APLICACIÓN DE LAS MATRICES INVERTIBLES EN CRIPTOGRAFÍA

Juan Carlos Cortés López
Gema Calbo Sanjuán

Juan Carlos Cortés López, Departamento de Matemática Aplicada
Universidad Politécnica de Valencia
Gema Calbo Sanjuán, Departamento de Matemáticas
I.E.S. Els Évols. L'Alcúdia (Valencia)

RESUMEN

Este trabajo pretende mostrar una aplicación de las matrices invertibles (y en particular de las matrices ortogonales) a la codificación de mensajes.

1. INTRODUCCIÓN

Para los matemáticos teóricos, una de las áreas más apasionantes de las matemáticas es la Teoría de Números, que se ocupa del estudio de las propiedades de éstos, y en particular, de los que se consideran su *materia prima*: los *números primos*, debido a que todo entero positivo es producto de números primos. Sin embargo, en los últimos años son ya muchos los científicos aplicados que han decidido interesarse por esta rama de las matemáticas, al encontrar entre sus más abstractos resultados, interesantes aplicaciones que permiten satisfacer ciertas demandas de la sociedad actual, y entre éstas, la que nos interesa en este trabajo: la criptografía. Un área de conocimiento que se ocupa del diseño de algoritmos para transmitir mensajes de forma segura.

En la década de los años cuarenta, donde se establece el origen de la criptografía, el uso de claves para enviar mensajes estaba prácticamente restringido al campo de la estrategia militar, por eso fue que las primeras investigaciones criptográficas se hicieron en el seno del ejército. Sin embargo, en este sentido en la actualidad las cosas han cambiado radicalmente y hoy día son muchas las situaciones cotidianas donde efectivamente, necesitamos hacer uso de la criptografía: cuando utilizamos la tarjeta de crédito en cualquier cajero automático para realizar una operación bancaria necesitamos identificarnos a través de una clave; cuando encendemos el móvil para realizar una llamada, éste nos pide antes que intro-

duzcamos un PIN (Personal Identification Number); cuando accedemos a nuestra cuenta de correo electrónico, el ordenador nos exige que utilicemos nuestra contraseña;...

Prácticamente todos los algoritmos eficientes diseñados para escenarios tanto de clave pública como privada, como pueden ser los conocidos métodos RSA, HG,...se basan en resultados de Teoría de Números. Se necesita un buen bagaje matemático en este área del Álgebra para comprender estos métodos, por lo que quedan fuera del alcance de los estudiantes del último curso de bachillerato o un primer curso universitario de una carrera tecnológica. El objetivo de estas páginas es mostrar un método sencillo para introducir las ideas básicas de la criptografía mediante el uso de herramientas básicas del álgebra matricial, que sí son conocidas en estos niveles educativos.

2. CODIFICANDO MENSAJES CON MATRICES ORTOGONALES

Para codificar un mensaje los elementos que se requieren son:

- Un emisor.
- Un receptor.
- Un mensaje.
- Un código.

Cuando hablamos de código, implícitamente estamos hablando de un método de codificación, es decir, algún algoritmo *biunívoco* que asigne a cada carácter del mensaje otro carácter. Este método hace que el mensaje enviado por el emisor se transforme en una cadena de símbolos ilegibles al resto de los receptores que no sean legales. Dependiendo de la calidad del método de codificación, el mensaje transformado, aunque sea capturado por receptores ilegales, será más o menos difícil de descifrar.

A continuación, veremos un método sencillo para codificar mensajes, basado en álgebra matricial. Lo primero que hacemos es elegir un código (1ª fase del proceso de codificación). Como el trabajo tiene carácter divulgativo, elegimos un código sencillo basado en invertir numéricamente la sucesión de las posiciones que ocupan las letras del abecedario (véase tabla 1).

A	B	C	D	E	F	G	H	I	J	K	L	M	N
27	26	25	24	23	22	21	20	19	18	17	16	15	14
Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	
13	12	11	10	9	8	7	6	5	4	3	2	1	

Tabla 1. Código utilizado en la 1ª fase del proceso de codificación.

Supongamos que deseamos enviar el siguiente mensaje:

QUEDAMOS EN EL ALTOZANO A LAS NUEVE

Desde luego una forma inmediata de codificar el mensaje sería, utilizando la tabla 1, escribir

10 6 23 24 27 15 12 8 23 14 23 16 27 16 7 12 1 27 14 12 27 16 27 8 14 6 23 5 23

Sin embargo, el método de cifrado empleado es extremadamente sencillo lo que sin duda hace muy vulnerable al mensaje. Veamos cómo mejorar el algoritmo de codificación utilizando matrices. Convengamos en separar los caracteres del mensaje en grupos de dos:

QU ED AM OS EN EL AL TO ZA NO AL AS NU EV EZ

Obsérvese que como hay un número impar de caracteres, hemos añadido a la última letra del mensaje otra letra (por ejemplo, la Z) para poder seguir trabajando, aunque esto no supondrá una desvirtuación del mensaje, ya que, el receptor al descodificarlo observará todo el mensaje con un último carácter técnico que evidentemente no concuerda, por lo que lógicamente lo desechará. A continuación, disponemos el mensaje así diseccionado en vectores columnas de dimensión dos, pero mediante el código de la tabla 1:

$$\begin{bmatrix} Q \\ U \end{bmatrix} = \begin{bmatrix} 10 \\ 6 \end{bmatrix} \;;\; \begin{bmatrix} E \\ D \end{bmatrix} = \begin{bmatrix} 23 \\ 24 \end{bmatrix} \;;\; \begin{bmatrix} A \\ M \end{bmatrix} = \begin{bmatrix} 27 \\ 15 \end{bmatrix} \;;\; \begin{bmatrix} O \\ S \end{bmatrix} = \begin{bmatrix} 12 \\ 8 \end{bmatrix} \;;\; \cdots \quad \textbf{(1)}$$

Ahora elegimos la transformación matricial que encripte aún más el mensaje (2ª fase del proceso de codificación). Tomamos la siguiente matriz quasi-ortogonal (con determinante uno, luego invertible):

$$A = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \Rightarrow A^{-1} = \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix}$$

llamada *matriz de codificación*, y transformamos los vectores dados en (1) mediante :

$$A \cdot \begin{bmatrix} Q \\ U \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 10 \\ 6 \end{bmatrix} = \begin{bmatrix} 26 \\ 16 \end{bmatrix} \;;\; A \cdot \begin{bmatrix} E \\ D \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 23 \\ 24 \end{bmatrix} = \begin{bmatrix} 70 \\ 47 \end{bmatrix}$$

$$A \cdot \begin{bmatrix} A \\ M \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 27 \\ 15 \end{bmatrix} = \begin{bmatrix} 69 \\ 42 \end{bmatrix} \;;\; A \cdot \begin{bmatrix} O \\ S \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 12 \\ 8 \end{bmatrix} = \begin{bmatrix} 32 \\ 20 \end{bmatrix} \;;\; \cdots$$

y procediendo así hasta el final, enviamos el siguiente mensaje codificado:

26 16 70 47 69 42 32 20...

Para descifrar el mensaje, el receptor legal, quien suponemos que conoce la matriz de codificación, debe actuar como sigue:

$$A^{-1}\cdot\begin{bmatrix}26\\16\end{bmatrix}=\begin{bmatrix}1&-1\\-1&2\end{bmatrix}\cdot\begin{bmatrix}26\\16\end{bmatrix}=\begin{bmatrix}10\\6\end{bmatrix}\quad;\quad A^{-1}\cdot\begin{bmatrix}70\\47\end{bmatrix}=\begin{bmatrix}1&-1\\-1&2\end{bmatrix}\cdot\begin{bmatrix}70\\47\end{bmatrix}=\begin{bmatrix}23\\24\end{bmatrix}\quad;\quad\cdots$$

obteniendo así la sucesión:

10 6 23 24...

Por lo que utilizando la tabla 1, el receptor descifrará el mensaje.

Analicemos ahora el método empleado:

- La matriz de codificación únicamente sirve para hacer más complejo el algoritmo de encriptación del mensaje y por lo tanto para conseguir una mayor seguridad del proceso.
- La característica esencial que debe tener la matriz de codificación es que debe ser invertible, para garantizar que la segunda fase del proceso de codificación sea reversible o biunívoca, es decir, se pueda descodificar el mensaje, a través de la matriz inversa.
- En realidad que la matriz de codificación sea ortogonal o quasi-ortogonal (y por tanto invertible), no es fundamental, únicamente esta elección es atractiva porque al tener determinante ± 1, los cálculos que se obtienen no son engorrosos. En el caso de que la matriz sea ortogonal a coeficientes enteros, queda garantizado que también será del mismo tipo.
- Para la técnica utilizada, se necesita que tanto el emisor como el receptor conozcan los elementos de ambas fases de codificación: el código de la tabla 1 y la matriz de codificación.
- El proceso de codificación se puede hacer más y más complejo añadiendo más fases al mismo. La característica de los algoritmos que definen estas fases, es que deben ser biyectivos, siendo posible calcular el algoritmo inverso.

En la ilustración anterior hemos trabajado con matrices cuadradas de orden dos, pero el proceso es compatible con cualquier otro tamaño. Veamos qué aspectos cambian cuando adaptamos las ideas a matrices cuadradas de orden tres. Lo haremos con el mismo mensaje que antes.

En primer lugar, dividimos el mensaje original en palabras de lon-

gitud tres:

QUE DAM OSE NEL ALT OZA NOA LAS NUE VEZ

(como antes, hemos tenido que añadir al final la letra Z). En segundo lugar, utilizando la tabla 1 efectuamos el primer paso de la codificación:

$$\begin{bmatrix} Q \\ U \\ E \end{bmatrix} = \begin{bmatrix} 10 \\ 6 \\ 23 \end{bmatrix} \quad ; \quad \begin{bmatrix} D \\ A \\ M \end{bmatrix} = \begin{bmatrix} 24 \\ 27 \\ 15 \end{bmatrix} \quad ; \quad \begin{bmatrix} O \\ S \\ E \end{bmatrix} = \begin{bmatrix} 12 \\ 8 \\ 23 \end{bmatrix} \quad ; \quad \ldots$$

A continuación, elegimos una matriz de codificación quasi-ortogonal

$$A = \begin{bmatrix} 1 & 0 & 2 \\ -1 & 1 & 0 \\ 1 & 0 & 3 \end{bmatrix} \Rightarrow A^{-1} = \begin{bmatrix} 3 & 0 & -2 \\ 3 & 1 & -2 \\ -1 & 0 & 1 \end{bmatrix}$$

y realizamos el segundo paso de la codificación:

$$A \cdot \begin{bmatrix} Q \\ U \\ E \end{bmatrix} = \begin{bmatrix} 1 & 0 & 2 \\ -1 & 1 & 0 \\ 1 & 0 & 3 \end{bmatrix} \cdot \begin{bmatrix} 10 \\ 6 \\ 23 \end{bmatrix} = \begin{bmatrix} 56 \\ -4 \\ 79 \end{bmatrix} \quad ; \quad A \cdot \begin{bmatrix} D \\ A \\ M \end{bmatrix} = \begin{bmatrix} 1 & 0 & 2 \\ -1 & 1 & 0 \\ 1 & 0 & 3 \end{bmatrix} \cdot \begin{bmatrix} 24 \\ 27 \\ 15 \end{bmatrix} = \begin{bmatrix} 54 \\ 3 \\ 69 \end{bmatrix}$$

$$A \cdot \begin{bmatrix} O \\ S \\ E \end{bmatrix} = \begin{bmatrix} 1 & 0 & 2 \\ -1 & 1 & 0 \\ 1 & 0 & 3 \end{bmatrix} \cdot \begin{bmatrix} 12 \\ 8 \\ 23 \end{bmatrix} = \begin{bmatrix} 58 \\ -4 \\ 81 \end{bmatrix} \quad \ldots$$

Ahora enviaremos el siguiente mensaje a nuestro receptor:

56 -4 79 54 3 69 58 -4 81...

quien descodificará el mensaje mediante la matriz inversa:

$$A^{-1} \cdot \begin{bmatrix} 56 \\ -4 \\ 79 \end{bmatrix} = \begin{bmatrix} 3 & 0 & -2 \\ 3 & 1 & -2 \\ -1 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 56 \\ -4 \\ 79 \end{bmatrix} = \begin{bmatrix} 10 \\ 6 \\ 23 \end{bmatrix} ; \; A^{-1} \cdot \begin{bmatrix} 54 \\ 3 \\ 69 \end{bmatrix} = \begin{bmatrix} 3 & 0 & -2 \\ 3 & 1 & -2 \\ -1 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 54 \\ 3 \\ 69 \end{bmatrix} = \begin{bmatrix} 24 \\ 27 \\ 15 \end{bmatrix}$$

a través de la cual se obtiene la sucesión:

10 6 23 24 27 15 12 8 23...

y mediante la tabla 1, se descifra el mensaje.

Antes hemos subrayado que el método puede hacerse más seguro aumentando el número de fases del proceso de codificación, pero en la prác-

tica esto también puede significar un aumento de las posibilidades de error (derivados del incremento de los cálculos que lleva implícito el método para codificar y descodificar).

Para aumentar las probabilidades de que el mensaje llegue correctamente, suelen añadirse al final del mismo lo que se denominan los dígitos de control. Por ejemplo, la letra del DNI es un carácter de control, o por ejemplo, cuando se da el número de la cuenta corriente bancaria, en medio del mismo, hay dos cifras que son los dígitos de control. Esta misma idea, puede implementarse en el método matricial anterior. Existen muchas formas de hacerlo. Por ejemplo, podemos añadir al final del mensaje dos números: el primero que nos indique el número de palabras que forman el mensaje (en el ejemplo utilizado, 7) y el número de veces que aparece la letra "e" (en el ejemplo, 5). Para efectuar el primer paso de la codificación, tendremos que ampliar la tabla 1, que debe posibilitar la introducción codificada de esta información. Una forma sería ir asignando a cada número entero no negativo (0,1,2,3,4,...) otro número, por ejemplo, continuando desde el principio con la tabla 1 (28,29,30,31,32,...), respectivamente. Con esta estrategia de control, nuestro receptor legal, deberá saber además de la nueva tabla 1 y la matriz de codificación, que al final del mensaje aparecerán unos dígitos de control así como su significado. En la ejemplificación que hemos dado nosotros, el mensaje codificado en su primera fase sería ahora

10 6 23 24 27 15 12 8 23 14 23 16 27 16 7 12 1 27 14 12 27 16 27 8 14 6 23 5 23 **35 33**

siendo 35 y 33 los números de control. El resto del proceso es igual antes.

3. CONCLUSIONES

El trabajo muestra una aplicación de las matrices a la codificación de mensajes. El atractivo que sin duda tiene esta actual temática entre el alumnado de un último curso de bachillerato o un primer curso científico-técnico universitario por estar familiarizados con el uso de claves, junto a la sencillez de las herramientas matemáticas que se requieren, hacen que las ideas que se han expuesto en estas páginas pueden ser aprovechadas en el aula en los niveles educativos citados.

BIBLIOGRAFÍA

[1] Mizrahi, A., Sullivan S. (1999): *Matemáticas Finitas*. 2ª edición. Ed. Limusa Wiley. México.

[2] Munuera, C. y Tena. J. (1997): *Codificación de la información*. Ed. Universidad de Valladolid. Valladolid.

[3] Pino Caballero, G. (1999): *Introducción a la criptografía*. Ed. RA-MA. Madrid.