Experiencias Docentes

Iniciación a la Criptología: una actividad extracurricular transversal

Introduction to Cryptology: a transverse extracurricular activity

José Manuel Sánchez Muñoz

Revista de Investigación

Volumen IX, Número 2, pp. 015–022, ISSN 2174-0410
Recepción: 15 Abr'18; Aceptación: 20 Jun'19

1 de octubre de 2019

Resumen

En este trabajo se presenta una experiencia extracurricular llevada a cabo en el I.E.S. Jaranda de Jarandilla de la Vera (Cáceres) donde se hace una exposición de una actividad de iniciación del alumnado a la encriptación y desencriptación de mensajes. La experiencia pone de manifiesto la importancia de la transversabilidad como herramienta metodológica de contenidos de distintas áreas pedagógicas, sin por ello menoscabar su atractivo para un alumnado completamente profano.

Palabras Clave: Criptología, cifrado de mensajes, desencriptación, transversabilidad, pedagogía extracurricular.

Abstract

This work presents an extracurricular experience carried out in Jaranda High School (Jarandilla de la Vera - Cáceres) where an exhibition of an activity of initiation of students to the encryption and decryption of messages is made. The experience highlights the importance of transversability as a methodological tool for content from different pedagogical areas, without undermining its appeal to a completely profane student body.

Keywords: Cryptology, encryption of messages, decryption, transversability, extracurricular pedagogy.

1. Antecedentes

La idea de trabajar de forma transversal e interdisciplinar distintos contenidos enmarcados dentro del curriculo es uno de los principales objetivos a los que los docentes nos enfrentamos todos los días en nuestras tareas cotidianas y el trabajo con nuestros alumnos.

Sin embargo uno de los grandes retos con los que debemos lidiar consiste en intentar mostrar a nuestros alumnos que en la vida real el conocimiento no es algo estanco y que, al contrario de lo que su intuición les hace creer, la asunción de retos y la superación de problemas aparentemente infranqueables a primera vista, tiene que ver con distintas areas para las que se preparan durante toda la secundaria.

De este modo y con la iniciativa de algunos profesores del claustro del I.E.S. Jaranda se preparó una actividad con la idea de poner de manifiesto la importancia de la transversabilidad, pensando en trabajar en distintos objetivos interdisciplinares no sólo pedagógicos, sino con la intención de mejorar el trabajo en equipo y la competitividad sana como herramienta de superación y satisfacción personal.

La iniciación a la criptología, esto es, la encriptación y desencriptación de mensajes, fue el hilo conductor que sirvió para que profesores de distintas áreas (Lengua, Inglés, Matemáticas, Orientación . . .) trabajaran de manera conjunta en la elaboración de esta actividad con la idea de conseguir en primer lugar que resultara a todas luces atractiva para el alumnado participante, y en segundo lugar se pudieran trabajar con ellos ciertos aspectos curriculares aparentemente lejanos para ellos de su cotidianidad con la que se enfrentan en el centro educativo.

2. Aspectos metodológicos

A pesar de que la actividad está diseñada desde un punto de vista completamente extracurricular, no por ello deja de trabajar ciertos aspectos curriculares que pueden resultar absolutamente aprovechables. De esta manera su diseño se realizó de un modo completamente coordinado entre todos los profesores de las distintas areas que participaron.

2.1. Descripción y fundamentos básicos

La actividad reúne un conjunto de técnicas y dinámicas que permiten a los alumnos desarrollar capacidades de comunicación, coordinación y trabajo en equipo, desarrollo ligüístico y científico y conocimiento histórico así como poner en práctica sus ideas creativas y aprendizaje racional mediante la desencriptación de mensajes cifrados.

Con la realización de la actividad planteada, el alumnado percibe la importancia de la interactuación de distintas areas del conocimiento, esto es la interdisciplinariedad, haciendo uso de técnicas metodológicas alternativas (análisis estadístico o comprensión ligüística) que contribuyen a su desarrollo cognitivo a la hora de enfrentarse con problemas, mejorando de este modo aspectos personales como la seguridad en uno mismo, autocontrol, trabajo en equipo, expresión oral en público, cálculo racional, etc.

"Iniciación a la Criptología: una actividad extracurricular transversal", pretende favorecer la mejora y el desarrollo de diferentes capacidades y habilidades que intervienen en la formación del alumno, contribuyendo en gran medida a una mejora del cálculo racional, trabajo en equipo, conocimiento del contexto histórico en el que se ambienta dicha actividad o desarrollo lingüístico. La metodología aplicada es indudablemente participativa, fomentando la cooperación y el trabajo en equipo, y estimulando la reflexión sobre la actividad, convirtiéndose así en un vehículo extraordinario para transmitir valores de tolerancia, respeto, solidaridad y crítica.

2.2. Definición de bloques de contenidos

1. *Area Orientación educativa:* apoyo al proceso de enseñanza - aprendizaje.

2. *Area Lingüística:* conocimiento y uso de las técnicas y estrategias para la producción de textos escritos, reconocimiento y uso de los elementos constitutivos de la palabra, la creación y valoración de textos.

3. *Area Geografía e Historia:* cifrado César, personajes históricos de la 2ª Guerra Mundial, entorno geográfico del Canal de la Mancha, desembarco de Normandía, invasión de europa ocupada nazi por los aliados, inteligencia británica y desencriptado de las comunicaciones nazis.

4. *Area Matemática:* matemática modular, obtención de porcentajes, presentación de resultados mediante un gráfico de barras o tabla de frecuencias.

2.3. Definición de objetivos o metas

1. Estimular el desarrollo de las capacidades cognitivas y simbólicas a traves del cálculo racional.

2. Conocer el mecanismo de encriptación de un mensaje con un cifrado César.

3. Conocer el mecanismo de desencriptado mediante el análisis de una tabla de frecuencias.

4. Estimular, favorecer y potenciar el conocimiento histórico del conflicto bélico de la 2ª Guerra Mundial.

3. Contextualización

3.1. Entorno histórico

La actividad se contextualiza en Mayo de 1944, un mes antes del desembarco de Normandía por el bando aliado. En la 2ª Guerra Mundial, la guerra criptográfica se convirtió en una de las herramientas de inteligencia y espionaje más potentes y efectivas. Las comunicaciones se realizaban a través de mensajes de radio encriptados. Los aliados podian captar estas comunicaciones con potentes antenas situadas en la costa británica, aunque éstas resultaban completamente ilegibles si no se conocía el método de desencriptado.

El cuartel general de la inteligencia británica para la lucha criptológica se situaba en la mansión victoriana de Bletchley Park, relativamente cerca de Londres, donde en su apogeo llegaron a trabajar cerca de 10.000 personas.

En Mayo de 1944 los aliados preparaban el desembarco para la invasión de la Europa ocupada nazi de un contingente de tropas a través del Canal de la Mancha, y comenzar a arrinconar al ejercito nazi para lograr la capitulación del alto mando alemán. Hitler conocía estos planes pero desconocía exactamente el lugar por el que lo harían. Hitler, desobedeciendo las recomendaciones de generales de su alto mando como Rommel, apostó que dicha invasión aliada se produciría desde las playas de Dover a través del paso de Calais, situado unas millas más al norte de donde se produjo realmente en las playas de Normandía, dado que la distancia a las playas francesas era mucho más corta.

En la 2ª Guerra Mundial la mayoría de las comunicaciones se producían por radio, de manera que cualquiera que tuviera una antera de recepción podía captar dichas transmisiones. Los británicos captaban estas comunicaciones cifradas desde las islas unas veces o desde centros de resistencia y espionaje en la europa ocupada otras, y en Bletchley Park se trabajaba en el descifrado de dichos mensajes interceptados.

3.2. Cifrado César

Se trata de un sistema de encriptación monoalfabético de desplazamiento muy antiguo, utilizado por los romanos en sus campañas militares, de ahí su nombre. El método de cifrado consiste en desplazar hacia la derecha el alfabeto tantos lugares como indica la denominada *semilla*. De esta manera, si la semilla es 4, la letra A se convierte en la letra E. En inglés se utiliza un alfabeto de 26 caracteres (evitando así el uso de la Ñ).

En realidad el método de encriptación utilizado por el ejército nazi (wehrmacht) era polialfabético realizado mediante unas máquinas muy potentes de escriptación denominadas ENIGMA. Además el alto mando mando alemán utilizaba otro sistema de encriptación de sus mensajes realizado con otras máquinas de cifrado denominadas LORENZ. Lógicamente el método de desencriptación de estas máquinas necesita de un álgebra abstracta muy potente que se sale del carácter pedagógico que se le quiere dar a la actividad, por eso al diseñar la actividad nos tomamos la licencia de "engañar" al alumnado con el fin de facilitar la misma.

El método de desencriptado de este cifrado consiste en identificar la semilla, esto es comparar el porcentaje de repetición de varios caracteres y con ello ver el número de posiciones que se desplazó cada caracter del alfabeto.

Figura 1. Algunas diapositivas de la presentación.

3.3. Descripción de la actividad

La actividad se realizó con alumnos de 2º y 1º de Bachillerato, 4º y 3º de ESO (14–17 años). Según entraban por la puerta se les entregaba una carta personal e intransferible donde se les exponía el contexto histórico y geográfico en el que se encontraban. Se convertirán por un instante en miembros de la inteligencia británica en la lucha criptológica contra los nazis. Se les entregaba una carta en el que se exponía el contexto histórico y la finalidad del trabajo que deben realizar durante la actividad. Como curiosidad su carta está firmada por el mismísimo Primer Ministro Wiston Churchil.

"Londres, 15 de Mayo de 1944

Estimados soldados,

Están a punto de embarcarse en una aventura en vivo. Olviden su origen y mantengan en secreto la operación de la que van a ser partícipes. En cuanto lean este documento se convertirán en miembros activos de la inteligencia aliada en su lucha contra el Reich Alemán de Adolf Hitler.

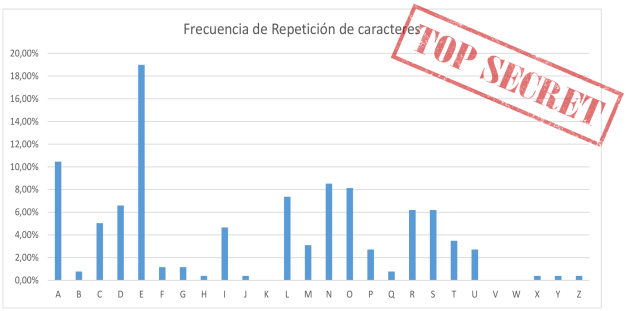
Están en Bletchley Park, una mansión victoriana del siglo XIX a las afueras de Londres, y sede de la Central de Inteligencia y Comunicaciones contra mensajes cifrados nazis alemanes. El bando aliado al que pertenecen, está preparando el desembarco de un contingente de tropas en Francia en una operación militar denominada Overlord, en el que nos jugamos la subsistencia del mundo libre que hoy conocemos. Para ello es fundamental conocer los planes nazis sobre nuestra operación, en qué fechas suponen dicho desembarco y lo más importante, dónde esperan que se produzca.

Recibirán adiestramiento criptoanalítico de una de nuestras mayores emiencias en el tema, el matemático Alan Turing, que les hará un pequeño esbozo de en qué consistirá su tarea de hoy, y cómo podrán descrifrar los mensajes cifrados nazis, y lo que es más importante, cuáles son los planes alemanes para contrarestar dicho desembarco.

Recuerden que deberán trabajar codo con codo con su compañero, en la complicada tarea de descifrar los mensajes cifrados interceptados por nuestras antenas de comunicaciones. Cuando tengan descifrado el mensaje pónganse en contacto con su instructor el Sr. Turing o cualquiera de sus colaboradores de Bletchley Parck. Tendrán que afinar su ingenio y seguir en todo momento las instrucciones definidas por su instructor, y comunicar las fechas para cuando los alemanes esperan nuestra maniobra de desembarco, y en qué puerto geográfico esperan que se produzca. De su trabajo depende que seamos capaces de engañar al bando enemigo y por lo tanto que la Operación Overlord pueda ser un éxito y podamos vencer al ejercito alemán.

Atentamente reciban un cordial saludo.

Primer Ministro del Reino Unido Wiston Churchil"



Texto cifrado interceptado:

```
TAQP CSDT CTBX VDEG TEPG PTAS THTB QPGR DSTJ CRDC
IXCV TCIT STBP HSTR XTCI DHTH TCIP BXAH DASP SDHT
CAPH EAPN PHST ACDG ITST UGPC RXPT CTAT CIDG CDST
ARPC PAST HRDC DRTB DHTA AJVP GTMP RIDT CTAF JTAD
GTPA XOPG PCET GDRG TTBD HFJT EJTS THTG TAEJ TGID
UGPC RTHS TRPA PXHA PUTR WPTH IXBP SPED SGXP HTGP
AXCX RXDS TABT HSTY JCXD
```

Figura 2. Tabla de frecuencias y mensaje cifrado.

A continuación se expuso una presentación donde se ponía de manifiesto el contexto histórico en el que se encontraban los participantes en la actividad, en qué consistía la encriptación mediante un cifrado César, como se realizaba la desencriptación mediante una comparativa con un patrón de una tabla de frecuencias, y finalmente la exposición del mensaje cifrado y la tabla de frecuencias en texto plano del mensaje interceptado.

Figura 3. Imágenes tomadas durante la realización de la actividad.

Al final varios grupos de alumnos consiguieron descifrar de forma exitosa el mensaje cifrado, que tenía una semilla 15. Identificada la semilla, lo único que tenían que hacer era desplazar hacia la izquierda tantos lugares como indicaba la semilla, de este modo por ejemplo la letra T en el mensaje cifrado se correspondía con la letra E en el texto plano o descifrado. La correspondencia es lógicamente biunívoca, no habiendo ninguna posibilidad de ambigüedad. El mensaje descifrado decía lo siguiente:

> *"El bando enemigo prepara el desembarco de un contingente de más de ciento sesenta mil soldados en las playas del norte de Francia en el entorno del Canal Desconocemos el lugar exacto en el que lo realizarán pero creemos que puede ser el puerto francés de Calais la fecha estimada podría ser al inicio del mes de junio."*

El mensaje en texto plano carecía de acentos, no olvide el lector que los alumnos estaban utilizando un alfabeto inglés de veintiséis caracteres.

4. Conclusiones

1. Cuando nuestro alumnado corre peligro de abandono del sistema convencional de aprendizaje, es el momento de que nosotros como docentes tengamos la responsabilidad de intentar atraerlos hacia el conocimiento y la formación: la motivación es una herramienta muy potente.

2. La transversalidad y la interdisciplinaridad permiten la contextualización de las actividades de aprendizaje. Si esa contextualización nos conduce de paso a una problemática actual y cercana (geográfica o virtualmente) y nos permite intervenir en ese contexto, estaremos motivando aún más a nuestro alumnado.

3. Los tiempos modernos que corren y la sociedad actual demandan necesariamente una escuela diferenciadora, donde las capacidades que han de desarrollar los alumnos no son las que de manera tradicional se han contemplado en nuestras programaciones curriculares. El currículo tiene, efectivamente, objetivos, contenidos, y otra serie de elementos que algunos consideramos obligaciones que nos coartan e impiden "hacer de otra forma", sin embargo, también contempla competencias clave o, si queremos, capacidades que han de desarrollarse, elementos transversales, indicaciones metodológicas, atención a la diversidad, que en definitiva es atender a la individualidad, pues todos somos iguales en derechos y diversos en naturaleza, intereses, destrezas. Ceñirse a los "contenidos" del currículo dejando al margen otros elementos igualmente prescriptivos es una decisión profesional, desacertada a mi juicio, que servirá para perpetuar el fracaso educativo.

4. Cabe destacar la buena aceptación por parte de docentes y alumnos que consideraron la realización de la actividad un recurso metodológico alternativo e innovador completamente aprovechable incluso desde un punto de vista curricular, aspecto a todas luces importante para la mejora de la enseñanza de algunos contenidos curriculares en el centro. No obstante, la actitud de docentes y alumnos con respecto a los objetivos planteados en la actividad con relación a la asimilación de contenidos transversales de varias disciplinas y la aplicabilidad de los mismos en el aula de clase, pusieron de manifiesto la utilidad de la actividad.

5. La actividad se plantea como totalmente replicable en multitud de niveles de secundaria y bachillerato, planteándose incluso la posibilidad de ampliarla a varias sesiones con la intención de utilizar métodos de cifrado polialfabéticos y trabajar con este pretesto la transversabilidad en el aula. Por ejemplo con mensajes cifrados en inglés en lugar de en castellano.

6. Es evidente que los alumnos reciben este tipo de actividades alternativas de un modo muy positivo y con una predisposición completamente distinta a la que realizan con las actividades curriculares cotidianas.

Referencias

[1] SÁNCHEZ MUÑOZ, José Manuel, *"Criptología Nazi. Los Códigos Secretos de Hitler"*, Revista Pensamiento Matemático, Vol. III, Nº 1, § Historias de Matemáticas, pp. 059–120, abril, 2013, ISSN 2174–0410, G.I.E. Pensamiento Matemático, Universidad Politécnica de Madrid, España.

[2] DECRETO 98/2016, de 5 de julio, por el que se establecen la ordenación y el currículo de la Educación Secundaria Obligatoria y del Bachillerato para la Comunidad Autónoma de Extremadura, DOE, Miércoles, 6 de julio, 2016.

[3] RIBERA, Anje, *"El día del mayor engaño"*, Diario El Correo, § Culturas, Historia, Martes, 7 de junio, 2016.

Sobre el autor:
Nombre: José Manuel Sánchez Muñoz
Correo electrónico: jmanuel.sanchez@educarex.es
Instituciones: I.E.S. Jaranda, Jarandilla de la Vera, Cáceres. G.I.E. Pensamiento Matemático, Universidad Politécnica de Madrid, España.