	X	Y	Z

9.1. Proseso de cifrado

Para llevar a cabo el proceso de cifrado se consideran la primera columna y el primer renglón de la tabla anterior como el par criptográfico correspondiente a cada letra dentro de la matriz de 5 X 5 mostrada en la tabla, de manera que justo en ese orden, renglón-columna, son las dos letras que sustituyen a cada una de las letras que pueden conformar el mensaje en claro.
Así, por ejemplo para la letra M el criptograma correspondiente es CB, en tanto que para la U es el par DE, de manera que de acuerdo con este algoritmo se puede observar que se sustituye el alfabeto A, B , C, D, E, F, . . . X, Y, Z por el alfabeto de cifrado AA, AB, AC, AD, AE, BA,. . . , EC, ED, EE, entre lo que destaca de manera importante que el criptograma correspondiente a un mensaje en claro cifrado con este algoritmo siempre contendrá el doble de caracteres que el texto plano, característica que no es precisamente lo más deseado ya que los criptogramas pueden alcanzar dimensiones muy grandes, complicados de manipular, y con la necesidad de un espacio de almacenaje duplicado al tamaño original.

Para ejemplificar el proceso de sustitución con base en la tabla anterior:

Mcla	P	O	L	Y	B	I	O	S	E	S	G	R	I	E	G	O
Sustitución	C E	C D	C A	E D	A B	B D	C D	D C	A E	D C	B B	D B	B D	A E	B B	C D

Cripto = CECDCAEDABBDCDDCAEDCBBDBBDAEBBCD

9.2. proceso de descifrado

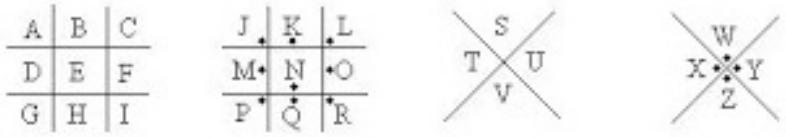
Para llevar a cabo el proceso inverso, esto es, el proceso de descifrado, se parte el criptograma a descifrar, leyendo éste de izquierda a derecha y tomando en cada ocasión un par de caracteres para llevarlos a la tabla de descifrado de manera que el primero lo ubicamos con su similar en la primera columna de la tabla y el segundo con su símil del primer renglón, entonces extendemos una línea imaginaria sobre la columna y el renglón identificados y en la celda donde éstas se intersecan se encuentra el carácter correspondiente al mensaje en claro de ese par de elementos del criptograma.
Por ejemplo, si se desea descifrar el criptograma AEDCDDDEADBDCD, de izquierda a derecha se toman los elementos que lo conforman de dos en dos, y se llevan a ala tabla de cifrado.
Después de desarrollar el descifrado para el criptograma se obtiene:

Cripto	AE	DC	DD	DE	AD	BD	CD
Mcla	E	S	T	U	D	I	O

Mcla: ESTUDIO

10. Pigpen

La cifra de sustitución monoalfabética perduró a través de los siglos en formas diversas.
Fue utilizada por los masones en el siglo XVIII para preservar la privacidad de sus archivos, y todavía la usan los niños hoy en día. La cifra no sustituye una letra por otra, sino que sustituye cada letra por un símbolo de acuerdo al siguiente modelo:



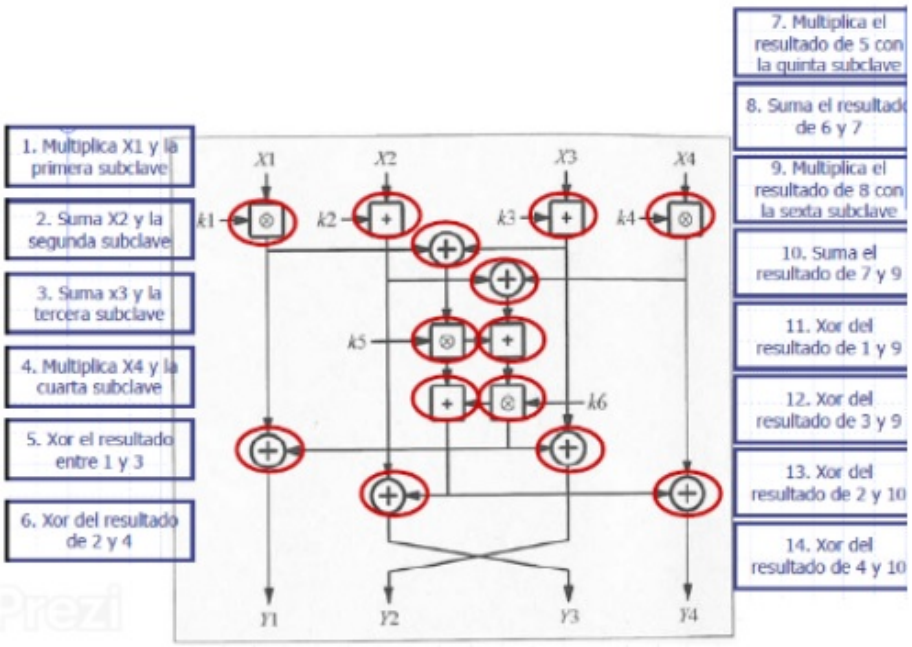
El método fue desarrollado por los francmasones a principios de los años 1700 para mantener registros y para la correspondencia (Newton, 1998, p. 113).
Ejemplo:

11. IDEA

IDEA-International Data Encryption Algorithm (Algoritmo Internacional de Cifrado de Datos) es un cifrador por bloques diseñado por Xuejia Lai y James L. Massey de la Escuela Politécnica Federal de Zùrich y descrito por primera vez en 1991.

- 1990: Xuejia Lai y James Massey (Swiss Federal Institute of Technology) proponen el PES (Proposed Encryption Standart).
- 1991: Los avances en el criptoanálisis diferencial hacen necesario introducir mejoras y lo modifican creando el IPES (Improved Proposed Encryption Standard).
- 1992: Los autores incluyen nuevas mejoras y proponen finalmente el algoritmo IDEA (International Data Encryption Algorithm).
- 1999: El Algoritmo IDEA demuestra ser mucho másseguro que DES y sus derivados y se comienza a usar en el sistema PGP, lo que hizo que tuviera muchos usuarios.

11.1. Proceso de cifrado



12. Gost

Es un algoritmo de cifrado simétrico por bloques que fue usado por la antigua Unión Soviética. Se basa en la red de Feistel emplea bloques de 64 bits y claves de 256 bits.

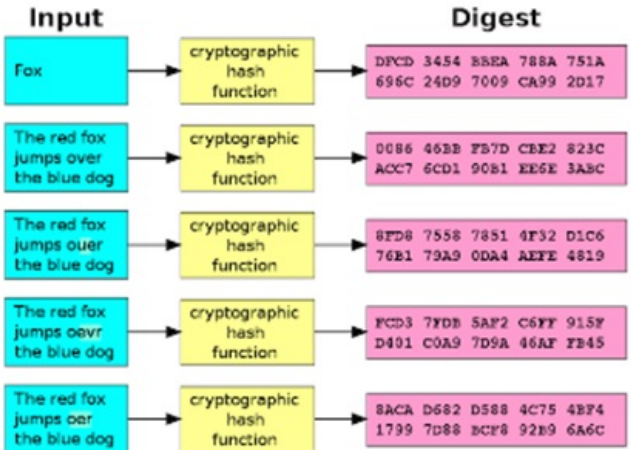
Desarrollado en la década de 1970, el estándar había sido marcado como “Top Secret” en 1990. Poco después de la disolución de la URSS, fue desclasificado y fue lanzado al público en 1994.

Los S-boxes aceptan una entrada de cuatro bits y producen una salida de cuatro bits. La sustitución S-box en la función redonda consiste en ocho cajas S 4 4. Los S-boxes dependen de la implementación: GOST tiene un tamaño de bloque de 64 bits y una longitud de clave de 256 bits. Sus S-boxes pueden ser secretos, y contienen aproximadamente 354 .

GOST es una red Feistel de 32 rondas. Su función circular es muy simple: agregue un módulo de subkey de 32 bits 232, coloque el resultado a través de una capa de S-boxes.

12.1. ¿Qué Es Un Hash Y Cómo Funciona?

Una función criptográfica hash- usualmente conocida como "hash"- es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud.



13. AES

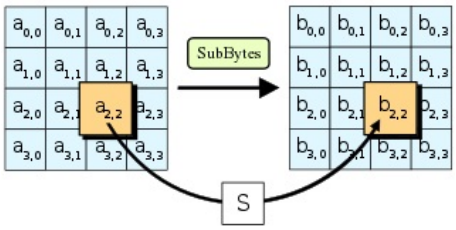
El algoritmo más utilizado hoy en día. La longitud de clave puede ser de 128 bits (10 rondas), 192 bits (12 rondas) o 256 bits (14 rondas) basado en sustituciones, permutaciones y transformaciones lineales, ejecutadas en varias veces en bloques de datos de 16 bytes.

13.1. Historia

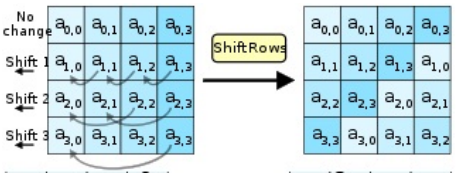
En 1997, el Instituto Nacional de Normas y Tecnología (NIST) decidió realizar un concurso para escoger un nuevo algoritmo de cifrado capaz de proteger información sensible durante el siglo XXI. Este algoritmo se denominó Advanced Encryption Standard (AES).

13.2. Etapa Inicial

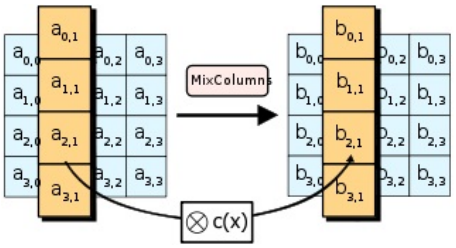
1. AddRoundKey
2. SubBytes — en este paso se realiza una sustitución no lineal donde cada byte es reemplazado con otro de acuerdo a una tabla de búsqueda.



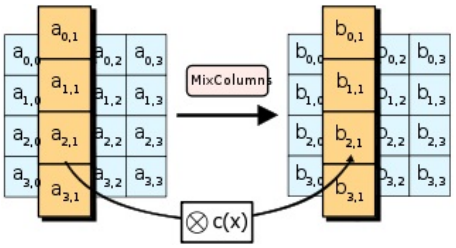
3. ShiftRows — en este paso se realiza una transposición donde cada fila del «state» es rotada de manera cíclica un número determinado de veces.



4. MixColumns — operación de mezclado que opera en las columnas del «state», combinando los cuatro bytes en cada columna usando una transformación lineal.



5. AddRoundKey — cada byte del «state» es combinado con la clave «round»; cada clave «round» se deriva de la clave de cifrado usando una iteración de la clave.



Referencias

[1] Hancarville, P. and Niemoeller, A., (1949). The Private Lives Of The Twelve Caesars. Girard, Kan.

[2] Wobst, R. (2001). Cryptology Unlocked. Wiley. p. 19

[3] Menezes, Alfred J.; Oorschot, Paul C. van; Vanstone, Scott A. (2001). Handbook of Applied Cryptography (Fifth ed.). p.251

[4] J. Smith. (1971) The design of Lucifer: a cryptographic device for data communications. IBM Research Report RC 3326, IBM T.J. Watson Research Center, Yorktown Heights, New York, USA.

[5] M. Luby and C. Rackoff. How to construct pseudorandom permutations from pseudorandom functions. SIAM Journal on Computing, 17(2), pp. 373–386, 1988.

[6] FIPS PUB 81 (1980) DES MODES OF OPERATION

[7] FIPS PUB 46-3 (1999) DATA ENCRYPTION STANDARD

[8] FIPS PUB 74 (1981) GUIDELINES FOR IMPLEMENTING AND USING THE NBS DATA ENCRYPTION STANDARD

[9] Coppersmith, D. (1994). The data encryption standard (DES) and its strength against attacks. IBM Journal of Research and Development, vol 38 n3, pp. 243–250

[10] Biham, E. Shamir, A. (1993). Differential Cryptanalysis of the Data Encryption Standard, pp. 15-17

[11] Kelly T. (1998) THE MYTH OF THE SKYTALE, Cryptologia, 22:3, pp.244-260

[12] Forouzan B. (2007) Cryptography and Network Security pp.81-83

[13] Kahn, D. (1996) The Codebreakers: The comprehensive history of secret communication from ancient times to the internet. pp.60

[14] Christensen, C., 2006. Polygraphic Ciphers. [online] Nku.edu. Disponible en: ¡https://www.nku.edu/ christensen/section %2019 %20playfair %20cipher.pdf¿[Recuperado el 17 de Abril 2020].