# Método de Hill

*José Galaviz*

## Introducción

- Lester S. Hill, Hunter College New York.
- 1929, American Mathematical Monthly.
- *Cryptography in al algebraic alphabet*.
- La unidad de cifrado ya no es el caracter, sino parejas de ellos (o más).
- Patentó una máquina para automatizar el cifrado (de sextetos).
- Extendió el trabajo en 1931: *Concerning Certain Linear Transformation Apparatus of Cryptography.*

## Codificación

- Cada letra del alfabeto inglés de 26 letras es mapeada en un número entre el 0 y el 25.
- Las operaciones se llevarán a cabo módulo 26.
- Cada pareja de letras es considerada como un vector de dos entradas con los códigos de cada una: (‘d’, ‘e’) = (3, 4).

## Idea

El digrama ($p_1$, $p_2$) es cifrado como:

$$\begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} m_{1,1} & m_{1,2} \\ m_{2,1} & m_{2,2} \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \end{pmatrix} \pmod{26}$$

## Ejemplo

La pareja (c, o) = (2, 14) se cifra como (W,E) = (22, 4) usando la matriz [9, 4; 5, 7]:

$$\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix} \begin{pmatrix} 2 \\ 14 \end{pmatrix} = \begin{pmatrix} 22 \\ 4 \end{pmatrix} \pmod{26}.$$

## Descifrar

$$M = \begin{pmatrix} m_{1,1} & m_{1,2} \\ m_{2,1} & m_{2,2} \end{pmatrix},$$

La matriz inversa es:

$$M^{-1} = \frac{1}{|M|} \begin{pmatrix} m_{2,2} & -m_{1,2} \\ -m_{2,1} & m_{1,1} \end{pmatrix} \pmod{26}.$$

En nuestro ejemplo: [5, 12; 15, 25].

## Además...

- No toda matriz tiene inverso en el sistema.
- Se requiere que su determinante tenga inverso en los enteros modulares que se estén usando (26 en nuestro caso).
- Por ejemplo [2, 12; 1, 14] tiene determinante 2 y no tiene inverso módulo 26.
- **Sólo si el determinante es primo relativo con el módulo**.
- Hay matrices que son su propio inversa: [2, 3; 25, 24].
- Claro, si uno posee la matriz de cifrado, puede obtener la de descifrado fácilmente.
- ¿Cuál es la clave del sistema?
- ¿Es simétrico o asimétrico?

## Criptoanálisis

- Si se están utilizando *n*-gramas y, por tanto, matrices de *n* x *n*, basta con tener $n^2$ parejas de texto-criptotexto para definir un sistema de ecuaciones que entrega matriz de cifrado (Pág. 125 de las notas de criptología).

# Recordar

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 |
| -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 | 0 |
| 25 | 24 | 23 | 22 | 21 | 20 | 19 | 18 | 17 | 16 | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 26 |

# Ejemplo

Imaginemos que capturamos un criptograma y sabemos como empieza...

| u | n | a | d | e | c | e | n | a | n | o | r | t | e |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 20 | 13 | 0 | 3 | 4 | 2 | 4 | 13 | **0** | **13** | 14 | 17 | 19 | 4 |
| 24 | 9 | 12 | 21 | 18 | 8 | 10 | 7 | **0** | **13** | 12 | 7 | 5 | 19 |
| Y | J | M | V | S | I | K | H | A | N | M | H | F | T |
| t | r | e | s | c | i | e | n | t | o | s | s | u | r |
| 19 | 17 | 4 | 18 | 2 | 8 | 4 | 13 | 19 | 14 | **18** | **18** | 20 | 17 |
| 5 | 6 | 4 | 16 | 24 | 14 | 10 | 7 | 19 | 11 | **0** | **8** | 18 | 23 |
| F | G | E | Q | Y | O | K | H | T | L | A | I | S | X |

# Ecuaciones

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 \\ 13 \end{pmatrix}=\begin{pmatrix} 0 \\ 13 \end{pmatrix}$$

$$13b=0$$
$$13d=13$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 \\ 8 \end{pmatrix}=\begin{pmatrix} 18 \\ 18 \end{pmatrix}$$

$$8b=18$$
$$8d=18$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 12 \\ 21 \end{pmatrix}=\begin{pmatrix} 0 \\ 3 \end{pmatrix}$$

$$12a+21b=0$$
$$12c+21d=3$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 5 \\ 6 \end{pmatrix}=\begin{pmatrix} 19 \\ 17 \end{pmatrix}$$

$$5a+6b=19$$
$$5c+6d=17$$

# b y d

| 26*k | 13b=0 | 8b=18 | b1 | b2 | 13d=13 | 8d=18 | d1 | d2 |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 18 | 0 | 2.25 | 13 | 18 | 1 | 2.25 |
| 26 | 26 | 44 | 2 | 5.5 | 39 | 44 | 3 | 5.5 |
| 52 | 52 | 70 | 4 | 8.75 | 65 | 70 | 5 | 8.75 |
| 78 | 78 | 96 | 6 | 12 | 91 | 96 | 7 | 12 |
| 104 | 104 | 122 | 8 | 15.25 | 117 | 122 | 9 | 15.25 |
| 130 | 130 | 148 | 10 | 18.5 | 143 | 148 | 11 | 18.5 |
| 156 | 156 | 174 | 12 | 21.75 | 169 | 174 | 13 | 21.75 |
| 182 | 182 | 200 | 14 | 25 | 195 | 200 | 15 | 25 |
| 208 | 208 | 226 | 16 | | 221 | 226 | 17 | |
| 234 | 234 | 252 | 18 | | 247 | 252 | 19 | |
| 260 | 260 | 278 | 20 | | 273 | 278 | 21 | |
| 286 | 286 | 304 | 22 | | 299 | 304 | 23 | |
| 312 | 312 | 330 | 24 | | 325 | 330 | 25 | |
| 338 | 338 | 356 | 26 | | 351 | 356 | | |

# Simplificando

$$\begin{aligned} 12a+21b&=0\\ 12c+21d&=3 \end{aligned} \qquad \begin{aligned} 12a+18&=0\\ 12c+5&=3 \end{aligned} \qquad \begin{aligned} 12a&=-18=8\\ 12c&=-2=24 \end{aligned}$$

$$\begin{aligned} 5a+6b&=19\\ 5c+6d&=17 \end{aligned} \qquad \begin{aligned} 5a+20&=19\\ 5c+20&=17 \end{aligned} \qquad \begin{aligned} 5a&=-1=25\\ 5c&=-3=23 \end{aligned}$$

# Finalmente

| 26*k | 12a=8 | a1 | 12c=24 | c1 | 5a=25 | a2 | 5c=23 | c2 |
|---|---|---|---|---|---|---|---|---|
| 0 | 8 | 0.67 | 24 | 2 | 25 | 5 | 23 | 4.6 |
| 26 | 34 | 2.83 | 50 | 4.17 | 51 | 10.2 | 49 | 9.8 |
| 52 | 60 | 5 | 76 | 6.33 | 77 | 15.4 | 75 | 15 |
| 78 | 86 | 7.17 | 102 | 8.50 | 103 | 20.6 | 101 | 20.2 |
| 104 | 112 | 9.33 | 128 | 10.67 | 129 | 25.8 | 127 | 25.4 |
| 130 | 138 | 11.5 | 154 | 12.83 | 155 | | 153 | |
| 156 | 164 | 13.67 | 180 | 15 | 181 | | 179 | |
| 182 | 190 | 15.83 | 206 | 17.17 | 207 | | 205 | |
| 208 | 216 | 18 | 232 | 19.33 | 233 | | 231 | |
| 234 | 242 | 20.17 | 258 | 21.50 | 259 | | 257 | |
| 260 | 268 | 22.33 | 284 | 23.67 | 285 | | 283 | |
| 286 | 294 | 24.5 | 310 | 25.83 | 311 | | 309 | |

La inversa (descifrar)

$$\begin{pmatrix} 5 & 12 \\ 15 & 25 \end{pmatrix}$$