Píldora nº 22: ¿Cómo se ataca por Gauss-Jordan la cifra de Hill?

Escena 1: El espacio de las claves en el cifrador de Hill

En la píldora anterior se indicaba que la matriz clave de Hill debía tener inversa, por lo que su determinante no podía ser 0 ni tener factores en común con el módulo de cifra. Por lo tanto, no todas las matrices serán válidas para la cifra en un cuerpo.

Por ejemplo, para una matriz clave de tamaño 2x2 y cifrando en módulo 27, existirán 27^4 = 531.441 matrices distintas, de las cuales 314.928 serán válidas. Si en el mismo cuerpo de las 27 letras mayúsculas del alfabeto español cifrásemos bloques de 16 letras, el número de matrices ascendería a 27^{256}, un número inmenso con 366 dígitos, mucho mayor incluso que cualquier clave simétrica actual. Sin embargo, además de su extrema lentitud, la cifra de Hill sucumbirá fácilmente ante un ataque con texto en claro conocido usando el método de Gauss-Jordan.

Escena 2: Las figuras de Gauss y de Jordan

Johann Karl Friedrich Gauss (1777-1855) fue, entre otras cosas, un destacado matemático alemán que contribuyó significativamente al desarrollo de la teoría de números. Conjuntamente con Wilhelm Jordan (1842–1899), geodesista también alemán, inventan el sistema conocido como Eliminación de Gauss-Jordan que permite encontrar matrices inversas.

Aplicando esta técnica en el ataque a una cifra de Hill en la que se conoce el texto en claro y el criptograma pero no la matriz clave, permitirá romper de una manera muy sencilla y con muy poco coste computacional dicha matriz clave y, por tanto, el algoritmo.

Escena 3: Ataque a Hill mediante Gauss-Jordan

Para encontrar la matriz clave de cifra, definiremos una matriz 2n-grámica como [(TextoEnClaro)|(TextoCifrado)] y realizaremos operaciones básicas de multiplicación de filas por una constante, así como restas de filas entre sí. Será muy sencillo obtener en una de estas dos matrices una matriz identidad y con ello deducir de la otra matriz resultante la matriz clave buscada. Supongamos la siguiente cifra en bloques de 3 letras del comienzo de El Quijote en módulo 27:

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

Definimos esa matriz 2n-grámica [(TextoEnClaro)|(TextoCifrado)] como se indica:

$$\begin{matrix} \text{Matriz Trigrámica} \\ \text{Texto en Claro} \\ \text{Texto Cifrado} \end{matrix} \begin{pmatrix} E & N & U & W & V & X \\ N & L & U & I & D & Q \\ G & A & R & D & D & O \\ D & E & L & I & T & Q \\ A & M & A & J & G & O \\ N & C & H & G & J & I \\ A & D & E & Y & M & G \\ C & U & Y & F & V & C \\ O & N & O & U & Ñ & T \\ M & B & R & R & L & L \end{pmatrix} = \begin{pmatrix} 4 & 13 & 21 & 23 & 22 & 24 \\ 13 & 11 & 21 & 8 & 3 & 17 \\ 6 & 0 & 18 & 3 & 3 & 15 \\ 3 & 4 & 11 & 8 & 20 & 17 \\ 0 & 12 & 0 & 9 & 6 & 15 \\ 13 & 2 & 7 & 6 & 9 & 8 \\ 0 & 3 & 4 & 25 & 12 & 6 \\ 2 & 21 & 25 & 5 & 22 & 2 \\ 15 & 13 & 15 & 21 & 14 & 20 \\ 12 & 1 & 18 & 18 & 11 & 11 \end{pmatrix}$$

Como en la primera fila las letras [ENU | WVX] se representan con los números [4 13 21 | 23 22 24] mod 27, para poner el valor 1 en el primer elemento de la matriz identidad, convertiremos ese valor 4 (la letra E) en un 1 multiplicando toda la fila por el inverso de 4 en 27, que es 7. Si en esa posición tuviésemos un número que no tiene inverso, como sería por ejemplo el 12 de la última fila, dado que la cifra de cada fila es independiente, podemos mover hacia la posición deseada la fila que queramos y que permita multiplicarla por el inverso correspondiente y obtener el valor 1 buscado.

[4 13 21 | 23 22 24] * 7 mod 27 = [1 10 12 | 26 19 6]

Dejaremos ahora toda la primera columna de las demás filas con el valor cero, haciendo operaciones de resta de cada fila con la primera fila que acabamos de modificar, en este caso:

a) 2ª fila = 2ª fila - 13 * 1ª fila

b) 3ª fila = 3ª fila - 6 * 1ª fila

c) 4ª fila = 4ª fila - 3 * 1ª fila

d) 6º fila = 6ª fila - 13 * 1ª fila

e) 8ª fila = 8ª fila - 2 * 1ª fila

f) 9ª fila = 9ª fila - 15 * 1ª fila

g) 10ª fila = 10ª fila - 12 * 1ª fila

Tras lo cual nos queda la siguiente matriz:

$$\begin{matrix} \textit{Matriz Trigrámica} \\ \textit{Texto en Claro} \\ \textit{Texto Cifrado} \end{matrix} \begin{pmatrix} 1 & 10 & 12 & 26 & 19 & 6 \\ 0 & 16 & 0 & 21 & 26 & 20 \\ 0 & 21 & 0 & 9 & 24 & 6 \\ 0 & 1 & 2 & 11 & 17 & 26 \\ 0 & 12 & 0 & 9 & 6 & 15 \\ 0 & 7 & 13 & 19 & 5 & 11 \\ 0 & 3 & 4 & 25 & 12 & 6 \\ 0 & 1 & 1 & 7 & 11 & 17 \\ 0 & 25 & 24 & 9 & 26 & 11 \\ 0 & 16 & 9 & 3 & 26 & 20 \end{pmatrix}$$

Repitiendo el mismo procedimiento para la segunda y tercera columnas, llegaremos a una matriz identidad en la izquierda.

$$\begin{matrix} \textit{Matriz Trigrámica} \\ \textit{Texto en Claro} \\ \textit{Texto Cifrado} \\ \textit{diagonalizada} \\ \textit{agrupando los} \\ \textit{vectores unitarios} \end{matrix} \begin{pmatrix} 1 & 0 & 0 & 2 & 5 & 7 \\ 0 & 1 & 0 & 3 & 5 & 8 \\ 0 & 0 & 1 & 4 & 6 & 9 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Escena 4: Rompiendo la clave

La traspuesta de la matriz que acompaña a la matriz identidad será la clave:

$$K = \begin{pmatrix} 2 & 3 & 4 \\ 5 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$$

Para comprobar este resultado, si se cifran las tres primeras letras del texto en claro ENU, se obtiene el criptograma WVX, y la cifra de Hill se ha roto con muy poco esfuerzo.

Madrid, diciembre de 2014

Autor del guion: *Jorge Ramió Aguirre*

Dirección Proyecto Thoth: *Jorge Ramió Aguirre, Alfonso Muñoz Muñoz*