Uso didáctico de la criptografía: La administración de secretos

Pino Caballero Gil
Carlos Bruno Castañeda

En este artículo se presenta un protocolo criptográfico para la administración de secretos como base para la enseñanza y aplicación de las matemáticas en enseñanza secundaria. La facilidad de comprensión del problema propuesto lo convierte en un arma eficaz para atraer la atención de los estudiantes en contenidos de difícil aprendizaje como polinomios y sistemas de ecuaciones.

Introducción

En los últimos treinta años el mundo de las matemáticas aplicadas ha vivido el mayor desarrollo de la historia. Las capacidades alcanzadas por los ordenadores han hecho que se aborden problemas de difícil tratamiento por medios clásicos. Además se han planteado nuevos retos. Campos y problemas que las matemáticas tradicionales daban por resueltos han recibido tratamientos (en algunos casos heurísticos) que avivan el ingenio de los científicos y que han servido como base para el desarrollo de nuevas disciplinas.

Por ejemplo la *criptografía* afronta problemas muy diversos y combina, en muchos casos de forma brillante, conceptos de análisis matemático, álgebra y/o geometría, con tecnologías actuales para resolver problemas del mundo desarrollado. La actualidad de los planteamientos criptográficos y la utilización directa de técnicas matemáticas los convierten en candidatos para realizar una mayor investigación en didáctica. Por sus características suponen una excelente cantera para la búsqueda de situaciones problemáticas que permitan la enseñanza de muy diversos tópicos en matemáticas.

Con los ordenadores y la facilidad al acceso de la información, la criptografía ha pasado de ser un campo que únicamente pertenecía a los círculos del poder y de la diplomacia a ser un problema actual y cotidiano en muchas otras esferas. El derecho a la intimidad y el uso promiscuo de informaciones personales la convierten en un campo de especial actualidad.

La palabra *protocolo* se suele utilizar para referirse a las costumbres y normas por las que se rige la formalidad diplomática, tales como la colocación a la mesa o el orden de los discursos. Enlazando su significado habitual con su significado criptográfico, un *protocolo criptográfico* no es más que un conjunto de normas, un algoritmo, para llevar a cabo comunicaciones entre diferentes partes.

El objetivo de un protocolo, al contrario de lo que ocurre en la criptografía más conocida, no se limita al simple hecho de mantener en secreto una determinada información. Así, por ejemplo, un protocolo criptográfico sería aquél donde los comunicantes desean compartir las partes de un secreto, o bien unir sus fuerzas para descubrir un secreto desconocido por cada uno de los participantes por separado. Ambas ideas corresponden a un tipo concreto de protocolo, conocido como *administración de secretos*. Dicho

protocolo se expondrá en un apartado posterior.

Objetivos didácticos

Con este trabajo se pretenden presentar algunos tipos de contenidos matemáticos que se pueden abordar desde el punto de vista de la criptografía. De hecho, el campo de los protocolos criptográficos constituye, por la originalidad de las ideas que se manejan, una herramienta útil para la enseñanza de diversos temas matemáticos. Aquí pretendemos mostrarlo haciendo una propuesta inicial para su desarrollo didáctico.

Este artículo no conforma una unidad didáctica para su desarrollo en el aula, aunque es difícil evitar dejarse tentar por las posibilidades que ofrece. Se puede tratar sobre las comunicaciones en entornos electrónicos y su uso cada vez más sofisticado, sobre el concepto de secreto y su compartimiento, o bien sobre la verificación de la confianza en un mundo cada día menos confiable. Esto nos permitiría captar la atención de los alumnos y poder elaborar un desarrollo didáctico más global. Aquí únicamente se indica dónde afloran los conceptos matemáticos que necesita un protocolo criptográfico susceptible de ser usado como recurso didáctico.

Contenidos

Los contenidos curriculares que se pueden abordar con esta herramienta giran en torno a *los números, naturales y enteros, sus operaciones y el lenguaje algebraico.* De manera facultativa permite introducir temas de creciente interés como la teoría de la información, la criptografía, la probabilidad o la informática.

Los números naturales se utilizan primordialmente para codificar la información alfabética que se desea guardar. Esta codificación puede sustituirse fácilmente por un cifrado permitiendo así abordar desde un primer momento temas propiamente criptográficos.

Los números enteros se utilizan realizando operaciones aritméticas con ellos tales como adición, sustracción, producto, división y potenciación. Utilizar con facilidad la jerarquía y las propiedades de estas operaciones es un objetivo primordial en la enseñanza secundaria. Este uso se lleva a un entorno donde el alumno puede valorar la importancia de su conocimiento. Además, para sacar partido a la potencia del recurso que representan los protocolos criptográficos será necesario, sin duda hacer uso de la calculadora u otros instrumentos de cálculo. De hecho, puede que el alumno se encuentre con problemas de grandes números o de operaciones repetitivas. En ese caso la utilización didáctica de estos instrumentos cobraría una importancia primordial para que el alumno pueda hacer un uso racional de los mismos.

El lenguaje algebraico es un tema siempre difícil de abordar en didáctica. El estudiante se tiene que enfrentar con un lenguaje no natural al que habitualmente se resiste. Mediante el protocolo criptográfico que se propone se plantean ecuaciones y sistemas de ecuaciones útiles por sí mismos como estructura matemática, sin representar problemas de planteamiento. Además se trabaja con polinomios y expresiones literales sencillas. No se requiere, en principio, el uso de operaciones con polinomios pero sí del valor numérico de estas expresiones algebraicas.

El alumno deberá hacer una valoración del lenguaje numérico y algebraico para resolver problemas reales. Podrá apreciar e incorporarse al uso del lenguaje numérico y al cálculo a través de actividades recreativas, permitiéndole alcanzar confianza y una sensibilidad en las propias capacidades para desarrollar actividades de este tipo. Sin duda reconocerá y valorará el uso racional de la calculadora y otros instrumentos para la realización de cálculos numéricos. Podrá captar la importancia de la precisión, el orden y la claridad en la realización de actividades de tipo numérico para alcanzar resultados.

Los contenidos curriculares que usa el protocolo criptográfico que desarrollamos se atienden en la actualidad en los ciclos de *Bachiller* y *Formación Profesional.* Dentro del marco de la *Educación Secundaria,* con esta actividad se logran tratar varios de los que se plantean para las etapas *obligatoria* y *post-obligatoria que la forman.*

Administración de secretos

A continuación realizamos la descripción de los fundamentos del *pro-*

tocolo criptográfico de administración de secretos que vamos a utilizar como herramienta didáctica.

Supongamos que **n** personas que denotamos $\mathbf{A}_i$, i=1,..., n desean compartir un secreto **c** de manera que se cumpla:

a) Cada persona $\mathbf{A}_i$ conocerá alguna información $\mathbf{a}_i$ (parte del secreto) desconocida para el resto del grupo.

b) El secreto **c** podrá obtenerse fácilmente mediante **k** cualesquiera de las informaciones $\mathbf{a}_i$.

c) El conocimiento de **k-1** cualesquiera de las informaciones $\mathbf{a}_i$ no es suficiente para descubrir el secreto **c**.

El conjunto $\{ \mathbf{a}_1, \mathbf{a}_2, ..., \mathbf{a}_n \}$ recibe el nombre de *esquema umbral* para el secreto **c**.

La utilidad de este tipo de esquema se manifiesta en situaciones donde **c** contiene instrucciones para alguna acción crucial de manera que para iniciarla sea necesario el consenso de al menos **k** partes, situaciones que podemos denominar de *quórum*. Por ejemplo, como ocurre en los banco a la hora de abrir la caja fuerte donde es necesaria la presencia simultánea del director y un número fijo de empleados responsables del banco. Este protocolo ha sido ideado para entornos de comunicaciones electrónicas y a distancia. En estas situaciones se desea compartir una información a la que deben acceder las personas adecuadas y en un número previamente fijado. No es posible verificar la presencia física de los comunicantes que intervienen pero sí se hace necesario asegurar de forma inequívoca la condición y el número de los que participan. Así podremos decir que *"No están todos los que son, pero sí son todos los que están"*.

En la práctica para asegurar un reparto equitativo y justo del secreto es necesaria la figura del *administrador de secretos*, ente ajeno al grupo que participa del problema que reparte y coordina el sistema. Es importante señalar que, tal y como se plantea en la criptografía moderna, el sistema de ocultación de la información es público incluso para un posible oponente y que es el sistema el que debe proveerse de su seguridad y de la confidencialidad de la información. Es decir, todos conocen los pasos que el administrador de secretos realiza, éste únicamente protege aquellas partes del proceso que no pueden ser elaboradas en público. Dependiendo de cómo se definan las circunstancias del problema la participación del administrador puede ser protagonista o bien reducirse a unas mínimas ejecuciones.

Existen muy diferentes esquemas matemáticos en los que un objeto queda determinado a partir de **k** elementos de un conjunto, siendo superfluo cualquier otro elemento adicional. Tales ejemplos pueden ser utilizados para la construcción de los esquemas umbral. Nosotros proponemos a continuación los sistemas de ecuaciones, así como los polinomios como herramientas para su construcción.

Aplicación de los polinomios y sistemas de ecuaciones

Consideremos un secreto **c** formado por una secuencia de **k** caracteres $\mathbf{c}_j$, j=1, 2,..., k, del conjunto de 29 símbolos **S** = { @, A, B,..., Z, . } (@ simboliza el espacio en blanco), o sea **c** es una frase secreta de **k** signos. Por sencillez en este planteamiento inicial se toma este número **k** como número de partes necesarias para recuperar el secreto.

En primer lugar es necesario traducir del lenguaje de las letras al de los números para poder operar. Esto se consigue mediante una correspondencia biunívoca **f** de **S** en $\mathbf{Z}_{29}$ (codificación). Por ejemplo la más sencilla que asigna a cada letra el orden que ocupa en el abecedario:

f:	@ → 0	F → 6	L → 12	Q → 18	W → 24
	A → 1	G → 7	M → 13	R → 19	X → 25
	B → 2	H → 8	N → 14	S → 20	Y → 26
	C → 3	I → 9	Ñ → 15	T → 21	Z → 27
	D → 4	J → 10	O → 16	U → 22	• → 28
	E → 5	K → 11	P → 17	V → 23	

Ejemplo: c = " H O L A "
f(c) = 8 16 12 1

Nota: Si el código es secreto, el proceso de codificación se transforma en un proceso de cifrado pues una vez codificado el texto no es susceptible de lectura por aquellos que no conozcan el código. Por tanto, en lugar del código propuesto, se podría trabajar con sistemas criptográficos clásicos como el de César o el de Vigénere.

Se considera cada uno de los enteros asignados a cada letra como coeficient secreto de un polinomio (con los signos alternados por razones de magnitud),

$$P(x) = \sum_{j=0}^{k-1} a_j x^j \text{ con } a_j = (-1)^j \cdot f(c_j).$$

En el ejemplo:
$P(x) = 8 - 16x + 12x^2 - x^3$

Para dividir el secreto en **n** partes se eligen al azar **n** números x_i, i=1,2,..., n, todos distintos y se calculan los valores $P(x_i)$. Ambos valores $(x_i, P(x_i))$ se distribuyen entre las **n** personas participantes del secreto.

En el ejemplo:

$x_1 = 2$ $P(x_1) = 8 - 32 + 48 - 8 = 16$
$x_2 = 4$ $P(x_2) = 8 - 64 + 192 - 64 = 72$
$x_3 = 9$ $P(x_3) = 8 - 144 + 972 - 729 = 107$
$x_4 = 6$ $P(x_4) = 8 - 96 + 432 - 216 = 128$
$x_5 = 3$ $P(x_5) = 8 - 48 + 108 - 27 = 41$

Las partes del secreto son:
(2,16) (4,72) (9,107) (6,128) y (3,41)

Para reconstruir el secreto son suficientes **k** partes cualesquiera puesto que mediante ellas se logra definir un sistema compatible de **k** ecuaciones con **k** incógnitas (los coeficientes a_0, a_1, ..., a_{k-1} del polinomio P(x)). Sin embargo si se reúnen menos de **k** partes, el sistema obtenido es indeterminado y por tanto, dado que tiene infinitas soluciones equiprobables, es imposible descubrir el secreto.

En el ejemplo:
Si se reúnen, A_1, A_2, A_4 y A_5 consiguen el sistema

$(2, 16) \rightarrow a_0 + a_1 2 + a_2 2^2 + a_3 2^3 = 16$
$(4, 72) \rightarrow a_0 + a_1 4 + a_2 4^2 + a_3 4^3 = 72$
$(6,128) \rightarrow a_0 + a_1 6 + a_2 6^2 + a_3 6^3 = 128$
$(3, 41) \rightarrow a_0 + a_1 3 + a_2 3^2 + a_3 3^3 = 41$

de donde resolviéndolo obtienen $a_0=8$, $a_1=-16$, $a_2=12$ y $a_3=-1$. De estos valores deducen $f(c_0)=a_0=8$, $f(c_1)=-a_1=16$, $f(c_2)=a_2=12$, $f(c_3)=-a_3=1$ y finalmente mediante la inversa de la función **f** descubren todas las partes del secreto $c_0=H$, $c_1=0$, $c_2=L$, $c_3=A$.

Algoritmo

Presentamos a continuación el proceso en forma de algoritmo.

Reparto de partes del secreto

Paso 1: Dados los valores en **n** y de **k**, y el secreto **c**, se obtiene f(c).

Paso 2: Se divide f(c) en **k** partes asignándoles signos alternados y denotándolos a_j, j=0,1,...,k-1.

Paso 3: Se generan **n** enteros aleatorios distintos x_i, i=1,2,...,n.

Paso 4: Se calculan para cada i=1,2,...,n.

$$P(x_i) = \sum_{j=0}^{k-1} a_j (x_i)^j$$

Paso 5: Se reparten entre los **n** usuarios las partes del secreto $(x_i, P(x_i))$, i=1,2,...,n.

Obtención del secreto

Paso 6: A partir de **k** partes cualesquiera, sin pérdida de generalidad consideramos $(x_i, P(x_i))$, i=1,2,...,k, se construye el sistema de **k** ecuaciones con **k** incógnitas a_0, a_1,..., a_{k-1}

$$a_0 + a_1 x_1 + a_2 x_1^2 + \ldots + a_{k-1} x_1^{k-1} = P(x_1)$$
$$a_0 + a_1 x_2 + a_2 x_2^2 + \ldots + a_{k-1} x_2^{k-1} = P(x_2)$$
$$\vdots$$
$$a_0 + a_1 x_k + a_2 x_k^2 + \ldots + a_{k-1} x k^{k-1} = P(x_k)$$

Paso 7: Al resolver dicho sistema se obtienen los valores de $(a_0, a_1,\ldots,a_{k-1})$, y al aplicar sobre $(a_0, -a_1, a_2, \ldots)$ f^{-1} se consigue el secreto **c**.

Aplicación en el aula

Para enseñar el mecanismo de la administración de secretos no es necesario disponer de medios excepcionales. Se puede plantear simplemente como un ejemplo del uso de los polinomios y de los sistemas de ecuaciones en la actualidad.

Actividad 1.

Supongamos una clase de 30 alumnos. El profesor escoge un secreto de 30 signos (*por ejemplo, "ESTE MENSAJE SE AUTODESTRUIRÁ"*). Divide la clase en 15 parajes entre las que reparte los pares de caracteres secretos en que se divide el mensaje.

E - S	T - E	@ - M	E - N	S - A
5 - 20	21 - 5	0 - 13	5 - 14	20 - 1
J - E	@ - S	E - @	A - U	T - O
10 - 5	0 - 20	5 - 0	1 - 22	21 - 16
D - E	S - T	R - U	I - R	A - •
4 - 5	20 - 21	19 - 22	9 - 19	1 - 28

Dividiendo el mensaje de dos en dos signos queda asegurado que los sistemas de ecuaciones a resolver por los alumnos serán de dos ecuaciones con dos incógnitas.

Cada uno de los 15 grupos de alumnos se encarga de aplicar la parte del algoritmo correspondiente al reparto de partes del secreto.

Paso 1: Obtienen f(c) (*por ejemplo f(c) = f(E, S) = (5,20)*.

Paso 2: Descubren el polinomio de primer grado P(x) correspondiente (*P(x) = 5 - 20 x*).

Paso 3: Escogen dos dígitos aleatorios distintos x_1 y x_2 (*por ejemplo 2 y 6*).

Paso 4: Calculan el resultado del polinomio para cada dígito obteniendo de esta forma cada grupo dos partes de secreto (x_1, $P(x_1)$) y (x_2, $P(x_2)$) (*P(2) = -35, P(6)=-115,, luego las partes quedan (2, –35) y (6, –115).*

Estas dos partes de cada grupo son intercambiadas entre los grupos para pasar a la segunda parte del algoritmo que es la obtención del secreto.

Paso 5: Construyen el sistema de dos ecuaciones con dos incógnitas a y b,

$a+bx_1=P(x_1)$
$a+bx_2=P(x_2)$

Por ejemplo
$a+2b= -35$
$a+6b= -115$

Paso 6: Resuelven el sistema calculando a y b, y mediante **f** aplicada sobre a y -b descubren el secreto que les corresponde. *(Resolviendo el sistema anterior se obtienen a=5 y b=-20, $f^{-1}(a)=E$, $f^{-1}(-b)=S$, luego el secreto es ES).*

Una vez que todos los grupos han descubierto sus secretos se acaba el juego reuniendo todos y reconstruyendo la frase secreta.

De esta forma se pueden crear pequeñas dificultades que permitan detectar los problemas con respecto a los objetivos curriculares que se hayan planteado con este recurso.

Sin duda si se desea llevar al alumno a reflexionar sobre el uso de los protocolos criptográficos se recomienda disponer de unos pocos medios más. Por ejemplo, proponemos un aula de materias con al menos un ordenador y un conjunto de calculadoras adecuado al número de alumnos.

Actividad 2. (Bosquejo)

Cada uno de los alumnos de la clase realiza una apuesta que se guarda en el ordenador del aula. Dicha apuesta deberá ser verificada algún tiempo después (por ejemplo para apuestas sobre un juego de estrategia o una competición deportiva o una prediccvión meteorológica). Dado que el ordenador está disponible para cualquier usuario, se hace necesario ocultar la información de las apuestas y protegerla de cualquier cambio posterior. Por tanto se decide que la información debe ser cifrada mediante un sistema de clave secreta (por ejemplo el sistema de César o de Vigénere) que pueda ser desarrollado por los miembros de la clase. El profesor o un alumno elegido o un grupo de la clase con respecto a otro o tal vez el azar de un programa informático juega el papel de administrador de secretos. Dicho administrador elige una clave secreta de cifrado y mediante ésta, cifra la información de las apuestas.

La clave es precisamente la información que se reparte mediante el protocolo de administración de secretos. De esa forma sólo la presencia de todos los miembros del grupo o un número cualificado de ellos permite desvelar la clave según el algoritmo descrito y con ello descifrar la información de la apuesta. Si la clave es lo suficientemente larga, en el proceso los alumnos tendrán que resolver sistemas de ecuaciones de mayor tamaño y donde los números que aparecen requerirán del uso de calculadoras.

Conclusiones

La utilización de protocolos criptográficos tales como el de reparto de secretos descrito en este trabajo representa una poderosa fuente de herramientas didácticas para la introducción y enseñanza de diversos tópicos matemáticos que tradicionalmente resultan para el alumnado temas de gran dificultad.

De esta forma, como si se tratara de un juego, los alumnos tienen que aprender su funcionamiento (manejando polinomios y resolviendo ecuaciones) si quieren lograr el objetivo final (descubrir el secreto). Además, para llevarlo a cabo necesitan cooperar y participar en grupo, lo que convierte a esta herramienta en una oportunidad para combinar objetivos didácticos y generales de la ESO.

Bibliografía

* P. CABALLERO GIL: **Criptografía digital: Una introducción matemática.** Memoria de Licenciatura, Jul. 1992.

* R. CARRETERO et al: **Diseño curricular de matemáticas 16-18.** Ed. Consejería de Educación y Ciencia, Sevilla, 1989.

* M. MIGNOTTE: **How to share a secret.** Lecture Notes in Computer Science vol *149* pp. 371-375, Springer Berlin Heidelberg new York, 1983.

* J. PASTOR: **Protocolos y Aplicaciones Criptográficas.** Seminario, jun. 1994.

* A. SALOMAA: **Public-Key Cryptography.** Springer Verlag, 1990.

* A. SGARRO: **Códigos secretos.** Pirámide, 1989.

* A. SHAMIR: **How to share a secret.** Communications of the ACM, vol *122* nº 11, p. 612, 1979.

* J.R. SNOW: **An application of Number theory to Cryptology.** Mathematics teacher, vol *82,* nº 1, Ene. 1989.

Pino Caballero Eril
Carlos Bruno Castañeda
Dto. Estadística e Investigación Operativa y Computación
Univ. de la Laguna (Tenerife)
I.F.P. La Laguna (San Benito).