Criptografía.

Apuntes de criptografía.

Autor:
Pedro Luis Morelos O.

2020

Índice

1. Visión general y sus aplicaciones.

Las personas siempre han tenido una gran fascinación manteniendo la información alejada de los demás, como cuando se está en la infancia, algunos tenían cierto *código* con sus amigos para que profesores, padres o demás personas que no quisiéramos que leyeran nuestro mensaje, no pudieran descifrarlo. La historia está llena de numerosos ejemplos.

Con los nuevos avances tecnológicos, el mundo está cada vez más conectado, con ello la demanda de la información y servicios electrónicos aumentan. La protección de los datos y de estos sistemas electrónicos son cruciales e importantes para nuestra forma de vivir.

Las técnicas necesarias para proteger los datos pertenecen al campo de la criptografía. Actualmente, la materia tiene tres nombres: **criptología, criptografía y criptoanálisis**.
Criptología. Refiere a los términos para el estudio de la comunicación a través de canales inseguros y problemas relacionados.
Criptografía. El proceso de diseñar sistemas para hacer esto es llamado criptografía.
Criptoanálisis. Trata con romper dichos sistemas.

Comunicaciones Seguras.

Un escenario básico de comunicación, como se muestra en la figura 1, en este escenario existen dos partes, a quienes llamaremos Alicia y Betito, los cuales quieren comunicarse entre ellos, y una tercera persona llamada Candie, la cual es una espía potencial.
Cuando Alicia quiere mandar un mensaje a Betito, éste recibe el nombre de **plaintext o texto plano**, ella lo encripta usando un método preestablecido con Betito. Usualmente el método de encriptación es conocido por Candie, lo que mantiene el mensaje en secreto es una llave.
Cuando Betito recibe el mensaje encriptado (llamado **ciphertext**), él tiene que realizar el proceso inverso de encriptación para poder regresar al *plaintext*, usando para ello la llave de descifrado.

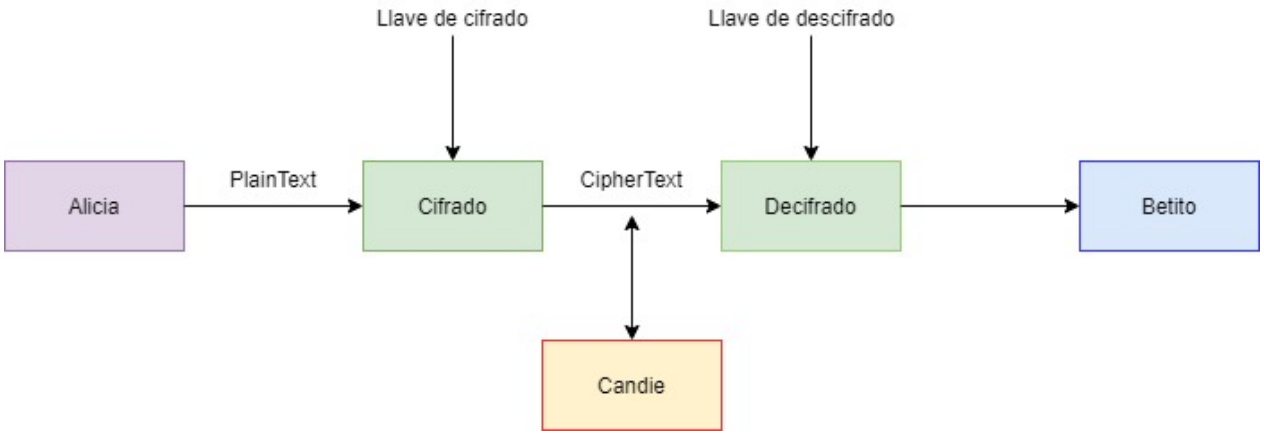


Figura 1: Escenario básico de comunicación.

Posibles ataques.

Existen 4 posibles ataques que Candie será capaz de hacer, la diferencia entre este tipo de ataques refiere a la cantidad de información, los cuales son:

- **Solo el texto cifrado.** Candie tiene una sola copa del texto cifrado.
- **Conociendo el texto plano.** Candie tiene una copia del texto cifrado y el texto plano correspondiente.
- **Escogiendo el texto plano.** Candie tiene acceso temporal a una máquina de descifrado, ella no puede abrirlo para encontrar la lleve, sin embargo ella puede cifrar un gran cantidad de textos planos elegidos adecuadamente y tratar de usar el resultado de dichos textos cifrados para deducir la clave.
- **Escogiendo el texto cifrado.** Candie tiene acceso temporal a una máquina de descifrados, usándola para descifrar varios símbolos de la cadena y tratar de usar dichos resultados para deducir la llave.

Aplicaciones de la criptografía.

Criptografía no solo hace referencia de cifrar y descifrar mensajes, también tiene que ver con resolver problemas de la vida real que requieren seguridad de la información. Existen cuatro principales objetivos, los cuales son:

- **Confidencialidad.** Candie no debería ser capaz de leer los mensajes enviados de Alicia a Betito.
- **Integridad de los datos.**Betito quiere estar seguro que los mensajes de Alicia no fueron modificados o alterados durante el envío.
- **Autenticación.** Betito quiere estar seguro que solo Alicia pudo haber enviado el mensaje que él recibió.
- **No repudio.** Alicia no puede decir que ella no envió el mensaje.

2. Fundamentos matemáticos.

En seguridad informática las matemáticas juegan un papel muy importante, es por ello que en está sección se mostrarán los conceptos fundamentales para poder entender los modos de cifrado que se presentarán en los capítulos siguientes.

2.1. Aritmética Modular.

Cuando se dividen dos enteros se tiene una ecuación que se ve como lo siguiente:

$$\frac{A}{B} = Q \ residuo \ R$$

Donde:
A es el dividendo
B es el divisor
Q es el cociente
R es el residuo

Para algunos cifrados solo se requiere saber cuánto es el **residuo** cuando se divide A entre B.
Para ello, existe un operador llamado *módulo* que se abrevia como mod.Dicha expresión queda representada como: **A mod B = R**

Por ejemplo:

$$\frac{17}{3} = 5 \ residuo \ 2$$

$$17 \ mod \ 3 = 2$$

Es importante resaltar que en aritmética modular solo existen dos operaciones: **suma y multiplicación**, aunque a pesar de ello también cumple la propiedad de tener su inverso, ya sea inverso multiplicativo o inverso aditivo, veremos como se calcula cada uno de ellos.

2.1.1. Inverso Aditivo.

Recordando, que un número sumado con su inverso es igual a 0. Generalmente este inverso tiene que ver con números negativos, pero como se mencionó antes, no existe la operación resta, es por ello que la suma de dos números positivos modulo C debe de ser 0, es decir:

$$A + A' \ mod \ C = 0$$

Supongamos que se está trabajando con mod = 26, y se quiere encontrar el inverso aditivo de 9. Debe de existir un número menor a 26 que cumpla la ecuación anterior

$$9 + A' \ mod \ 26 = 0$$

Como se mencionó, el número que se busca debe ser menor al modulo C (para este ejemplo 26), por lo cual, esto nos asegura que la suma siempre será menor o igual a 26. Para que un número **A mod C = 0**, A debe de ser múltiplo de C, en este caso será igual a C, lo que quiere decir que:

$$9 + A' = 26$$

$$A' = 26 - 9$$

$$A' = 17$$

$$9 + 17 \ mod \ 26 = 0$$

Por lo tanto 17 es el inverso aditivo de 9 cuando se trabaja con modulo 26. Y viceversa el inverso aditivo de 17 será 9, por lo que ya no se requiere calcular de nuevo el inverso, debido a que será el mismo.

2.1.2. Inverso Multiplicativo.

También es importante recordar que la multiplicación de un número con su inverso es igual a 1, en aritmética modular el inverso se define como: **A mod C = A'**. Viendo dicha ecuación de otra manera:

$$(A * A') \ mod \ C = 1$$

Siguiendo con el ejemplo anterior, ahora queremos encontrar el inverso multiplicativo de 9.

$$(9 * 1) \ mod \ 26 = 9$$

$$(9 * 2) \ mod \ 26 = 18$$

$$(9 * 3) \ mod \ 26 = 1$$

Por lo tanto A' de 9 es igual a 3, y de igual manera, ya no es necesario calcular el inverso de 3, porque este siempre será 9 cuando se trabaja con mod = 26.

2.2. Un algoritmo especial.

Este algoritmo es de gran ayuda en lo que refiere a conocer si el MCD de dos números es 1 y a encontrar el inverso multiplicativo de un número a través de un método y no estar probando con todos los números del anillo a ver cual es el indicado.

2.2.1. Algoritmo de Euclides.

Para saber si los números escogidos son los correctos debe cumplir lo siguiente:

$$MCD(a, b) = 1$$

en otro caso no cumple la condición y por lo tanto dichos números no pueden usarse.

Veamos dos ejemplos de este método.

$$MCD(482, 1180) =?$$

$$1180 = 482(2) + 216$$

$$482 = 216(2) + 50$$

$$216 = 50(4) + 16$$

$$50 = 16(3) + 2$$

$$16 = 2(8) + 0$$

Lo importante es fijarse en la penúltima ecuación, si el segundo número que suma es 1 o diferente, esto nos determina el **MCD(a,b)**.
En este caso es 2, por lo tanto el **MCD(482,1180) = 2**

Ahora probemos con:

$$MCD(15, 26) =?$$

$$26 = 15 + 11$$

$$15 = 11 + 4$$

$$11 = 4(2) + 3$$

$$4 = 3 + 1$$

$$3 = 1(3) + 0$$

Si ponemos atención a la penúltima ecuación, vemos que el segundo término que suma es 1, por lo cual el **MCD(15, 26) = 1**, lo que quiere decir que 15 es un número valido para el alfabeto 26. Ahora la pregunta es **¿Cómo encontramos el inverso multiplicativo de 15 ?**

2.2.2. Algoritmo de Euclides Extendido.

Para poder responder a la pregunta anterior, haremos uso del ejemplo donde los números si cumplen la condición, lo primero que debemos de hacer es lo siguiente.

$$11 = 26 - 15...(d)$$

$$4 = 15 - 11...(c)$$

$$3 = 11 - 4(2)...(b)$$

$$1 = 4 - 3...(a)$$

Antes de continuar, es importante saber que la última ecuación donde sumamos 0, no se toma en cuenta, además de que, no debemos de sustituir ningún valor, sabemos que $4(2) = 8$, pero ese 8 no nos sirve, debemos dejarlo indicado tal y como está.

Ahora veamos como se desarrolla este algoritmo.

Partimos de la ecuación (a)

$$1 = 4 - 3$$

Vemos que en la ecuación (b), tenemos una igualdad con 3, por lo cual sustituimos la ecuación (b) en 3.

$$1 = 4 - (11 - 4(2))$$

Haciendo las operaciones algebraicas, tenemos:

$$1 = 4 - 11 + 4(2)$$

$$1 = 4(3) - 11$$

Ahora, este procedimiento lo repetimos hasta, acabar las ecuaciones previamente numeradas. Sustituyendo (c) en 4

$$1 = (15 - 11)(3) - 11$$

$$1 = 15(3) - 11(3) - 11$$

$$1 = 15(3) - 11(4)$$

Sustituimos (d) en 11

$$1 = 15(3) - (26 - 15)(4)$$

$$1 = 15(3) - 26(4) + 15(4)$$

$$1 = 15(7) - 26(4)$$

Tomando en cuenta la siguiente afirmación

$$1 = ax + by$$

$$a' \ mod \ b = x$$

Si revisamos nuestro resultado, tenemos:

$$1 = 15(7) + 26(-4)$$

$$15' \ mod \ 26 = 7$$

De esta manera es como se obtiene el inverso multiplicativo de un número

2.3. Álgebra lineal.

2.3.1. Multiplicación de matrices.

Una matriz es un arreglo rectangular en renglones (filas) y columnas. Las dimensiones de una matriz indican el número de filas y columnas en ese orden. Suponga que una matriz tiene M filas y N columnas, se dice que el orden de la matriz es MxN

Suponga que tenemos las matrices A, B, de tamaño 2x3 y 3x3, respectivamente, para poder multiplicarlas debemos de ver que el número de columnas de la primera matriz sea igual número de filas de la segunda. Para este caso, esta condición cumple, por lo cual ahora tendremos una matriz del orden de filas de la primera columna x columnas de la segunda (2x3). Para realizar la multiplicación se hace de la siguiente manera:

$$A \cdot B = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} = \begin{pmatrix} 30 & 36 & 42 \\ 66 & 81 & 96 \end{pmatrix}$$

Para entender este resultado, debe de tomar la primera fila de la matriz A y la primera columna de la matriz B, y hacer la suma de la multiplicación entre cada termino correspondiente, posteriormente selecciona la columna 2 y 3 de la matriz B, una vez llegado aquí, seleccionamos la segunda fila de la matriz A y repetimos el proceso.

Ejemplo de los primeros tres términos.

$$(1 \cdot 1) + (2 \cdot 4) + (3 \cdot 7) = 30$$
$$(1 \cdot 2) + (2 \cdot 5) + (3 \cdot 8) = 36$$
$$(1 \cdot 3) + (2 \cdot 6) + (3 \cdot 9) = 42$$

2.3.2. Multiplicación de un número escalar.

Ahora que sabe la multiplicación entre matrices, **¿Qué pasa si solo quiero multiplicar un número a una matriz?**.
La respuesta es que multiplica cada término por dicho número. Sea A la matriz:

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 2 & 4 & 1 \end{pmatrix}$$

Si deseamos multiplicar la matriz A por 3, es decir, 3A, tenemos:

$$3A = \begin{pmatrix} 1 \cdot 3 & 2 \cdot 3 & 3 \cdot 3 \\ 4 \cdot 3 & 5 \cdot 3 & 6 \cdot 3 \\ 2 \cdot 3 & 4 \cdot 3 & 1 \cdot 3 \end{pmatrix}$$

$$\therefore$$

$$3A = \begin{pmatrix} 3 & 6 & 9 \\ 12 & 15 & 18 \\ 6 & 12 & 3 \end{pmatrix}$$

2.3.3. Matriz identidad.

Una matriz importante que nos servirá para la siguiente sección, la característica de está matriz de NxN, es que las entradas en la diagonal desde la parte superior izquierda hasta la parte inferior derecha son 1 y el resto de las entradas o números son 0.

Ejemplo de una matriz 3x3 identidad.

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

Una de las características de esta matriz identidad (I), es que si multiplicamos una matriz A por la matriz identidad obtenemos la misma matriz.

$$A * I = A$$

2.3.4. Matriz inversa.

Al igual que en la aritmética modular, existe el inverso multiplicativo de la matriz A, que como resultado en vez de darnos 1, nos da la matriz identidad, pero recordar que no existe la operación división. Esto quiere decir que:

$$A * A^{-1} = I$$

Ahora la pregunta que nos hacemos es: **¿Cómo calculamos la matriz inversa de A?**
Lo que debemos de hacer primero, es una matriz doble, del lado izquierdo la matriz A, mientras que por el lado derecho, necesitamos de la matriz identidad. Sea

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 2 & 4 & 1 \end{pmatrix}$$

$$A^{-1} = \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 4 & 5 & 6 & 0 & 1 & 0 \\ 2 & 4 & 1 & 0 & 0 & 1 \end{array}\right)$$

Ahora a través de procesos de sumas, restas, multiplicaciones, divisiones debemos convertir la matriz de lado izquierdo en la matriz identidad.

$$R_2 = R_2 - 4R_1$$

$$A^{-1} = \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & -3 & -6 & -4 & 1 & 0 \\ 2 & 4 & 1 & 0 & 0 & 1 \end{array}\right)$$

$$R_3 = R_3 - 2R_1$$

$$A^{-1} = \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & -3 & -6 & -4 & 1 & 0 \\ 0 & 0 & -5 & -2 & 0 & 1 \end{array}\right)$$

$$R_2 = R_2 \cdot \frac{-1}{3}$$

$$A^{-1} = \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 1 & 2 & \frac{4}{3} & -\frac{1}{3} & 0 \\ 0 & 0 & -5 & -2 & 0 & 1 \end{array}\right)$$

$$R_1 = R_1 - 2R_2$$

$$A^{-1} = \left(\begin{array}{ccc|ccc} 1 & 0 & -1 & -\frac{5}{3} & \frac{2}{3} & 0 \\ 0 & 1 & 2 & \frac{4}{3} & -\frac{1}{3} & 0 \\ 0 & 0 & -5 & -2 & 0 & 1 \end{array}\right)$$

$$R_3 = R_3 \cdot \frac{-1}{5}$$

$$A^{-1} = \left(\begin{array}{ccc|ccc} 1 & 0 & -1 & -\frac{5}{3} & \frac{2}{3} & 0 \\ 0 & 1 & 2 & \frac{4}{3} & -\frac{1}{3} & 0 \\ 0 & 0 & 1 & \frac{2}{5} & 0 & -\frac{1}{5} \end{array}\right)$$

$$R_2 = R_2 - 2R_3$$

$$A^{-1} = \left(\begin{array}{ccc|ccc} 1 & 0 & -1 & -\frac{5}{3} & \frac{2}{3} & 0 \\ 0 & 1 & 0 & \frac{8}{15} & -\frac{1}{3} & \frac{2}{5} \\ 0 & 0 & 1 & \frac{2}{5} & 0 & -\frac{1}{5} \end{array}\right)$$

$$R_1 = R_1 + R_3$$

$$A^{-1} = \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -\frac{19}{15} & \frac{2}{3} & -\frac{1}{5} \\ 0 & 1 & 0 & \frac{8}{15} & -\frac{1}{3} & \frac{2}{5} \\ 0 & 0 & 1 & \frac{2}{5} & 0 & -\frac{1}{5} \end{array}\right)$$

$$\therefore$$

$$A^{-1} = \begin{pmatrix} -\frac{19}{15} & \frac{2}{3} & -\frac{1}{5} \\ \frac{8}{15} & -\frac{1}{3} & \frac{2}{5} \\ \frac{2}{5} & 0 & -\frac{1}{5} \end{pmatrix}$$

2.3.5. Determinantes.

Se define como la asignación de un número escalar a una matriz cuadrada.
Veamos como se calcula el determinante de una matriz 2x2.
Sea A la matriz.

$$A = \begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix}$$

Para calcular su determinante, multiplicamos la diagonal que empieza de la parte superior izquierda y le restamos la multiplicación de la diagonal superior derecha.

$$|A| = \begin{vmatrix} 3 & 2 \\ 2 & 3 \end{vmatrix}$$

$$|A| = \begin{vmatrix} 5 \end{vmatrix}$$

Ahora veremos como obtener el determinante de una matriz 3x3.

$$A = \begin{pmatrix} 3 & 2 & 1 \\ 1 & 2 & 4 \\ 5 & 7 & 6 \end{pmatrix}$$

El proceso es similar al determinante 2x2, con la diferencia que ahora se requiere de 3 multiplicaciones, para ello, las dos primeras filas de la matriz las duplicamos debajo de la última. Procedemos con la multiplicación de la diagonal que empieza en la parte superior izquierda, después le sumamos la multiplicación de la diagonal que se encuentra un renglón abajo de la primera y repetimos este proceso una vez más. Ahora le restamos la multiplicación de la diagonal superior derecha sumada con la multiplicación de las diagonales que se encuentran 1 y 2 filas más abajo respectivamente.

$$|A| = \begin{vmatrix} 3 & 2 & 1 \\ 1 & 2 & 4 \\ 5 & 7 & 6 \end{vmatrix}$$

$$|A| = \begin{vmatrix} 3 & 2 & 1 \\ 1 & 2 & 4 \\ 5 & 7 & 6 \\ 3 & 2 & 1 \\ 1 & 2 & 4 \end{vmatrix}$$

Para explicarlo mejor, las operaciones a realizar quedan:
$(3 \cdot 2 \cdot 6) + (1 \cdot 7 \cdot 1) + (5 \cdot 2 \cdot 4) - (1 \cdot 2 \cdot 5) - (4 \cdot 7 \cdot 3) - (6 \cdot 2 \cdot 1)$

$$|A| = \begin{vmatrix} -23 \end{vmatrix}$$

2.4. Álgebra de boole.

De este tema , lo que necesitamos saber es acerca de las compuertas lógicas, las cuales trabajan con estados lógicos (0,1). Lo único que presentaremos son las tablas de verdad de cada una de ellas.

AND		
A	B	Salida
0	0	0
0	1	0
1	0	0
1	1	1

OR		
A	B	Salida
0	0	0
0	1	1
1	0	1
1	1	1

NAND		
A	B	Salida
0	0	1
0	1	1
1	0	1
1	1	0

NOR		
A	B	Salida
0	0	1
0	1	0
1	0	0
1	1	0

XOR		
A	B	Salida
0	0	0
0	1	1
1	0	1
1	1	0

XNOR		
A	B	Salida
0	0	1
0	1	0
1	0	0
1	1	1

YES	
A	Salida
0	0
1	1

NOT	
A	Salida
0	1
1	0

La compuerta lógica que utilizaremos será la compuerta XOR, aunque también es bueno conocer las tablas de verdad de las demás compuertas.

3. Criptografía clásica

Los métodos para hacer que los mensajes sean ocultos a los enemigos han sido importantes a través de la historia. En la presente sección serán presentados algunos de estas técnicas utilizadas, dichas técnicas son muy vulnerables para ser usadas actualmente, en especial con el poder actual de las computadoras, y en un futuro, los métodos mas utilizados también serán vulnerables pero otros nuevos surgirán.

Antes de empezar, es necesario hacer algunas aclaraciones pertinentes:

- *plaintext* será escrito en **minúsculas** mientras que el *ciphertext* se escribirá en **mayúsculas**.
- A las letras del alfabeto se le asignará un número.

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

Notas. Aunque algunas personas empiezan a enumerar desde 1, por convención se empieza con a = 0 y así sucesivamente, si el alfabeto contiene N caracteres el último caracter le correspondería el número N-1.
Dependiendo del alfabeto en que se trabaje, serán los caracteres utilizados, en español son 27 mientras que en inglés los caracteres utilizados son 26, el número total de caracteres a utilizar se le conoce como ***anillo***.

- Los espacios y signos de puntuación son omitidos, esto es porque si los espacios se dejan en el mensaje habría dos posibilidades, la primera de ellas es que se mostraría información de la estructura del mensaje mientras que por otro lado a través del conteo de la frecuencia, simplificaría el proceso de descifrado.

3.1. Cifrado de Cesar.

Es un tipo de cifrado por sustitución en el que una letra en el texto original es reemplazada por otra letra que se encuentra un número fijo de posiciones, en el caso de este cifrado el corrimiento es de **3** posiciones. Por ejemplo a la letra **a** se le asigna la letra **d**.Este cifrado trabaja con aritmética modular, lo esencial es conocer como calcular el inverso aditivo de un número. (sección 2.1.1)

Una vez familiarizado con aritmética modular, suponga que los ejemplos presentados se trabajaran en el alfabeto inglés (26 caracteres). La función de cifrado corresponde a:

$$C = (p + 3) \ mod \ 26$$

Para poder descifrar el mensaje, es importante calcular el inverso aditivo de 3, en este caso corresponde al numero 23, la función de descifrado queda de la siguiente manera:

$$p = (C + 23) \ mod \ 26$$

Ejemplo:

$$C(r) = (17 + 3) \ mod \ 26 = 20 = U$$
$$p(U) = (20 + 23) \ mod \ 26 = 17 = r$$

3.2. Shift Cipher.

Al igual que el cifrado de Cesar, es un cifrado por sustitución mono alfabética, debido a que una letra A es siempre reemplazada por una letra B. La diferencia con el cifrado del Cesar, es que el corrimiento puede variar, en vez de hacer el corrimiento de 3 posiciones, tenemos 26 posibles desplazamientos (0 al 25). A este nuevo valor le llamaremos K

La función de descifrado corresponde a:

$$C = (p + K) \ mod \ 26$$

Mientras que para descifrar, recordar que debemos de encontrar el inverso aditivo de K, representado como K', esta función de descifrado ahora es:

$$p = (C + K') \ mod \ 26$$

Nota. No es recomendable usar un corrimiento de 0 , debido a que no se modificaría nada, y el plaintext sería igual que al ciphertext.Ahora veremos unos ejemplos.

K = 0; K'=26

$$C(r) = (17 + 0) \ mod \ 26 = 17 = R$$
$$p(R) = (17 + 26) \ mod \ 26 = 17 = r$$

K = 18; K'=8

$$C(r) = (17 + 18) \ mod \ 26 = 9 = J$$
$$p(J) = (9 + 8) \ mod \ 26 = 17 = r$$

3.3. Affine Cipher.

El cifrado anterior puede ser generalizado y ligeramente más seguro de la siguiente manera. Se escogen dos enteros α y β, recordando que se está trabajando en el alfabeto inglés(N=26 caracteres), α debe de cumplir la condición de que el Máximo Común Divisor MCD (α, N) = 1, la función de cifrado es de la siguiente manera:

$$C = (\alpha p + \beta) \ mod \ 26$$

Ahora para poder encontrar la función de descifrado, es necesario encontrar el inverso de α, que, como se puede ver, sería encontrar el inverso multiplicativo (sección 2.1.2), mientras que para β corresponde al inverso aditivo. Una vez teniendo en cuanta esto, y despejando a **p** de la función de cifrado, la función de descifrado queda de la siguiente manera:

$$p = \alpha'(C + \beta') \ mod \ 26$$

¿Por qué es importante que el MCD(α, N) = 1?

Utilicemos un $\alpha = 2$ y β=1

$$C(c) = (2(2) + 1) \ mod \ 26 = 5 = F$$
$$C(p) = (15(2) + 1) \ mod \ 26 = 5 = F$$
$$C(t) = (19(2) + 1) \ mod \ 26 = 13 = N$$
$$C(g) = (6(2) + 1) \ mod \ 26 = 13 = N$$

Como se puede ver, dos letras diferentes nos llevan a un mismo resultado, si se quiere descifrar, el primer problema al que nos enfrentamos es que no existe el inverso multiplicativo de 2, si de todos modos queremos utilizar una división, que como sabríamos estaría mal implementado, cuando descifremos la letra N, ¿Qué letra le correspondería en el plaintext, t o g ?

Es por ello que para α se utiliza un entero que cumpla con la condición antes mencionada, ahora para poder visualizarlo utilicemos el mismo $\beta = 1$, pero un $\alpha = 3$

$$C(c) = (2(3) + 1) \ mod \ 26 = 7 = H$$

$$C(p) = (15(3) + 1) \ mod \ 26 = 20 = U$$

Como se puede ver, dos letras que antes nos llevaban a una misma letra, ahora nos dan resultados diferentes. Y aquí si existe el inverso de α el cual es 9, y para β ' = 25 .Ocupando la función de descifrado:

$$p(H) = 9(7 + 25) \ mod \ 26$$

Aplicando la multiplicación y el módulo respectivamente a β ':
9*25 mod 26 = 17
La ecuación podría verse de la siguiente:

$$p(H) = (9(7) + 17) \ mod \ 26 = 2 = c$$

$$p(U) = (9(20) + 17) \ mod \ 26 = 15 = p$$

¿Cuántos posibles α, son los que puedo escoger ?
Existe una fórmula para determinar cuantos α son los que cumplen la condición antes mencionada, la cual se presenta a continuación.

$$\phi(n) = p(1 - \frac{1}{p})$$

donde p son los números primos que componen a n.

Por ejemplo, supongamos que estamos trabajando con un alfabeto de solo 12 caracteres.

$$\phi(12) = \phi(2^2 * 3) = 2^2 * 3(1 - \frac{1}{2})(1 - \frac{1}{3})$$

$$\phi(12) = 2 * 2 * 3(\frac{1}{2})(\frac{2}{3})$$

$$\phi(12) = 2(2)$$

$$\phi(12) = 4$$

Esto significa que cuatro números son los que cumplen la condición para N = 12, los α que cumplen la condición son: $\alpha = 1, 5, 7, 11$

Nota. Un método para conocer si se cumple la condición de que el MCD de dos números sea 1 y la manera de encontrar el inverso multiplicativo de un número sin hacerlo a la fuerza bruta se presentan en las secciones 2.2.1 y 2.2.2

3.4. Vigenere Cipher.

A diferencia de los métodos anteriores, este cifrado es considerado de sustitución poli alfabético, al contrario que los cifrados anteriores que eran mono alfabéticos, cada carácter a cifrar NO siempre se sustituye por el mismo carácter en el texto cifrado, es decir, es un sistema en el que hay implicados varios alfabetos y dependiendo de ciertas circunstancias se aplica uno u otro.

Es considerado un cifrado simétrico, debido a que tanto el receptor y el emisor deben de usar la misma clave tanto para descifrar como cifrar respectivamente.

Para poder utilizar, este cifrado se debe de hacer uso de una tabla como la que se muestra a continuación.

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

Figura 2: Tabla de Vigenere alfabeto inglés.

¿Cómo cifrar y descifrar?

Suponga que:

plaintext: holamundo

clave: luis

Para cifrar, lo primero que debemos de hacer es poner la clave de bajo de del plaintext, repitiendo la clave tantas veces como haga falta.

h	o	l	a	m	u	n	d	o
l	u	i	s	l	u	i	s	l

Una vez teniendo esto, buscamos en la tabla anterior la intersección entre la letra del plaintext y la letra de la clave, las filas corresponden al plaintext mientras que las columnas a la clave. Para cifrar la letra **h** del ejemplo, se hace de la siguiente manera.

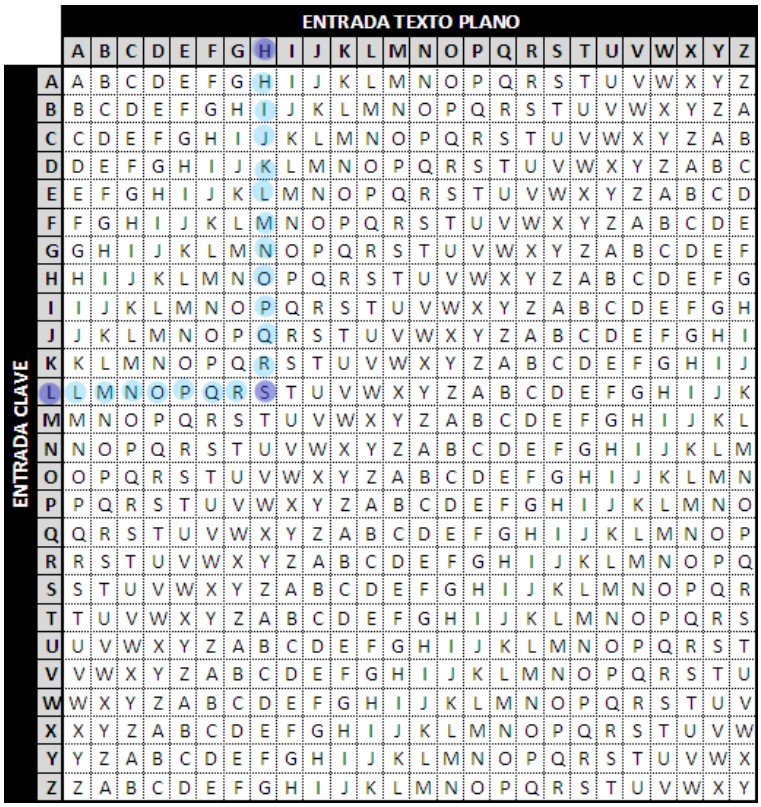


Figura 3: Ejemplo de cifrado.

Como se puede ver, en este caso, la letra **h** se sustituye por la letra **s**,y así repetimos este procedimiento hasta acabar con el plaintext. Para este ejemplo, **el texto cifrado sería: SITSXOVVZ**

Para descifrar, nos posicionamos en la letra correspondiente a la clave, una vez ahí, buscamos horizontalmente dónde está la letra correspondiente al ciphertext, y solo nos queda recorrer hacía arriba para encontrar la letra del plaintext.

Como se pudo ver, no es complicado utilizar este tipo de cifrado, pero ahora supongamos que se ha cifrado un mensaje utilizando este método y que lo interceptamos, **¿Es posible descifrarlo sin conocer la clave?**.
La respuesta es sí, siempre y cuando el mensaje sea suficientemente largo para poder hacer el criptoanálisis correspondiente, dicho método se presenta a continuación.

Para poder desarrollar este método, supongamos que se intercepto el siguiente mensaje:
ttjyyrvpzjzjzfhioomptbbnfgohtjzvtucxtbvrotjpwcrqjzzeokzpwwasfbyerwmpmsvyeway
woihdkziewiigsmoysrcziricsolpgjqpciihodxtbbjzfhimsxefgzapkzvpxpweydhdkciykzj
pzgmyzjzpbjxvbjatbbasoomekvwtkdpwbjxrwqijcpyahcmdhdqprvvwwikuinxvwnwxsnpz
ktsffcilfomdogptcrrlbymymjycstidmjylfzlzzymyuhmys

1.- Lo primero que tenemos que hacer, es tratar de encontrar la longitud de la clave con la que fue cifrado el mensaje, para ello, debemos de buscar en el texto secuencia de letras que se repiten.

ttjyyrvpzjzjzfhioomptbbnfgohtjzvtucxtbvrotjpwcrqjzzeo kz p ww asfbyerwmpmsvyeway
woihdkziew ii gsmoysrcziricsolpgjqpc ii hodxtbbjzfhimsxefgzap kz vpxpweydhdkciy kz j
pzgmyzjzpbjxvbjatbbasoomekvwtkdpwbjxrwqijcpyahcmdhdqprvv ww ikuinxvwnwxsnpz
ktsffcilfomdogptcrrlbymymjycstidmjylfzlzzymyuhmys

Ahora lo que debemos de hacer es contar la distancia entre estas letras repetidas, y obtener el máximo común divisor.
kz : 80, 16
ww : 152
ii : 24
MCD(80, 16, 152, 24) : 4

Esto quiere decir que la longitud más probable de la palabra clave con la que fue cifrada, es de 4 caracteres.

2.- Una vez sabemos cual es la longitud de la cadena, lo que sigue es dividir el criptograma(ciphertext) en K subcriptogramas, (para este caso es 4 subcriptogramas, debido a que la longitud es 4), una vez realizado esto, estaríamos en posición de poder realizar un ataque simple de tipo estadístico. Cuando tengamos los K subcriptogramas, de cada subcriptograma hacemos una tabla de frecuencia con el número de veces que cierta letra apareció en dicho subcriptograma.
Para dividir el criptograma en 4 subcriptogramas, lo que consiste es numerar cada letra del 1 al 4, (marcar con 4 colores diferentes o como el lector prefiera, pero identificando siempre 4 grupos), repitiendo el proceso hasta terminar el criptograma, de ahí, para el subcriptograma 1, agrupamos todas aquellas letras que tengan el número 1, y se repite el proceso para obtener los K subcriptogramas.

Los cuatro subcriptogramas correspondientes al ejemplo, son:

C_1	tyzzotftttowjowfrmewdegyzcpphtzmfppedypypvtsetwrjadpwuvxzfldtlycdlzyy
C_2	trjfobgjubtczkwbwswokwssisgcobfsgkxykkzzbbbokkbwchhrwiwskffocbmsmfzus
C_3	jvzhmbozcvjrzzaymvaizimrrojidbhxzzpdczgjjjbovdjqpcdvinnntcogryjtjzyh
C_4	ypjipnhvxrpqepsepyyhiiocilqixjieavwhijmzxaamwpxiymqvkxwpsimprmyiylmm

Ahora haciendo la tabla de frecuencia correspondiente a cada subcriptograma, tenemos:

	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
C_1	1	0	2	5	4	4	1	1	0	2	0	3	2	0	3	7	0	2	1	9	1	2	5	1	7	6
C_2	0	9	4	0	0	5	3	2	2	2	8	0	2	0	5	0	0	2	8	2	2	0	7	1	1	4
C_3	2	3	4	4	0	0	2	3	4	9	0	0	3	3	4	2	1	4	0	2	0	5	0	1	3	9
C_4	3	0	1	0	3	0	0	3	10	3	1	2	7	1	1	8	3	2	2	0	0	3	3	5	6	1

Figura 4: Tabla de frecuencias.

Como se mencionó, es importante conocer el idioma en el que se está trabajando, al inicio del documento se dijo que los ejemplos corresponden al idioma inglés, está información es de gran importancia debido a que para poder realizar el ataque, debemos de saber cuales son las letras que aparecen con mayor frecuencia en cada idioma, para el caso del idioma inglés las letras más repetidas son: **a, e, o, t**.

Para realizar el ataque, nos posicionamos en la tabla de la figura anterior, en esas 4 letras, sumamos cada frecuencia y el resultado lo ponemos en una nueva tabla empezando por la letra **a**, posteriormente, nos recorremos una posición a la derecha de las 4 letras mencionadas y repetimos el procedimiento colocando el resultado en la letra **b**, y así sucesivamente hasta llenar la tabla con los 4 subcriptogramas, es importante recordar que estamos trabajando con aritmética modular, por lo cual cuando lleguemos a la letra z, el siguiente corrimiento será hacia la letra a.
Esta nueva tabla corresponde a:

	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
C_1	17	8	8	14	8	16	10	8	5	7	11	17	9	6	8	19	6	7	12	15	11	14	16	4	14	15
C_2	7	21	12	14	8	13	20	7	18	11	18	5	12	10	20	9	9	15	20	10	8	14	12	15	12	17
C_3	8	7	15	11	9	16	15	9	14	20	12	6	8	13	11	12	14	13	4	10	10	22	8	9	15	17
C_4	7	1	5	7	19	10	3	9	18	6	3	14	11	4	7	19	7	7	8	13	8	6	15	9	10	4

Figura 5: Tabla de frecuencias.

Las letras con color morado son las letras que mayor se repiten, mientras que las azules son las siguientes más repetidas, una vez esto de cada subcriptograma seleccionamos una letra y trataremos de encontrar la llave, cabe recalcar que la llave tiene una alta probabilidad de ser una palabra perteneciente al idioma, por lo cual, la llave para este ejemplo es: **love**.

Ahora que ya conocemos la llave, todavía nos queda descifrar el mensaje, este método de descifrado, puede parecer tedioso, pero es muy sencillo, y con la tecnología de ahora, puede hacerse uso de ella para reducir el tiempo de descifrado.

Una vez hecho el proceso de descifrado correspondiente, el plaintext es:

Ifoundaloveformedarlingjustdiverightinandfollowmyleadwellifoundagirlbeautifulandsweet ineverknewyouwerethesomeonewaitingformebecausewewerejustkidswhenwefellinlovenot knowingwhatitwasiwillnotgiveyouupthistimedarlingjustkissmeslowyourheartisall iownandinyoureyesyouareholdingmine

Finalmente haciendo el mensaje mas claro:

I found a love for me darling just dive right in and follow my lead well i found a girl beautiful and sweet i never knew you were the someone waiting for me because we were just kids when we fell in love not knowing what it was i will not give you up this time darling just kiss me slow your heart is all i own and in your eyes you are holding mine

Nota. A pesar de que el cifrado de Vigenere es poli alfabético, éste también puede ser representado mediante una fórmula, tanto para cifrar como descifrar. Dichas fórmulas son:

$$C_i = (p_i + k_i) \ mod \ 26$$
$$p_i = (C_i + k_i') \ mod \ 26$$

Donde:
C_i es el i-ésimo carácter del ciphertext.
p_i es el i-ésimo carácter del plaintext
k_i es el i-ésimo carácter de la clave/llave utilizada.
k' es el inverso aditivo de k.
26 es el anillo de nuestro alfabeto (inglés).

3.5. Otros cifrados.

Ahora veremos otros cifrados clásicos, cómo se hacía para cifrar y descifrar utilizando dichos métodos.

3.5.1. Kama-sutra Cipher.

Es un cifrado de sustitución utilizado aproximadamente en el siglo 4. El kama-sutra recomienda que las mujeres deben de estudiar 64 artes incluyendo cocina, masajes, entre otros, la lista también incluye algunas artes menos obvias como ajedrez, carpintería. El número 45 en la lista es **mlecchita-vikalpa**, el cual es el arte de la escritura secreta. La técnica consistía en emparejar las letras de manera aleatoria, por ejemplo:

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

Supongamos que se quiere cifrar la palabra *cryptography*, utilizando este método, buscando en la tabla, la letra C, vemos que le corresponde la letra P, para la letra R, en la tabla está emparejado con la letra O. Siguiendo este proceso el cifrado quedaría de la siguiente manera:

PODCQRXOSCBD

Para descifra es exactamente lo mismo pero ahora con el ciphertext, buscando la letra P en la tabla, observamos que tiene la letra c, y así sucesivamente hasta encontrar el plaintext.

3.5.2. Pig pen Cipher.

Cifrado utilizado en el siglo 18, este cifrado no sustituye una letra por otra, más bien sustituye una letra por un símbolo. El alfabeto es escrito como en la siguiente figura, y cada letra es cifrada reemplazándola por el símbolo correspondiente a la porción del pig pen que contiene dicha letra.

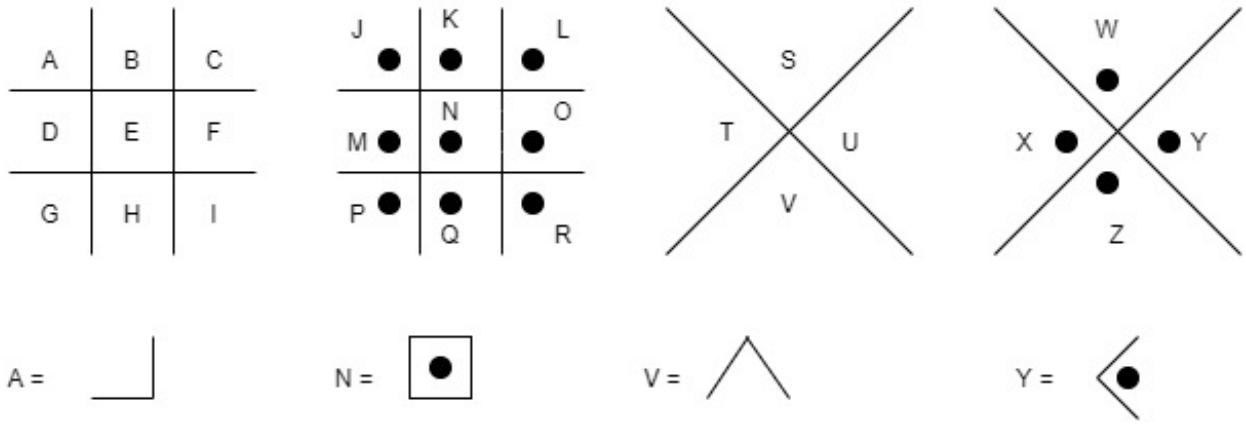


Figura 6: Pig pen cipher.

3.5.3. Atbash Cipher.

Este cifrado es muy similar al kama-sutra cipher, solo que en vez de ordenar las letras de forma aleatoria, se invierte el alfabeto y se hacen los pares, por ejemplo a = Z, b = Y, c = X, ... , y así sucesivamente, la tabla correspondiente para este cifrado es la siguiente.

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

Al igual que en el cifrado de kama-sutra solo se tiene que buscar la letra en la tabla y sustituirla por su correspondiente par, tanto para cifrar como para descifrar.

3.5.4. Rail Fence Cipher.

Este cifrado no sustituye una letra por otra, utiliza las mismas letras que el mensaje original, solo que las va alternando y separando en nuevas lineas.
Primero se selecciona un número N, cuyo número será las líneas a utilizar, la primera letra va en la primera línea, la segunda letra en la segunda línea y volvemos a repetir hasta que ya no haya letras. Para cifrar lo único que queda es escribir la primera línea seguida de la segunda y así sucesivamente. Por ejemplo, se utiliza un $\mathbf{N = 3}$ con la palabra *cryptography*.

c p g p
r t r h
y o a y

Ciphertext = CPGPRTRHYOAY

Una vez teniendo el texto cifrado se debe de contar la cantidad de letras y dividirlas entre N, una vez llegado a este punto ahora en vez de escribir linea por linea se tiene que escribir de arriba a abajo de derecha a izquierda.

Ciphertext = CPGPRTRHYOAY, longitud = 12, N = 3
C P G P
R T R H
Y O A Y
Plaintext = cryptography

4. Cifrados por bloques

En los cifrados de sustitución mono alfabética, si se cambia una letra en el plaintext, exactamente una letra cambiaba en el ciphertext, esto hacia más fácil encontrar la llave a través de un análisis de frecuencia.

En el cifrado de Vigenere, el uso de un bloque de letras correspondiente a la longitud de la llave, dificultaba el análisis de frecuencia, pero como vimos, a pesar de que es un método bastante tedioso, en especial si se hace de forma manual, fue posible descifrar el mensaje.

Los cifrados por bloques evitan estos problemas, encriptando un bloque de letras simultáneamente. Un cambio de un carácter en el bloque del plaintext deberá cambiar potencialmente todos los caracteres en el bloque correspondiente que se está cifrando.

Una manera mejor de ilustrar este procedimiento es:

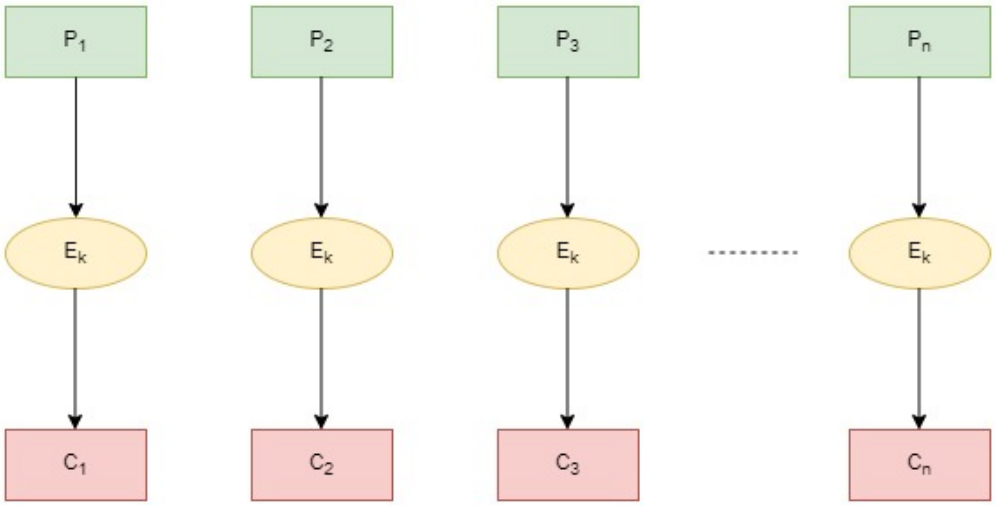


Figura 7: Cifrado por bloques.

4.1. Hill Cipher.

Inventado en 1929 por Lester Hill. Este cifrado fue el primero en utilizar métodos algebraicos en criptografía.
Por ejemplo en el caso de Vigenere se mostró la fórmula por la cual puede ser representado el cifrado o descifrado, en aquel tiempo no se veía así, es por ello que se presentó el uso de la tabla. Para este cifrado es importante tener conocimientos en álgebra lineal, sino se tiene, revise la sección 2.3

Para poder hacer el cifrado

- Primero seleccionamos un número **m** y hacemos una matriz **K** de dimensiones **mxm**.
- La llave que ocuparemos es una palabra que contenga **mxm** caracteres.
- El mensaje es escrito como una serie de filas, para ello, de cada letra obtenemos su valor numérico como en los cifrados clásicos, está será nuestra matriz p.
- El cifrado es sólo una multiplicación de la matriz del texto plano con la matriz de la llave y puede representarse como:

  $$C = (p * K) \ mod \ n$$

  Donde n es el anillo del alfabeto en el que estamos trabajando.
- Para poder descifrar el mensaje, necesitamos obtener la matriz inversa de K.

  $$p = (C * K^{-1}) \ mod \ n$$

Nota. Para que k^{-1} exista el MCD(determinante(k), n) = 1

Supongamos que tenemos la siguiente llave.

$$K = \begin{pmatrix} 9 & 13 \\ 2 & 3 \end{pmatrix}$$

y el plaintext es luis, por lo cual el ciphertext sería:

$$p \cdot K = \begin{pmatrix} 11 & 20 \\ 8 & 18 \end{pmatrix} \cdot \begin{pmatrix} 9 & 13 \\ 2 & 3 \end{pmatrix} = \begin{pmatrix} 139 & 203 \\ 108 & 158 \end{pmatrix}$$

aplicando el módulo correspondiente al alfabeto inglés.

$$C = \begin{pmatrix} 9 & 21 \\ 4 & 2 \end{pmatrix}$$

Esta llave fue escogida, debido a que cumple la condición para tener inversa, si calculamos la matriz inversa sin aritmética modular tendríamos:

$$K^{-1} = \begin{pmatrix} 3 & -13 \\ -2 & 9 \end{pmatrix}$$

Recuerde que en aritmética modular no existen los números negativos, por lo cual la nueva matriz será:

$$K^{-1} = \begin{pmatrix} 3 & 13 \\ 24 & 9 \end{pmatrix}$$

Ahora para descifrar, ya tenemos los elementos, solo nos queda aplicar la fórmula descrita con anterioridad.

$$C \cdot K^{-1} = \begin{pmatrix} 9 & 21 \\ 4 & 2 \end{pmatrix} \cdot \begin{pmatrix} 3 & 13 \\ 24 & 9 \end{pmatrix} = \begin{pmatrix} 531 & 306 \\ 60 & 70 \end{pmatrix}$$

Nuevamente aplicamos, el modulo correspondiente.

$$p = \begin{pmatrix} 11 & 20 \\ 8 & 18 \end{pmatrix}$$

Nota. Si quiere saber cómo obtener la matriz inversa o calcular el determinante de una matriz revise las secciones 2.3.4 y 2.3.5 respectivamente.

4.2. Modos de operación

Un cifrado por bloques sólo permite cifrar texto de una longitud igual a la del bloque que tiene definido. Los bloques generalmente no se concatenan uno detrás de otro tal cual, sino que mezclan utilizando lo que se llama modos de operación. Esta característica aplica unicamente a los algoritmos de cifrado por bloques y es sumamente importante para mantener la seguridad de la clave.

Estos cifrados pueden tener diferentes modos de operación permitiendo a los usuarios escoger el modo adecuado de acuerdo a los requerimientos de la aplicación. En este documento se mostrarán 4 de los 5 modos de operación más comunes. Para mostrar los ejemplos correspondientes, el plaintext para todos los modos será:

p_1			p_2		
10	50	9	10	50	9
p_3			p_4		
10	50	9	10	50	9

La llave a utilizar es:

$$E_k = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix}$$

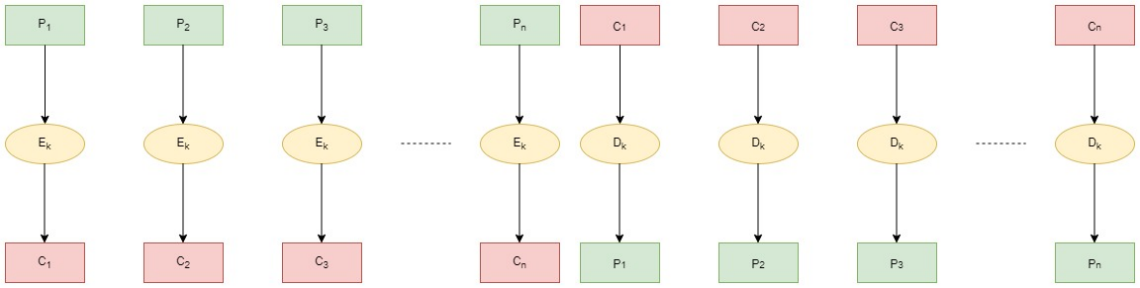
En algunos modos, se requiere de un vector inicial, el cual será:

IV		
9	99	11

Finalmente, cabe aclarar que, el anillo en esta ocasión será **256**.

4.2.1. Electronic CodeBook (ECB)

Los modelos correspondientes para cifrar y descifrar un bloque de información con este modo de operación corresponden a las siguientes figuras.



(a) ECB cifrado (b) ECB descifrado

Figura 8: Electronic CodeBook

Si prestamos atención al diagrama del cifrado, la ecuación que lo describe es:

$$C_1 = E_k \cdot P_1$$

$$C_2 = E_k \cdot P_2$$

$$\therefore \ para \ el \ n-esimo \ bloque$$

$$C_n = E_k \cdot P_n$$

La ecuación correspondiente al descifrado es:

$$P_1 = D_k \cdot C_1$$

$$P_2 = D_k \cdot C_2$$

$$\therefore \ para \ el \ n-esimo \ bloque$$

$$P_n = D_k \cdot P_n$$

Siguiendo el diagrama y con las formula correspondiente, el proceso para cifrar el cualquier bloque es el mismo, y en este caso como los cuatro plaintext son los mismos, nada requerimos hacer el proceso de uno, para encontrar los cuatro.
Este proceso requiere de la multiplicación de la llave con el bloque del plaintext que se quiere cifrar.

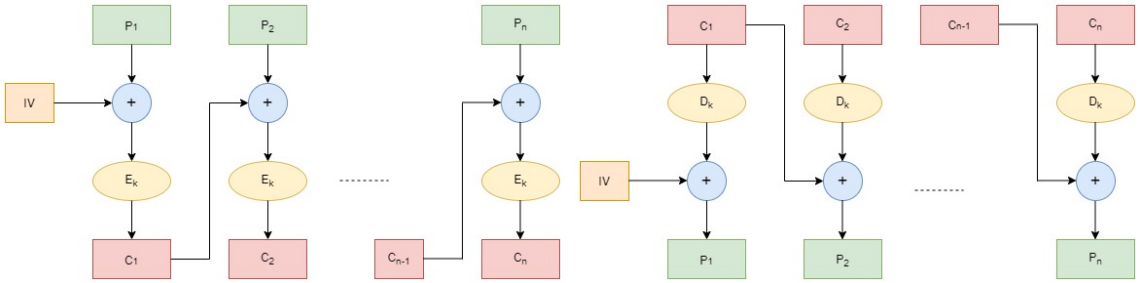
$$P_1 \cdot E_k = \begin{pmatrix} 10 & 50 & 9 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix} = \begin{pmatrix} 309 & 351 & 402 \end{pmatrix}$$

Si le aplicamos el modulo 256, obtenemos:

$$C_1 = \begin{pmatrix} 53 & 95 & 146 \end{pmatrix}$$

4.2.2. Cipher Block Chaining (CBC)

A continuación veremos el siguiente modo de operación, los diagramas que describen su funcionamiento, las respectivas fórmulas de cifrado y descifrado y un ejemplo de como se desarrolla.



(a) CBC cifrado (b) CBC descifrado

Figura 9: Cipher Block Chaining

Poniendo atención en el diagrama, para el primer bloque, primero hacemos la compuerta xor entre el vector inicial con el primer bloque del plaintext, (si desea revisar el tema de álgebra de boole revise la sección 2.4), teniendo el resultado, obtenemos su valor decimal y lo multiplicamos con la llave de cifrado.

$$C_1 = E_k \cdot (IV \oplus P_1)$$

$$C_2 = E_k \cdot (C_1 \oplus P_2)$$

$$\therefore$$

$$C_n = E_k \cdot (C_{n-1} \oplus P_n)$$

Ahora analizando el diagrama del descifrado, tenemos:

$$P_1 = IV \oplus (D_K \cdot C_1)$$

$$P_2 = C_1 \oplus (D_K \cdot C_2)$$

$$\therefore$$

$$P_n = C_{n-1} \oplus (D_K \cdot C_n)$$

Como se puede ver, para poder cifrar el bloque 2, se requiere haber cifrado con anterioridad el bloque 1, no es como el modo anterior que se cifraba de manera independiente. Veamos el procedimiento para cifrar el bloque 1.

$$IV = \begin{pmatrix} 9 & 99 & 11 \end{pmatrix}$$

Lo primero que indica la formula es hacer la compuerta lógica XOR del vector inicial con P_1, para ello, de cada uno de los valores pasamos del sistema decimal al sistema binario y hacemos la operación correspondiente.

$$9 : 1001$$

$$99 : 1100011$$

$$11 : 1011$$

$$10 : 1010$$

$$50 : 110010$$

$$9 : 1001$$

Haciendo las operaciones, tenemos:

$$1001 \oplus 1010 = 0011$$

$$1100011 \oplus 110010 = 1010001$$

$$1011 \oplus 1001 = 0010$$

Ahora estos valores, obtenemos su valor decimal y lo multiplicamos con la llave.

$$IV \oplus P_1 = \begin{pmatrix} 3 & 81 & 2 \end{pmatrix}$$

$$(IV \oplus P_1) \cdot E_k = \begin{pmatrix} 3 & 81 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix} = \begin{pmatrix} 349 & 429 & 511 \end{pmatrix}$$

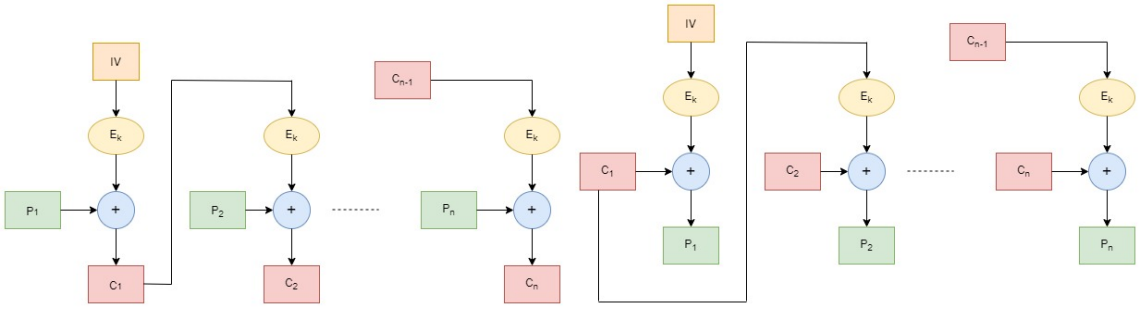
Aplicando el modulo ...

$$C_1 = \begin{pmatrix} 93 & 173 & 255 \end{pmatrix}$$

Así es como se cifra un bloque, lo que sigue es repetir el procedimiento para cifrar los demás bloques, tomando como guía la formula de cifrado.

4.2.3. Cipher Feedback (CFB)

Al igual que con los dos modos anteriores, veremos los diagramas correspondientes, sus fórmulas y un ejemplo de cifrado.



(a) CFB cifrado (b) CFB descifrado

Figura 10: Cipher Feedback

Mirando la secuencia del diagrama, para cifrar tenemos:

$$C_1 = (E_k \cdot IV) \oplus P_1$$

$$C_2 = (E_k \cdot C_1) \oplus P_2$$

$$\therefore$$

$$C_n = (E_k \cdot C_{n-1}) \oplus P_n$$

Ahora, para descifrar tenemos ...

$$P_1 = (E_k \cdot IV) \oplus C_1$$

$$P_2 = (E_k \cdot C_1) \oplus C_2$$

$$\therefore$$

$$P_n = (E_k \cdot C_{n-1}) \oplus C_n$$

Una particularidad es que para cifrar como para descifrar, hacemos uso de E_k.

Veamos como es el procedimiento para cifrar el primer bloque.

$$IV \cdot E_k = \begin{pmatrix} 9 & 99 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix} = \begin{pmatrix} 526 & 612 & 709 \end{pmatrix}$$

Aplicando el modulo 256, tenemos

$$IV \cdot E_k = \begin{pmatrix} 14 & 100 & 197 \end{pmatrix}$$

Ahora a estos valores, al igual que los valores del bloque 1 del plaintext, pasamos a trabajar con el sistema binario.

$$14 : 1110$$

$$100 : 1100100$$

$$197 : 11000101$$

$$10 : 1010$$

$$50 : 110010$$

$$9 : 1001$$

Solo nos queda realizar la compuerta XOR con los valores de P_1:

$$1110 \oplus 1010 = 0100$$

$$1100100 \oplus 110010 = 1010110$$

$$11000101 \oplus 1001 = 11001100$$

Pasando al sistema decimal...

$$0100 = 4$$

$$1010110 = 86$$

$$11001100 = 204$$

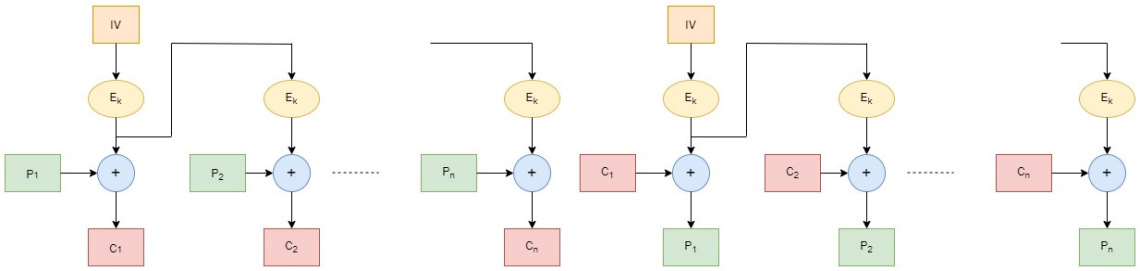
Finalmente tenemos que:

$$C_1 = \begin{pmatrix} 4 & 86 & 204 \end{pmatrix}$$

Este fue el procedimiento de como realizar el cifrado para un bloque, solo nos queda repetir el procedimiento tomando como guía la formula descrita de cifrado para este modo de operación.

4.2.4. Output Feedback (OFB)

El último modo de operación que veremos, los diagramas correspondientes, son:



(a) OFB cifrado (b) OFB descifrado

Figura 11: Output Feedback

Analizando el diagrama...

$$C_1 = (E_k \cdot IV) \oplus P_1 = O_1(IV) \oplus P_1$$

$$C_2 = (E_k \cdot (E_k \cdot IV)) \oplus P_2 = O_2(IV) \oplus P_2$$

$$\therefore$$

$$C_n = O_n(IV) \oplus P_n$$

Ahora para descifrar...

$$P_1 = (E_k \cdot IV) \oplus C_1 = O_1(IV) \oplus C_1$$

$$P_2 = (E_k \cdot (E_k \cdot IV)) \oplus C_2 = O_2(IV) \oplus C_2$$

$$\therefore$$

$$P_n = O_n(IV) \oplus C_n$$

Al igual que el modo anterior, solo se requiere la llave de cifrado para el proceso de cifrado y descifrado.

Si ponemos atención debido a que el vector inicial y el plaintext es el mismo para todos los modos de operación, para el bloque 1 de este modo es el mismo que el bloque 1 del modo Cipher Feedback, ya a que se realizan las mismas operaciones, cambia a partir del bloque 2.

Como en el cifrado del bloque 1, el resultado de multiplicar la llave por el vector inicial fue:

$$IV \cdot E_k = \begin{pmatrix} 14 & 100 & 197 \end{pmatrix}$$

Volviendo a multiplicar por la llave, tenemos:

$$(E_k \cdot (E_k \cdot IV)) = \begin{pmatrix} 14 & 100 & 197 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix} = \begin{pmatrix} 2581 & 2301 & 2218 \end{pmatrix}$$

Aplicando el módulo 256...

$$(E_k \cdot (E_k \cdot IV)) = \begin{pmatrix} 21 & 253 & 170 \end{pmatrix}$$

Ahora solo nos queda resolver la compuerta lógica, cuyo resultado final es:

$$C_2 = \begin{pmatrix} 31 & 207 & 163 \end{pmatrix}$$

Si se tiene curiosidad por resolver los ejercicios y tener un mejor entendimiento de como funcionan los modos de operación presentados, se anexan las respuestas de cada uno de ellos.

ECB					
C_1			C_2		
53	95	146	53	95	146
C_3			C_4		
53	95	146	53	95	146
CBC					
C_1			C_2		
93	173	255	101	111	111
C_3			C_4		
69	69	171	33	163	199
CFB					
C_1			C_2		
4	86	204	42	208	121
C_3			C_4		
151	151	47	242	250	206
OFB					
C_1			C_2		
4	86	204	31	207	163
C_3			C_4		
93	39	116	0	78	98

5. Data Encryption Standard.(DES)

5.1. Un poco de historia.

En 1973 la Oficina Nacional de Estándares (NBS por sus siglas en inglés), que posteriormente se convirtió en el Instituto Nacional de Estándares y Tecnología (NIST), emitió una solicitud pública buscando un algoritmo criptográfico para convertirse en un estándar nacional. IBM envió un algoritmo llamado LUCIFER en el año de 1974, el cual fue enviado a la Agencia de Seguridad Nacional, quien fue la encargada de revisarla y después de unas modificaciones, retornó una versión que fue la parte esencial del algoritmo DES. En 1975 fue realizado DES con una licencia gratuita para su uso, en 1977 se hizo de este algoritmo como el algoritmo de encriptación oficial, el cual fue retirado en 2005.

Este algoritmo es un cifrado por bloques, el cual cifra 64 bits y requiere de una llave de 56 bits, para poder cifrar un solo bloque requiere de 16 rondas.

5.2. Lo que necesito para entender su funcionamiento.

Para poder entender el cifrado, se requiere de las siguientes imágenes.

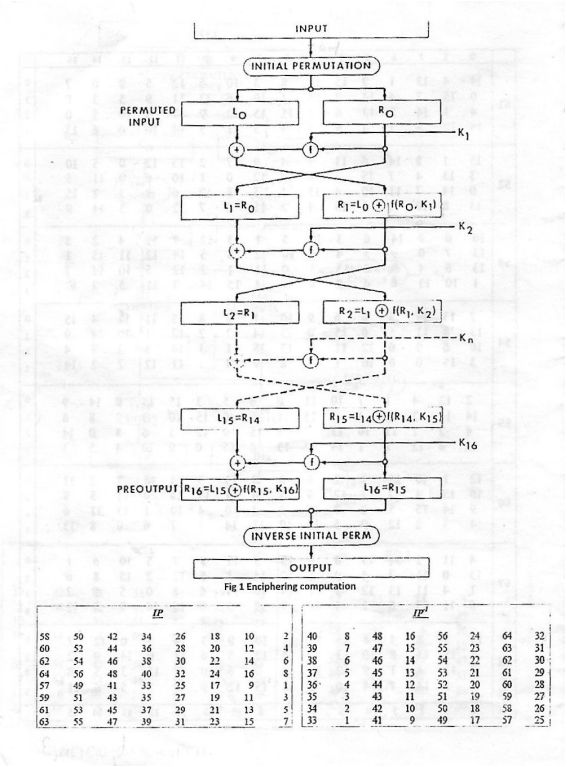


Fig 1 Enciphering computation

IP

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

IP^{-1}

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

(a) Peoceso de las 16 rondas

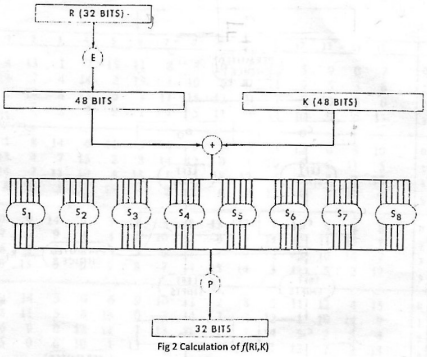


Fig 2 Calculation of f(R,K)

E BIT-SELECTION TABLE

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

P

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

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

(b) Función de expansión

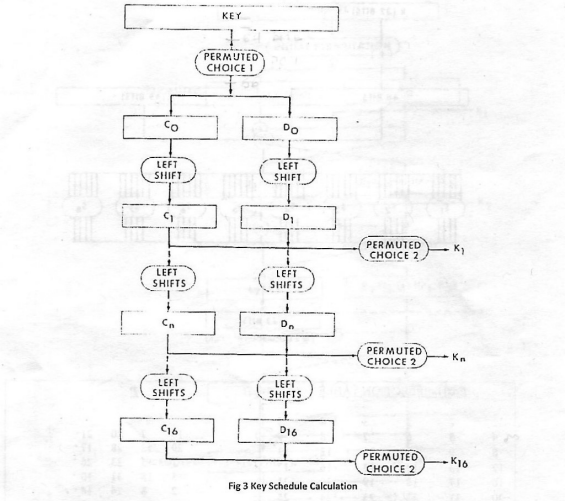


Fig 3 Key Schedule Calculation

PC-1

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

PC-2

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

(c) Calculo de las llaves

		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
S1		14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7	0
		0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8	1
		4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0	2
		15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13	3
S2		15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10	0
		3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5	1
		0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15	2
		13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9	3
S3		10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8	0
		13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1	1
		13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7	2
		1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12	3
S4		7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15	0
		13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9	1
		10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4	2
		3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14	3
S5		2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9	0
		14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6	1
		4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14	2
		11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3	3
S6		12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11	0
		10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8	1
		9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6	2
		4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13	3
S7		4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1	0
		13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6	1
		1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2	2
		6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12	3
S8		13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7	0
		1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2	1
		7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8	2
		2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11	3
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	

(d) Uso de las cajas

Figura 12: Algoritmo DES

5.3. Entendiendo el cifrado.

Viendo solo las imágenes, no se entiende el proceso, ni como interpretar el proceso así ni como utilizar cada una de las tablas, es por ello que. como lo hemos hecho hasta el momento, vamos a realizar un ejemplo donde trataremos de explicar su funcionamiento.

Para poder ejemplificar, nuestros datos serán:
Llave : Asegurar
plaintext: Diamantes falsos

Como se mencionó, DES cifra bloques de 64 bits, y cada letra contiene 8 bits, para cifrar el primer bloque, debemos de dividir el mensaje en bloques de 8 letras, por lo cual el primer bloque corresponde a **Diamante**. Antes de comenzar con los diagramas, del primer bloque a cifrar, debemos de obtener su valor hexadecimal y convertirlo al sistema binario.

Letra	Hexadecimal	Binario	bits acumulados
D	0x44	0100 0100	8
i	0x69	0110 1001	16
a	0x61	0110 0001	24
m	0x6d	0110 1101	32
a	0x61	0110 0001	40
n	0x6e	0110 1110	48
t	0x74	0111 0100	56
e	0x65	0110 0101	64

Empezando en el diagrama (a), de la entrada o bloque a cifrar tenemos que hacer una permutación inicial, para poder hacerla, observamos que en la parte de abajo hay una tabla que tiene por título IP, donde cada número significa el bit correspondiente de la palabra, por ello en la tabla anterior se agrego una columna llamada bits acumulados.

Observemos que el primer bit que marca es el bit 58, el cual corresponde al segundo bit de la última letra (1), el siguiente bit es el bit 50, (1), una característica, es que si empezamos de izquierda a derecha, siempre se van restando 8 bits, eso significa que iremos subiendo una letra pero en la misma posición, en otras palabras, tomaremos toda la columna de bits.

Habiendo terminado el proceso la tabla IP queda de la siguiente manera.

IP		
Binario	Hexadecimal	bits acumulados
1111 1111	FF	8
0100 0000	40	16
1110 1001	E9	24
1001 1110	9E	32
0000 0000	00	40
1111 1110	FE	48
0010 1010	2A	56
0010 0000	20	64

Para obtener L_0 y R_0 los primeros 32 bits corresponden a L_0 y los otros 32 bits a R_0, es decir L_0 = FF40E99E mientras que R_0 = 00FE2A20

Siguiendo con el diagrama, observamos que hay una K_1, para obtenerlo, lo primero que debemos de hacer es repetir la tabla con la palabra Diamante pero ahora con la llave.

Letra	Hexadecimal	Binario	bits
A	0x41	0100 0001	8
s	0x73	0111 0011	16
e	0x65	0110 0101	24
g	0x67	0110 0111	32
u	0x75	0111 0101	40
r	0x72	0111 0010	48
a	0x61	0110 0001	56
r	0x72	0111 0010	64

Ahora observemos el diagrama del inciso (c) , al igual que con el bloque, debemos de hacer una permutación pero ahora con la llave y utilizando la tabla PC-1. EL proceso es el mismo, la característica aquí es que no se ocupan todos los bits, una palabra de 64 bits pasa a tener 56 bits.

El resultado de esta tabla es:

PC-1
0000 000
0 1111 11
11 1111 1
110 1011

1010 101
0 0001 11
00 0000 0
000 0010

Ahora el siguiente paso es hacer grupos de 8 bits y obtener su valor hexadecimal, los primeros 28 bits corresponderán a C_0 y los otros 28 bits corresponderán a D_0
Tenemos que C_0 = 00FFFEB mientras que D_0 = AA1C002.

Continuando con el diagrama, tenemos que hacer una rotación de bits, pero **¿Cuántos bits tengo que rotar?**, para ello debemos de ver la tabla que esta en la parte inferior del inciso (b), dependiendo del número de rondas es el número de bits que tenemos que rotar, como es la primera ronda, solo debemos de rotar un bit, el cual lo vamos a posicionar en la parte final de la cadena.

C_0	0000	0000	1111	1111	1111	1110	1011
C_1	0000	0001	1111	1111	1111	1101	0110
D_0	1010	1010	0001	1100	0000	0000	0010
D_1	0101	0100	0011	1000	0000	0000	0101

Obteniendo los valores hexadecimales, tenemos que $C_1 = 01FFFD6$ mientras que $D_1 = 5438005$

Es importante recordar que los bits de C_1 corresponden a los bits del 1 al 28, mientras que D_1 del bit 29 al 56. Considerando esto, siguiendo el diagrama (c) solo nos queda hacer la permutación 2, correspondiente a la tabla PC-2 , cuyo resultado es:

PC-2
1111 00
00 1011
0110 11
10 1110
1000 00
11 0000
0011 10
00 0001

Y con esto hemos obtenido K_1 cuyo valor hexadecimal es: 0xF0B6EE830381

Regresando al diagrama del inciso (a), vemos que R_0 y K_1 pasan a una función la cual corresponde al inciso (b).

R tiene 32 bits, por lo cual pasa a una función de expansión para tener 48 bits, dicha tabla es E Bit selection table. Haciendo la expansión, tenemos el siguiente resultado.

E bit selection table

0000 00
00 0001
0111 11
11 1100
0001 01
01 0100
0001 00
00 0000

Ahora que R_0 y K_1 tienen la misma longitud, se procede a realizar la compuerta lógica que anteriormente ya hemos trabajado, solo para recordar que se trabaja en el sistema binario. Al hacer la compuerta lógica, el resultado obtenido es:

E	0000	0000	0001	0111	1111	1100	0001	0101	0100	0001	0000	0000
K_1	1111	0000	1011	0110	1110	1110	1000	0011	0000	0011	1000	0001
$E \oplus K_1 1$	1111	0000	1010	0001	0001	0010	1001	0110	0100	0010	1000	0001

Lo que sigue es tomar los primeros 6 bits para S_1, los siguientes 6 bits para S_2 y así sucesivamente hasta obtener S_8

S	Binario	Fila	Decimal	Columna	Decimal	Valor Tabla
S_1	111100	10	2	1110	14	5
S_2	001010	00	0	0101	5	11
S_3	000100	00	0	0010	2	9
S_4	010010	00	0	1001	9	2
S_5	100101	11	3	0010	2	12
S_6	100100	10	2	0010	2	15
S_7	001010	00	0	0101	5	0
S_8	000001	01	1	0000	0	1

Para obtener los valores, de fila y columna, el primer y último bit corresponden al valor binario de la fila, mientras que del bit 2 al 5, corresponden al valor binario de la columna, dichos valores obtenemos su valor decimal y lo único que nos queda es buscar en la tabla correspondiente, la cual corresponde al inciso (d) de la figura. Es importante ver que Cada S tiene su propia tabla, debido a que cada tabla tiene valores distintos en la misma posición.

El valor hexadecimal, es: $0x5B92CF01$, lo que resta es hacer la tabla p, para ello obtenemos de nuevo el valor binario y hacemos esta nueva tabla, cuyo resultado es: $p =$ 0x556CE90A

p es el resultado de $f(R_0, K_1)$, ahora nuevamente regresamos al inciso (a) de la imagen, de acuerdo a la imagen $L_1 = R_0$, mientas que para $R_1 = L_0 \oplus p$.

$L_0 =$ 0xFF40E99E
$f =$ 0x556CE90A
Realizando la compuerta lógica:

L_0	1111	1111	0100	0000	1110	1001	1001	1110
f	0101	0101	0110	1100	1110	1001	0000	1010
$L_0 \oplus f$	1010	1010	0010	1100	0000	0000	1001	0100

$\therefore$
$L_1 =$ 0x 00FE2A20
$R_1 =$ 0xAA2C0094

Finalmente esta solo fue una ronda de este algoritmo, como se mencionó, para cifrar un solo bloque se requieren de 16 rondas para terminar el proceso, restarían 15 rondas mas para cifrar este primer bloque y posteriormente otras 16 rondas para el siguiente bloque.

6. Advanced Encryption Standard. (AES)

Las características más importantes de este cifrado son:

- Procesa bloques de 128 bits.
- Las claves para cifrar pueden ser de 128 bits, 192 bits o 256 bits de tamaño.
- Utiliza una matriz de estado 4x4. La manera de colocar los datos van de arriba hacia abajo empezando por el lado izquierdo y recorriéndose hacia la derecha.
- Al igual que con DES, se trabaja con varias rondas, dependiendo del número de bits de la clave es el número de rondas.

  128 bits : 10 rondas.

  192 bits : 12 rondas.

  256 bits : 14 rondas.
- Nuevamente, por cada ronda se ocupará una sub clave diferente, una por cada ronda.

El siguiente diagrama describe el proceso de este algoritmo.

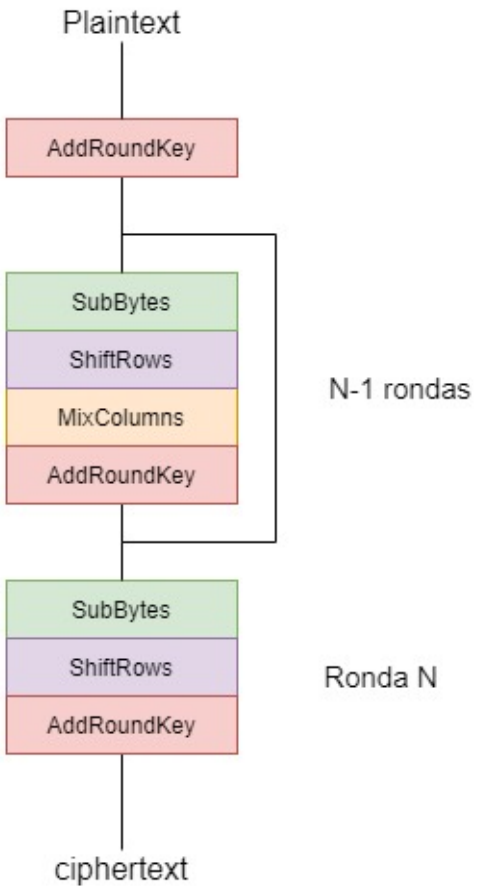


Figura 13: Algoritmo AES.

El proceso de *AddRoundKey* es la operación de $plaintext \oplus key$ Para la función *SubBytes* se requiere de la siguiente tabla.

		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	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

Figura 14: Tabla del algoritmo AES.

Supongamos que el bit corresponde a: 06, el primer digito corresponde al eje x mientras que el segundo al eje y, dicho valor se actualiza en la matriz de estado, el cual sería 6f.

La función *ShiftRows* corresponde a un barrido de las filas, a la primera fila no se le hace nada, a la segunda fila se le hace un corrimiento de una posición, la tercera fila se le hace el corrimiento de 2 posiciones,mientras que a la fila 4 se recorren 3 posiciones.

MixColumns consiste en multiplicar cada una de las columnas de la matriz de estado por un polinomio fijo, el cual es:

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

Finalmente, la función *AddRoundKey* realiza la función xor, entre la matriz de estado actual y la sub clave correspondiente a la ronda, es decir, $matrizdeestado \oplus subllaveN$

Para la generación de la sub llave, de la matriz inicial de la llave inicial, se toma la última columna y se pasa a la función *RotWord*, la cual rota al primer byte una posición.

Teniendo esta rotación, se utiliza la función *SubBytes*, posteriormente se aplica la función xor, de esta nueva columna, con la columna que se encuentra 3 posiciones más atrás (columna 1).

Llegando a este punto, se aplica nuevamente la función xor, con la siguiente tabla, cada columna representa el número de rondas correspondientes.

Round	1	2	3	4	5	6	7	8	9	10
RCON	01	02	04	08	10	20	40	80	1b	36
	00	00	00	00	00	00	00	00	00	00
	00	00	00	00	00	00	00	00	00	00
	00	00	00	00	00	00	00	00	00	00

Este resultado es la primera columna de la nueva llave, finalmente solo repetimos el proceso de la función xor de la nueva palabra con la columna que se encuentra 3 posiciones más atrás de la llave inicial (columna 2,3,4) .

Todo este proceso se repite N veces para encontrar cada sub llave, de cada ronda correspondiente.

7. RSA

7.0.1. Cifrado simétrico y cifrado asimétrico

En los cifrados por bloques vistos con anterioridad, fueron un cifrado simétrico, debido a que para poder cifrar se requiere de una misma clave, la cual debe de ser compartida entre la persona que envía y quien recibe el mensaje.

Ahora veremos otro tipo de cifrado, donde no se requiere compartir la llave para cifrar o descifrar, lo único que si cambia es que cada persona utiliza dos llaves, una de ellas es de tipo público, lo que quiere decir que cualquier persona puede acceder a ella, mientras que la otra llave, es privada, por lo que, solo la persona propietaria es responsable de su uso.

Como cualquier persona puede acceder a la llave pública, ésta se usa para cifrar el mensaje, mientras que la llave privada se utiliza para descifrar.

7.1. Cifrado RSA.

La idea se basa en la factorización de números primos, propuesta por Rivest, Shamir y Adleman en el año de 1997, es por eso que el algoritmo el conocido como RSA.

Para entender el funcionamiento del algoritmo, Betito escoge dos números primos muy grandes p y q, y los multiplica para obtener un n.

$$n = p \cdot q$$

A parte de ello, Betito también selecciona un exponente (e) definido como:

$$\phi(n) = (p-1)(q-1)$$

$$1 < e < \phi(n)$$

$$MCD(e, \phi(n)) = 1$$

Ahora definimos a un numero d, como el inverso multiplicativo de e, para ello solo recordemos la afirmación utilizada en la sección 2.2.2, la cual es:

$$a' \ mod \ b = x$$

Ahora para el caso de $e, d, \phi(n)$ definimos a d como:

$$d = e^{-1} \ mod \ \phi(n)$$

La llave pública de Betito, hará uso de los números e, n, estos números se los puede pasar a Alicia, sin revelar cuales son los valores de p, q que definen a n. Para la llave privada, Betito ocupará los números d, n. Definimos la función de cifrado y descifrado como:

$$C = m^e \ mod \ n$$

$$m = C^d \ mod \ n$$

Al ver estás ecuaciones se estará preguntando cómo es que estas dos ecuaciones funcionan, si ocupan dos números diferentes. Pongamos atención a la función de descifrado.

$$m = C^d \ mod \ n$$

En la función de cifrado se define a $C = m^e$, sustituyendo en la función de descifrado.

$$m = (m^e)^d \ mod \ n$$

Y como e, d son inversos multiplicativos, tenemos que:

$$m = m \ mod \ n$$

Está es la explicación de por qué funciona este algoritmo, la fortaleza radica en los números primos muy grandes, debido a que para encontrar los valores, requiere de un costo computacional muy alto.
Ahora veremos un ejemplo, para entender mejor las ecuaciones descritas anteriormente.

plaintext: luis
$p = 11$
$q = 3$
$n = 33$
$\phi(n) = 20$
$e = 7$
$MCD(e, \phi(n)) = 1$
Aplicando el algoritmo de euclides y el algoritmo de euclides extendido...

$$20 = 7(2) + 6$$

$$7 = 6 + 1$$

$$6 = 1(6) + 0$$

$$1 = 7 - 6 \ \ (a)$$

$$6 = 20 - 7(2) \ \ (b)$$

Sustituyendo (b) en (a)

$$1 = 7 - (20 - 7(2))$$

$$1 = 7(3) - 20$$

Tenemos que el inverso multiplicativo de 7 es 3, $\therefore d = 3$

Recordando que a cada letra se le asigna un número.

l	u	i	s
11	20	8	18

Solo nos queda aplicar la formula de cifrado.

$$C(l) = 11^7 = 19487171 \ mod \ 33 = 11$$

$$C(u) = 20^7 = 1280000000 \ mod \ 33 = 26$$

$$C(i) = 8^7 = 2097152 \ mod \ 33 = 2$$

$$C(s) = 18^7 = 612220032 \ mod \ 33 = 6$$

Tenemos que C = 11 26 2 6, aplicando la fórmula de descifrado...

$$m(11) = 11^3 = 1331 \ mod \ 33 = 11$$

$$m(26) = 11^3 = 17576 \ mod \ 33 = 20$$

$$m(2) = 2^3 = 8 \ mod \ 33 = 8$$

$$m(6) = 6^3 = 216 \ mod \ 33 = 18$$

Lo importante a recordar, es que tanto e como d tiene que ser respecto a $\phi(n)$, si se hace con respecto a n, el resultado será incorrecto.

8. Funciones HASH

Un componente básico de algunos algoritmos criptográficos es conocido como funciones hash. Cuando una función hash satisface ciertas condiciones, pueden ser usadas para hacer unos algoritmos más eficientes.

Una función hash utilizada en criptografía toma como entrada un mensaje de cualquier longitud y produce como salida un mensaje digerido de una longitud fija. El diagrama que describe lo descrito previamente es:

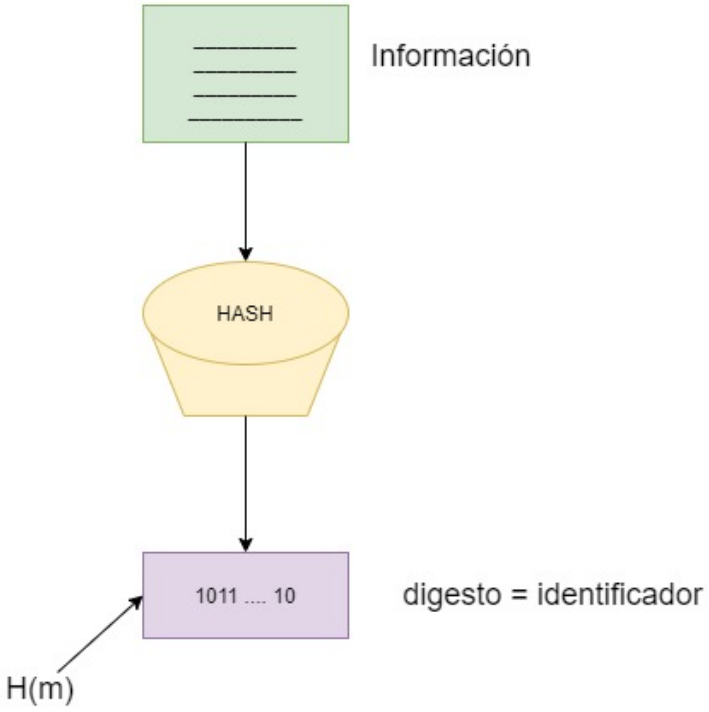


Figura 15: Diagrama de las funciones HASH.

Entre las características de las funciones HASH, tenemos:

- Procesa cualquier tamaño de información.
- Funciones de sólo salida.
- Se rompe cuando $H(m_1) = H(m_2)$.
- Un cambio mínimo en la entrada debe de cambiar por completo la salida.

9. Firma Digital

Para este último tema, pongamos la siguiente situación.

Suponga que Alicia quier mandarle un mensaje a Betito, se va a hacer a través del cifrado asimétrico visto, además de utilizar el cifrado asimétrico se va a utilizar la función HASH. El proceso que tendrá que hacer Alicia para realizar la firma digital se presenta a continuación.

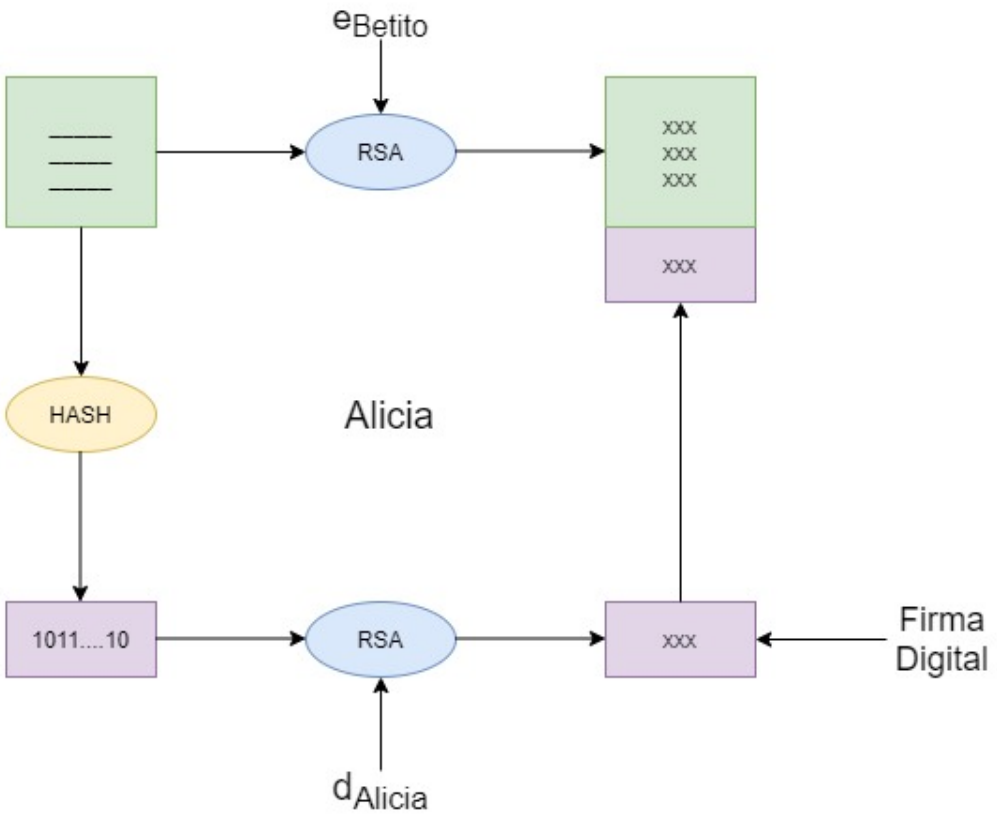


Figura 16: Escenario de cifrado para Alicia.

El proceso que debe de seguir Alicia es el siguiente:

- La parte superior izquierda es el plaintext a mandar, si continuamos hacia abajo, se le aplica cualquier función HASH, la cual recordemos nos dará un resultado único.
- Una vez teniendo el digesto de la función, debemos de cifrar con el algoritmo RSA aplicando la llave privada de Alicia, el resultado se le conoce como firma digital.
- Regresando nuevamente al plaintext, el mensaje se cifrará con la llave pública del destinatario, en este caso con la llave pública de Betito.
- Ahora que tenemos el plaintext cifrado y la firma digital del emisor, solo nos queda unir ambas partes, dependiendo de los involucrados, es como se unen ambos archivos, en este ejemplo primero se coloca el ciphertext y en la parte final se une la firma digital.

- Finalmente, solo se tiene un archivo, el cual será enviado al emisor.

Ahora veamos el proceso que debe de seguir el receptor, en este caso Betito.

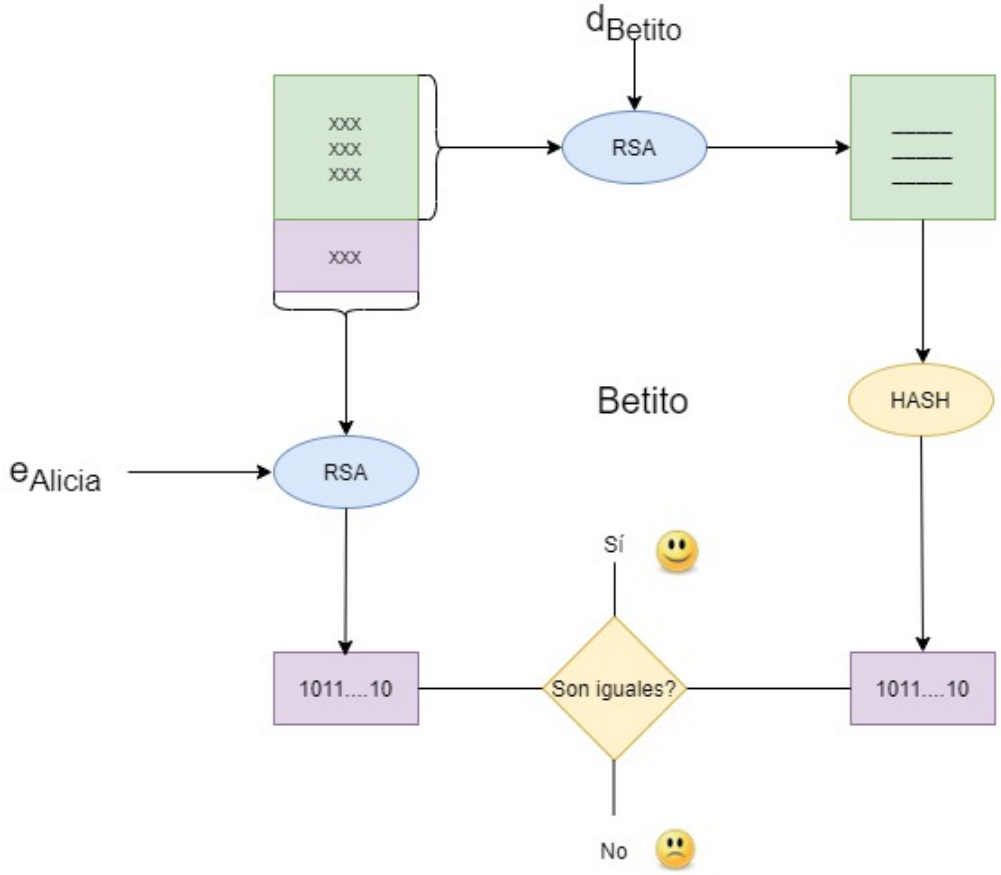


Figura 17: Escenario de descifrado para Betito.

- Betito recibe un solo archivo, pero dentro de el se tienen dos partes, el programa identifica y separa la parte correspondiente al ciphertext y a la firma digital.
- El ciphertext, fue cifrado con la llave pública del receptor, es decir, la llave publica de Betito, por lo que para descifrar utilizaremos su llave privada.
- Ahora que tenemos el plaintext, es como tener la primera parte del cifrado de Alicia, debemos de pasar el plaintext por la misma función HASH, y nos debe de dar el mismo digesto que con el que fue cifrado.
- A la parte correspondiente de la firma digital cifrada, se requiere de la llave pública del emisor (Alicia), para tener el digesto descifrado.
- Por último, solo nos queda comparar ambos digestos, si son iguales o son diferentes.

Si los digestos coinciden, a parte de tener una carita feliz, podemos asegurar:

- Confidencialidad, ya que si se cifra con la llave pública de Betito, es mensaje solo se puede descifrar con llave privada de él, Candie no podrá leer el mensaje.
- Betito se asegura que durante el envío, el mensaje no fue alterado (integridad de los datos).
- Autenticación, debido a que el digesto fue cifrado con la llave privada de Alicia, y el descifrado del mismo fue correcto, nos asegura que solo Alicia pudo haber escrito el mensaje.
- No repudio, al haber concluido lo anterior, Alicia no puede negar que ella fue la responsable de haber enviado el mensaje, recordar que el uso de la llave privada es responsabilidad de la persona propietaria.