# HISTORIA DE LA CRIPTOLOGÍA

AUTOR: LUIS FRANCISCO URREA

San Marcos

# Historia de la criptología

# ÍNDICE

La raíz de la palabra se encuentra en los vocablos griegos krypto (ocultar) y logos (ciencia), es decir, podemos hablar de la criptología como la ciencia que se ocupa del estudio de lo oculto. Aunque el nombre original de nuestro curso es criptografía, se hace necesario recurrir a la definición global para entrar a definir sus partes.

Mantener lejos del dominio público información de carácter religioso, militar o científico es una de las primeras tareas que exige el uso de información escrita en clave (cifrada), algunas referencias hablan del uso de la escritura hierática (jeroglífica) por los antiguos sacerdotes egipcios, así también, en la antigua babilonia y a partir de la escritura cuneiforme existen indicios de mensajes cifrados. Las primeras referencias del uso de la criptografía junto a las técnicas que permiten conocer el mensaje oculto se remiten a la época de los griegos. Uno de los primeros objetos que se conocen para cifrar mensajes es conocido como la escítala lacedemonia, su uso previsto en apariencia para transmitir información con propósitos militares hace necesario que quien reciba el mensaje cuente con una clave que le permita identificar el mecanismo de cifrado, a partir del uso adecuado de la clave de encriptación, registrada en un bastón de madera. Así el mensaje y la clave se envían por separado al mismo destinatario, el cifrado consiste en enmascarar el significado real de un texto a partir de alterar el orden de los signos que lo componen.

Escítala lacedemonia

Testigo con base en un bastón, empleados por los griegos para ocultar información.

## Cifrado por desplazamiento

El cifrado de César es el primer método de cifrado monoalfabético de que se tiene información.

### Ejemplo

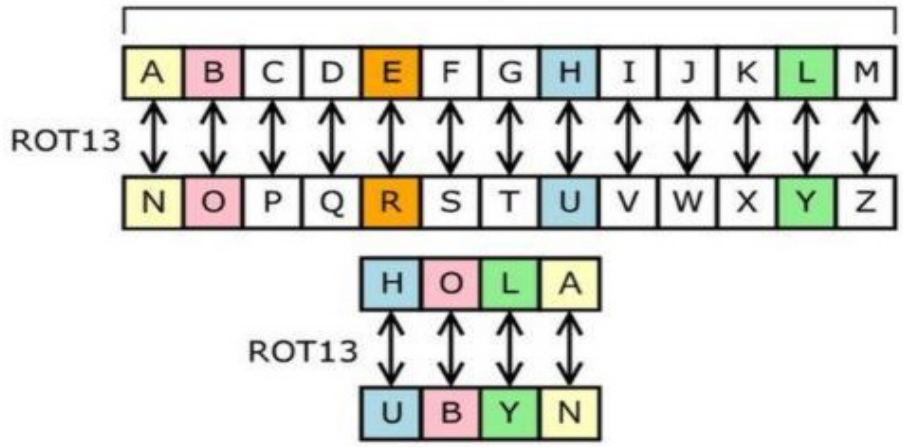
A continuación, les quiero saludar de una forma muy especial a través de un mensaje cifrado usando el método César:

"Ñuqziqzupbf nx ohefb pq oeucgbsenrun"

Este método del que se atribuye su uso al emperador romano Julio César en el año 300 a. C., fue usado para enviar mensajes de carácter militar a los generales del ejército romano, su descifrado es simple si conocemos la clave, pero ¿y dónde está la clave?, la clave, la clave, la clave…. por cierto, en el mensaje encriptado que tenemos algunos renglones atrás olvidé indicar la clave de cifrado, para este mensaje usé la clave Rot 13. Así y a partir de esta técnica se puede observar que los mensajes se escriben reemplazando las letras del mensaje original "en claro" por un desplazamiento de las mismas, un número de posiciones equivalente a la clave.

**Descifrado**

Procedimiento de aplicar técnicas para obtener el mensaje en claro a partir de un texto cifrado.




En esta imagen se muestra la codificación de la palabra 'HOLA' con una clave = 13.

Figura 5. Cifrado César
Fuente: propia

## Ejemplo

Así, para expresar en términos matemáticos un modelo general que se pueda aplicar a cualquier método de cifrado por desplazamiento, podemos usar la expresión:

$$Ck=m+k(mod\ n)$$ *Así, por ejemplo cuando k=3 tenemos el cifrado de césar*

Es claro que, en la antigüedad, por el escaso número de personas que sabían leer, y el uso poco extendido del latín, este método ofrecía elevada seguridad, hoy en día cualquier niño que sepa leer podrá encontrar fácilmente, la forma de descifrar un mensaje escrito bajo esta codificación, la aplicación de técnicas estadísticas, o una tabla completa como la de la imagen con n permutaciones puede llevar a conocer la clave.

Será entonces su misión apreciado estudiante, descifrar el mensaje que he incorporado como base para la explicación del cifrado César.

A continuación, haré una breve referencia de algunos de los métodos de cifrado que evolucionan a lo largo de la historia y sus aportes al desarrollo de la criptografía y el criptoanálisis que usamos en nuestros modernos sistemas de encriptación.

En el año 150 a. C., el historiador griego Polibio, desarrolla un esquema para enviar mensajes, que, de forma original, no tiene como propósito cifrarlos, pero que por la complejidad para descifrar y leer el mensaje original se constituye en base para el diseño de sistemas criptográficos posteriores, así en una matriz cuadrada de 5X5 registra un mensaje.

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 1 | A | B | C | D | E |
| 2 | F | G | H | IJ | K |
| 3 | L | M | N | O | P |
| 4 | Q | R | S | T | U |
| 5 | V | W | X | Y | Z |

Tabla 1. Esquema de Polibio
Fuente: propia

En este método el mensaje se escribe en números y para desencriptar, o conocer el mensaje en claro se hace necesario ir a la matriz y encontrar la letra que se ubica en la fila y columna del número que corresponde. Así por ejemplo el número 55 es la letra Z. Aunque de forma inicial su creador no lo pensó como un método de encriptación, su uso posterior es la base de múltiples sistemas de encriptación, y a partir de él, se genera el método que se conoce como sustitución monoalfabética multiliteral.

**Multiliteral**

Varios símbolos o letras pueden representar en el texto cifrado un sólo carácter del mensaje en claro.

### Instrucción

Les invito a desencriptar el siguiente mensaje usando el cifrado numérico de Polibio:

"11454513311411144514151445133221131541133414341513154235313422 4 445434 34545133433434514424114451"

Una debilidad clásica de los métodos de sustitución o desplazamiento es su susceptibilidad al aplicar técnicas estadísticas para encontrar el mensaje original, puesto que el texto cifrado, contiene las mismas estructuras del alfabeto que se usa para el mensaje en claro. Así, conforme avanza la historia se desarrollan métodos más complejos para aplicar técnicas criptográficas. El cifrado de Polibio se conoce como uno de los métodos de sustitución por alfabetos independientes más conocido.

### Instrucción

Para reforzar los temas que hemos visto hasta ahora les invito a desarrollar el recurso de aprendizaje: memonota.

La vulnerabilidad en los sistemas de cifrado que se asocian a letras o códigos, radica en la predictibilidad estadística, porque se encuentra ligado de forma intima al alfabeto bajo el cual se origina el mensaje, así, se hace necesario el desarrollo de métodos de cifrado que además de cifrar el mensaje puedan entregar una información en claro en apariencia válida, pero con un mensaje distinto al mensaje original, es decir, confundir a quien intercepte y descifre el mensaje para que crea que está leyendo el mensaje en claro, cuando en realidad están leyendo una información errada creada a propósito a partir del cifrado de la información. Estos métodos se conocen bajo la denominación de métodos de sustitución homofónica. En estos métodos se puede sustituir una letra por otras (varias) que puedan tener un sonido semejante, así puede una letra como la A ser reemplazada por combinaciones de números como 01, 08, 17, 25 a partir de una tabla creada con anterioridad y compartida por emisor y receptor para ser usada como clave, se genera así, una correspondencia uno a varios, en este método a diferencia del cifrado por sustitución que lo hace, uno a uno.

**Homofónica**

En cifrado, hace referencia a un texto cifrado que expresa un mensaje coherente pero diferente al original, con el propósito de generar confusión ante una posible intercepción de la comunicación.

## Sustitución polialfabética

Estos métodos se basan en el uso de varios alfabetos que desvíen la atención del analista en función de modificar las características básicas del lenguaje en el que se encuentra el mensaje en claro. Uno de los primeros métodos de este tipo que se conocen es el que diseñó León Alberti, que se conoce con el nombre de cifrado de Albertí, a partir del uso de dos discos, uno con el alfabeto occidental que está acompañado de números y un disco interno que reúne en desorden las letras del alfabeto latino. Así, para conocer el mensaje en claro se hacen coincidir una letra del alfabeto clásico y una del latino (este par de letras son la clave) y con los discos en la posición fijada por la clave se hace la sustitución de las letras cifradas que coincidan con la posición equivalente en el mensaje en claro. De esta forma se envía el mensaje cifrado, para desencriptar se hace la operación inversa. Cuando luego de cierto número de palabras se desplazan los discos para continuar leyendo el mensaje, decimos que el cifrado es polialfabético.

Figura 6. Cifrado de Alberti
Fuente: Wikipedia

## Cifrado de Vigenere

Este método de cifrado es uno de los que más amplio y extendido uso tiene en la historia de la criptografía y en la historia del hombre, puesto que tras su propuesta de desarrollo en el año 1586 por el diplomático francés Blaise de Vigenere, el primer criptoanálisis conocido que descifra de forma acertada esta técnica sólo fue publicado hasta el año 1863.

Friedrich Wilhelm Kasiski, autor del libro, desarrolla y explica la técnica de criptoanálisis por sustitución polialfabética y hace énfasis en el cifrado de Vigenere. Para este análisis busca fragmentos repetidos de texto iguales dentro del texto cifrado y mide su longitud, está será la longitud de la clave de cifrado. El libro se titula "La escritura secreta y el arte del descifrado" aún en la actualidad algunos organismos de inteligencia usan el cifrado de Vigenere con variaciones en su estructura original.

Este cifrado se hace a partir de una matriz cuadrada compuesta por alfabetos regulares, en ella se escriben en cada columna todos los alfabetos disponibles iniciando el alfabeto en la letra que corresponde al rótulo de la columna superior, no se emplea la letra ñ. Para el cifrado de forma inicial se ubica el mensaje en la línea que el escritor decida, y la clave se repite de forma continua a partir de la misma posición en que se encuentra el mensaje original, pero en las filas siguientes.

La expresión o fórmula que representa el cifrado a partir del método de Vigenere se denota de la siguiente forma:

Donde la clave K= ++… está compuesta por cada uno de los desplazamientos que señala la clave a partir del alfabeto básico.

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

Tabla 2.
Fuente: propia

Pasos para cifrar o encriptar un mensaje usando este método

1. Pensar en una palabra que se va a usar como clave que debe tener una longitud inferior al mensaje que se va a encriptar, por ejemplo, podemos usar la palabra palo.

2. Escribir el mensaje que se va a cifrar, debe ser escrito sin espacios entre las palabras, por ejemplo, "cumpletusmetas".

3. Escribimos la palabra clave inmediatamente debajo del mensaje en claro, y se hacen coincidir las letras de la clave con cada una de las letras del mensaje, la clave debe ser escrita todas las veces que se alcance, si quedan letras sin ocupar de la clave se ignoran las letras faltantes. Para este ejemplo:

| Mensaje | C | U | M | P | L | E | T | U | S | M | E | T | A | S |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Clave | P | A | L | O | P | A | L | O | P | A | L | O | P | A |

Tabla 3.
Fuente: propia

4. Vamos a la fila en la que se encuentra la primera letra de la palabra clave en la tabla de Vigenere y a la columna de la primera letra del mensaje. La letra que se ubica en la intersección, será la primera letra que se usa para el mensaje cifrado.

5. Se repite el proceso descrito en el paso 4 hasta que todo el mensaje se encuentre cifrado, así para nuestro ejemplo el mensaje cifrado es:

"RUWEAEEJIMOIPS"

Apreciados estudiantes, como podemos observar es fácil el uso de este método cuando conocemos la clave de cifrado, pues para descifrar sólo es necesario desarrollar el proceso en orden inverso, les invito a comprobar la validez del texto cifrado que les he propuesto a través del cifrado de Vigenere.

## Pero, ¿y si desconocemos la clave?

Como he mencionado antes, el secreto del descifrado del método de Vigenere se lo debemos a Friedrich Wilhelm Kasiski que descifró el método para encontrar la clave de cifrado en métodos polialfabéticos que aplica a la perfección sobre el método de Vigenere, a continuación, una sencilla exposición del criptoanálisis:

Antes de iniciar debemos aclarar que el método de Vigenere usa un sistema de cifrado simétrico, es decir, que la clave de cifrado es la misma clave que se usa para descifrar el mensaje, por tanto, el emisor y el receptor deben ponerse de acuerdo y conocer la clave para poder enviar el mensaje cifrado de modo que el destinatario lo pueda descifrar.

Como expliqué en la exposición del cifrado, por ser polialfabético una letra del mensaje en claro puede corresponder a dos o más letras del menaje cifrado.

## Ejercicio de aplicación

Vamos ahora a intentar romper un mensaje cifrado con el código de Vigenere, en este ejemplo. Vamos a usar el siguiente mensaje cifrado que es muy común en los blogs y publicaciones relacionadas con la criptografía:

"onuwnyasccwsafpulmbwnhpulnmleuladñpulnxscushqmiknjuhnyzdlnkdlpmlñyshdgm-
fduqwdyuuccxmlxwldclwdwwfzwmlvukdlpm"

Para intentar conocer el texto en claro debemos realizar el siguiente procedimiento:

a. El primer paso consiste en descubrir la longitud de la clave, para este fin Kasiski recomienda encontrar secuencias de caracteres que se repiten en el texto cifrado con mucha probabilidad, estas secuencias también tienen equivalencia en el mensaje antes de cifrar. Entonces busquemos en el mensaje cifrado secuencias de texto, este procedimiento lo vamos a desarrollar usando una herramienta en línea para aplicar el método kasiski y buscar las secciones repetidas y sus frecuencias de aparición:

| Vigenere Repeat Distance Repeated Sequence | Spacing | Possible length of key (or factors) 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| PUL | 8 | x | | x | | | | x | | | | | | | | | | | | |
| PUL | 12 | x | x | x | | x | | | | | | x | | | | | | | | |
| ULN | 12 | x | x | x | | x | | | | | | x | | | | | | | | |
| KDL | 44 | x | | x | | | | | | | x | | | | | | | | | |
| DLP | 44 | x | | x | | | | | | | x | | | | | | | | | |
| LPM | 44 | x | | x | | | | | | | x | | | | | | | | | |
| PULN | 12 | x | x | x | | x | | | | | | x | | | | | | | | |
| KDLP | 44 | x | | x | | | | | | | x | | | | | | | | | |
| DLPM | 44 | x | | x | | | | | | | x | | | | | | | | | |
| KDLPM | 44 | x | | x | | | | | | | x | | | | | | | | | |

Figura 7. Kasiski estadística
Fuente: propia

b. El resultado muestra las repeticiones en el texto cifrado y el espaciado entre ellas. Los factores del espaciado están indicados por X. Si un factor es común a muchos de los espacios, entonces esta es probablemente la longitud de la palabra clave.

Como se puede observar por estadística la longitud de clave más probable es dos, cuatro u once. Que son los valores que más repeticiones presentan, así tenemos entonces nuestra primera pista.

Si alguien se tomó el trabajo de ocultar un texto mediante cifrado, es poco probable que use una clave muy corta, así que de entrada descartaremos la longitud dos, seguimos con el siguiente valor (cuatro), existe una alta probabilidad que la longitud de la clave sea 4 pues en la secuencia PUL aparece dos veces, separada en 8 y 12 posiciones, así al calcular el MCD entre estos dos números enteros obtenemos el valor 4, entonces vamos a considerar esta como la longitud probable de la clave.

c. Como tenemos la longitud probable de la clave, y conocemos el método de encriptación sabemos que todo el texto cifrado es una combinación entre clave y texto en claro, y si la longitud de la clave es 4 entonces todo el criptograma se puede dividir en cuatro subcriptogramas (la longitud de la clave es 4 entonces el texto cifrado debe contener repetidas n veces las cuatro letras de la clave), para dividir el criptograma en los subconjuntos correspondientes a las letras de la clave debemos tener en cuenta entonces que por ser la longitud de la clave 4, al crear el primer subconjunto debo tomar los caracteres 1, 5, 9, 13, 17, …+4…

Así en detalle, para obtener las letras de cada subcriptograma podemos elaborar una rejilla numerada de 1 a 4 tantas veces como sea necesario de acuerdo al tamaño del criptograma original y extraer las letras que se encuentren ubicadas en la columna que corresponde al número. Así, para el subcriptograma 1 las letras que se ubican en la columna 1, para el dos las letras que se ubican en la dos y así sucesivamente.

| 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| O | N | U | W | N | Y | A | S | C | C | W | S | A | F | P | U | L | M | B | W |
| N | H | P | U | L | N | M | L | E | U | L | A | D | Ñ | P | U | L | N | X | S |
| C | U | S | H | Q | M | I | K | N | J | U | H | N | Y | Z | D | L | N | K | D |
| L | P | M | L | Ñ | Y | S | H | D | G | M | F | D | U | Q | W | D | Y | U | U |
| C | C | X | M | L | X | W | L | D | C | L | W | D | W | W | F | Z | W | M | L |
| U | K | D | L | P | M | | | | | | | | | | | | | | |

Tabla 4.
Fuente: propia

El subcriptograma uno, está conformado por todas las letras que se encuentran en la columna rotulada con el número uno, el segundo por los del dos y así para los demás, se deben extraer las cifras o caracteres en el orden en que aparecen en el texto, así nuestros subconjuntos (4) del criptograma original quedarían así:

- Subcriptograma 1: ONCALNLEDLCQNNLLÑDDDCLDDZUP
- Subcriptograma 2: NYCFMNHUNNUMJYNPYGUYCXCWWKM
- Subcriptograma 3: UAWPBPMLPXSIUZKMSMQUXWLWMD
- Subcriptograma 4: WSSUWULAUSHKHDDLHFWUMLWFLL

d. A partir de esta subdivisión se puede realizar un ataque estadístico simple, para este caso creamos una nueva rejilla con base en el alfabeto español, ¿Por qué sabemos que está en español el mensaje? Porque apareció la letra ñ. En esta rejilla, se hace el conteo estadístico de cuántas veces aparecen las letras de nuestro alfabeto en cada subcriptograma, así tenemos:

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | Ñ | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 0 | 3 | 6 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 6 | 0 | 4 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 |
| 2 | 0 | 0 | 3 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 3 | 5 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 3 | 0 | 2 | 1 | 4 | 0 |
| 3 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 2 | 4 | 0 | 0 | 0 | 3 | 1 | 0 | 2 | 0 | 3 | 0 | 3 | 2 | 0 | 1 |
| 4 | 1 | 0 | 0 | 2 | 0 | 2 | 0 | 3 | 0 | 0 | 1 | 5 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 0 | 4 | 0 | 4 | 0 | 0 | 0 |

Tabla 5.
Fuente: propia

e. Vamos a revisar ahora la posición absoluta de cada una de las letras dentro de nuestro alfabeto

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | Ñ | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |

Tabla 6.
Fuente: propia

Entonces, al aplicar métodos estadísticos en primera instancia nos basamos en las letras que más se repiten en el idioma español que son: A, E, O. Al hacer nuestro análisis la A se encuentra en la posición cero, la E se encuentra a cuatro caracteres de la A y la O, se encuentra 11 puestos más allá de la E.

f. En cada subconjunto del criptograma principal, se hace la búsqueda de las tres letras que más se repitan, es decir, que la suma de las frecuencias de sus apariciones sea la más alta (esta frecuencia nos entrega una alta posibilidad que estas sean las letras que forman la palabra clave) con base en las cuales se encripto el mensaje. Se hace necesario crear dos nuevas tablas para usarlas así:

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | Ñ | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $C_A$ | 1 | 0 | 3 | 6 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 6 | 0 | 4 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 |

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | Ñ | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $C_A$ | 3 | 1 | 4 | 6 | 1 | 0 | 1 | 6 | 0 | 4 | 1 | 8 | 1 | 5 | 4 | 7 | 2 | 2 | 0 | 0 | 0 | 1 | 1 | 7 | 0 | 7 | 8 |

Tabla 7.
Fuente: propia

En la tabla se encuentran las frecuencias absolutas de aparición de cada una de las letras del alfabeto bajo el cual ha sido cifrado el mensaje

Las flechas señalan las posiciones que deben ser sumadas para obtener el valor total de la suma de las letras que más se repiten en el idioma usado de acuerdo a las posiciones que las separan, recuerde apreciado estudiante que hablamos de las letras A, E, O y su separación absoluta en el idioma español es 4 y 11 caracteres de forma respectiva, así la suma total de las frecuencias se calcula para cada una de las letras del alfabeto.

Así, en el criptograma que se analiza vemos que la letra que coincide con la más alta suma de frecuencias relativas es la letra L, que además aparece seis veces en el subcriptograma. En segundo lugar, está la letra Z, que aparece en la suma de frecuencias con valor total 8 y en el subcriptograma aparece una sola vez. A partir de este análisis, podemos inferir que la primera letra de la clave es la L.

El mismo procedimiento se realiza con los restantes subcriptogramas para encontrar en cada uno la letra que con las condiciones analizadas en el numeral anterior pueda formar parte de la clave, el orden de las letras se define por el orden de cada subcriptograma, así la primera letra es del subcriptograma uno, la segunda del dos y en el mismo sentido se hallan las demás.

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | Ñ | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $C_B$ | 0 | 0 | 3 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 3 | 5 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 3 | 0 | 2 | 1 | 4 | 0 |

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | Ñ | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $C_B$ | 0 | 1 | 4 | 1 | 0 | 0 | 5 | 1 | 5 | 7 | 5 | 0 | 4 | 5 | 3 | 0 | 0 | 0 | 1 | 3 | 2 | 8 | 1 | 2 | 4 | 7 | 0 |

Tabla 8.
Fuente: propia

Así, la letra U aparece ocho veces en la suma de las frecuencias relativas y tres veces escrita en el subcriptograma, entonces se considera que se trata de la segunda letra de la clave.

El procedimiento para validar las otras dos letras de la clave corresponde a ustedes apreciados estudiantes; una vez que haya concluido el desarrollo completo del proceso encuentra que la clave completa de cifrado es la palabra LUIS. Con ella procedemos a descifrar el mensaje, en la actividad propuesta, por favor escriba el mensaje cifrado con el código Vigenere, el mensaje en claro y la clave.

### Instrucción

Como actividad adicional les propongo descifrar el mensaje en claro contenido en el siguiente criptograma creado, usando el método de Vigenere.

"anenmdtbs dv joeoi coszxiid mz nuvwter khrsg he oupctoxvarli"

### Reflexionemos

Acabamos de ver el procedimiento para descifrar un mensaje encriptado con un método creado hace más de 500 años, ¿se pueden imaginar cómo puede ser el procedimiento para desencriptar un mensaje cifrado con los modernos algoritmos de cifrado?

### Instrucción

Para profundizar respecto a la evolución de la criptografía por favor realicen la actividad de aprendizaje: control de lectura ¿De qué nos protegemos? Con base en el siguiente artículo:

La criptografía clásica
Santiago Fernández

También les invito a revisar el recurso de aprendizaje: caso modelo, y a desarrollar la actividad: crucigrama, los cuales permitirán una mejor aprehensión de sus conocimientos.

# Aspectos importantes de la criptología

## Objetivos de un sistema criptográfico

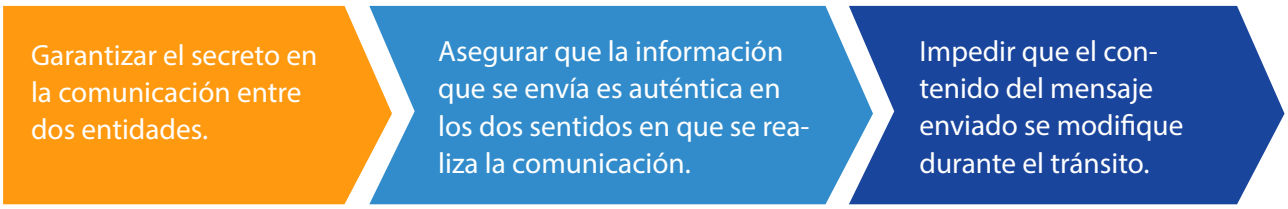



Figura 8. Objetivos de un sistema criptográfico
Fuente: propia

La criptografía entonces se basa en métodos matemáticos y en la actualidad se vale de herramientas informáticas y telemáticas; emplea diferentes métodos y técnicas con el fin de proteger o encriptar archivos o mensajes a través de algoritmos con el uso de una o varias claves. Así, y de acuerdo a los algoritmos que se usan, podemos encontrar diferentes sistemas para encriptar o cifrar la información.

## Criptosistemas

La existencia de distintos tipos de sistemas de cifrado se conoce como criptosistema, así, a partir del uso de estos sistemas de cifrado podemos asegurar al menos tres de los cuatro aspectos de la seguridad informática:

- Confidencialidad: asegura que los mensajes o archivos sólo puedan ser legibles únicamente para el emisor y el receptor.
- Integridad: garantiza que el mensaje o archivos no sean modificados por terceros durante su tránsito por los medios de transmisión o dispositivos intermediarios existentes en el recorrido entre origen y destino.
- No repudio: evitar que quien ha enviado el mensaje y/o el dispositivo que se empleó para generarlo puedan negar que han generado este mensaje o comunicación.

A partir de los aportes de Shannon (1948) y otros autores, se definen los criptosistemas como una combinación de un conjunto de cinco elementos o quíntupla de la forma (M, C, K, E, D) en la cual:

- M: representa el conjunto completo de mensajes en claro o texto plano, es decir, mensajes que se encuentran sin cifrar, pero que se desean convertir a texto cifrado.

- C: representa el conjunto de todos los mensajes que han sido cifrados, es decir, ya se encuentran en forma de criptogramas.

- K: por esta letra se representa la clave o el conjunto de claves que se usan para crear los criptogramas.

- E: representa el conjunto de transformaciones de cifrado, expresa el grupo o familia de funciones que se efectúa sobre cada uno de los elementos de M para conseguir un elemento en el conjunto C. Así, cada valor posible de la clave K, genera una transformación diferente que se denota por la expresión EK.

- D: representa el conjunto de transformaciones cuando el texto se descifra, funciona de forma semejante a E.

Por consiguiente, para cualquier criptosistema creado se cumple la expresión:

DK(EK(m))=m

Lo que significa que cualquier mensaje M, que se cifra con la clave K y posteriormente se descifra usando la misma clave, se obtiene el mensaje original M.

Shannon (1947), propone entonces la estructura que debe tener un criptosistema para cumplir los principios expuestos:

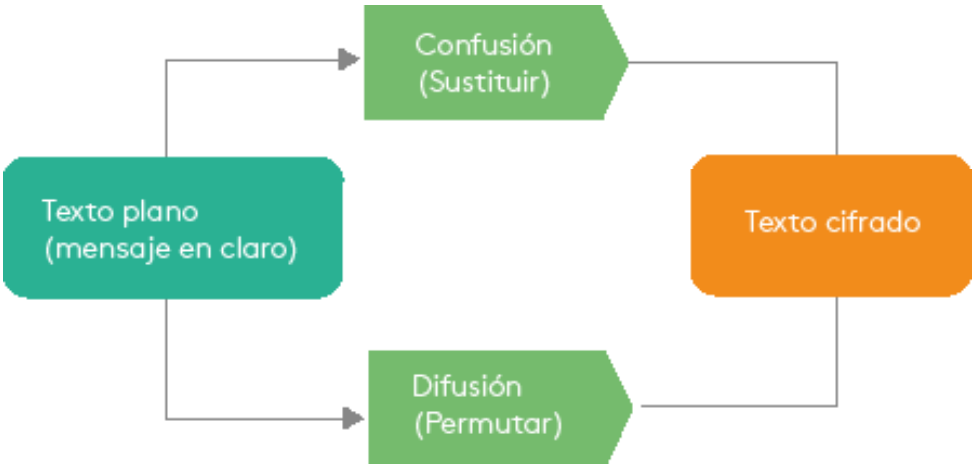



Figura 9. Criptosistema Shanon
Fuente: propia

De seguro nos hemos encontrado con este mensaje de una popular aplicación de mensajería instantánea.

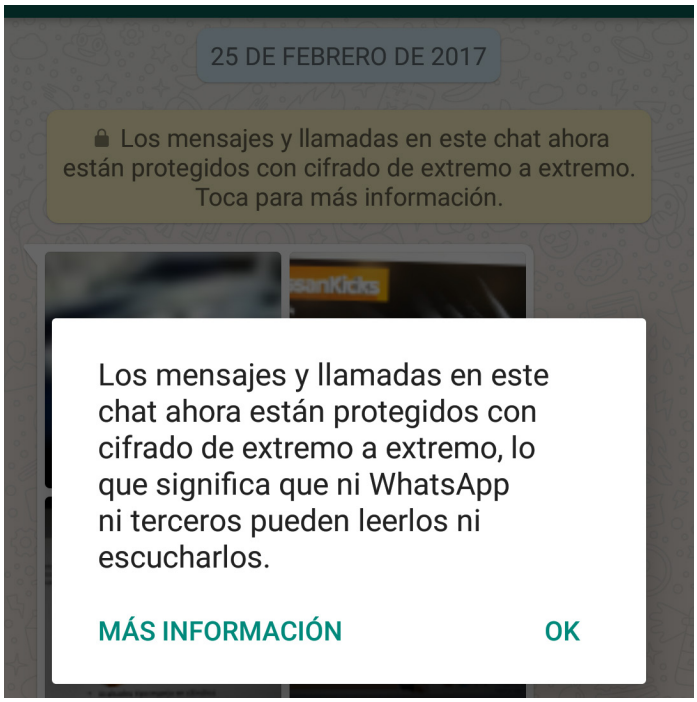



Figura 10. Cifrado WhatsApp
Fuente: WhatsApp

En la actualidad y a partir del tipo de claves y uso de los criptosistemas existen dos tipos:

- Criptosistemas de clave privada: también se conocen como simétricos, y esa simetría se expresa porque el criptosistema emplea la misma clave K tanto para crear o cifrar el mensaje como para descifrarlo. Esta situación genera una debilidad, la clave debe ser compartida por un medio público entre el emisor y receptor, entonces ¿cómo puedo transmitir la clave sin que caiga en manos equivocadas?

- Criptosistemas de clave pública: se conocen bajo la denominación de asimétricos, así el sistema usa dos claves, una clave kp , o clave privada y kp como clave pública. Se pueden emplear de forma indiscriminada una para cifrar E y otra para descifrar D. Una característica que se destaca es la posibilidad de intercambiar entre las dos claves, así se usa la pública para cifrar y la privada para descifrar o en sentido contrario. Para asegurar la seguridad de este tipo de criptosistemas las claves no deben permitir descifrarse entre sí, así, si tengo la clave pública no puedo descifrar la privada y viceversa.

Una ventaja del uso de los criptosistemas de clave pública es la gran gama de posibilidades que ofrece para intercambiar información a través de canales públicos como la internet, esto al tener en cuenta que sólo viaja por el canal la clave pública.

## Criptoanálisis

El concepto complementario a la criptografía es el de criptoanálisis, esta palabra compuesta tiene origen en los vocablos griegos kryptós que significa oculto y analyein que se traduce como desatar, así, lo podemos definir como el estudio de los principios y mecanismos necesarios para descifrar un mensaje sin conocer su clave de cifrado.

### Instrucción

Antes de seguir, les invito a revisar la infografía que hemos desarrollado sobre este tema: Técnicas de criptoanálisis.

Entonces solo hablamos de criptoanálisis cuando intentamos quebrar un mensaje cifrado a partir de intentar descifrar su clave o claves sin conocer el algoritmo a partir del cual se hace la encriptación. Entonces, como resultado del análisis de un cifrado podemos obtener una rotura total del mensaje, con lo que logramos obtener la clave de cifrado y, por ende, deducir el algoritmo que se usa; no conseguimos obtener la clave, pero conocemos y explicamos el algoritmo de cifrado y no logramos obtener la clave ni el algoritmo, pero logramos extraer los caracteres del mensaje cifrado que contienen el mensaje en claro.

**Quebrar**

En criptografía se conoce como el procedimiento para atacar un criptosistema y comprometer su seguridad a partir de obtener las claves.

Las técnicas que con mayor frecuencia se usan para desarrollar procesos de criptoanálisis son:

- Fuerza bruta: para un mensaje cifrado se aplican o prueban todas las claves posibles, este proceso se repite hasta encontrar la correcta. En lo general, este método se puede combinar con un ataque por diccionario, en los métodos modernos de cifrado, este ataque puede requerir de miles o millones de años para descifrar la clave, así cuando por fin se logre acceder al mensaje este ya no tendrá ningún valor.

- Análisis de frecuencias: el criptoanálisis de Kasiski que practicamos en este capítulo se basa en este método, así que en los que conocemos como métodos de sustitución será útil usar este análisis a partir de la búsqueda de patrones repetidos en el texto para llegar a la clave.

- Criptoanálisis diferencial: se desarrolla a partir del cifrado de cadenas de texto semejantes y se comparan con el cifrado final. La comparación permite reconocer diferencias para deducir cómo funciona el algoritmo.

- Análisis matemático: los algoritmos modernos de codificación se basan en problemas matemáticos que en apariencia no tienen solución, así, por ejemplo, en 1977 quienes desarrollaron el código RSA que se basa en factorizaciones de número enteros muy grandes consideraron que para factorizar un número entero de 129 cifras se necesitaban según los cálculos y herramientas de procesamiento disponibles a la fecha cerca de 40 trillones de años. Pero gracias al crecimiento de las herramientas automáticas para el procesamiento de información y por ende el desarrollo de nuevos métodos matemáticos en 1994 un grupo de matemáticos encabezado por Arjen Lenstra, rompió el cifrado para encontrar el mensaje oculto que decía: "Las palabras mágicas son delicados quebrantahuesos"

En este mismo orden de ideas, ¿podría un algoritmo de cifrado creado con las herramientas actuales resistir al menos cinco años sin ser quebrado?

## La seguridad de un sistema criptográfico

De acuerdo a las técnicas de criptoanálisis y los procedimientos que se puedan aplicar, la seguridad en este tipo de sistemas puede verse comprometida en niveles como:

- El atacante puede obtener parte del texto en claro, o, de la clave, se conoce como deducción de información.

- Con base en el texto cifrado se obtiene el texto en claro, se denomina deducción de una instancia.

- Con el criptoanálisis que se desarrolla se obtiene un algoritmo que produce un texto cifrado equivalente al original. Se conoce como deducción global.

- Cuando se presenta lo que conocemos como ruptura total, el análisis logra obtener la clave y descifrar por completo el mensaje en claro con ella.

El procedimiento que hemos desarrollado a lo largo de este ejercicio de introducción a la criptografía, es un tipo de criptoanálisis. Se trata de la criptografía de uno de los primeros métodos de criptoanálisis creado en el mundo y se conoce bajo el apellido de su creador, como el método Kasiski.

Así, apreciados estudiantes, espero que este breve recorrido por la historia y los conceptos clave de la criptología les suministre los elementos necesarios para abordar con éxito este apasionante curso que estoy seguro, les abre un amplio abanico de posibilidades de desarrollo a nivel profesional.

### Instrucción

Hemos llegado al final de este eje, los invito entonces a realizar la actividad de aprendizaje: demostración de roles y la evaluación objetiva en relación con los referentes que desarrollamos en él.

# BIBLIOGRAFÍA


Díaz, G., Mur, F., Sancristóbal, E., Alonso, M. y Piere, J. (2004). Seguridad en las comunicaciones y en la información. Madrid, España: Universidad Nacional de Educación a Distancia.

Fernández, S. (2004). La criptografía clásica. Revista Sigma, (24), 119-142.

Galende, J. (1995). Historia de la escritura cifrada. Madrid, España: Editorial Complutense.

García, R. (2009). Criptografía clásica y moderna. Recuperado de https://ebookcentral.proquest.com/lib/bibliotecafuaasp/detail.action?docID=3182091.

Lucena, M. (2010). Criptografía y seguridad en computadores. Recuperado de https://ldc.usb.ve/~figueira/cursos/Seguridad/Material/ManuelLucena/cripto.pdf

Molina, M. (2000). Seguridad de la información. Criptología. Bogotá, Colombia: El Cid.

Navarro, D. (2007). Derrotado, pero no sorprendido: reflexiones sobre la información secreta en tiempo de guerra. Recuperado de https://ebookcentral.proquest.com/lib/bibliotecafuaasp/detail.action?docID=3216475.

Ortega, T. y López, G. (2006). Introducción a la criptografía: historia y actualidad. Recuperado de https://ebookcentral.proquest.com

Shannon, C. (1949). Communication theory of secrecy systems. Bell Systems Technical Journal, 28, 656–675.

Singh, S. (2002). The code book: the secret history of codes and code-breaking, Londrés, Inglaterra: Fourth Estate.

San Marcos

**www.usanmarcos.ac.cr**

San José, Costa Rica