suma+ 79
Artículos
Julio 2015
pp. 27-33

Cómo compartir un secreto usando sistemas de ecuaciones lineales

Alberto Cano Rojas
José María Luna Ariza
Ángela Rojas Matas

Supongamos que deseamos compartir una información secreta entre varias personas de modo que ninguna de ellas conozca el secreto pero cuando se junten un número autorizado de ellas sí que puedan averiguarlo completamente. En este trabajo se muestra una interesante aplicación de los sistemas de ecuaciones lineales a este tema que ha conseguido atraer la atención del nuestro alumnado de la asignatura de Álgebra Lineal.

Palabras clave: Innovación Docente, Álgebra Lineal, Resolución de Sistemas de Ecuaciones Lineales, Motivación del proceso Enseñanza-Aprendizaje, Universidad.

Abstract

Secret sharing is a cryptographic method that aims to distribute a secret information among several people so that none of them know the secret. The secret can be reconstructed only when a sufficient number of shares are combined together. This work presents an interesting application of systems of linear equations for sharing secrets that has attracted the attention of our students from the subject of linear algebra.

Keywords: Teaching Innovation, Linear Algebra, Solving Systems of Linear Equations, Motivation of the Teaching-Learning Process, University.

Existen ocasiones donde una información secreta no es deseable que esté en manos de una sola persona. Puede interesar que varias personas posean parte de dicha información y que sólo se consiga recuperar la información completa si juntamos a varias de estas personas. Por ejemplo, al dueño de una empresa puede que le interese que ningún empleado de la misma posea la clave que abre la caja fuerte. Por el contrario, puede repartir entre 6 empleados, por ejemplo, parte de la información secreta, de forma que para conseguir la clave de la caja fuerte tengan que juntarse al menos 3 de los 6 empleados. Este sería un ejemplo de cómo compartir un secreto (6, 3). También se conoce con el nombre de esquema umbral (6, 3).

Estos protocolos criptográficos fueron publicados por primera vez por el criptógrafo Shamir (1979) del MIT.(Massachusetts Institute of Technology) y por Blakley (1979). Actualmente tienen aplicaciones en:

— El control de accesos
— La apertura de cajas de seguridad
— La inicialización de dispositivos militares
— Etc.

Podemos comprobar el gran interés que despierta este tipo de protocolo criptográfico viendo la gran

Artículo recibido en *Suma* en ****** de 2012 y aceptado en **** de 2013

cantidad de publicaciones relacionadas con el tema (Chang y otros, 2008; M. Ulutas, V. Nabiyev, 2009; R. Zhao y otros, 2009; P. Y. Lina, C. S. Chang, 2010; X. Hei, X. Du, 2012). Por esta razón pensamos que podría ser un tema de interés para los alumnos de la asignatura de Álgebra Lineal de primer curso de Ingeniería Informática.

Los esquemas umbrales se pueden llevar a cabo con distintos métodos. El esquema umbral que vamos a usar en ese trabajo usa los sistemas de ecuaciones lineales que se estudian en Álgebra Lineal.

Planteamiento del esquema

Vamos a ver un esquema (3, 2). Participan 3 personas y sólo cuando se junten 2 de ellas podrán recuperar el secreto. Supongamos que el secreto es un número s.

El dueño del secreto escoge un vector (x_1, x_2) donde $x_1 = s$ (lo hace coincidir con el secreto) y x_2 es elegido de forma aleatoria.

Para cada participante i calcula: $a_{i1}x_1 + a_{i2}x_2 = b_i$, donde los coeficientes son elegidos aleatoriamente también.

Como tenemos tres participantes, tendremos el siguiente sistema lineal:

$$\left.\begin{aligned} a_{11}x_1 + a_{12}x_2 &= b_1 \\ a_{21}x_1 + a_{22}x_2 &= b_2 \\ a_{31}x_1 + a_{32}x_2 &= b_3 \end{aligned}\right\}$$

El dueño del secreto hace pública la matriz de los coeficientes del sistema:

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \\ a_{31} & a_{32} \end{pmatrix}$$

Y le proporciona al participante 1 el valor b_1 al participante 2 el valor b_2 y al participante 3 el valor b_3.

Supongamos que la matriz A es de rango 2 y que cualesquiera dos filas de A son linealmente independientes.

Cuando se junten dos cualesquiera de los participantes obtendrán un sistema lineal de dos ecuaciones con dos incógnitas compatible determinado cuya solución única podrán conseguir resolviendo el sistema, obteniendo así el secreto.

Por ejemplo, supongamos que en un esquema (3, 2) se sabe que la matriz A es:

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 2 \\ 4 & 7 \end{pmatrix}$$

Al primer participante se le da 12, al segundo se le da 14 y al tercero se le da 54 de forma secreta a cada uno de ellos.

Se puede recuperar el secreto en los tres casos siguientes:

1) Si se juntan los participantes 1 y 2
2) Si se juntan los participantes 1 y 3
3) Si se juntan los participantes 2 y 3

Por ejemplo, si se juntan los participantes 1 y 3, el sistema será:

$$\left.\begin{aligned} x_1 + x_2 &= 12 \\ 4x_1 + 7x_2 &= 54 \end{aligned}\right\}$$

Resolviendo obtenemos el secreto $x_1 = s = 10$. El mismo resultado se obtendrá en los otros dos casos.

Cómo debe ser la matriz para un esquema umbral

En un esquema (4, 3) se sabe que la matriz A es:

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 2 \\ 1 & 3 & 4 \\ 1 & 4 & 7 \end{pmatrix}$$

Al primer participante se le da 4, al segundo 3, al tercero 2, al cuarto 1.

En el ejemplo anterior se puede obtener el secreto siempre:

— Si se juntan los participantes 1, 2 y 3 se obtiene un sistema lineal de 3 ecuaciones con 3 incógnitas donde la matriz de los coeficientes es:

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 2 \\ 1 & 3 & 4 \end{pmatrix}$$

cuyo determinante es no nulo. Por tanto, el sistema es un sistema compatible determinado, cuya solución es $x_1 = 5$. Por lo tanto, el secreto es 5.

— Si se juntan los participantes 1, 2 y 4 se obtiene también un sistema con solución única y el secreto es 5.

— Si se juntan los participantes 1, 3 y 4 se obtiene también un sistema con solución única y el secreto es 5.

— Si se juntan los participantes 2, 3 y 4 se obtiene también un sistema con solución única y el secreto es 5.

Por lo tanto, la matriz A debe ser de rango 3 y cualesquiera tres filas de la matriz deben ser linealmente independientes para que los sistemas anteriores sean sistemas compatibles determinados

Supongamos que tenemos un esquema (4, 3) donde la matriz A fuera la siguiente:

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 2 \\ 1 & 3 & 4 \\ 2 & 3 & 3 \end{pmatrix}$$

Al primer participante se le da 4, al segundo 3, al tercero 2, al cuarto 7.

— Si se juntan los participantes 1, 2 y 3, se obtiene un determinante no nulo de la matriz de los coeficientes, por tanto, el sistema es un sistema compatible determinado (las tres filas de A son linealmente independientes), entonces se puede recuperar el secreto.

— Si se juntan 1, 2 y 4 se obtiene un determinante nulo de la matriz de los coeficientes (las tres filas de A son linealmente dependientes) y el sistema es un sistema compatible indeterminado. Entonces no se puede recuperar el secreto ya que habría infinitas soluciones. Por lo tanto esa matriz A no sería una matriz válida para un esquema (4, 3).

Para que la matriz sea válida para un esquema (4, 3) debe ser una matriz en la que tres filas cualesquiera de ella sean linealmente independientes, o lo que es lo mismo, cualquier submatriz formada por tres filas de debe ser de rango 3.

Esquema umbral con congruencias

La idea anterior puede adaptarse fácilmente para trabajar con congruencias. Esto nos va a permitir repartir un texto o una imagen digital. Veámoslo con un ejemplo.

Supongamos que tenemos la palabra secreta «MAR» y que tenemos un alfabeto de 27 caracteres como el siguiente:

A 0	B 1	C 2	D 3	E 4	F 5	G 6	H 7	I 8	J 9	K 10	L 11	M 12	N 13	Ñ 14
O 15	P 16	Q 17	R 18	S 19	T 20	U 21	V 22	W 23	X 24	Y 25	Z 26			

Entonces «MAR» equivale a {12, 0, 18}. Trabajaremos con módulo $m = 27$.

Usamos la matriz siguiente para hacer un esquema (3, 2):

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 2 \\ 4 & 6 \end{pmatrix}$$

El primer elemento de la lista secreta es $s = 12$. Entonces, $x_1 = s = 12$ y $x_2 = 3$ es elegido aleatoriamente. Se calcula a continuación:

$$y_1 = x_1 + x_2 = 15 \pmod{27} \rightarrow O$$

$$y_2 = x_1 + 2x_2 = 18 \pmod{27} \rightarrow R$$

$$y_3 = 4\ x_1 + 6x_2 = 66 = 12 \pmod{27} \rightarrow M$$

La misma idea se aplica al segundo elemento de la lista secreta. En este caso $x_1 = s = 0$ y $x_2 = 5$ es elegido aleatoriamente.

$$y_1 = x_1 + x_2 = 5 \pmod{27} \rightarrow F$$
$$y_2 = x_1 + 2x_2 = 10 \pmod{27} \rightarrow K$$
$$y_3 = 4\ x_1 + 6x_2 = 30 = 3 \pmod{27} \rightarrow D$$

Por último, repetimos para el tercer elemento de la lista secreta: $x_1 = s = 18$ y $x_2 = 4$ que es elegido aleatoriamente.

$$y_1 = x_1 + x_2 = 22 \pmod{27} \rightarrow V$$
$$y_2 = x_1 + 2x_2 = 26 \pmod{27} \rightarrow Z$$
$$y_3 = 4\ x_1 + 6x_2 = 96 = 15 \pmod{27} \rightarrow O$$

Al primer participante se le proporciona *OFV*, al segundo *RKZ* y al tercero *MDO* de forma secreta a cada participante. La matriz A será pública.

¿Cómo se averigua el secreto? Es sencillo. Hay que deshacer lo que hemos hecho anteriormente.

Supongamos que se juntan los participantes 1 y 3, por ejemplo. El participante 1 aporta $OFV = \{15, 5, 22\}$ y el participante 3 aporta $MDO = \{12, 3, 15\}$.

Para recuperar la primera letra del mensaje secreto se debe resolver el sistema:

$$\left.\begin{array}{r} x_1 + x_2 = 15 \pmod{27} \\ 4\ x_1 + 6x_2 = 12 \pmod{27} \end{array}\right\}$$

Este sistema se puede expresar matricialmente de la forma:

$$\begin{pmatrix} 1 & 1 \\ 4 & 6 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 15 \\ 12 \end{pmatrix} \pmod{27}$$

¿Será

$$H = \begin{pmatrix} 1 & 1 \\ 4 & 6 \end{pmatrix}$$

inversible módulo 27?

Se puede hacer de dos formas, o bien por operaciones elementales por filas o bien usando determinantes pero trabajando módulo 27.

Si lo hacemos por operaciones elementales:

$$\left(\begin{array}{cc|cc} 1 & 1 & 1 & 0 \\ 4 & 6 & 0 & 1 \end{array}\right) \overset{f_2 \rightarrow f_2 - 4f_1}{\rightarrow}$$
$$\overset{f_2 \rightarrow f_2 - 4f_1}{\rightarrow} \left(\begin{array}{cc|cc} 1 & 1 & 1 & 0 \\ 0 & 2 & -4 & 1 \end{array}\right) =$$
$$= \left(\begin{array}{cc|cc} 1 & 1 & 1 & 0 \\ 0 & 2 & 23 & 1 \end{array}\right) \pmod{27}$$

Hallamos el inverso de 2 módulo 27 y resulta ser 14 ya que $2 \times 14 = 28 = 1 \pmod{27}$. Entonces:

$$\overset{f_2 \rightarrow f_2(14)}{\rightarrow} \left(\begin{array}{cc|cc} 1 & 1 & 1 & 0 \\ 0 & 2\times 14 & 23\times 14 & 1\times 14 \end{array}\right) =$$
$$= \left(\begin{array}{cc|cc} 1 & 1 & 1 & 0 \\ 0 & 1 & 25 & 14 \end{array}\right) \pmod{27} \overset{f_1 \rightarrow f_1 - f_2}{\rightarrow}$$
$$\overset{f_1 \rightarrow f_1 - f_2}{\rightarrow} \left(\begin{array}{cc|cc} 1 & 0 & -24 & -14 \\ 0 & 1 & 25 & 14 \end{array}\right) =$$
$$= \left(\begin{array}{cc|cc} 1 & 0 & 3 & 13 \\ 0 & 1 & 25 & 14 \end{array}\right) \pmod{27}$$

$$\overset{f_2 \rightarrow f_2(14)}{\rightarrow} \left(\begin{array}{cc|cc} 1 & 1 & 1 & 0 \\ 0 & 2\times 14 & 23\times 14 & 1\times 14 \end{array}\right) =$$
$$= \left(\begin{array}{cc|cc} 1 & 1 & 1 & 0 \\ 0 & 1 & 25 & 14 \end{array}\right) \pmod{27} \overset{f_1 \rightarrow f_1 - f_2}{\rightarrow}$$
$$\overset{f_1 \rightarrow f_1 - f_2}{\rightarrow} \left(\begin{array}{cc|cc} 1 & 0 & -24 & -14 \\ 0 & 1 & 25 & 14 \end{array}\right) =$$
$$= \left(\begin{array}{cc|cc} 1 & 0 & 3 & 13 \\ 0 & 1 & 25 & 14 \end{array}\right) \pmod{27}$$

Por lo tanto, la inversa es:

$$H^{-1} = \begin{pmatrix} 3 & 13 \\ 25 & 14 \end{pmatrix} \pmod{27}$$

Efectivamente, podemos comprobar cómo $HH^{-1} = I \pmod{27}$.

Hay que observar que no podríamos haber calculado la inversa si 2 no hubiera tenido inverso módulo 27.

Si se hubiera hecho con determinantes, hubiéramos razonado de la siguiente forma:

$$|H| = \begin{vmatrix} 1 & 1 \\ 4 & 6 \end{vmatrix} = 2 \neq 0$$

Entonces:

— Matriz adjunta de H:

$$\begin{pmatrix} 6 & -4 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 6 & 23 \\ 26 & 1 \end{pmatrix} (mod\ 27)$$

— Matriz transpuesta de la anterior:

$$\begin{pmatrix} 6 & 26 \\ 23 & 1 \end{pmatrix}$$

— Dividimos por el determinante, o lo que es lo mismo, multiplicamos por el inverso de 2 que era 14:

$$H^{-1} = 2^{-1} \begin{pmatrix} 6 & 26 \\ 23 & 1 \end{pmatrix} =$$

$$= 14 \begin{pmatrix} 6 & 26 \\ 23 & 1 \end{pmatrix} = \begin{pmatrix} 84 & 364 \\ 322 & 14 \end{pmatrix} =$$

$$= \begin{pmatrix} 3 & 13 \\ 25 & 14 \end{pmatrix} (mod\ 27)$$

Observar que el último paso exige dividir por el determinante, o lo que es lo mismo, multiplicar por el inverso del determinante. Por lo tanto debe ocurrir que el determinante tenga inverso módulo 27. Esto se cumple siempre que sea primo relativo con el módulo. Como 2 y 27 son primos relativos, 2 tiene inverso módulo 27 que, como ya sabemos, era 14. En general, una matriz es inversible módulo m si y sólo si su determinante es primo relativo con m.

El sistema se puede resolver ahora:

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = H^{-1} \begin{pmatrix} 15 \\ 12 \end{pmatrix} =$$

$$= \begin{pmatrix} 3 & 13 \\ 25 & 14 \end{pmatrix} \begin{pmatrix} 15 \\ 12 \end{pmatrix} =$$

$$= \begin{pmatrix} 201 \\ 543 \end{pmatrix} = \begin{pmatrix} 12 \\ 3 \end{pmatrix} (mod\ 27)$$

Por lo tanto, el primer número secreto es 12 que se corresponde con una *M*. De la misma forma se obtienen el resto de números secretos.

Una observación: hemos tenido que resolver sistemas lineales de dos ecuaciones con dos incógnitas donde sólo se desea el valor de la primera incógnita. Se podría resolver también por el método de Cramer de la siguiente forma:

$$\left.\begin{aligned} h_{11}x_1 + h_{12}x_2 &= b_1 \\ h_{21}x_1 + h_{22}x_2 &= b_2 \end{aligned}\right\} \Rightarrow x_1 = \frac{\begin{vmatrix} b_1 & h_{12} \\ b_2 & h_{22} \end{vmatrix}}{\begin{vmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{vmatrix}} \ (mod\ 27)$$

De todas formas, se tendrá que calcular el inverso de

$$|H| = \begin{vmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{vmatrix} (mod 27)$$

para poder hallar el secreto.

El módulo, en este caso 27, no es primo y esto dificulta el cálculo de matrices válidas en el esquema umbral. Para que una matriz sea inversible, en la aritmética habitual, es suficiente con que su determinante sea no nulo. Eso no ocurre exactamente así cuando se trabaja con congruencias. En el caso anterior, por ejemplo, es necesario que $|H|$ no sólo sea no nulo sino que además debe ser primo relativo con el módulo 27.

El uso módulos primos facilita este asunto. Así, si trabajamos por ejemplo, con módulo 31 que es primo, cualquier matriz H con determinante no nulo será inversible y podremos calcular sin ningún problema el inverso de

$$|H| = \begin{vmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{vmatrix} (mod 31)$$

Cómo compartir una imagen secreta

El esquema umbral desarrollado anteriormente se puede aplicar a imágenes digitales (Thien y Lin,

2002). Una imagen digital en escala de grises no es más que una matriz donde cada elemento de la matriz nos da el nivel de gris del píxel correspondiente.

En esta sección vamos a aplicar las ideas anteriores a la imagen secreta que se muestra en la figura 1. Vamos a desarrollar concretamente un esquema (3, 2), por ejemplo.

Figura 1. Imagen secreta

Las imágenes en escala de grises más habituales tienen 256 niveles de gris (desde 0 hasta 255). Como trabajar módulo 256 puede traer problemas porque 256 no es primo, vamos a trabajar con 251 que es el número primo más próximo. Cogeremos una imagen en escala de grises donde el nivel de gris máximo va a ser 250. Si no es así, los valores superiores a 250 se pondrán a 250. Todos los niveles de gris de la imagen de la figura 1 están entre 0 y 250.

La matriz pública será, por ejemplo, la siguiente:

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

Crearemos tres matrices del mismo tamaño que la imagen secreta, en principio con todos sus elementos nulos, que indicaremos por S_1, S_2 y S_3, una para cada participante.

A cada nivel de gris de la imagen secreta se le aplicará el siguiente proceso:

— Sea g el nivel de gris de la imagen secreta correspondiente al píxel situado en la posición (i,j). Elegiremos un valor aleatorio entre 0 y 250.

— Haremos: $x_1 = g$, $x_2 = a$

— Efectuaremos el producto:

$$A\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}=\begin{pmatrix} s_1 \\ s_2 \\ s_3 \end{pmatrix} \pmod{251}$$

— Entonces hacemos:
$S_1(i,j) = s_1$, $S_2(i,j) = s_2$, $S_3(i,j) = s_3$,

De esta forma se obtienen las imágenes de la figura 2. Al participante i-ésimo se le proporciona la imagen S_2.

Como vemos, ningún participante puede *ver* el secreto sino que recibe una imagen

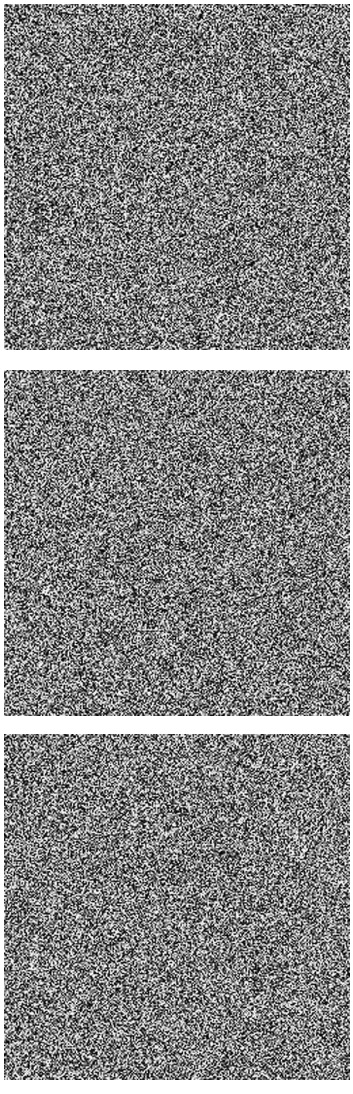

Figura 2. Imágenes S_1, S_2 y S_3

en escala de grises con aspecto aleatorio. Sin embargo, cuando dos de ellos se junten sí que podrán recuperar la imagen secreta de la figura 1.

La creación de las imágenes por parte del dueño del secreto y la posterior recuperación de la imagen secreta la hemos realizado con Matlab pero también puede hacerse con Octave, que es una versión libre de Matlab. El código fuente se encuentra disponible para su descarga desde la web en: <http://www.uco.es/users/i52caroa/secretos.zip>.

Conclusión

Hemos visto en este trabajo cómo el Álgebra Lineal se puede aplicar a un tema de interés para un alumno de primer curso de Ingeniería Informática. Además usamos en esta actividad conocimientos que los alumnos trabajan en otras asignaturas de primero ya que necesitan saber Programación, Matemática Discreta (donde estudian las congruencias) y Álgebra lineal.

Creemos que con este tipo de actividades conseguimos motivar más a nuestro alumnado.

El método desarrollado en este trabajo, en su versión más simple, sin el uso de congruencias, puede aplicarse a alumnos de Bachillerato.

Referencias bibliográficas

Blakley, G. R. (1979), «Safeguarding cryptographic keys», *Proceedings of the 1979 National Computer Conference,* n.º 48, 313-317.

Chang, C. C., C. C. Lin, C. H. Lin y Y. H. Chen (2008), «A novel secret image sharing scheme in color images using small shadow images», *Information Sciences,* vol. 178, n.º 11, 2433–2447.

Hei, X. y X. Du (2012), «Two matrices for Blakley's secret sharing scheme», *Proceedings on IEEE International Conference on Communications (ICC),* 810-814.

Lina, P. Y., y C. S. Chan (2010), «Invertible secret image sharing with steganography», *Pattern Recognition Letters*, vol, 31, n.º 13, 1887–1893.

Shamir, A. (1979), «How share a secret», *Communications of the ACM,* vol. 22, nº. 11, 612-613.

Thien, C. C., y J.C. Lin (2002), «Secret image sharing», *Computer and Graphics,* vol. 26, nº. 5, 765-770.

Ulutas, M., V. NABIYEV (2009), «Improvements in Geometry-Based Secret Image Sharing Approach with Steganography», *Mathematical Problems in Engineering,* 1-12.

Zhao, R., J. Zhao, F. Dai y F. Zhao (2009), «A new image secret sharing scheme to identify cheaters», *Computer Standards & Interfaces,* vol. 31, n.º 1, 252–257.

Alberto Cano Rojas
Departamento de Informática y Análisis Numérico, Universidad de Córdoba.

José María Luna Ariza
Departamento de Informática y Análisis Numérico, Universidad de Córdoba.

Ángela Rojas Matas
Departamento de Matemáticas, Universidad de Córdoba y miembro de la Sociedad Andaluza de Educación Matemática «Thales».