Revista Digital EducaMadrid

ISSN: 1697-7378

Resultados (/web/revista-digital/inicio?p_p_id=community_content_browser_WAR_cms_tools&p_p_lifecycle=1&p_p_state=maximized&p_p_mode=view&_community_content_browser_WAR_cms_tools_struts_action=%2Fcommunity_content_browser%2Fbrowser)

IES La Serna. Gymkhana matemática. Criptografía

Revista Digital Educamadrid

Fecha de publicación 30 de noviembre de 2017

Experiencias

Nivel. ESO

Resumen

Utilizando diferentes tipos de codificación de mensajes basados en métodos reales que se usaron a lo largo de la historia se trabaja con el alumnado varios enunciados relacionados con los sólidos platónicos. El objetivo de codificar este tipo de mensajes es introducir otra actividad paralela de construcción de poliedros regulares utilizando la papiroflexia u origami.

Autora

Elena Recio Díaz

IES La Serna (Fuenlabrada)

1. INTRODUCCIÓN

La criptografía y la teoría de códigos son muchas veces totalmente desconocidas por nuestros alumnos y, sin embargo, este campo se aplica con mucha frecuencia en la matemática aplicada.

La idea surge como trabajo final del curso ofrecido por el CTIF Madrid-Sur titulado “Estructuras Algebraicas”. En una parte del curso se trabaja la criptografía por lo que parece interesante plantear una actividad relacionada con esta parte de las matemáticas, tan importante y útil en la actualidad, y acercar a los alumnos al mundo de la teoría de códigos.

Se plantea la posibilidad de poner en práctica esta actividad en las jornadas culturales del Centro utilizando el formato de gymkhana matemática que suele resultar atractivo para los alumnos.

La actividad se completa con otra de carácter manipulativo, en la que los alumnos construyen los sólidos platónicos mediante la papiroflexia u origami. Ambas actividades se complementan al implementar en los mensajes cifrados información sobre los poliedros regulares.

2. OBJETIVOS GENERALES

- Dar a conocer la teoría de códigos en el aula.
- Utilizar diferentes estrategias para descifrar mensajes encriptados.
- Trabajar en equipo fomentando así el aprendizaje cooperativo.
- Reconocer las características y propiedades de los poliedros regulares.
- Aprender a operar utilizando la aritmética modular.
- Recorrer diferentes momentos históricos apoyados en la necesidad de ocultar mensajes en conflictos bélicos hasta llegar a la seguridad actual en Internet.

3. DESARROLLO DE LA EXPERIENCIA

3. 1. Contextualización

La experiencia se llevó a cabo el jueves 21 de abril de 2016 durante las jornadas culturales que cada año organiza el IES La Serna de Fuenlabrada.

Durante cuatro sesiones diferentes, de unos 50 minutos cada una fueron participando en la experiencia un total de 78 alumnos de 3º y 4º ESO. Se hicieron grupos de 2, 3 o 4 alumnos a los que se les repartió una hoja de respuestas y la hoja de enunciados que se incluye a continuación.

Los alumnos comenzaron a resolver las pruebas rápidamente y prácticamente sin ayuda complementaria por parte de los docentes que acompañaban la actividad. Se comprobaba cada una de las respuestas y los alumnos avanzaban en la consecución de las pruebas.

Con un ambiente de absoluto trabajo y compañerismo se desarrollaron las cuatro sesiones en un clima distendido y cooperativo.

3. 2. La actividad

GYMKHANA MATEMÁTICA. CRIPTOGRAFÍA

LA ESCÍTALA

El pueblo espartano (Grecia sVI al SIV a.C. aprox.) utilizó este sistema de codificación para enviar mensajes secretos.

En un bastón se enrolla una tira, generalmente de cuero. El mensaje se escribe en la tira a lo largo del bastón junto con otro texto de relleno si es necesario. Luego se envía la cinta de cuero al receptor. Para descifrar el mensaje hay que volver a enrollar la tira en un bastón con las mismas características.

PRUEBA 1. ¿Qué quiere decir este espartano en su mensaje?

EDOERCRGLRLGMUAUTOIUAASLEEELDTTATSDAORRRRURRPOIEANOFOCASEPRORANS

Nota: Puede ayudarte construir una tabla de 8X8

CRIPTOSISTEMA DE CÉSAR

Julio César utilizó este sistema para encriptar los mensajes importantes de contenido militar. Encripta utilizando un desplazamiento de tres espacios.

PRUEBA 2. ¿Qué les enseñaba César a sus súbditos?

BIZRYLBPRKMLIFBAOLCLOJXALMLOPBFPZXOXPZRXAOXAXP

Nota: Puede ayudarte para descifrarlo la siguiente tabla.

Mensaje en claro	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Mensaje cifrado	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

POLYBIUS (S II a.C)

Este método de cifrado consiste en sustituir cada letra por sus “coordenadas”.

PRUEBA 3. ¿Puedes averiguar el mensaje de Polybius?

51 13 43 31 44 11 51 41 24 43 44 42 51 33 51 43 31 32 43 31 11 24 11 34 44 24 42 11 33 22 54 13 11 24 51 34

Nota: Puede ayudarte a descifrar el mensaje esta tabla de doble entrada.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I,J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

CÓDIGO VIGENÈRE

Se trata de un criptosistema simétrico, es decir, utiliza la misma clave para cifrar y descifrar.

Está basado en el Criptosistema de César pero incluye la dificultad de una palabra clave que hace que la decodificación de una misma letra pueda ser diferente según el lugar que ocupe en el mensaje.

Vamos a estudiar este método en dos partes. La primera, que llamaremos codificación Vigenère inicial consistirá en asociar un número a cada letra y encriptar el mensaje utilizando este código.

PRUEBA 4. Vigenère inicial

Descifra el siguiente mensaje en el que hemos utilizado como sistema de cifrado el método que hemos denominado “Vigènere inicial” en el que cada letra ha sido sustituida por un número.

5 12 4 15 4 5 3 1 5 4 18 15 5 19 21 14 16 15 12 9 5 4 18 15 6 15 18 13 1 4 15 16 15 18 4 15 3 5 3 1 18 1 19 16 5 14 20 1 7 15 14 1 12 5 19

Nota: Puede ayudarte a descifrar el mensaje la siguiente tabla.

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

Una vez que hemos entendido esta simplificación del código Vigènere nos será más fácil codificar y descodificar utilizando el código Vigènere.

En éste último debemos utilizar una palabra clave que añadiremos a nuestro mensaje y que nos servirá para introducir diferentes codificaciones para la misma letra. Esta palabra clave también se traduce numéricamente y se suma (módulo 26) a la codificación de Vigenère inicial.

PRUEBA 5. Código Vigenère.

24 17 1 17 16 12 6 23 18 19 8 25 1 19 15 24 1 23 23 15 13 10 21 15 19 20 24 12 6 10 20 19 25 9 13 20 23 23 7

Nota: La palabra clave que hemos utilizado es SERNA. Sobreescribe la clave al mensaje y resta la codificación de esta clave. Para decodificar el mensaje resultante utiliza Vigenère inicial. (No olvides que el número máximo es 26. El número 27 es aquí el 1, el 28 el 2…A los números negativos debes sumarles 26 para entrar en el rango de posibles valores)

3. 3. Soluciones de la gymkhana

PRUEBA 1. ¿Qué quiere decir este espartano en su mensaje?

E	D	0	E	R	C	R	G
L	R	L	G	M	U	A	U
T	O	I	U	A	A	S	L
E	E	E	L	D	T	T	A
T	S	D	A	O	R	R	R
R	U	R	R	P	O	I	E
A	N	O	F	O	C	A	S
E	P	R	O	R	A	N	S

Colocando las letras en la matriz que damos como ayuda y leyendo el mensaje en vertical podemos leer: “El tetraedro es un poliedro regular formado por cuatro caras triangulares”.

PRUEBA 2. ¿Qué les enseñaba César a sus súbditos?

Utilizando la tabla de decodificación que consiste en asignar a cada letra la que se encuentra tres posiciones a su derecha conseguimos averiguar que César les decía a sus súbditos:” El cubo es un poliedro formado por seis caras cuadradas”.

PRUEBA 3. ¿Puedes averiguar el mensaje de Polybius?

Para descifrar este mensaje jugamos a “los barquitos”. Cada letra se codifica utilizando sus coordenadas en la tabla de doble entrada que podemos dar como ayuda. Las letras I, J tienen la misma codificación pero podemos descartar una u otra por el contexto.

Así el mensaje escondido es” El octaedro tiene ocho caras triangulares”

PRUEBA 4. Vigenère inicial.

Realmente este código no existió como tal pero me ha parecido que podía ayudar este sistema fácil para poder entender el código Vigenère que directamente les podría parecer más difícil. Simplemente hemos sustituido cada

letra del abecedario por un número empezando por el 1.

El mensaje es:” El dodecaedro es un poliedro formado por doce caras pentagonales”

PRUEBA 5. Código Vigenère.

La decodificación de este mensaje consta de varios pasos.

1. Insertamos la clave al mensaje encriptado:

24	17		1	17	16	12	6	23	18	19	8		25	1	19	15	24
S	E		R	N	A	S	E	R	N	A	S		E	R	N	A	S

1	23	23	15	13	10		21	15	19	20	24
E	R	N	A	S	E		R	N	A	S	E

12	6	10	20	19	25	9	13	20	23	23	7
R	N	A	S	E	R	N	A	S	E	R	N

2. Traducimos las letras de la palabra clave por el número correspondiente y se lo restamos (módulo 26) al número codificado.

24	17		1	17	16	12	6	23	18	19	8		25	1	19	15	24
S	E		R	N	A	S	E	R	N	A	S		E	R	N	A	S
19	5		18	14	1	19	5	18	14	1	19		5	18	14	1	19

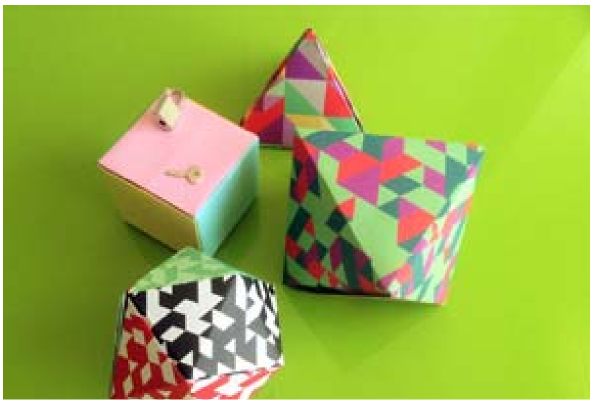
1	23	23	15	13	10		21	15	19	20	24
E	R	N	A	S	E		R	N	A	S	E
5	18	14	1	19	5		18	14	1	19	5

12	6	10	20	19	25	9	13	20	23	23	9
R	N	A	S	E	R	N	A	S	E	R	N
18	14	1	19	5	18	14	1	19	5	18	14

3. Al restar el mensaje que obtenemos es:

5 12 9 3 15 19 1 5 4 18 15 20 9 5 14 5 22 5 9 14 20 5 3 1 18 1 19 20 18 9 1 14 7 21 12 1 18 5 19

4. Utilizando la decodificación que he denominado Vigenère inicial obtenemos el mensaje: “El icosaedro tiene veinte caras triangulares”



4. METODOLOGÍA

- Aprendizaje cooperativo: los alumnos trabajan en equipo fomentando de esta forma el aprendizaje cooperativo.
- Aprender a aprender: la estructura de las actividades en orden creciente de dificultad y con una ayuda en cada una de ellas favorece la consecución de esta competencia. Tanto el nivel de dificultad paulatinamente más complejo como las notas que ayudan a la resolución de los enigmas hacen que los alumnos necesiten poco apoyo del profesor.
- Transversalidad en los contenidos: se pretende acercar con esta actividad a los alumnos a distintas áreas de conocimiento. En matemáticas trabajaremos la aritmética modular, la geometría y la resolución de problemas pero también nos acercamos a la historia de diferentes civilizaciones.

5. EVALUACIÓN

Al tratarse de una actividad englobada en las Jornadas Culturales del Centro se trata de dar un carácter lúdico a la participación del alumnado por lo que la evaluación consiste en premiar al equipo que concluya correctamente las cinco pruebas en el menor tiempo posible.

En cada una de las cuatro sesiones se premia por tanto a uno de los grupos que colaboran entre ellos para conseguir descifrar los enigmas.

6. CONCLUSIONES

La actividad ha sido muy bien recibida por los alumnos, de hecho nos sorprendió la rapidez con la que entendieron el ejercicio y la motivación que surgió en ellos desde el comienzo.

La estructura de gymkhana y la posibilidad de trabajar en equipo ayudaron sin duda a que los alumnos participaran activamente en la actividad.

Desde el departamento de matemáticas se piensa ampliar en cursos sucesivos este tipo de actividad con actividades complementarias como la visualización de la película “The Imitation Game” y también se valora la posibilidad de efectuar cambios en los mensajes encriptados interactuando con otros departamentos didácticos.

BIBLIOGRAFÍA

Singh, S. (1999). *Los códigos secretos*. Madrid. Debate.

Benito Sualdea, A. (2016) La necesidad de cifrar la información: teoría de códigos y criptografía. Ponencia presentada en el *Curso Estructuras Algebraicas* del CTIF Madrid Sur.

Departamento de matemáticas del IES Alameda de Osuna. *Criptografía*. https://sites.google.com/site/deptmatiesao/actividades/criptografia

Fecha de publicación: 30 de noviembre de 2017