Colegio de Estudios Científicos y Tecnológicos del Estado de Puebla

Plantel Chignahuapan

Módulo 2, Submódulo 3

CRIPTOGRAFIA CLASICA Y MODERNA

Integrantes:

Edgar Esteban Ríos González	No.23
Juan Saúl Rodríguez Arroyo	No.25
Ana Irene Vega Hernández	No.42
Yanet Moredia Rosete	No.18

SMEC3A

Introducción

Los siguientes temes que se presentan en este texto son se basan en el tema “Criptografía clásica y moderna” que habla sobre los diferentes tipos de encriptación y codificación así como ha evolucionado tras el transcurso de los años y también las diferentes técnicas y sistemas que se han utilizado.

Los siguientes subtemas en los que se divide el tema principal son: Encriptación de la antigüedad, codificación, cifradores del siglo XIX, criptosistemas clásicos, máquinas de cifrar y encriptación del siglo XXI en los cuales se dan a conocer las distintas técnicas de encriptación.

Justificación

Elegimos este tema porque se nos hizo interesante e importante, para conocer las diferentes formas de la codificación y encriptación en la antigüedad y sus diferencias con los métodos de encriptación en la actualidad y como se desarrollaron los diferentes métodos utilizados y su evolución a través del tiempo.

Objetivo

Nuestro objetivo como equipo es dar a conocer los diferentes métodos de encriptación y sus diferencias entre los métodos de la antigüedad y los métodos actuales los cuales se siguen ocupando en la actualidad.

CRIPTOGRAFIA CLASICA Y MODERNA

La criptografía tradicionalmente se ha definido como la parte de la criptología que se ocupa de las técnicas, bien sea aplicadas al arte o la ciencia, que alteran las representaciones lingüísticas de mensajes, mediante técnicas de cifrado o codificado, para hacerlos ininteligibles a intrusos (lectores no autorizados) que intercepten esos mensajes. Por tanto el único objetivo de la criptografía era conseguir la confidencialidad de los mensajes. Para ello se diseñaban sistemas de cifrado y códigos. En esos tiempos la única criptografía que había era la llamada criptografía clásica.

Encriptación en la antigüedad

De las primeras constancias que se tienen de algo parecido a una “contraseña” dentro de un mensaje viene del antiguo Egipto. Para evitar que el enemigo interceptara un mensaje y escribiera uno nuevo para confundirlos el Faraón incluía en sus comunicados una palabra clave en un sitio determinado del texto y que el receptor conocía de antemano. Por ejemplo: La palabra “pirámide” debe ser la cuarta palabra del tercer renglón. Con un rápido vistazo al texto se podía comprobar y si no fuera así… pues ya puedes suponer la suerte que corría el mensaje y el mensajero.

En la antigüedad se trataba de ocultar los mensajes Griegos y Chinos, desde muy antiguo hicieron uso de la “tinta invisible” (agua con limón que aparece al calentar) y escribían con ella intercalando el “secreto” entre los renglones de un mensaje sin importancia escrito con tinta normal. Pero a veces no bastaba con esconder los mensajes, también había que hacerlos ilegibles.

De las primeras constancias criptológicas que existen se encuentra en el Antiguo Testamento.

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

Para escribir “HOLA” sería “SLOZ”.

En el 204 a. C. Pobilío describe un código que sirve tanto para mensajes escritos como ópticos a través de antorchas. Este sería algo así como el primer telégrafo visual. La idea es cifrar una letra con un par de números comprendidos entre 1 y 5 siguiendo esta tabla:

CLAVE

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

Aquí “HOLA” sería “23353211″. Y por ejemplo, para indicar la letra “B” con antorchas, se pondría 1 antorcha a la derecha y 2 a la izquierda. Supongo que este sistema no valdría para mensajes muy largos.

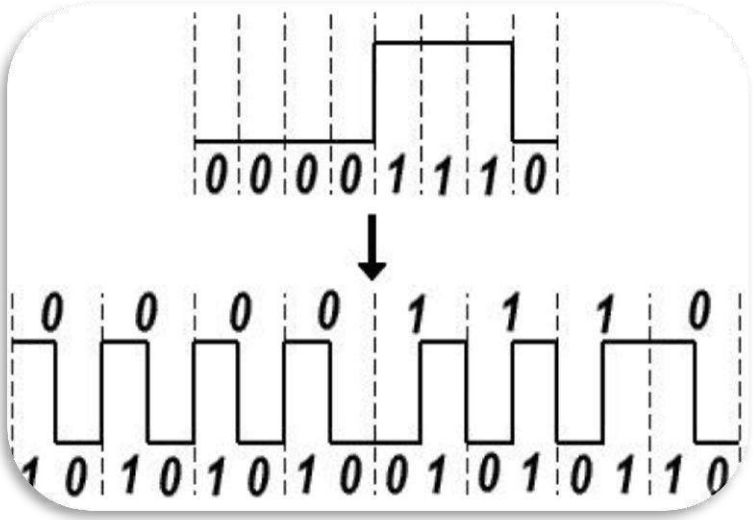
Codificación

La codificación es la transformación de la formulación de un mensaje a través de las reglas o normas de un código o lenguaje predeterminado.

Conocemos a la codificación como cualquier operación que implique la asignación de un valor de símbolos o caracteres a un determinado mensaje verbal o no verbal

con el propósito de transmitirlo a otros individuos o entidades que compartan el código.

La codificación es algo tan simple como lo que realizamos a diario cuando transformamos imágenes visuales o entidades conceptuales en palabras, oraciones, textos y las comunicamos a aquellos que nos rodean. También es codificación aquellas operaciones más complejas que implican códigos compartidos por menos interlocutores, como puede ser un mensaje cifrado o información emitida mediante el código Morse. Metafóricamente, además, se puede hablar de mensajes codificados cuando estos encierran un valor críptico o ininteligible para el público medio.

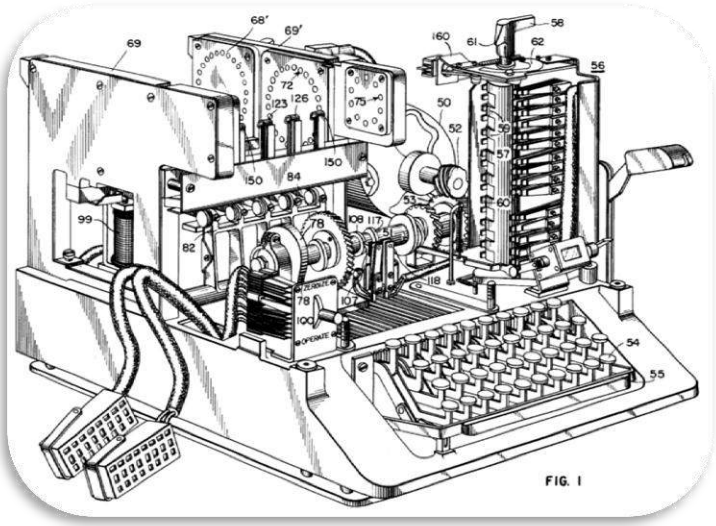


En informática, por lo tanto, la codificación es también aquella operación que tiene lugar para enviar datos de un lugar a otro, procesarlos y obtener resultados a partir de ellos. Todas las operaciones informáticas están cifradas en código binario, o bien, combinaciones más o menos complejas de unos y ceros que ocurren constantemente.

A su vez, determinadas operaciones con ordenadores requieren un segundo nivel de codificación. Son aquellas que precisan de aspectos de seguridad y confidencialidad y, por ende, implican la creación de mensajes cifrados que sólo pueden ser leídos por cierto tipo de ordenadores o por el usuario que los ha creado, como ocurre con las contraseñas y datos personales en transacciones en línea.

Cifradores del siglo XIX

Algunos de los ejemplos de lo último son el trabajo de Charles Babbage, en la época de la Guerra de Crimea, sobre el criptoanálisis matemático de los cifrados polialfabéticos, redescubierto y publicado algo después por el prusiano Fiedrich Kasiski. En esa época, el conocimiento de la criptografía consistía normalmente en reglas generales averiguadas con dificultad; véase, por ejemplo, los escritos de Auguste Kerckhoffs sobre criptografía a finales del siglo XIX. Edgar Allan Poe desarrolló métodos sistemáticos para resolver cifrados en los años 1840. Concretamente, colocó un anuncio de sus capacidades en el periódico de Filadelfia Alexander's Weekly (Express) Messenger, invitando al envío de cifrados, que él procedía a resolver. Su éxito creó excitación entre el público durante unos meses. Más tarde escribió un ensayo sobre los métodos criptográficos que resultaron útiles para descifrar los códigos alemanes empleados durante la Primera Guerra Mundial.



Proliferaron métodos matemáticos en la época justo anterior a la Segunda Guerra Mundial (principalmente con la aplicación, por parte de William F. Friedman, de las técnicas estadísticas al desarrollo del criptoanálisis y del cifrado, y la rotura inicial de Marian Rejewskide la versión del Ejército Alemán del sistema Enigma). Tanto la criptografía como el criptoanálisis se han hecho mucho más matemáticas desde la Segunda Guerra Mundial. Aun así, ha hecho falta la popularización de los ordenadores y de Internet como medio de comunicación para llevar la criptografía efectiva al uso común por alguien que no sea un gobierno nacional u organizaciones de tamaño similar.

Criptosistemas clásicos

Los sistemas de cifra podían clasificarse de varias formas, siéndola más aceptada aquella que toma en cuenta la característica del secreto de la clave, dando lugar a Criptosistemas de clave secreta y Criptosistemas de clave pública.

A comienzos del siglo XX el uso de la criptografía en las transmisiones de mensajes cobra una importancia inusitada por los tiempos que corrían (Primera y Segunda Guerras Mundiales), originando esto un gran auge tanto de las técnicas como de las máquinas de cifrar.

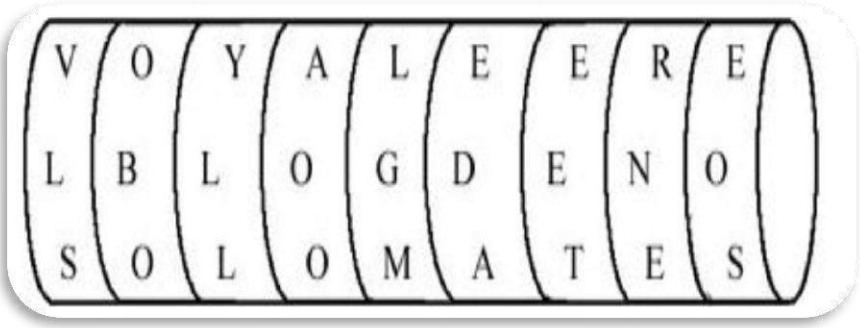
Muchos de los criptosistemas clásicos, en particular aquellos que transforman el mensaje en claro aplicando técnicas de sustitución y transposición, basan su seguridad principalmente en el secreto de la transformación o algoritmo de cifra. Es ésta también una diferencia fundamental con respecto a los sistemas modernos, en los que el algoritmo se hace público puesto que la fortaleza del sistema reside en la imposibilidad computacional de romper una clave secreta. Observe que el hacer público el algoritmo de cifra permite al criptólogo evaluar la calidad del software desarrollado, en tanto será estudiado por la comunidad científica intentando buscar un defecto, una puerta falsa, una rutina innecesaria, una codificación no depurada.

De todos los sistemas clásicos, cuya diversidad es enorme nos servirán como apoyo para profundizar y aplicar algunos conceptos que sobre criptosistemas, seguridad informática, teoría de la información, de los números y de la complejidad de los algoritmos han sido estudiados en los capítulos anteriores. Un ejemplo es el siguiente:

La escítala

Ya en siglo V antes de J.C. los lacedemonios, un antiguo pueblo griego, usaban el método de la escítala para cifrar sus mensajes. El sistema consistía en una cinta que se enrollaba en un bastón y sobre el cual se escribía el mensaje en forma longitudinal. Una vez escrito el mensaje, la cinta se desenrollaba y era entregada almensajero; si éste era interceptado por cualquier enemigo, lo único que se conseguía era un conjunto de caracteres o letras distribuidas al parecer de forma aleatoria en dicha cinta.

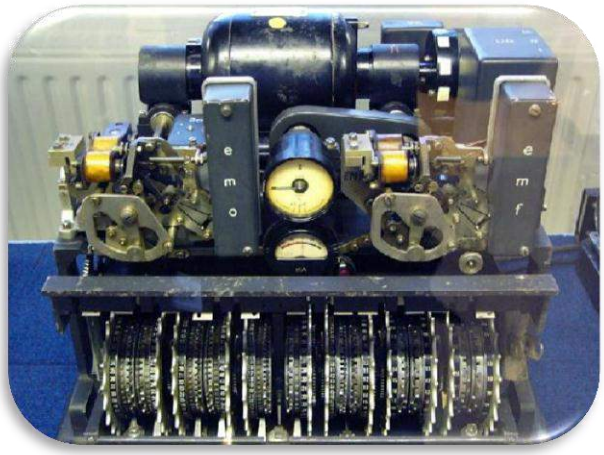
En este sistema no existe modificación alguna del mensaje; es decir, éste va en claro desde el transmisor hacia el receptor, por lo que de un cifrador por transposición.



Máquinas de cifrar (siglo XX) y estadística del lenguaje

La máquina alemana de cifrado Lorenz, usada en la Segunda Guerra Mundial para el cifrado de los mensajes para los generales de muy alto rango, su nombre Enigma.

Enigma era el nombre de una máquina que disponía de un mecanismo de cifrado rotatorio, que permitía usarla tanto para cifrar como para descifrar mensajes. Varios de sus modelos fueron muy utilizados en Europa desde inicios de los años 1920.



Su fama se debe a haber sido adoptada por las fuerzas militares de Alemania desde 1930. Su facilidad de manejo y supuesta inviolabilidad fueron las principales razones para su amplio uso. Su sistema de cifrado fue finalmente descubierto y la lectura de la información que contenían los mensajes supuestamente protegidos es considerada, a veces, como la causa de haber podido concluir la Segunda Guerra Mundial a los menos dos años antes de lo que hubiera acaecido sin su descifrado.

Typex (1937): Typex fue la variante británica de la máquina Enigma, usada de 1937. Al igual que esta, Typex era una máquina de rotores, pero tenía 5, en comparación con los 3-4 que solía tener las diferentes versiones. Normalmente los dos primeros rotores permanecían inmóviles durante el cifrado, aunque podían ser movidos a mano. Estos dos rotores adicionales proveían a la máquina un plus de seguridad adicional similar al que las clavijas proveían a la Enigma.

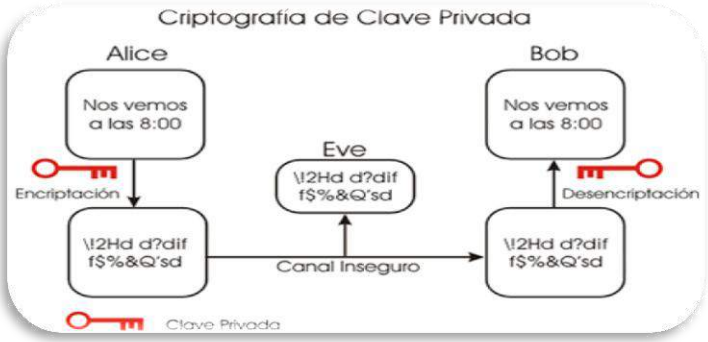
SIGABA: Fue la variante americana de la máquina Enigma, usada durante la Segunda Guerra Mundial hasta los 50. Básicamente, SIGABA era similar a Enigma, se basaba en una serie de rotores para encriptar los caracteres de un texto plano. Aunque la diferencia más llamativa era que SIGABA empleaba 15 rotores en vez de los 3 que usaba Enigma.

Encriptación del siglo XXI

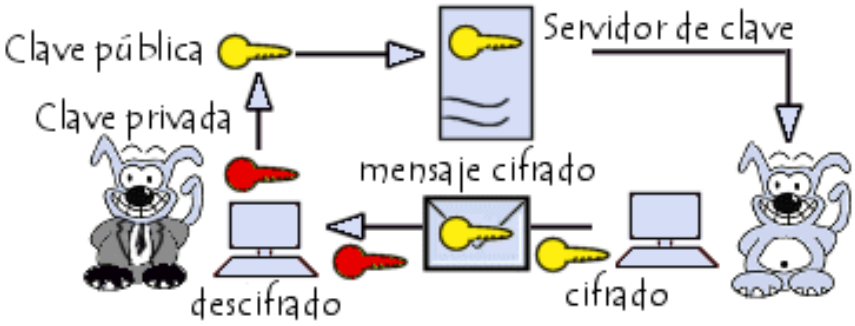
En la actualidad la encriptación se basa en los medios tecnológicos como las tecnologías de la información y la comunicación como las computadoras a diferencia del siglo XX que se utilizaban las máquinas de cifrar.

Los tipos de encriptación del siglo XXI más comunes son de los siguientes tipos:

Encriptación mediante claves simétricas: son las funciones más clásicas, es decir, se utiliza una determinada clave en la transformación de la información encriptada para conseguir desencriptarla, el problema reside en la necesidad de que todas las partes conozcan la clave.



Encriptación mediante claves asimétricas o públicas: existen también sistemas asimétricos de cifrado o de clave pública, cada usuario dispone de dos claves, una pública, que debe revelar o publicar para que los demás puedan comunicarse con él, y una privada que debe mantener en secreto.



Encriptación mediante códigos de integridad: se utilizan funciones matemáticas que derivan de una huella digital a partir de un cierto volumen de datos (una huella tiene de 128 a 160 bits). Es teóricamente posible encontrar dos mensajes con idéntica huella digital; pero la probabilidad es ínfima. Si se manipulan los datos la huella cambia; y modificar los datos de forma tan sabia para obtener la misma huella es algo computacionalmente inabordable en un plazo razonable.

	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

Encriptación mediante firma digital: Dado un mensaje, basta calcular su huella digital y cifrarla con la clave secreta del remitente para obtener simultáneamente la seguridad de que el contenido no se manipula (integridad), y de que el firmante es quien dice ser (autenticación). Las firmas digitales suelen ir asociadas a una fecha. La fecha de emisión (y posiblemente la fecha de vencimiento de validez) suelen proporcionarse en texto claro, e incorporarse al cálculo de la huella digital, para ligarlas irrenunciablemente.

Conclusiones

Juan Saúl Rodríguez arroyo:

En mi opinión mi tema se me hizo muy interesante porque comprendí los distintos métodos de codificación en la antigüedad y las diferencias que hay entre los métodos de a hora y los de antes, para mí la codificación es la transformación de un mensaje a través de reglas o normas de un código o lenguaje predeterminado.

Al igual la codificación es cualquier operación que implique la asignación de un valor de símbolos o caracteres a un determinado mensaje verbal o no verbal con el propósito de transmitirlo a otros individuos o entidades que compartan el código.

La codificación se ocupó en la antigüedad más a menudo en las guerras ya que los ejércitos aplicaban esto para que los contrarios no descubrieran los diferentes mensajes que se llevaban.

También medí cuenta de las similitudes que tienen las máquinas de encriptación en la antigüedad a lo que hoy en día ocupamos la computadora para realizar diferentes métodos de encriptación para proteger información o claves importantes como las de banco.

Yanet Moredia Roste:

Este tema de la encriptación es importante ya que es un tema, que casi nadie conoce, a pesar de que es muy antiguo. El conocer este tipo de encriptación nos ayuda a conocer un poco más de la historia.

La encriptación tiene diferentes maneras de hacerlo, y es interesante conocerlas porque este método lo utilizaban en la guerra para comunicarse.

En la actualidad aún existen pero ya son muy diferentes alguna ya que, nosotros las llegamos a inventar y otras simplemente se modifican con forme pasa el tiempo, se hace esto ya que casi nadie conoce el método.

Ojala que este tema se diera conocer más ya que, es importante y sería una manera de revivir la historia en la actualidad.

La encriptación es un método que no es muy utilizado y si nosotros lo llegáramos a utilizar en algún grupo social sería muy difícil descifrarlo ya que ese tipo de gente no lo conoce y a la vez sería bueno darlo a conocer.

Edgar Esteban Ríos González:

Al hacer tanta investigación de este tema y sus distintos subtemas llegue a la conclusión de que los métodos de encriptación se empezaron a utilizar desde la antigüedad y se fueron usando en las guerras mundiales para lograr que distintos mensajes llegaran a otras personas sin que personas sin autorización pudieran leerlo ya que debían descifrarse y solo los científicos podían hacerlo.

También me di cuenta de que en la antigüedad los métodos de encriptación eran mecánicos en su mayoría a diferencia de los métodos que utilizamos en la actualidad que por lo general se hace mediante computadoras.

Yo creo que si se manejara más la encriptación en la vida diaria sería muy útil ya que en cualquier situación en la que se requiera de forma urgente a personas con estos conocimientos sería más fácil descifrar claves y códigos.

También pude diferenciar varios métodos y obtuve mucho conocimiento con el que ya puedo aplicar mis conocimientos para proteger documentos o algunas claves.

Ana Irene Vega Hernández:

Mi conclusión de esto es que la encriptación se ha definido como la parte de la criptología que se ocupa de las técnicas, bien sea aplicadas al arte o la ciencia, que alteran mensajes, mediante técnicas de cifrado o codificado, para hacerlos ininteligibles a intrusos que intercepten esos mensajes. Por tanto el único objetivo de la criptografía era conseguir la confidencialidad de los mensajes. Para ello se diseñaban sistemas de cifrado y códigos. En esos tiempos la única criptografía que había era la llamada criptografía clásica.

Yo creo que este conocimiento me puede ser útil en la vida diaria ya que en algunas ocasiones puedo necesitar estos métodos para proteger claves y archivos.

Aprendí también que en la guerra utilizaban la encriptación para enviar mensajes si que fueran leidos por personas no autorizadas.