Universidad Nacional Autónoma de México
Facultad de Ciencias

Proyecto Final Análisis Numérico
Semestre 2025-1

Cifrado de Hill

Integrantes:

Luna García Aarón Abdi
Mendoza Granillo Leonardo Cuauhtémoc
Monroy García Zoé Abigail

Índice

Introducción

¿Qué es la criptografía?

La **criptografía** es un método de protección de la información y las comunicaciones mediante el uso de códigos, de modo que sólo aquellos a quienes está destinada la información puedan leerla y procesarla.

En la era digital moderna, la criptografía se ha convertido en una herramienta esencial de ciberseguridad para proteger la información confidencial de hackers y otros delincuentes cibernéticos.

Puede emplearse para ocultar cualquier forma de comunicación digital, incluidos texto, imágenes, video o audio. En la práctica, la criptografía se emplea principalmente para transformar mensajes en un formato ilegible (conocido como texto cifrado) que sólo el destinatario autorizado puede descifrar en un formato legible (conocido como texto sin formato) empleando una clave secreta específica.

La criptografía moderna se ha vuelto significativamente más avanzada con el tiempo. Sin embargo, la idea general sigue siendo la misma y se ha fusionado en torno a cuatro principios fundamentales.

- ➔ Confidencialidad: sólo puede acceder a la información cifrada la persona a la que está destinada y nadie más.
- ➔ Integridad: la información cifrada no se puede modificar en el almacenamiento ni en tránsito entre el remitente y el receptor previsto sin que se detecten alteraciones.
- ➔ No repudio: el creador/remitente de la información cifrada no puede negar su intención de enviar la información.
- ➔ Autenticación: se confirman las identidades del remitente y del destinatario, así como el origen y el destino de la información.

Usos comunes para la criptografía

- ➔ Contraseñas: Se utiliza frecuentemente para validar la autenticidad de las contraseñas y también para proteger las contraseñas almacenadas.

- ➔ Criptomonedas: Se basan en complejos sistemas de cifrado de datos que requieren grandes cantidades de potencia de cálculo para descifrarlos. A través de estos procesos de descifrado, se “acuñan” nuevas monedas y entran en circulación.

- ➔ Navegación web segura: Protege a los usuarios de los ataques de intermediario (MitM) y de las escuchas clandestinas. Los protocolos Secure Sockets Layer (SSL) y Transport Layer Security (TLS) se basan en criptografía de clave pública para proteger los datos enviados entre el servidor web y el cliente y establecer canales de comunicación seguros.

- ➔ Firmas electrónicas: Se utilizan para firmar documentos importantes en línea y se pueden validar para evitar fraudes y falsificaciones.

- ➔ Autenticación: Ayudar a confirmar y verificar la identidad de un usuario y autenticar sus privilegios de acceso.

- ➔ Comunicaciones seguras: Mantener una conversación privada, autenticación de mensajes y proteger las comunicaciones bidireccionales, como las conversaciones de video, los mensajes instantáneos y el correo electrónico.

La criptografía puede garantizar la confidencialidad e integridad tanto de los datos en tránsito como de los datos en reposo. También puede autenticar a remitentes y destinatarios entre sí y proteger contra el repudio.

¿Qué es el cifrado?

El **cifrado** es un método de seguridad que consiste en codificar datos sin formato para convertirlos en datos cifrados, el cuál sólo puede descifrar el usuario con una clave. Sólo las partes autorizadas con la clave secreta correcta, conocida como clave de descifrado, pueden descifrar los datos.

El cifrado puede proteger los datos en reposo, en tránsito y mientras se procesan, independientemente de si los datos están en un sistema informático o

en la nube. Por esta razón, el cifrado se volvió fundamental para los esfuerzos de seguridad en la nube y las estrategias de ciberseguridad en general.

Según el informe *Costo de una filtración de datos* de IBM, las organizaciones que usan cifrado pueden reducir el impacto financiero de una filtración de datos en más de 220.000 USD.

Los algoritmos de cifrado modernos han reemplazado el estándar de cifrado de datos obsoleto para proteger los datos. Estos algoritmos protegen la información y fomentan las iniciativas de seguridad, incluida la integridad, la autenticación y el no repudio.

Los algoritmos primero autentican un mensaje para verificar el origen. A continuación. comprueban la integridad para verificar que los contenidos no hayan cambiado. Finalmente, la iniciativa de no repudio evita que los envíos nieguen la actividad legítima.

Tipos de cifrado de datos: asimétrico y simétrico

El cifrado **simétrico** es un tipo de método de criptografía en el que se utiliza la misma clave tanto para cifrar (convertir el texto plano en texto cifrado) como para descifrar (revertir el texto cifrado al texto plano). Este enfoque es uno de los más antiguos y ampliamente usados en criptografía.

El cifrado **asimétrico**, también conocido como criptografía de clave pública, cifra y descifra los datos utilizando dos claves asimétricas criptográficas independientes. Estas dos claves se conocen como "clave pública" y "clave privada".

¿Cómo funciona el cifrado de datos?

El cifrado comienza con identificar la información confidencial que requiere protección. Esta información puede ser mensajes, archivos, fotografías, comunicaciones u otros datos. Estos datos existen en texto sin formato: la forma original y legible que necesita protección.

Los algoritmos de cifrado transforman este texto sin formato en texto cifrado al codificar los datos en una secuencia de caracteres ilegible. Este proceso garantiza que solo los destinatarios previstos puedan leer los datos originales.

Cifrado Hill

El cifrado de Hill es un método de criptografía simétrica basado en álgebra lineal. Fue inventado por el matemático estadounidense Lester S. Hill en 1929. Este cifrado utiliza matrices y operaciones matemáticas sobre un alfabeto para cifrar y descifrar mensajes, haciendo uso de transformaciones lineales.

El cifrado de Hill utiliza una **clave** que es una matriz cuadrada invertible (en aritmética modular) y emplea la multiplicación de matrices para transformar bloques de texto plano en texto cifrado.

En general, al utilizar el cifrado de Hill son necesarios los siguientes elementos:

- Un natural mayor a 1 k, el cual definirá el tamaño de los bloques de información así como el tamaño de la matriz que será usada para cifrar la información
- Un módulo m, el cual tiene relación con el tipo de dato que estamos usando, por ejemplo, si estamos trabajando con textos, m puede ser 26, pues corresponde a la cantidad de letras (sin contar ñ ni acentos) que hay en el abecedario.
- La matriz de cifrado de k por k, la cual está conformada por elementos, que pueden ser elegidos al azar o no, que deberá cumplir con las siguientes características:
    - ☐ Todos sus elementos deberán encontrarse en módulo m
    - ☐ Deberá tener determinante distinto de 0 , es decir, |k|≠0
    - ☐ La matriz k deberá ser invertible en Z_m
    - ☐ El determinante de k y la base deberán ser primos relativos, i,e, mcd(|k|, m)=1

Donde el algoritmo funciona de manera general tal que:

1. Se divide la información en bloques de k elementos
2. Cada uno de los bloques es multiplicado por la matriz llave de dimensión $k \times k$
3. Se toma el módulo m de los resultados
4. Se vuelven a unir de acuerdo a la estructura de la información

Para poder descifrar la información únicamente es necesaria la matriz llave, pues es un algoritmo de cifrado simétrico, el algoritmo a seguir es el mismo como si estuviéramos realizando el cifrado pero con la diferencia de que se usa la matriz inversa de k en Z_m

Donde esta puede ser encontrada como:

$M_k^{-1} = C^T |M_k|^{-1}$

Donde C^T es la matriz de cofactores de M_k transpuesta

El tipo de información que se puede encriptar es bastante amplia, podemos cifrar texto basándonos en la representaciones ASCII, datos computacionales traduciendolos a base 10 o hexadecimal, imágenes, audio, etc. Todo dependerá de la estructura que le demos.

Como todo en esta vida, se tienen ventajas y desventajas de usar este algoritmo de cifrado:

Ventajas:

- Ocultar las frecuencias de las datos individuales
- Simplicidad al usar la multiplicación e inversión de matrices para el cifrado y el descifrado,
- Alta velocidad y alto rendimiento.

Desventajas:

- Se necesita de matrices de dimensiones grandes para mejorar el encriptamiento
- Son susceptibles a roturas usando métodos de álgebra lineal que incluyen traspuestas y reducción gaussiana

Desarrollo del proyecto

Ejemplificamos dos escenarios donde puede ser usado el Cifrado Hill, siendo el primero de ellos el encriptado de textos y el segundo el encriptado de imágenes.

Encriptado de textos

Consideraciones del trabajo

Para el desarrollo de esta parte, consideraremos que las letras, caracteres y símbolos permitidos son: las 52 letras del alfabeto (mayúsculas-minúscula), 10 dígitos numéricos (del 0 al 9) así como una lista de caracteres especiales, en ese orden. En la siguiente tabla, se muestra la asignación numérica que se dará a cada uno de los caracteres anteriormente mencionados:

Carácter	Asignación	Carácter	Asignación	Carácter	Asignación
A	0	O	28	4	56
a	1	o	29	5	57
B	2	P	30	6	58
b	3	p	31	7	59
C	4	Q	32	8	60
c	5	q	33	9	61
D	6	R	34	punto(“.”)	62
d	7	r	35	coma(“,”)	63
E	8	S	36	dos puntos(“:”)	64
e	9	s	37	¿	65
F	10	T	38	?	66
f	11	t	39	!	67
G	12	U	40	¡	68
g	13	u	41	guión(“-”)	69
H	14	V	42	guión bajo(“_”)	70
h	15	v	43	gato(“#”)	71
I	16	W	44	punto y coma(“;”)	72
i	17	w	45	pesos(“$”)	73
J	18	X	46	más(“+”)	74
j	19	x	47	et(“&”)	75

K	20	Y	48	igual(“=”)	76
k	21	y	49	(	77
L	22	Z	50	)	78
l	23	z	51	%	79
M	24	0	52	/	80
m	25	1	53	*	81
N	26	2	54	espacio(“ ”)	82
n	27	3	55		

De esta manera, estaremos trabajando con 83 por lo que usaremos módulo 83. Esta tabla será implementada como un diccionario dentro del código, para así aprovechar las propiedades de este al momento de pasar de texto a números y viceversa, donde el símbolo de gato tendrá un significado especial.

La anterior lista de caracteres puede seguir aumentando según la necesidad o nivel de complejidad que deseamos abarcar, sin embargo, hay dos principales razones por las cuales tomemos 83 caracteres: representatividad y cumplimiento de supuestos.

- Representatividad: Consideramos que con esta cantidad de caracteres es posible representar de manera adecuada la gran mayoría de textos incluyendo aquellos en inglés y algunas otras lenguas.
- Cumplimiento de supuestos: Como parte de las condiciones necesarias para el Cifrado Hill, es necesario que el mínimo común múltiplo entre el módulo y el determinante de la matriz sea 1, por lo que al escoger nuestro módulo un número primo,podemos asegurar que siempre se cumplirá.

Como sabemos, este es un encriptamiento por bloques, es decir, es necesario n datos por bloque, por lo que si no existen datos necesarios para llenar dicha matriz, usaremos el símbolo “#” para rellenar esos espacios. Es importante tener en claro que el símbolo “#” solo sirve de relleno cuando tratamos con textos no cifrados, cuando ciframos el texto el símbolo “#” puede representar algún carácter.

Dado que gracias a lo anterior podemos rellenar espacios faltantes, se dará libertad al elegir el tamaño de los bloques a utilizar en el encriptado.
El cifrado Hill aplicado a la parte de cifrado de textos, se ve de la siguiente manera:

1. Elegimos una matriz llave de $k \times k$ (Que cumpla los supuestos), donde los elementos de este deberán estar en módulo 83.

$$\begin{pmatrix} 12 & 22 & 6 \\ 2 & 4 & 2 \\ 0 & 3 & 1 \end{pmatrix}$$

2. Tomamos nuestro texto y lo dividimos en bloque de k elementos, en el caso donde el último bloque no tenga k elementos, agregamos el carácter "#" cuantas veces sea necesaria para que coincida.
   Continuando con el ejemplo, usamos una frase corta como "Inti lluqsimun" ("Ha salido el sol" en Quechua), la cual tiene 13 caracteres, se dividiría en bloques tal que:

Bloque
Int
i" "l
luq
sim
un#

3. Bloque por bloque, usando la tabla, traducimos los caracteres a su valor correspondiente.
   Traducimos

Bloque	Asignación
Int	(16, 27, 39)
i" "l	(17,82,23)
luq	(23,41,33)
sim	(37,17,25)

un#	(41,27,71)

4. Bloque por bloque, multiplicamos la matriz llave por cada bloque que ahora tiene datos numéricos. Por ejemplo, para el primer bloque

$$\begin{pmatrix} 12 & 22 & 6 \\ 2 & 4 & 2 \\ 0 & 3 & 1 \end{pmatrix} \begin{pmatrix} 16 \\ 27 \\ 39 \end{pmatrix} = \begin{pmatrix} 1020 \\ 218 \\ 120 \end{pmatrix}$$

   La frase entera por bloques quedaría:

Bloque	Asignación	Multiplicación
Int	(16, 27, 39)	(1020, 218, 120)
i” “l	(17,82,23)	(2146,408,269)
luq	(23,41,33)	(1376,276,156)
sim	(37,17,25)	(968,192,76)
un#	(41,27,71)	(1512,332,152)

5. Al resultado de cada producto, aplicamos módulo 83

Bloque	Asignación	Multiplicación	Módulo
Int	(16, 27, 39)	(1020, 218, 120)	(24, 52,37)
i” “l	(17,82,23)	(2146,408,269)	(71, 76, 20)
luq	(23,41,33)	(1376,276,156)	(48,27,73)
sim	(37,17,25)	(968,192,76)	(55,26,76)
un#	(41,27,71)	(1512,332,152)	(18,0,69)

6. Volvemos a traducir de número a dígito

Bloque	Asignación	Multiplicación	Módulo	Nuevo bloque
Int	(16, 27, 39)	(1020, 218, 120)	(24, 52,37)	M0s
i” “l	(17,82,23)	(2146,408,269)	(71, 76, 20)	#=K
luq	(23,41,33)	(1376,276,156)	(48,27,73)	Yn$
sim	(37,17,25)	(968,192,76)	(55,26,76)	3N=
un#	(41,27,71)	(1512,332,152)	(18,0,69)	JA-

7. Reconstruimos en el mismo orden que obtuvimos el bloque “M0s#=KYn$3N=JA-”

De esta manera, tenemos un mensaje cifrado usando el cifrado Hill. Es importante mencionar que cambiar el orden, la asignación numérica, la cantidad de elementos a considerar y la matriz llave, lo que nos daría resultados distintos a los obtenidos con nuestro planteamiento, dando así la posibilidad de crear una gran cantidad de encriptamientos distintos.

Implementación en código

Elegiremos como lenguaje de programación python, apoyándonos de las librerías numpy para realizar las operaciones necesarias que corresponden a las matrices.

No usaremos una matriz llave en general, sino que el programa dará libertad acerca de la matriz llave que el usuario decida elegir, implementando también una opción de generar aleatoriamente una matriz de tamaño k, propuesta por el usuario.

Ejemplos:

Usando la matriz anteriormente usada, como matriz llave

$$\begin{pmatrix} 12 & 22 & 6 \\ 2 & 4 & 2 \\ 0 & 3 & 1 \end{pmatrix}$$

El texto

“Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.”

Se encripta como:

q:t#q+o?xUH+PFnqPk42d(0OIzHl=WP2s7Jvb,&0IF&Nn&wQlkT09bL%LKuR!aZt¡Wwp1*aK-*06
tNs)9e6l9.HVqI_q!4DFZpco?!aZw?t_:Lwm?%A*JHa4W¿l_=Ic2ay+(OKDD)ay+XF2WcOjLPe6ce*
nJz-7mKR6!zuQ8(VETpQV,qiOOub!4D6?tbuMuZww+%¿YNH
5Z$e5T5uKBJFo!HfM:BB+ra?5/qgRk7IHn-)%LYHT3&wOCQVhBiHHsQCXw(g2RiPQZdNs)o.&Sl
#8(VGiU09bBeD!+sR0QQ2n#8CQVhpkNEHtqX1wqV*Ltu5_Guf150b,&l1c:yMt_vf2k!P)tyNFQI6U
l9aBp+nEgVR$qw6pZNwi56lTsvPR&jsNs)Gi4zDfxX5McN9iZm/0PWPLH.&jsY$k2Dbs=*JD=;/6=
m:bsKb;T9r¿=0r

El texto:

“Andrei Nikolayevich Kolmogorov (Tambov, 25 de abril de 1903-Moscu, 20 de octubre de 1987) fue un matematico ruso que realizo aportes de primera linea en los contenidos de teoria de la probabilidad y de topologia. Estructuro el sistema axiomatico de la teoria de la probabilidad, utilizando el lenguaje teoria de conjuntos, donde los elementos son eventos. Trabajo en logica constructivista; en las series de Fourier; en turbulencias y mecanica clasica. Fundo la teoria de la complejidad algoritmica. En 1929, bajo la supervision del matematico Nikolai Luzin, alcanzo el doctorado en la Universidad Estatal de Moscu.”

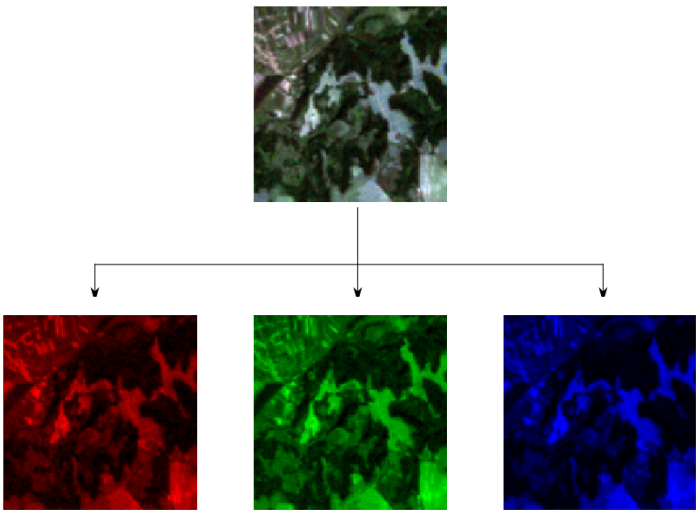
Se encripta como:

3tc45W*1GQTn¿Z$d*4o?iERf9B¡#lxaZK
m)GMNM%1PWPOEDjJ+PWPNA2dx¡-;uGzK(-YPWP&ue8
vpkNnYNH3(fg!eTy4Z!Xi=-*07NzOubZ7(NsPKqNvmOvZjA4*6
t6L:PWPZNw9-ak;B¿B)uKBQu/5_ul=W+.v=16(TnnYNFD4150PWPBe_ZNwc;FZs+Q:LMmXPWP
MX,-6n;94V
j¿=!M)wb,&Y;D9qRdf!As=vgZ%Ro7NzOubnYNvYBFD4150PWPBe_ZNwc;FZs+Q:L1hLulzvZj!uc
Y;D8cKq-fxuL#eSvTt2SBnYNPHpxd!Ajuo1C#Hc68K(TnCw)%52Aju,T5M¡DXF2AjusPrw/Dl1bIc2
C¿h.k4KEBB+r$z,MRzq.ce8&Ic2Be_,9R!Ntb*nnYNE0wJ$8DMyQu/b,&/Z,¡1bqoU:N,PgQW9h=G
B+k_J-4V
jL;!0wbvYBFD4150PWPBe_l=Wu2qxw+¿QF¿YNEXtZ+7#4Il1ct$Zww5cwAl1bBe_0.-qB.q.cETpP
WP;eLfFv6yV$oW*1GQTnY¡Z99EHj9¿YN)¡P
Zbnm¡c5e#htEcZIc2Be_RX:V63Ebw¿QF2k98(VHe¡nYN-;uDyj

Encriptado de Imágenes

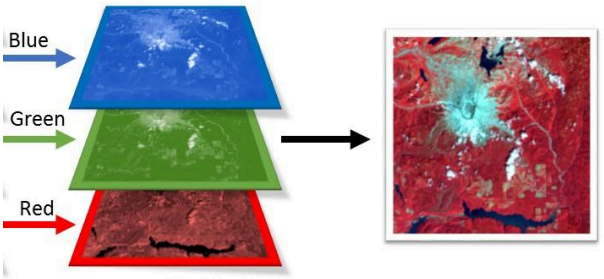
Consideraciones del trabajo.

Esta parte del trabajo fue desarrollada considerando imagenes a color que cumplan con la condición de ser tridimensionales (ancho, alto, colores), es decir, tengan un parte para el color rojo, otra para el color verde y otra para el color azul (colores RGB) en formatos png, jpg,jpeg,etc.



Además, se trabajará con el módulo 256, que corresponde a la cantidad de posibilidades de colores que se tiene en cada color (rojo, azul y verde). También en esta ocasión restringimos la dimensión las matrices llaves a matrices de 3×3 para aprovechar la estructura de la imagen.

Cada imagen está constituida por pixeles, por ejemplo, si tenemos una imagen de tamaño $40x40$ tenemos 1600 pixeles, donde cada pixel está relacionado a una coordenada y está compuesto por 3 partes, parte roja, parte verde y parte roja.



Siendo esta condición la que aprovecharemos para encriptar de una manera más efectiva.

El cifrado Hill en imagenes de color (RGB) se vería de la siguiente manere:

1. Escogemos una matriz de $3x3$, donde los elementos deberán estar en el módulo 256, que será nuestra matriz llave. Ejemplo:

$$\begin{pmatrix} 3 & 11 & 7 \\ 17 & 101 & 179 \\ 0 & 227 & 23 \end{pmatrix}$$

2. Elegimos nuestra imagen, la transformamos a forma matricial y la dividimos en pixeles. Un pixel en forma matricial tiene la forma:

$$[[2] \quad [44] \quad [178]]$$

   Donde cada entrada corresponde a un nivel de cada color (RGB), esta matriz, tiene dimensiones (1,1,3), por lo que se redimensiona a una matriz de $3x1$

3. Multiplicamos la matriz llave por cada pixel en forma de matriz redimensionada

$$\begin{pmatrix} 3 & 11 & 7 \\ 17 & 101 & 179 \\ 0 & 227 & 23 \end{pmatrix} \begin{pmatrix} 2 \\ 44 \\ 178 \end{pmatrix} = \begin{pmatrix} 1736 \\ 36340 \\ 14082 \end{pmatrix}$$

4. Obtenemos módulo 256 del resultado

$$\begin{pmatrix} 1736 \\ 36340 \\ 14082 \end{pmatrix} mod(256) = \begin{pmatrix} 200 \\ 244 \\ 2 \end{pmatrix}$$

5. Regresamos a la dimensión original el pixel y sustituimos el pixel viejo por este nuevo pixel
6. Reconstruimos la imagen de su forma matricial

Implementación en código

Elegiremos como lenguaje de programación python, apoyándonos de las librerías numpy para realizar las operaciones necesarias que corresponden a las matrices.
El usuario deberá indicar los 9 números que constituyen la matriz llave, así como la ruta de la imagen a encriptar/desencriptar, dando libertad de guardar con el nombre que desee la imagen encriptada o desencriptada

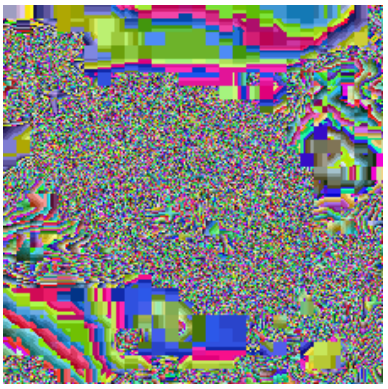
Ejemplo:

Usando la matriz llave

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$$

La imagen (la impresión es en blaco y negro, por lo que no se aprecian los colores):

La imagen encriptada se ve como:



Es importante mencionar que, se puede tener mayor libertad al cifrar imágenes, podríamos unir las 3 matrices que componen la imagen en sentido vertical y tomar los bloques de manera vertical, después encriptar y regresar a la forma original; podríamos realizar lo mismo pero uniendo de manera horizontal, y tomando los píxeles horizontales. Podremos usar cualquier otra llave de dimensión que queramos para cifrar,etc.

¿Cómo desencriptar?

Imaginemos que tenemos una matriz M de dimensión $k \times k$ que funciona como nuestra llave para encriptar información, y ahora queremos desencriptarla. El algoritmo de desencriptación es el mismo pero con la diferencia de que en lugar de usar la matriz M, usamos su inversa módulo m, la cual podemos obtener de la siguiente manera:

1. Sabemos que podemos ver a la inversa de una matriz como:

   $$M^{-1} = \frac{1}{|M|} Adj(M)$$

2. Buscamos ahora un número x tal que $|M| * x = 1\, mod(m)$, de este modo $\frac{1}{|M|} = x\, mod(m)$
3. Sustituimos $M^{-1} = x * Adj(M)$
4. Finalmente obtenemos módulo m en cada uno de los elementos de a matriz

De esta manera obtenemos la matriz inversa que usaremos para desencriptar la información, aquí se nota la importancia de que el determinante de la matriz

llave sea distinto de 0 y que sea primo relativo del módulo m, para sí poder asegurar que tiene inverso en Z_m

Conclusiones

- **Luna García Aarón Abdi:**

  El cifrado Hill es un método interesante dentro de la criptografía clásica, ya que combina principios matemáticos, como álgebra lineal y aritmética modular, con la seguridad del cifrado polialfabético.

  El uso de matrices y vectores lo convierte en un cifrado avanzado para su época. Esto lo hace más robusto que otros métodos. Introduce múltiples alfabetos al cifrar varias letras a la vez, lo que complica los intentos de descifrado sin la clave. Por otra parte, frente a cifrados modernos, el cifrado Hill es inseguro, ya que no puede manejar ataques computacionales avanzados.

  El cifrado Hill es un excelente ejemplo educativo para entender cómo las matemáticas pueden aplicarse a la criptografía. Representa un puente entre los métodos de cifrado simples y los sistemas más complejos usados hoy en día.

- **Mendoza Granillo Leonardo Cuauhtémoc:**

  El Cifrado Hill es un algoritmo simple, que podríamos decir tiene como base las matrices y el álgebra modular, donde podemos ver al álgebra modular como un cambio de base donde tomamos el primer elemento de este nuevo número. Como ya observamos, puede tratar con diferentes tipos de datos, de diferentes maneras de acuerdo a nuestras necesidades, haciendo un algoritmo a mi parecer completo en el sentido de la cantidad gigantes de posibilidades que existen, en contraste a la complejidad de su funcionamiento. Sin embargo, al ser un algoritmo antiguo, diseñado para satisfacer las necesidades de seguridad de esos años, claramente es poco eficiente en cubrir las demandas de seguridad de hoy en día, eso no elimina el hecho de que es un algoritmo base para el entendimiento de lo que es encriptar y que ha sido y puede seguir siendo mejorado, además de ser base para algunos otros algoritmos.

- **Monroy García Zoé Abigail:**

  El algoritmo del cifrado de Hill hace uso del álgebra modular y es una gran aplicación de la criptografía, así mismo, destaca por su simplicidad y capacidad para manejar diferentes tipos de datos, pues se desarrolla de gran forma en el campo de la seguridad de la información.

  Aunque es un método robusto y muy avanzado para su época, considerando que podemos hacer encriptado de textos e imágenes, algo que me parece algo muy completo. Sabemos que presenta limitaciones frente a los avances tecnológicos modernos, pues es difícil satisfacer tanta demanda de seguridad que se presenta en la actualidad. De igual forma da una base sólida para comprender los principios fundamentales del cifrado y su evolución hacia métodos más complejos.

Referencias Formato APA

- Ibm. (2024, 18 julio). Criptografía. IBM. https://www.ibm.com/mx-es/topics/cryptography
- Ibm. (2024, septiembre 9). ¿Qué es el cifrado? Definición de cifrado de datos. IBM. https://www.ibm.com/mx-es/topics/encryption
- Ibm. (2024, 18 julio). ¿Que es la ciberseguridad?. IBM. https://www.ibm.com/mx-es/topics/cybersecurity
- Ibm. (2024, 11 octubre). ¿Qué es el cifrado end to end?. IBM. https://www.ibm.com/mx-es/topics/end-to-end-encryption
- Ibm. (2024, 11 octubre). ¿Qué es un ataque cibernetico?. IBM. https://www.ibm.com/mx-es/topics/cyber-attack
- Tomé, C. (2017, 11 enero). Criptografía con matrices, el cifrado de Hill. Cuaderno de Cultura Científica. https://culturacientifica.com/2017/01/11/criptografia-matrices-cifrado-hill/
- Wikipedia. (2023, 27 septiembre). Cifrado Hill. Wikipedia, la Enciclopedia Libre. https://es.wikipedia.org/wiki/Cifrado_Hill