INTERPOLACIÓN POLINÓMICA Y LA DIVISIÓN DE SECRETOS

Ángela Rojas Matas,
Universidad de Córdoba
Alberto Cano Rojas,
Universidad de Córdoba

RESUMEN.

La división o reparto de secretos es un tema de completa actualidad en el ámbito de la criptografía. Se ocupa de que un secreto no esté en manos de una sola persona sino que participen varias y que sólo se pueda recuperar el secreto cuando se junten un número determinado de ellas.
Además de interesante, este tema se puede convertir en un recurso didáctico en nuestras clases de Matemáticas tanto a nivel de bachillerato como a nivel universitario.

Nivel educativo: Bachillerato, Universidad.

1. INTRODUCCIÓN.

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 se juntan varias de estas personas. Por ejemplo, el director de un banco puede interesarle que ningún empleado de la misma posea la clave que abre la caja fuerte. Por el contrario, puede repartir entre 5 empleados, por ejemplo, parte de la información, de forma que para conseguir la clave de la caja fuerte tengan que juntarse al menos 3 de los 5 empleados. Esta idea se conoce como esquema umbral (5,3).

El primer artículo sobre este tema fue publicado en 1976 por A. Shamir, un criptógrafo muy conocido (Shamir, 1976). En su artículo Shamir propone el uso de polinomios para llevar a cabo un esquema umbral para el reparto de un número secreto. Posteriormente se han publicado una gran cantidad de trabajos. Por ejemplo en el artículo de Thien (Thien et al., 2002) explica cómo aplicar el esquema de Shamir para compartir una imagen secreta. En el artículo de Parakh (Parakh, 2011) se propone una variación del método de Shamir.

2. ESQUEMA DE SHAMIR.

La idea es muy sencilla. Supongamos que nos interesa hacer un esquema (6,3). Eso quiere decir que hay 6 participantes y que sólo al juntar al menos a 3 de ellos es posible recuperar el secreto.

Supongamos que la clave secreta es $s=1234$. El distribuidor del secreto escogerá dos números cualesquiera, que indicaremos a_1 y a_2, con los que construirá el polinomio de segundo grado: $P(x)=s+a_1 x+a_2 x^2$

Supongamos que $a_1=166$ y que $a_2=94$, entonces:

$$P(x)=s+a_1 x+a_2 x^2=1234+166x+94x^2$$

Calculamos 6 puntos cualesquiera del polinomio del polinomio, por ejemplo: (1, 1494), (3, 2578), (4, 3402), (6, 5614), (8, 8578), (11, 14434). Estos datos se suelen llamar "sombras" en los esquemas de reparto de secretos..

El distribuidor reparte aleatoriamente estos puntos entre sus seis empleados de confianza. Sólo cuando se junten al menos tres de ellos tendremos datos suficientes para poder construir el polinomio $P(x)$. Una vez construido el polinomio será fácil recuperar el secreto s ya que: $s=P(0)$

Supongamos que al empleado nº 1 se le da el primer punto, al empleado nº 2 el segundo punto, y así en adelante. Como el polinomio desconocido tiene 3 coeficientes a determinar harán falta un mínimo de tres puntos para poder determinarlo. Si se juntan tres o más sí que podrán reconstruir el polinomio.

Por ejemplo, supongamos que se juntan los empleados 2, 5 y 6. El sistema a resolver sería:

$$\left.\begin{array}{l} s+3a_1+9a_2=2578 \\ s+8a_1+64a_2=8578 \\ s+11a_1+121a_2=14434 \end{array}\right\}$$

En el sistema anterior aparece el famoso determinante de Vandermonde:

$$\begin{vmatrix} 1 & a & a^2 \\ 1 & b & b^2 \\ 1 & c & c^2 \end{vmatrix}=(b-a)(c-a)(c-b)=(8-3)(11-3)(11-8)$$

Este determinante es no nulo, por lo tanto, el sistema es compatible determinado y podremos resolverlo, hallando el valor de *s*. La idea de Shamir es sencilla, el secreto se hace coincidir con el término independiente del polinomio y el grado del polinomio depende del número mínimo de empleados que deben juntarse para poder obtenerlo.

Para un esquema (6, 3) como el anterior, el polinomio debía ser de grado 2, para que el polinomio a determinar tenga 3 incógnitas y hagan falta como mínimo 3 puntos para poder determinarlo.

Esta idea se puede aplicar para compartir una imagen secreta, como fue propuesta en Thien (Thien et al., 2002). En este caso el secreto es cada uno de los niveles de gris que componen una imagen digital y el esquema de reparto de secretos anteriormente explicado se aplica a cada uno de los píxeles de la imagen.

3. UN VARIACIÓN DEL ESQUEMA SHAMIR.

Vamos a tratar en esta sección otro esquema de reparto de secretos Parakh, 2011). Es una variación de la idea de Shamir. Explicamos el método con un esquema (4,4).

Supongamos que deseamos compartir varios números secretos s_0, s_1, s_2 y s_3, por ejemplo. Averiguamos el polinomio interpolador que pasa por los puntos $(0, s_0), (1, s_1), (2, s_2), (3, s_3)$ que indicaremos por $P(x)$, que será en este caso un polinomio de grado 3. Evaluamos el polinomio en 4 puntos distintos de la forma:

$$D_1 = P(4), D_2 = P(5), D_3 = P(6), D_4 = P(7)$$

Damos al primer participante el punto $(4, D_1)$, al segundo el punto $(5, D_2)$, etc.

Está claro que cuando se junten los 4 participantes, tendrán cuatro puntos para averiguar el polinomio que pasa por ellos, es decir, el polinomio interpolador $P(x)$. Después bastará con evaluar dicho polinomio en 0, 1, 2 y 3 para obtener los tres números secretos.

La idea se representa en la figura 1. Los primeros 4 puntos sirven para averiguar el polinomio interpolador y los 4 puntos siguientes nos permiten averiguar las 4 sombras.

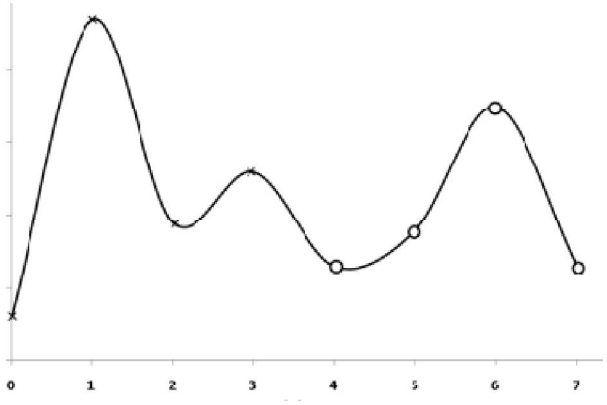

Figura 1. Idea del método

En la figura 2 se muestran algunos de los polinomios que pasan por los tres últimos puntos (es decir, cuando se juntan los tres últimos participantes). En este caso, hay infinitos polinomios interpoladores de grado 3 que pasan por esos tres puntos y seremos incapaces de saber cuál es el verdadero polinomio interpolador y, por lo tanto, no podremos saber los números secretos.

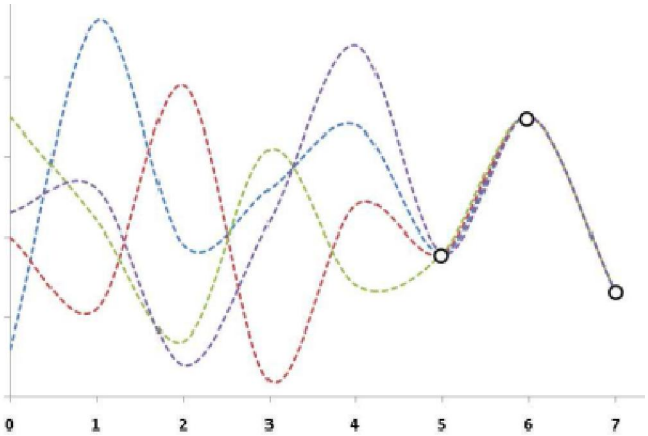

Figura 2. Si se juntan 3 de los participantes

Por ejemplo, si los números secretos fueran 7, 12, 31 y 82. El polinomio interpolador $P(x)$ que pasa por los puntos (0,7), (1,12), (2, 31), (3, 82) sería $P(x)=3x^3-2x^2+4x+7$. Después evaluamos el polinomio en 4, 5, 6 y 7 obteniendo 183, 352, 607 y 966 que serían las sombras de los 4 participantes.

En lo que sigue vamos a presentar una actividad desarrollada con nuestros alumnos en la que el secreto a dividir o repartir es un mensaje secreto.

Supongamos que el mensaje fuera: "BLANCO" y que usamos el siguiente alfabeto compuesto de 31 caracteres (incluye 27 letras, el punto, los símbolos de interrogación y el espacio en blanco indicado por *).

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Q	R	S	T	U	V	W	X	Y	Z	.	¿	?	*
17	18	19	20	21	22	23	24	25	26	27	28	29	30

Vamos a hacer un esquema (4, 3). Cogemos el mensaje en grupos de tres letras. A cada grupo de tres letras se le aplican las ideas anteriores.

- Primeras tres letras "BLA": se corresponden con {1, 11, 0}. Interpolamos por (0, 1), (1, 11), (2, 0) obteniendo el polinomio interpolador y después evaluamos dicho polinomio en 3, 4, 5 y 6 obteniendo -32, -85, -159, -254.
- Siguientes tres letras "NCO": se corresponden con {13, 2, 15}. Interpolamos por (0, 13), (1, 2), (2, 15) obteniendo el polinomio interpolador y después evaluamos dicho polinomio en 3, 4, 5 y 6 obteniendo 52, 113, 198, 307.
- Al participante 1 se le proporcionan los datos {-32, 52}, al participante 2 los datos {-85, 113,}, al participante 3 {-159, 198}, al participante 4 {-254, 307}.

Supongamos que se reúnen los tres primeros participantes, entonces:

- Con los puntos (3, -32), (4, -85), (5, -159) obtienen el polinomio interpolador que después evaluarán en 0, 1 y 2, obteniendo 1, 11, 0 que se corresponden con las letras "BLA".
- Repetirán la acción anterior obteniendo el resto del mensaje "NCO".
- Juntando las dos partes se recuperará el mensaje completo.

Las ideas anteriores se pueden usar a nivel de bachillerato, ya que el problema implica solamente la resolución de sistemas de ecuaciones lineales. Sin embargo, en primer curso de Ingeniería Informática, que es la titulación de nuestros alumnos, se puede hacer un paso más: hacer las cuentas en $\mathbb{C}_{31}$. Ahora las operaciones se realizarán módulo 31. Nuestros alumnos de Álgebra Lineal ya conocen la aritmética modular que han estudiado en la asignatura de Matemática Discreta que cursan simultáneamente a la asignatura de Álgebra Lineal. Por lo tanto, no hay ningún problema en trabajar con congruencias módulo 31 en lugar de trabajar con la aritmética habitual.

El proceso es el mismo que describimos anteriormente sólo que las sombras de los participantes serían:

- Participante 1: {-32, 52} mod 31={30,21}="*U"
- Participante 2: {-85, 113} mod 31={8, 20}="IT"
- Participante 3: {-159, 198} mod 31={27, 12}="•M"
- Participante 4: {-32, 52} mod 31={25,28}="Y¿"

Al trabajar en módulo 31, cualquier número enteros se convertirá en el resto de la división entera de dicho número entre 31, es decir, se convertirá en un número entre 0 y 30 que se puede hacer corresponder con un carácter del alfabeto. De esta forma, las sombras que reciben cada uno de los participantes son mensajes de texto también.

La forma de recuperar el mensaje secreto es idéntica a la forma descrita anteriormente sólo que ahora deberemos trabajar en $\mathbb{Z}_{31}$. Así para recuperar las tres primeras letras del mensaje oculto con los tres primeros participantes deberemos averiguar el polinomio interpolador que pasa por los puntos (3, 30), (4, 8) y (5, 27) trabajando módulo 31.

El polinomio interpolador será: $P(x)=s_0+s_1x+s_2x^2$

$$\left.\begin{array}{l} s_0+3s_1+9s_2=30 \\ s_0+4s_1+16s_2=8 \\ s_0+5s_1+25s_2=27 \end{array}\right\}$$

En el sistema anterior aparece de nuevo el determinante de Vandermonde:

$$\begin{vmatrix} 1 & a & a^2 \\ 1 & b & b^2 \\ 1 & c & c^2 \end{vmatrix} = (b-a)(c-a)(c-b) = (4-3)(5-3)(5-4) = 2$$

Cualquier número no nulo será inversible módulo 31 (ya que 31 es un número primo). De hecho, el inverso de 2 módulo 31 es 16, ya que: $2\times 16 = 32 = 1 \pmod{31}$

Aplicando, por ejemplo, usando el método de Cramer podremos resolver el sistema:

$$s_0 = \frac{\begin{vmatrix} 30 & 3 & 9 \\ 8 & 4 & 16 \\ 27 & 5 & 25 \end{vmatrix}}{\begin{vmatrix} 1 & 3 & 9 \\ 1 & 4 & 16 \\ 1 & 5 & 25 \end{vmatrix}} = \frac{684}{2} = 2^{-1}\ (684) = 16\ (2) = 32 = 1 \pmod{31}$$

$$s_1 = \frac{\begin{vmatrix} 1 & 30 & 9 \\ 1 & 8 & 16 \\ 1 & 27 & 25 \end{vmatrix}}{\begin{vmatrix} 1 & 3 & 9 \\ 1 & 4 & 16 \\ 1 & 5 & 25 \end{vmatrix}} = \frac{-331}{2} = 2^{-1}\ (-331) = 16\ (10) = 160 = 5 \pmod{31}$$

$$s_2 = \frac{\begin{vmatrix} 1 & 3 & 30 \\ 1 & 4 & 8 \\ 1 & 5 & 27 \end{vmatrix}}{\begin{vmatrix} 1 & 3 & 9 \\ 1 & 4 & 16 \\ 1 & 5 & 25 \end{vmatrix}} = \frac{41}{2} = 2^{-1}\,(41) = 16\,(10) = 160 = 5 \pmod{31}$$

Por lo tanto, el polinomio interpolador es:

$P(x) = s_0 + s_1 x + s_2 x^2 = 1 + 5x + 5x^2$

Evaluamos el polinomio para 0, 1 y 2, obteniendo:

- p(0)=1=1 (mod 31) $\Rightarrow$ letra "B"
- p(1)=11=11 (mod 31) $\Rightarrow$ letra "L"
- p(2)=31=0 (mod 31) $\Rightarrow$ letra "A"

Razonando de la misma forma se completa el ejercicio.

Ya para terminar, comentar que en clase de Álgebra Lineal, hemos realizado una actividad algo más complicada: el reparto de una imagen secreta entre varios participantes. Hemos implementado tanto el método de Shamir como el método de Parakh.

REFERENCIAS.

PARAKH, A., SUBHASH, K. (2011). Space efficient secret sharing, Information Sciences, 181(2), 335-341.

SHAMIR, A. (1976). How share a secret, Communications of the ACM, 22 (11), 612-613.

THIEN, C.C., LIN, J.C. (2002) Secret image sharing, Computer and Graphics, 26 (5), 765-770.