CIFRADO HILL

Implementación en python

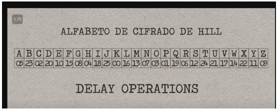
Facultad de Ciencias
Universidad Nacional de Ingeniería

Julio 2023

Table of Contents

Table of Contents

El cifrado Hill



- Desarrollado por Lester S. Hill en 1929
- Sentó las bases para futuros desarrollos en criptografía y fue un precursor de los cifrados de bloque modernos.
- Su importancia radica en su contribución temprana al uso de las matemáticas y el álgebra lineal en la criptografía

Table of Contents

Pasos del Cifrado Hill

Tenemos la palabra a cifrar : EJEMPLO
Con una matriz clave:

$$C = \begin{pmatrix} 17 & 5 & 2 \\ 3 & 17 & 21 \\ 20 & 7 & 19 \end{pmatrix}$$

Consideramos el alfabeto inglés para el cifrado

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

Pasos del cifrado Hill

1. Enumeramos las letras de la palabra (usando la tabla del alfabeto anterior), y si faltan letras para completar la dimensión, se completa con espacios.

$$\underset{4}{E}\,\underset{9}{J}\,\underset{4}{E}\,\underset{12}{M}\,\underset{15}{P}\,\underset{11}{L}\,\underset{14}{O}\,\underset{26}{\_}\,\underset{26}{\_}$$

2. Ubicamos cada bloque de números en orden vertical, obteniendo una matriz 3×3

$$A = \begin{pmatrix} 4 & 12 & 14 \\ 9 & 15 & 26 \\ 4 & 11 & 26 \end{pmatrix}$$

Pasos del cifrado Hill

3. Como la matriz clave es invertible, pues $|C| = 4169$ y este número es coprimo con 27, la matriz será invertible en módulo 27.
4. Multiplicando $C \times A$

$$M = C \times A = \begin{pmatrix} 121 & 301 & 420 \\ 249 & 522 & 1030 \\ 219 & 554 & 956 \end{pmatrix}$$

5. Aplicando módulo 27 a la matriz M

$$M \bmod 27 = \begin{pmatrix} 13 & 4 & 15 \\ 6 & 9 & 4 \\ 3 & 14 & 11 \end{pmatrix}$$

Pasos del cifrado Hill

6. Expresamos los números de la matriz con sus respectivas letras y obtenemos el cifrado

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

$$B = \begin{pmatrix} 13 & 4 & 15 \\ 6 & 9 & 4 \\ 3 & 14 & 11 \end{pmatrix}$$

$N\,G\,D\,E\,J\,O\,P\,E\,L$
13 6 3 4 9 14 15 4 11

Pasos del Descifrado Hill

1. Hallamos la matriz inverso modular de la matriz C

$$D = C^{-1} \bmod 27 = \begin{pmatrix} 16 & 0 & 4 \\ 6 & 11 & 0 \\ 25 & 13 & 20 \end{pmatrix}$$

2. Multiplicamos esta matriz con la matriz B que nos obtuvimos anteriormente

$$\begin{pmatrix} 16 & 0 & 4 \\ 6 & 11 & 0 \\ 25 & 13 & 20 \end{pmatrix} \times \begin{pmatrix} 13 & 4 & 15 \\ 6 & 9 & 4 \\ 3 & 14 & 11 \end{pmatrix} = \begin{pmatrix} 220 & 120 & 284 \\ 144 & 123 & 134 \\ 463 & 497 & 647 \end{pmatrix}$$

Pasos del Descifrado Hill

3. Aplicamos módulo 27 a nuestra matriz anterior

$$\begin{pmatrix} 4 & 12 & 14 \\ 9 & 15 & 26 \\ 4 & 11 & 26 \end{pmatrix}$$

4. Finalmente, obtenemos el mensaje descifrado

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

$$\underset{4\ 9\ 4\ 12\ 15\ 11\ 14\ 26\ 26}{E\ J\ E\ M\ P\ L\ O\ \_\ \_}$$

Calculo de la Matriz Inversa Modular y el uso del Algoritmo de Euclides

- Expliquemos ahora el proceso de descodificación de un mensaje. Imaginemos que el receptor recibe el siguiente mensaje: "EHAHTDINRKQOPUSKVLKMUFNG"; y quiere conocer su significado.
  Para descodificar el mensaje hay que utilizar el mismo método anterior, el cifrado de Hill, pero utilizando como clave la matriz inversa: A^{-1} (mod 27); de la matriz A de codificación.
  Por lo tanto, se empieza de nuevo transformando el mensaje en sucesión de ternas numéricas asociadas: (4, 7, 0), (7, 20, 3), (8, 13, 18), (10, 17, 15), (16, 21, 19), (10, 22, 11), (10, 12, 21), (5, 14, 6); obteniendo la siguiente matriz:

Calculo de la Matriz Inversa Modular y el uso del Algoritmo de Euclides

$\begin{pmatrix} 4 & 7 & 8 & 10 & 16 & 10 & 10 & 5 \\ 7 & 20 & 13 & 17 & 21 & 22 & 12 & 14 \\ 0 & 3 & 18 & 15 & 19 & 11 & 21 & 6 \end{pmatrix}$; y tenemos la matriz llave o clave: $\begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 1 & 0 & 6 \end{pmatrix}$; entonces para poder decodificar el mensaje ya encriptado; se necesita que la matriz de la transformación lineal utilizada, la clave, sea una matriz invertible. La matriz de nuestro ejempo lo es, puesto que su determinante es no nulo,det$(A) = 22$.

Calculo de la Matriz Inversa Modular y el uso del Algoritmo de Euclides

- Entonces la matriz inversa de A, que es la necesaria para decodifcar un mensaje cifrado es:
$A^{-1} = \begin{pmatrix} 24/22 & -12/22 & -2/22 \\ 5/22 & 3/22 & -5/22 \\ -4/22 & 2/22 & 4/22 \end{pmatrix}$; pero estamos trabajando con los enteros módulo 27 y vamos a transformar la matriz inversa anterior en una matriz con números enteros módulo 27. Para empezar se necesita el inverso del número 22. Se ve fácilmente que: $22 \times 16 = 352$, que es igual a 1, módulo 27, luego $22^{-1} = 16$. Y la matriz inversa se transforma, módulo 27, en:

Calculo de la Matriz Inversa Modular y el uso del Algoritmo de Euclides

$$\begin{pmatrix} 24/22 & -12/22 & -2/22 \\ 5/22 & 3/22 & -5/22 \\ -4/22 & 2/22 & 4/22 \end{pmatrix} = \begin{pmatrix} 24*16 & -12*16 & -2*16 \\ 5*16 & 3*16 & -5*16 \\ -4*16 & 2*16 & 4*16 \end{pmatrix}$$

$= \begin{pmatrix} 384 & -192 & -32 \\ 80 & 48 & -80 \\ -64 & 32 & 64 \end{pmatrix}$; y pasando a modulo 27,

resultaría: $\begin{pmatrix} 6 & 24 & 22 \\ 26 & 21 & 1 \\ 17 & 5 & 10 \end{pmatrix}$.Pero, ¿cómo podemos saber que el inverso del número 22 es igual a 16 en módulo 27?. Es ahí donde entra a tallar el "Algoritmo extendido de Euclides":

Calculo de la Matriz Inversa Modular y el uso del Algoritmo de Euclides

Ejemplo: Vamos a calcular el inverso de 22 en módulo 27. Para ello aplicamos el algoritmo extendido de Euclides:

$$\begin{aligned}27 &= 1 \times 22 + 5\\ 22 &= 4 \times 5 + 2\\ 5 &= 2 \times 2 + 1\\ 2 &= 2 \times 1\end{aligned}$$

;por tanto: 1 = mcd(27,22). Ahora sustituimos de abajo a arriba los restos: 1 = 5-2.2 = 5 - 2(22-4.5) = 27-22-2(22-4(27-22)) = 9 .27 - 11.22. Pasando a modulo 27, tenemos que: 1 = 9*27 - 11*22 = 9*0 - 11*22. Por lo tanto el inverso de 22 es: -11; sin embargo nosotros queremos el inverso de 22 dentro del espacio de los numeros naturales, por ende se aplica el modulo 27 al número: -11.

Calculo de la Matriz Inversa Modular y el uso del Algoritmo de Euclides

Entonces tenemos: x= -11(mod 27); sin embargo: -11 = 16(mod 27); y por transitividad: -11 = 16 (mod 27); resultando x = 16 (mod 27), teniendo el inverso positivo de 22 en modulo 27, el numero: 16.

- Luego; mutiplicando la inversa de la matriz por la matriz cifrada; se obtiene: $\begin{pmatrix} 192 & 588 & 756 & 798 & 1018 & 830 & 810 & 542 \\ 251 & 605 & 499 & 632 & 876 & 733 & 533 & 432 \\ 103 & 249 & 381 & 405 & 567 & 390 & 440 & 235 \end{pmatrix}$; y sacando cada componente el módulo en 27; quedaría: $\begin{pmatrix} 3 & 21 & 0 & 15 & 19 & 20 & 0 & 2 \\ 8 & 11 & 13 & 11 & 12 & 4 & 20 & 0 \\ 22 & 6 & 3 & 0 & 0 & 12 & 8 & 19 \end{pmatrix}$; entonces traduciéndolo; el mensaje original sería: " DIVULGANDOLASMATEMATICAS".

Table of Contents

Table of Contents

Resultados

Para realizar el ejemplo explicativo se utilizó el código para generar la matriz clave aleatoria

```
Ingrese la palabra a cifrar: EJEMPLO
Ingrese la dimension de la matriz clave: 3
Matriz clave:
[[17  5  2]
 [ 3 17 21]
 [20  7 19]]
Texto cifrado: NGDEJOPEL
Inverso Modular de la Matriz clave:
 [[16  0  4]
 [ 6 11  0]
 [25 13 20]]
Texto descifrado: EJEMPLO
```

Resultados

- Dimensión de la matriz clave
- Limitación del alfabeto

```
C:\Users\eri_h\anaconda3\pyt
Ingrese la palabra a cifrar: Hola Mundo
Ingrese la dimension de la matriz clave: 3
Matriz clave:
[[12 19 16]
 [ 2 23 14]
 [ 7 18  2]]
Texto cifrado: NE LKGWDCZSY
Inverso Modular de la Matriz clave:
 [[20 14 12]
 [26 13 25]
 [20 23 17]]
Texto descifrado: HOLA MUNDO
Press any key to continue . . .
```

- Inversibilidad de la matriz clave

```python
# Función para generar una matriz clave aleatoria invertible
def generate_key(n):
    while True:
        key = np.random.randint(0, 27, size=(n, n))
        det = int(np.round(np.linalg.det(key))) % 27
        try:
            det_inv = sp.mod_inverse(det, 27)
            return key
        except ValueError:
            pass
```

Resultados

- Límite en pantalla

```
Ingrese la palabra a cifrar: hola
Ingrese la dimension de la matriz clave: 24
Matriz clave:
[[16  4 19 20 17 21 17  6  4  1 12  9 10  7 10 19 21 12  8 12 23 23 17  6]
 [ 9 14 23  5 25 15 12 25  6 17 24 22 22  2 25 24 17  9  9 10 18  4 22 18]
 [22  5  5  7 13 20 11 18  7  4 25 15 11 14 17  4 23 18  7  1 12  9 13 14]
 [ 8  6 13  7 15 22 16 18  1  9 16 20 12  3  6 16  4 21  7  3  0 19  8 23]
 [ 8 11  4  3 14 23 10  5  9  2  6 13 10  7 25 12 18 26 25 26  3 25 14 23]
 [24 26  0 10 18 10  5  8 14  4 21  8  4 21 12 24 14  0 11 11  2 26  8 21]
 [ 8 16  6 12 20 11 19 26  6 17 14 13 26 10 11  9 26 13 26 24  6 24  3 11]
 [17 14  2 23 25  3 17 22  4  3 10 26 13 25 23  8  8 13 11  6 19 26  9 23]
 [26  8 17 12 21 10  6 14  2 14 21 23  8 11  4 18 22 12 12  7 15 13 15 21]
 [13 17  6  6  0  9  0  8  7 10 24  1 23 26 10 12 12 19 26 11 14 13 25 21]
 [10 10  6  9 19  2  3  5 24 26  9  5 14  1 18 10 21  2  7 24  6 19  2 24]
 [ 4 20 21 14 26 23 12 24 15  2 14 12 23 15  0  3 17  7  2 22  1 22  0 22]
 [13 21  0 13 19 19 13 15 13 16  1 17 10  9 15 16  5 25 24  5  5 18 18  9]
 [11  1  9 25 25 13 12 18 15  9  1 23  4 12 20 13 21 25 20 16 23 15 15 12]
 [22  6 10 19 19 20 25 13 16 10  5 21 22  0  7  5 26 11  8 23 11 19  3  7]
 [24 21  1  4 14  0 19  6  7 15 20  1 12 18 12  5 10  8  9  7 21  6 26 23]
 [12 25 17 16 21 19 20  5 14 12 13 16  7  1 23 17  7  7  1  1 21 12  9 15]
 [25 25 17 26  1 12 18 26 11 13 19 14 24  9 13  0 14 20 26 22 11 13  7 22]
 [25 17  1 16  5  3  4 13  0 20 14  5 17 11  4 25 16  5 26 11  1 12 15 17]
 [11 11 25  1 24 26 16 15  6 13  1 24  0 18 11 14  8  2  8 20 15 19  0 22]
 [ 9  8 25 11 10 20  9 14  3  7  3  1 13 24 16  0  6 12  9 21 12 25 26 26]
 [11  7 18 26  7 14  5  2 10 22  2  3 22 14 21 19  7 20 10 13 10  9 16 15]
 [13 14  8 20 16 10  7 16 25 13  5 18 13 15 13 12 17 16  2  0  1 16  1 13]
 [ 2  6  1 12 13 15  1 23  0 16  9 26  6 22 23 15 22 14 13  1 19  6 24  8]]
Texto cifrado: OYXRMUEQXQIHFNXSCMLBEYLW
```

```
Ingrese la palabra a cifrar: hola
Ingrese la dimension de la matriz clave: 25
Matriz clave:
[[21 11  8  7 19  1 18 10 12  3  0  0 21  1  8  7 16 12  3  6  6 20 22  0
   7]
 [ 1 12 18 11 19 16 16  9 26 17 16  6  3 13 17  5  1  6 20 15  9  9  5 14
  16]
 [23 19 25  0 10 17  2  9  6 16 11 13 25 12 23  3 25 21 14  1  9  5 25  0
  17]
 [20 14  6  8 12  2 13  5  3 22 12  3  6 14 22 19 22  7 23  9 12 19 11 26
   8]
 [23 26 18 25 10 16 26  9  8 23 23  3  1 12  4  4  7  0 23 10 22 15  8 18
  11]
 [14 16  5 13 17  0  4 17 26 16  7 15 26 15 15  7 21  3  9 12 10  6 26 25
  21]
 [ 2 23  6 16  6  6 17  3 19  6  8 14 19 12  3 23  4 18 23 11  9 21  5  8
  25]
 [ 0 10  1 14 17  1 21 14 22  7  9 20 19  9 26 22  1  1 22  6 14 24  0  0
  23]
 [16 22 15  6 12 11  6  3 26 25 11 14  7 16 13  3 16 15 23  7 25 25 13 21
  19]
 [ 3 12 15 24 15  0  4 13  4 23 25 10 19 23  2 13 12 19  8  0 13 25 15  1
```

Resultados

- Desempeño y eficiencia:
  El tiempo requerido para cifrar o descifrar un mensaje crece de manera cuadrática en relación con el tamaño del mensaje.
  Cuando se tratan mensajes muy largos, y dimensiones de la matriz clave muy grandes, el código puede volverse ineficiente y el tiempo de cifrado o descifrado puede volverse significativamente mayor.

Desventajas del cifrado Hill

- Vulnerabilidad a ataques de fuerza bruta
- Ataque de texto cifrado conocido
- Mejores alternativas criptográficas disponibles

Table of Contents

Referencias

Stallings, W. (2017). Criptografía y seguridad de la información. Pearson Educación.
Immune Technology Institute. Tipos de criptografía ¿Cuáles son los más comunes para la privacidad de las comunicaciones?
https://immune.institute/blog/tipos-de-criptografia-seguridad-online/