DECODIFICANDO RUNAS CON MATRICES

Cuando comencé a leer El Hobbit de Tolkien, en la primera página se mostraba en inglés el título de libro junto con un subtítulo en runas germánicas:

ᚦᛖ ᚺᚠᛒᛒᛁᛏ
ᚠᚱ
ᚦᛖᚱᛖ ᚠᚾᛞ ᛒᚠᚳᚻ ᚠᚷᚠᛁᚾ

Luego nos cuentan cómo las runas se escribían mediante cortes o incisiones en madera, para después decirnos que en el Mapa de Thror hay una mano que señala a la puerta secreta y debajo hay una inscripción:

ᚠᛁᚢᛖ ᚠᛟᛏ ᚺᛁᚷᚺ ᚦᛖ ᛞᚠᚱ ᚠᚾᛞ ᚦᚱᛟ ᛞᚠᛗ ᚹᚠᚱᚻ ᚠᛒᚱᛖᛋᛏ ⁝ᚦ. ᚦ.

Donde las últimas dos runas son las iniciales de Thror y Thrain. Al sureste del mapa también se lee:

ᛋᛏᚠᚾᛞ ᛒᛗ ᚦᛖ ᚷᚱᛖᛗ ᛋᛏᚠᚾᛖ ᚹᚺᛖᚱ ᚦᛖ ᚦᚱᚢᛋᚺ ᚺᚾᚠᚺᚺᛋ ᚠᚾᛞ ᚦᛖ ᛋᛖᛏᛏᛁᛝ ᛋᚢᚾ ᚹᛁᚦ ᚦᛖ ᚩᚠᛋᛏ ᚩᛁᚷᚺᛏ ᚠᚠ ᛞᚢᚱᛁᚾᛋ ᛞᚠᛗ ᚹᛁᚩᚩ ᛋᚺᛁᚾᛖ ᚢᛈᚠᚾ ᚦᛖ ᚺᛖᛗᚺᚠᚩᛖ.

Notemos que aunque no estemos familiarizados con las runas, es posible determinar el significado de los dos enunciados anteriores, apoyadonos unicamente en la similitud de estas con nuestro alfabeto y al contexto que se envuelve con el lenguaje inglés usual.

Se podría decir que la traducción de un lenguaje a otro es un ejericicio de decodificación.

Lo anterior puede ser motivación para estudiar algunos ejemplos de criptografía, la cual es el arte de codificar mensajes para ocultar su significado y que este pueda ser decodificado una vez recibido el mensaje. Existen muchas formas de hacer esto. Por ejemplo, si recorremos el abecedario ciclicamente 2 letras:

$A \to C$	$E \to G$	$I \to K$	$M \to O$	$Q \to S$	$U \to W$	$Y \to A$
$B \to D$	$F \to H$	$J \to L$	$N \to P$	$R \to T$	$V \to X$	$Z \to B$
$C \to E$	$G \to I$	$K \to M$	$O \to Q$	$S \to U$	$W \to Y$	
$D \to F$	$H \to J$	$L \to N$	$P \to R$	$T \to V$	$X \to Z$	

Palabras arbitrarias como LEY o SECRETO se codifican como NGA o UGETGVQ, respectivamente.

Ahora, quisieramos utilizar matrices numéricas para codificar un mensaje, para poder hacerlo, hay que asignar valores numéricos a nuestro alfabeto. La asiganción más obvia sería asignar los valores del 1 al 26 para nuestros 26 caracteres posibles.

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

Supongamos que queremos codificar el mensaje HELLO WORLD. Para esto, vamos a dividir el mensaje en partes de dos caracteres, es decir:

HE LL OW OR LD

Ahora, vamos a asignar un vector columna de dos entradas a cada parte del mensaje, la entradas son los valores númericos asignados a cada letra. Lo vectores resultantes son:

$$\begin{pmatrix} 8 \\ 5 \end{pmatrix} \quad \begin{pmatrix} 12 \\ 12 \end{pmatrix} \quad \begin{pmatrix} 15 \\ 23 \end{pmatrix} \quad \begin{pmatrix} 15 \\ 18 \end{pmatrix} \quad \begin{pmatrix} 12 \\ 4 \end{pmatrix}$$

Finalmente, hay que elegir una llave para codificar el mensaje, esta llave solo debe conocerla el receptor del mensaje. Como ya lo mencionamos, nuestra llave será una matriz de 2×2. Hay que elegirla invertible, esto es fundamental, como veremos a la hora de decodificar el mensaje. Supongamos que es:

$$\begin{pmatrix} 2 & 3 \\ 1 & 1 \end{pmatrix}$$

Para codificar el mensaje basta con multiplicar por la izquierda a cada vector por la matriz llave. Así, el mensaje codificado serán los vectores:

$$\begin{pmatrix} 31 \\ 13 \end{pmatrix} \quad \begin{pmatrix} 60 \\ 24 \end{pmatrix} \quad \begin{pmatrix} 99 \\ 38 \end{pmatrix} \quad \begin{pmatrix} 84 \\ 33 \end{pmatrix} \quad \begin{pmatrix} 36 \\ 16 \end{pmatrix}$$

Cuando el receptor reciba este mensaje, lo único que tendrá que hacer para decodificarlo será multiplicar por la izquierda a cada vector por la inversa de la matriz llave, de la cual es poseedor. Finalmente, al reasignar los valores alfabéticos a los valores numéricos, el mensaje se revelará al receptor.

Es importante observar que para esta codificación no hubo ambiguedad en la asignación de los valores numéricos a los caracteres, pues fue una correspondencia biunívoca entre ellos. Además, al ser la matriz llave invertible, la recuperación de los vectores originales también pudo ocurrir sin errores. Es bien sabido que cuando es posible que haya interferencia en la transmisión de un mensaje, existen códigos(los cuales no son más que un subconjunto apropiado de palabras) para corregir errores en la transmisión. Por supuesto que esto reduce la variedad de mensajes que pueden ser transmitidos.

Como ejercicio final, utilizaremos una matriz llave de 3×3 para codificar el mensaje con runas inscrito al comienzo del texto:

ᚠᛁᚢᛖ ᚠᛟᛏ ᚺᛁᚷᚺ ᚦᛖ ᛞᚠᚱ ᚠᚾᛞ ᚦᚱᛟ ᛞᚠᛗ ᚹᚠᚴᚺ ᚠᛒᚱᛖᛋᛏ ⁝ᚦ. ᚦ.

Lo primero es asignar valores numéricos a las runas, para complicar la codificación, ahora eligiremos un orden descendente.

ᚠ→ 26	ᛖ→ 22	ᛁ→ 18	ᛗ→ 14	ᛈ→ 10	ᛏ→ 6	ᛉ→ 2
ᛒ→ 25	ᚠ→ 21	᛭→ 17	ᚾ→ 13	ᛇ→ 9	ᚦ → 5	ᛗ→ 1
ᛋ→ 24	ᚷ→ 20	ᚺ→ 16	ᛝ→ 12	ᚱ→ 8	ᚢ→ 4	
ᛞ→ 23	ᚻ→ 19	ᚴ→ 15	ᛟ→ 11	ᛋ→ 7	ᚹ→ 3	

Separemos el mensaje ahora en partes de tres caracteres:

ᚠᛁᚢ ᛖᚠᛟ ᛏᚻᛁ ᚷᚻᚦ ᛖᛞᚠ ᚱᚠᚾ ᛞᚦᚱ ᛟᛞᚠ ᛗᚹᚠ ᚴᚺᚠ ᛒᚱᛖ ᛋᛏ

Asignemos vectores columna de tres entradas a cada parte. Dado que la última parte solo tiene dos caracteres, colocaremos una entrada igual a 0.

$$\begin{pmatrix} 21 \\ 18 \\ 4 \end{pmatrix} \begin{pmatrix} 22 \\ 21 \\ 11 \end{pmatrix} \begin{pmatrix} 6 \\ 19 \\ 18 \end{pmatrix} \begin{pmatrix} 20 \\ 19 \\ 5 \end{pmatrix} \begin{pmatrix} 22 \\ 23 \\ 26 \end{pmatrix} \begin{pmatrix} 8 \\ 26 \\ 13 \end{pmatrix} \begin{pmatrix} 23 \\ 5 \\ 8 \end{pmatrix} \begin{pmatrix} 11 \\ 23 \\ 26 \end{pmatrix} \begin{pmatrix} 1 \\ 3 \\ 26 \end{pmatrix} \begin{pmatrix} 15 \\ 16 \\ 26 \end{pmatrix} \begin{pmatrix} 25 \\ 8 \\ 22 \end{pmatrix} \begin{pmatrix} 7 \\ 6 \\ 0 \end{pmatrix}$$

Elegimos la matriz invertible:

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

Al multiplicar por la izquierda, el mensaje codificado queda de la siguiente forma:

$$\begin{pmatrix} 39 \\ 18 \\ 22 \end{pmatrix} \begin{pmatrix} 43 \\ 21 \\ 32 \end{pmatrix} \begin{pmatrix} 25 \\ 19 \\ 37 \end{pmatrix} \begin{pmatrix} 39 \\ 19 \\ 24 \end{pmatrix} \begin{pmatrix} 45 \\ 23 \\ 49 \end{pmatrix} \begin{pmatrix} 34 \\ 26 \\ 39 \end{pmatrix} \begin{pmatrix} 28 \\ 5 \\ 13 \end{pmatrix} \begin{pmatrix} 34 \\ 23 \\ 49 \end{pmatrix} \begin{pmatrix} 4 \\ 3 \\ 29 \end{pmatrix} \begin{pmatrix} 31 \\ 16 \\ 42 \end{pmatrix} \begin{pmatrix} 33 \\ 8 \\ 30 \end{pmatrix} \begin{pmatrix} 13 \\ 6 \\ 6 \end{pmatrix}$$