

DECODIFICANDO RUNAS CON MATRICES

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

Þ M H F B B I T
F R
Þ M R M F T W B F K h F X F I T

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

Þ I N M F X T H I X H Þ M W F R F T W Þ R X W F R Þ F T h F B R M Y T : Þ . Þ .

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

Y T F T W B R Þ M X R M R Y T F T M Þ H M R Þ M Þ R N Y H h T F h h Y F T W Þ M Y M T T I X
Y N T Þ I Þ Þ M T F Y T T I X H T F F W N R I T Y W F R Þ I T Y H I T M N C F T Þ M h M R H F T M .

Notemos que aunque no estemos familiarizados con las runas, es posible determinar el significado de los dos enunciados anteriores, apoyados únicamente 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 ejercicio de decodificación.

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

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

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 asignación más obvia sería asignar los valores del 1 al 26 para nuestros 26 caracteres posibles.

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

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 numéricos asignados a cada letra. Lo vectores resultantes son:

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

Finalmente, hay que elegir una llave para decodificar 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 ambigüedad 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:

FIDM F8T HIXH BM MFR FTX PRX MFA PFTH FBRMHT :B. B.

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

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

Separemos el mensaje ahora en partes de tres caracteres:

የሰበሰቡ ስምዎች በጥንቃቄ ተመልክተው የሚገኙትን አስተያየቶችና ጥያቄዎች ያስቀመጣቸዋል።

Asignemos vectores columna de tres entradas a cada parte. Dado que la última parte solo tiene 2 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:

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