Códigos y criptografía

Práctica 2: Cifrado Hill y cifrado de permutación (caso particular del Hill)

- Usaremos las funciones de la práctica 1
  - **letranumero(texto)**
  - **inv_modulo(A,m)**

Recuerda que si quieres trabajar con más caracteres de 27, solo tienes que modificar tu alfabeto en la función *letranumero* y tener en cuenta su nueva longitud, a la que estamos llamando *m*

1.Función cifrado=cifro_hill (A, m, texto)

Esta función tiene tres entradas, la matriz que será la clave, el número de elementos de nuestro alfabeto y el texto a cifrar

Se debe comprobar que la matriz es adecuada para este tipo de cifrado, es decir comprobar que tiene inversa módulo m.

La salida debe ser el texto cifrado, cuando tengamos una matriz adecuada y un mensaje de error en caso contrario .

Ejemplos

>> cifrado=cifro_hill([2 1 3;2 3 4;7 8 1],27,'esta matriz es valida')

cifrado =

gklmjobrvffqwhdsyz

>> cifrado=cifro_hill([2 1 3;2 1 4;0 0 1],27,'esta matriz no es valida')

Debe de dar un mensaje de error

Ahora tendríamos que hacer una función para descifrar un criptograma obtenido mediante un cifrado Hill, pero ¿hace falta hacerla?

Ejemplo

criptograma : dosselmdrpmrdxueee

matriz de cifrado: [2 1 3;2 1 1;0 4 1]

¿Cómo puedo obtener el mensaje original sin construir una nueva función?

2.- Cifrado de permutación (caso particular del cifrado hill)

Para cifrar con este método, necesitamos conocer:

- Texto claro: un texto de longitud n, que es el que queremos cifrar
- Clave: una de las n! permutaciones del grupo Sn

Y como resultado tendremos el texto cifrado

Texto cifrado: el resultado de aplicar al texto claro la clave.

Ejemplo

Si n=5, seleccionamos una de las 5! permutaciones de 5 elementos para nuestra clave, por ejemplo clave ={3 2 5 1 4} (el elemento que está en el lugar 3 se va al 1, el del 2 se queda en el 2, el del 5 se va al 3 ….)

Si texto claro = 'colas', al aplicarle la permutación obtenemos

Texto cifrado = losca.

Cuando el texto es más largo que la clave, se divide el texto en bloques del tamaño de la clave y aplicamos a cada bloque la clave. En caso de que el último bloque se quede con menos elementos, se le añaden letras superfluas.

Como Sn es grupo para la composición de permutaciones, cada permutación tiene su inversa y para descifrar lo único que hay que hacer es aplicar la permutación inversa al criptograma

Para nuestro ejemplo clave $^{-1}$ = {4 2 1 5 3} que al aplicársela a 'losca' lo convierte en 'colas'

El cifrado de permutaciones es un caso particular al cifrado Hill. Solo hay que tener en cuenta que aplicar la permutación p={3,2,5,1,4} a {a,b,c,d,e}es lo mismo que hacer el producto

$$\begin{pmatrix} 0 & 0 & 1 & 0 & \mathbf{0} \\ 0 & 1 & 0 & 0 & \mathbf{0} \\ 0 & 0 & 0 & 0 & \mathbf{1} \\ 1 & 0 & 0 & 0 & \mathbf{0} \\ 0 & 0 & 0 & 1 & \mathbf{0} \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \\ e \end{pmatrix} = \begin{pmatrix} c \\ b \\ e \\ a \\ d \end{pmatrix}$$

Lo que queremos en este apartado es que utilices la función

cifrado=cifro_hill (A, m, texto)
para hacer un cifrado de permutación. Observa que lo único que necesitaremos será una *función que convierta una permutación en una matriz.*

2.- Vamos a hacer una función para asegurarnos de que si queremos introducir un vector que represente a una permutación, en efecto lo introducimos bien y de verdad sea una permutación.

Function permuta=permutación_v(p)

Esta función tiene por entrada una permutación y por salida:

permuta= 1 si es una permutación el vector introducido

permuta=0 si no es permutación el vector intrroducido

Ejemplos

>> permuta=permutacion_v([3 5 2 7])

permuta = 0

>> permuta=permutacion_v([3 4 2 1])

permuta =1

3.- Function mat_p=matper (p)

Esta función tendrá que realizar lo siguiente:

- Comprobar que 'p' es efectivamente una permutación
- Si 'p' es permutación debe construir la matriz (mat_p) asociada a la permutación. En caso de no ser 'p' una permutación: mensaje de error

Ejemplo

>> mat_per=matper([3 1 2 5 4])

mat_per =

0 0 1 0 0

1 0 0 0 0

0 1 0 0 0

0 0 0 0 1

0 0 0 1 0

Ahora ya podemos cifrar con clave una permutación, usando el cifrado Hill

4.- Function [texto, cifrado]=cifro_permutacion (p , texto)

- La entrada será la permutación y el texto a cifrar
- La función debe de comprobar que *p* es efectivamente una permutación
- La salida el texto claro y el texto cifrado usando Hill , en caso de ser posible y en caso de no ser posible, mensaje de error

Ejemplo

>> [texto,cifra]=cifro_permutacion([2 5 4 1 3], 'hola me voy de puente')

texto =hola me voy de puente

cifra =omahlvdyeopneeuewwtw

5.- Function [cifra,claro]=descifro_permutacion(p, cifrado)

Esta función tiene por entrada la permutación (p) y el texto cifrado (con la permutación p), la salida debe ser el texto cifrado y el claro

Ejemplos

>> [cifra,claro]=descifro_permutacion([5 1 3 4 2], 'ymvoeeardirsndewimos')

cifra =ymvoeeardirsndewimos

claro =mevoyairdesendrismow

>> [cifra,claro]=descifro_permutacion([7 1 3 4 2], cifra)

error

Si conocemos un texto claro , su cifrado asociado con Hill y el orden de la clave, podemos encontrar la matriz de cifrado. Ver fotocopias del final, obtenidas del libro:

Seguridad informática y Criptografía

El autor del libro es: Jorge Ramió Aguirre

En Moodle tienes el enlace a este libro

Antes de hacer la función 6, debes de trabajar un poco con el anexo de la práctica 2, y/o tener clara la presentación de 'cifrado Hill' que se encuentra en conceptos teóricos del tema 3 de moodle

6.- ***Función cripto_hill (textoclaro, textocifrado , orden)***

Entradas: Un texto claro, el criptograma asociado y el orden de la matriz. Pero la longitud de los textos debe de ser mayor o igual al orden de la matriz al cuadrado

Salida: matriz de cifrado

Libro Electrónico de Seguridad Informática y Criptografía v4.1

Capítulo 9: Sistemas de Cifra Clásicos Página 371

¿Es seguro el cifrador de Hill?

Si con el sistema de Hill se cifran bloques de 8 caracteres, incluso en un cuerpo tan pequeño como n = 27 el espacio de claves aumenta de forma espectacular, comparable con DES.

Si el módulo de cifra es un primo p, entonces el número de claves válidas es cercano al máximo posible: p^x donde $x = d^2$, con d el tamaño de N-grama o de la matriz clave.

No obstante, el sistema no es seguro. Debido a su linealidad será muy fácil hacer un ataque con texto claro conocido según el método de Gauss Jordan y encontrar así la matriz clave K.

Esto es debido a que aparecen los llamados vectores unitarios en el criptograma o en el texto en claro, o bien los obtenemos aplicando este método.

Capítulo 9: Sistemas de Cifra Clásicos Página 372

Ataque al cifrado de Hill por Gauss Jordan

El método consiste en escribir una matriz 2N-grámica con los elementos del texto en claro y los elementos del criptograma. En esta matriz realizamos operaciones lineales (multiplicar filas por un número y restar filas entre sí) con el objeto de obtener los vectores unitarios.

Por ejemplo podemos romper la matriz clave K teniendo:

```
M = ENU NLU GAR DEL AMA NCH ADE CUY ONO ...
C = WVX IDQ DDO ITQ JGO GJI YMG FVC UÑT ...
```

E	N	U	W	V	X		4	13	21		23	22	24
N	L	U	I	D	Q		13	11	21		8	3	17
G	A	R	D	D	O		6	0	18		3	3	15
D	E	L	I	T	Q		3	4	11		8	20	17
A	M	A	J	G	O	=	0	12	0		9	6	15
N	C	H	G	J	I		13	2	7		6	9	8
A	D	E	Y	M	G		0	3	4		25	12	6
C	U	Y	F	V	C		2	21	25		5	22	2
O	N	O	U	Ñ	T		15	13	15		21	14	20

Capítulo 9: Sistemas de Cifra Clásicos

Operaciones en la matriz de Gauss Jordan

Vamos a dejar en la primera columna un número uno en la fila primera y todas las demás filas un cero. Luego multiplicamos el vector (4 13 21 | 23 22 24) por el inv (4, 27) = 7. Así obtenemos 7(4 13 21 | 23 22 24) mod 27 = (1 10 12 | 26 19 6). Si esto no se puede hacer con la primera fila movemos los vectores. Hecho esto vamos restando las filas respecto de esta primera como se indica:

$$\left(\begin{array}{ccc|ccc} 4 & 13 & 21 & 23 & 22 & 24 \\ 13 & 11 & 21 & 8 & 3 & 17 \\ 6 & 0 & 18 & 3 & 3 & 15 \\ 3 & 4 & 11 & 8 & 20 & 17 \\ 0 & 12 & 0 & 9 & 6 & 15 \\ 13 & 2 & 7 & 6 & 9 & 8 \\ 0 & 3 & 4 & 25 & 12 & 6 \\ 2 & 21 & 25 & 5 & 22 & 2 \\ 15 & 13 & 15 & 21 & 14 & 20 \end{array}\right)$$

a) 2ª fila = 2ª fila – 13∗1ª fila mod 27
b) 3ª fila = 3ª fila – 6∗1ª fila mod 27
c) 4ª fila = 4ª fila – 3∗1ª fila mod 27
d) 5ª fila ya tiene un 0
e) 6ª fila = 6ª fila – 13∗1ª fila mod 27
f) 7ª fila ya tiene un 0
g) 8ª fila = 8ª fila – 2∗1ª fila mod 27
h) 9ª fila = 9ª fila – 15∗1ª fila mod 27

Matriz clave de Hill criptoanalizada

Repetimos este procedimiento ahora para algún vector en cuya segunda columna tenga un número con inverso en 27 y lo mismo para la tercera columna, moviendo si es preciso los vectores.

Como la mitad izquierda de la matriz 2N era el texto el claro, la parte derecha de la matriz con vectores unitarios corresponderá a la traspuesta de la clave.

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 2 & 5 & 7 \\ 0 & 1 & 0 & 3 & 5 & 8 \\ 0 & 0 & 1 & 4 & 6 & 9 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right) \Rightarrow \quad K = \begin{pmatrix} 2 & 3 & 4 \\ 5 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$$

Compruebe que la clave es la utilizada en este cifrado.