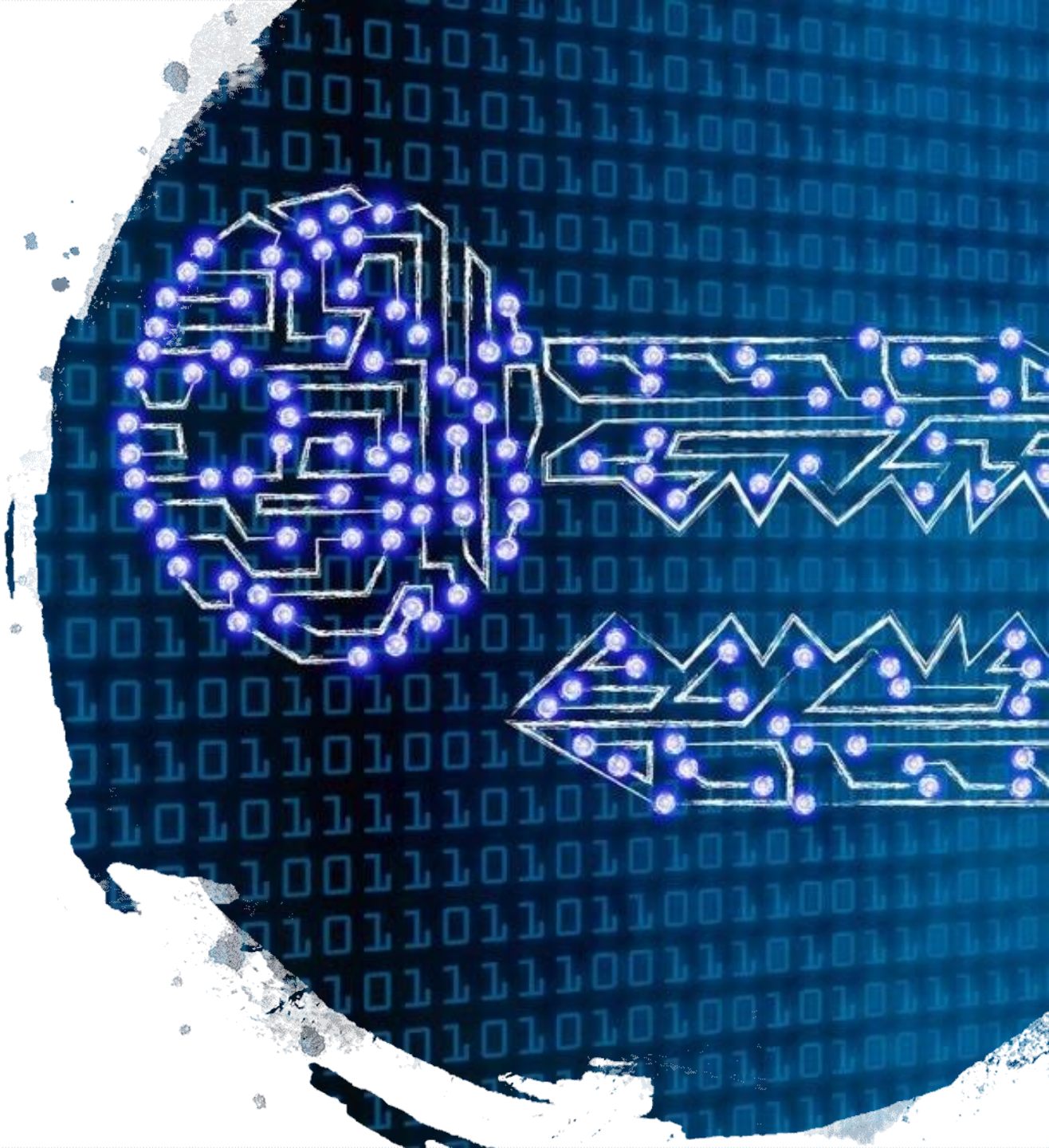
CÓDIGOS LINEALES EN CRIPTOGRAFÍA



Integrantes:

Santos Méndez, Manuel José – 18001167
Palma Salvatierra, Harim Abdalá – 18001882
Flores Martínez, Jair Alexander - 18002715

AGENDA

- Historia de la Criptografía
- La Criptografía
- Definiciones
- Métodos de Cifrado (Cifrado de Hill)
- Ventajas & Desventajas
- Aplicación

La humanidad y su necesidad por comunicar sus ideas…

¿Y si necesitamos transmitir un mensaje que no queremos que nadie más conozca?

Esto queda obsoleto...

A PARTIR DE ESA NECESIDAD NACE:

LA CRIPTOGRAFÍA

¿Qué es la criptografía?

CRIPTOLOGÍA

"CIENCIA DE ESCRIBIR O DESCIFRAR CLAVES"

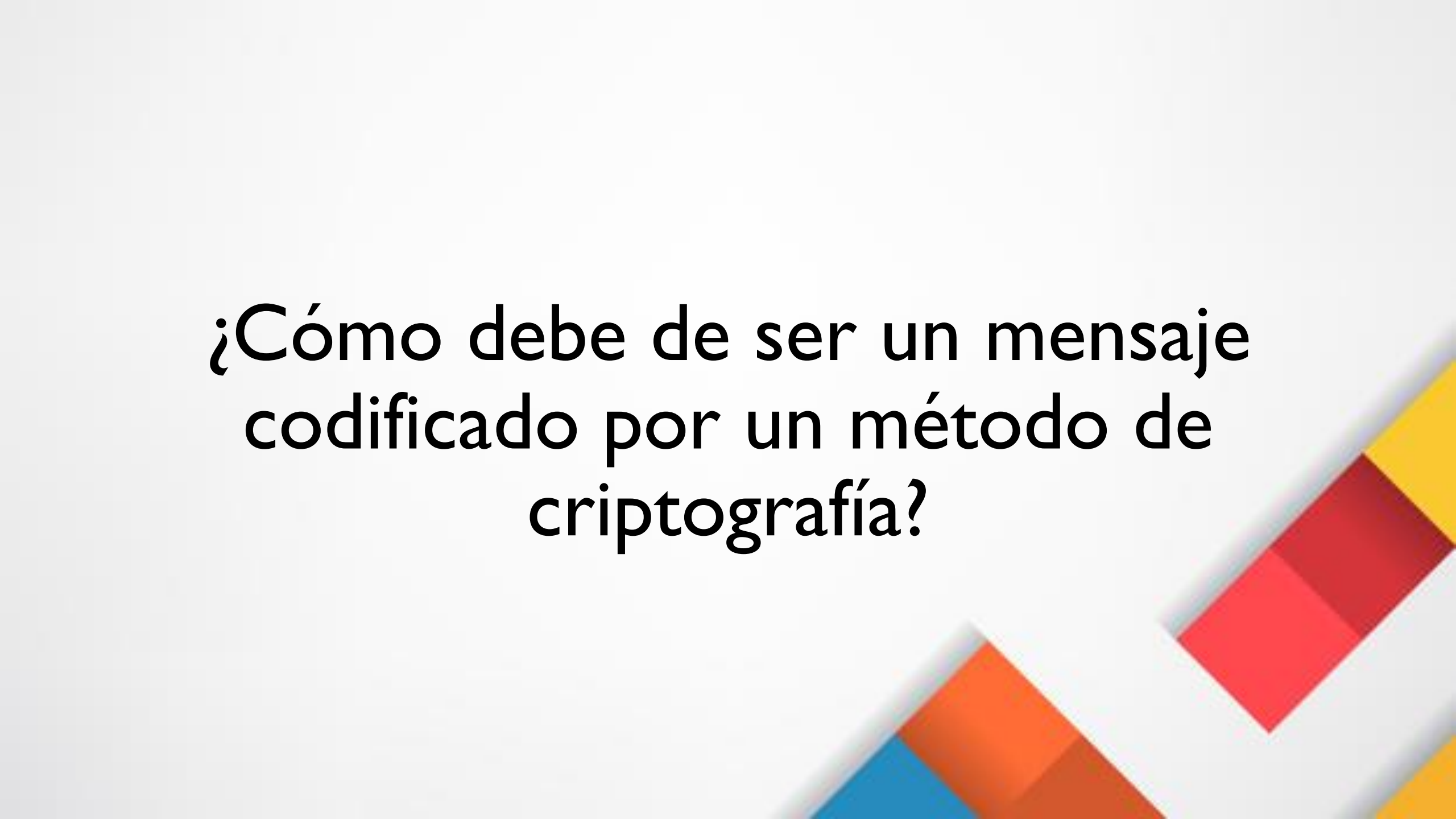
Del griego Krypto= ocultos y logos = CIENCIA

La criptografía es el estudio de las técnicas para proteger las comunicaciones sensibles por medio de encriptración de datos y su posterior descifrado.

Usos más comunes en la actualidad

- Autentificar la identidad de usuarios.
- Autentificar y proteger el sigilo de comunicaciones personales y de transacciones comerciales y bancarias.
- Proteger la integridad de transferencias electrónicas de fondos.

¿Cómo debe de ser un mensaje codificado por un método de criptografía?



PRIVADO

Solamente aquel que envió y aquel que recibe debe tener acceso al contenido del mensaje.

SUSCRITO

La persona que la recibió debe de poder verificar si el remitente es realmente la persona que dice ser y tener la capacidad de identificar si un mensaje puede haber sido modificado.

ELEMENTOS COMUNES DEL CIFRADO

- Algoritmo cifrador (cifra y descifra datos)
- Claves de cifrado
- Longitud de clave (claves largas)
- Texto (información a cifrar)
- Texto cifrado (información después de cifrar)

Método Hill

Este método fue desarrollado por Lester S. Hill en 1929.

Matemático y educador estadounidense que estaba interesado en las aplicaciones de las matemáticas a las comunicaciones

- Es un método de cifrado por sustitución.
- El texto plano del mensajes es sustituido por un texto cifrado que sigue un sistema regular.
- Este método de cifrado es de tipo poligráfico esto quiere decir que el cifrado actúa sobre grupos de caracteres.
- Fue el primer método práctico que podía operar sobre grupos de más de 3 símbolos.

Cómo cifrar un mensaje con el método Hill

1. Se asocia cada letra del alfabeto con un número.

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
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

2. SE ELIJE DE FORMA ALEATORIA UNA MATRIZ DE D × D ELEMENTOS LOS CUALES SERÁN LA CLAVE A UTILIZAR.

Ejemplo: matriz 3x3

$$\mathbf{A}=\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$$

3. Los elementos de la matriz de d × d serán enteros entre 0 y 25, además la matriz M debe ser inversible en $\mathbb{Z}_{26}^{n}$

4. Para la encriptación, el texto es dividido en bloques de d elementos los cuales se multiplican por la matriz d × d.

5. Todas las operaciones aritméticas se realizan en la forma modulo 26, es decir que 26 = 0, 27 = 1, 28 =2 etc.

6. Dado un mensaje a encriptar debemos tomar bloques del mensaje de "d" caracteres y aplicar: M×Pi=C, donde C es el código cifrado para el mensaje Pi

Ejemplo

Si tomamos la siguiente matriz como clave: $A = \begin{pmatrix} 5 & 17 & 20 \\ 9 & 23 & 3 \\ 2 & 11 & 13 \end{pmatrix}$

Para encriptar el mensaje "CODIGO" debemos encriptar los seis caracteres de "CODIGO" en bloques de 3 caracteres cada uno.

el primer bloque

$$P_1 = \text{"COD"} = \begin{pmatrix} 2 \\ 14 \\ 3 \end{pmatrix} \qquad P_2 = \text{"IGO"} = \begin{pmatrix} 6 \\ 8 \\ 14 \end{pmatrix}$$

$$A \cdot P_1 = \begin{pmatrix} 5 & 17 & 20 \\ 9 & 23 & 3 \\ 2 & 11 & 13 \end{pmatrix} \begin{pmatrix} 2 \\ 14 \\ 3 \end{pmatrix} = \begin{pmatrix} 308 \\ 349 \\ 197 \end{pmatrix} = \begin{pmatrix} 22 \\ 11 \\ 15 \end{pmatrix} (\text{mod } 26)$$

El primer bloque "COD" se codificara como “WLP"

Segundo bloque

$$A \cdot P_2 = \begin{pmatrix} 5 & 17 & 20 \\ 9 & 23 & 3 \\ 2 & 11 & 13 \end{pmatrix} \begin{pmatrix} 8 \\ 6 \\ 14 \end{pmatrix} = \begin{pmatrix} 422 \\ 252 \\ 264 \end{pmatrix} = \begin{pmatrix} 6 \\ 18 \\ 4 \end{pmatrix} (\text{mod } 26)$$

El segundo bloque "IGO" se codificara como “GSE"

Luego 'CODIGO' encriptado equivale a ‘WLPGSE’.

*Observar que las dos "O" se codificaran de forma diferente.

Cómo descifrar un mensaje con el método Hill

1. Para desencriptar se usa la matriz inversa de la usada para encriptar.

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
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

Se debe de tomar en cuenta que la matriz elegida sea invertible en módulo 26. Las matrices en donde su determinante sea 0 o múltiplo de 2 o 13 (2 y 13 son factores comunes para módulo 26) no podrán ser utilizadas.

El determinante de $A = \begin{pmatrix} 5 & 17 & 20 \\ 9 & 23 & 3 \\ 2 & 11 & 13 \end{pmatrix}$ es 9.

Para hallar la inversa de la matriz modulo 26, utilizamos $A^{-1} = C^{T} \cdot \left(\det(A)\right)^{-1}$

La matriz inversa es igual a $A^{-1} = \begin{pmatrix} 18 & 23 & 21 \\ 5 & 23 & 1 \\ 3 & 15 & 16 \end{pmatrix} (\mathrm{mod}\, 26)$

Esta matriz es la que se usa para descifrar, se multiplica por cada bloque de tres, “WLP" y "GSE“.

Ventajas y Desventajas

Desventajas

- El cifrado de Hill termina siendo un sistema inseguro en su aplicación.
- Utilizando métodos de álgebra lineal en un "ataque con texto claro conocido" puede romperse el código y descubrir la matriz clave de encriptado.
- Un ataque con texto claro conocido significa que el analista que quiere romper el código dispone de un ejemplo de "texto en claro", es decir, de un mensaje original, con el correspondiente mensaje cifrado.

Ventajas

- Las ventajas en comparación a otros métodos es que debido a que utiliza algoritmos simétricos generalmente, tiende a ser más rápido que sistemas de clave publica.
- Cuando el tamaño de la clave es grande y sin método para conseguir el texto original y codificado se vuelve ”seguro”.

Aplicación

¡GRACIAS POR SU ATENCIÓN!