

Criptografía: un tema de interés en el currículo de matemáticas de secundaria

Cryptography: a Theme of Interest in the High School Mathematics Curriculum

CLARISSA DE ASSIS OLGIN
Universidade Luterana do Brasil
clarissa_olgin@yahoo.com.br
orcid.org/0000-0001-5560-9276

Resumen: Este artículo discute la importancia de desarrollar el trabajo con temas a lo largo del Currículo de Matemáticas de Enseñanza Media, presentando el tema Criptografía como una posibilidad didáctica para explorar un conjunto de situaciones problema que involucran contenidos matemáticos. La elección del tema Criptografía se debió a su relevancia, ya que se utiliza en diferentes situaciones de la vida moderna, ya sea en auditorías electrónicas, autenticación de pagos electrónicos, transacciones financieras digitales, seguridad de datos digitales confidenciales, entre otros. De esta forma, el objetivo es presentar el tema Criptografía como generador de situaciones didácticas aplicables en el currículo de Matemáticas, posibilitando la revisión y profundización de la comprensión de los conceptos matemáticos. Como resultado de la investigación realizada, se presenta un conjunto de actividades que exploran el tema y sus aplicaciones, así como actividades didácticas para introducir, ejercitar, repasar y profundizar los contenidos de aritmética, funciones y matrices.

Palabras clave: Temas de interés, criptografía, escuela secundaria, contenidos matemáticos.

Abstract: This paper discusses the importance of developing work with themes throughout the High School Mathematics Curriculum, presenting the topic Cryptography as a didactic possibility to explore a set of problem situations involving mathematical contents. The choice of the topic Cryptography was due to its relevance, since it is used in different situations of modern life, whether in electronic audits, electronic payment authentication, digital financial transactions, security of confidential digital data, among others. In this way, the objective is to present the topic Cryptography as a generator of didactic situations applicable in the Mathematics curriculum, enabling the review and deepening of the understanding of mathematical concepts. As a result of the research carried out, a set of activities is presented that explore the theme and its applications, as well as didactic activities to introduce, exercise, review and deepen the contents of arithmetic, functions and matrices.

Keywords: Themes of interest, cryptography, high school, mathematical contents.

1. Introducción

Este artículo busca discutir la pertinencia de trabajar con temas del Currículo de Matemática, que posibiliten el desarrollo de contenidos matemáticos, en la Enseñanza Media, de forma contextualizada y que la formación de los estudiantes esté enfocada al ejercicio de la ciudadanía. Asimismo, investigaciones brasileñas en el área de Educación indican que el desarrollo de contenidos ocurre de forma fraccionada, descontextualizada y dissociada de la realidad. Para cambiar este escenario, Silva (2009) argumenta que la disciplina de Matemática necesita favorecer el trabajo con contenidos matemáticos

para que no se desvinculen de otras áreas del conocimiento, en la actualidad y necesitan ser importantes para la vida y formación de los estudiantes, así como deben estar relacionados con las Matemáticas mismas, con su historia y aplicaciones y con la vida en sociedad.

Teniendo en cuenta los aspectos antes mencionados, esta investigación se justifica por la importancia que tiene el docente de Matemáticas de buscar diversos recursos didácticos y metodológicos para el desarrollo del proceso de enseñanza y aprendizaje y que puedan ser aplicados en las clases de Matemáticas (Groenwald & Franke, 2007), buscando desarrollar en los estudiantes habilidades y destrezas que les ayuden a resolver problemas, saber comunicarse, trabajar en equipo, tomar decisiones, crear estrategias para la resolución de problemas matemáticos y su vida cotidiana.

En este sentido, se cree que al desarrollar contenidos matemáticos mediante temas de interés para la vida en sociedad y que tengan conexiones entre los contenidos aprendidos en el aula y el mundo en que viven, será posible formar estudiantes que sepan vivir en sociedad, preparados para el mercado laboral y para estudios superiores (Olgin, 2011, 2015).

Así, este artículo destaca la importancia de desarrollar y utilizar actividades didácticas adaptadas y adecuadas a la realidad de los estudiantes y que les permitan resolver problemas, tener autonomía en el proceso de resolución y puedan verificar sus hipótesis y trabajar en grupo. Por tanto, el objetivo de este trabajo es presentar el tema Criptografía como generador de situaciones didácticas aplicables en el currículo de Matemáticas de Enseñanza Media, posibilitando la revisión y profundización de la comprensión de los conceptos matemáticos y su uso en situaciones problema.

2. Temas en el Currículo de Matemáticas en la escuela secundaria

Según Olgin (2015), es necesario desarrollar contenidos matemáticos por medio del trabajo con diferentes temáticas, que permitan contemplar, en el currículo escolar, una educación para la ciudadanía crítica, transformadora y contextualizada, que permita a los estudiantes involucrarse en cada materia de manera diferente para repasar, profundizar, ejercitar y estudiar los contenidos escolares, especialmente las matemáticas.

Según Selbach (2010), los estudiantes construyen su conocimiento cuando atribuyen significado a lo que se enseña. Así, un posible camino para el proceso de enseñanza y aprendizaje de contenidos matemáticos es señalado por Olgin (2015), cuando presenta el trabajo mediante temas de interés, ya que tal estudio se refiere a la necesidad de desarrollar conocimientos para posibilitar la participación de los estudiantes en una lista de materias que les permitan interactuar tanto con contenidos matemáticos como con diferentes contextos, de modo que puedan observar su aplicabilidad en la vida en sociedad.

El autor toma como referencia para la selección de posibles temas a abordar a lo largo del Currículo de Matemáticas los estudios de Doll Jr. (1997) sobre el uso de las cuatro “R” (riqueza, recursividad, relaciones y rigor) para construir un currículo posmoderno; Skovsmose (2006), respecto de la educación matemática crítica; Silva (2009), en lo que se refiere a los criterios de elección y organización de contenidos matemáticos de secundaria (riqueza, reflexión, realidad, responsabilidad, recursividad, relaciones, rigor y resignificación).

Las referencias mencionadas permitieron al autor constatar que para la selección de materias relevantes a desarrollar en el Currículo de Matemática, es necesario considerar: su contribución a la formación de los estudiantes; la posibilidad de ampliar la red de conocimiento intraescolar y extraescolar; la contextualización de contenidos matemáticos; la discusión acerca del papel de las Matemáticas como forma de transformación de la sociedad; la recontextualización de contenidos matemáticos; la factibilidad de asociar el tema y los contenidos matemáticos; las posibilidades metodológicas para el desarrollo del trabajo con temas; y la posibilidad de reflexionar (pensar y repensar) respecto de diferentes temas.

Así, el conjunto de temas que se pueden desarrollar, junto con el contenido matemático, se puede ver en la Figura 1.

Figura 1
Clasificación de Temas de Interés¹

Temática	Descripción	Posibles subtemas
Contemporaneidad	Se refiere a materias que permiten la interacción con contenidos matemáticos, mostrando su aplicabilidad en la sociedad actual.	Criptografía, Medios de comunicación (Internet) y Teoría de grafos.
Político-Social	Se trata de abordar temas relevantes para la formación de los estudiantes como sujetos críticos, reflexivos y comprometidos con la sociedad.	Economía, educación fiscal, contaminación acústica, trabajo y consumo, impuesto a la renta, deuda externa e interna y programas sociales.

¹ De acuerdo con Olgin (2015, p. 65), los temas de interés son materias importantes para la formación de los estudiantes, siendo “temas modernos que pueden enriquecer el Currículo de Matemáticas de secundaria, permitiendo el desarrollo de contenidos matemáticos. Permitiendo dotar a los estudiantes de valores sociales, culturales, políticos y económicos, con el fin de satisfacer las necesidades y objetivos de los estudiantes”.

Temática	Descripción	Posibles subtemas
Cultura	Discute temas relacionados con las artes musicales, escénicas, visuales y deportivas, considerando aspectos relacionados con las tradiciones locales.	Artes y deportes.
Medio Ambiente	Se trata de temas que abordan las cuestiones del medio ambiente y la acción humana, trayendo a colación los conflictos sociales existentes por las diferentes formas de explotación de los bienes ambientales.	Fuentes de energía, radiactividad, pesticidas, agua, reciclaje de basura y deforestación.
Conocimiento Tecnológico	Tiene como objetivo trabajar con las tecnologías y sus diversos recursos para el desarrollo de habilidades matemáticas y computacionales, como es un requisito del mundo moderno.	Computación gráfica, ondas sísmicas y programa de posicionamiento global (GPS).
Salud	Aborda temas importantes para el bienestar de los ciudadanos, así como temas relacionados con la prevención y control de enfermedades, cuidado de la alimentación, saneamiento básico, vivienda adecuada, calidad del aire y del agua, entre otros.	Enfermedades, alimentación, educación sexual y saneamiento básico.
Temas Locales	Permite la selección de temas que relacionan el contenido matemático con cuestiones de la realidad en la que se inserta el estudiante.	Tráfico e impactos de las tasas de mortalidad y natalidad.
Intramatemática	Se refiere al desarrollo de temas específicos en Matemáticas que se han desarrollado a lo largo de la historia.	Números de Fibonacci, Números Áureos, Fractales, Ecuaciones Diofánticas y Patrones Matemáticos.

Fuente: Adaptado de Olgin (2015).

Así, en este trabajo, los temas de interés para el Currículo de Matemáticas deben tener en cuenta el qué enseñar, entendido como la relación de los contenidos matemáticos con los temas relevantes para la formación de los estudiantes. El cómo enseñar está relacionado con las metodologías, recursos, ambientes y procesos que se pueden utilizar en el desarrollo del trabajo con los temas. La razón de enseñar se relaciona con la posibilidad de desarrollar el proceso de enseñanza y aprendizaje de las Matemáticas mediante temas que permitan la construcción de conceptos matemáticos, así como la reanudación, desarrollo y ampliación de contenidos previamente estudiados y la exploración de temas importantes para la formación del profesor de matemáticas.

Tomando los aspectos mencionados anteriormente, se entiende que para el desarrollo de los temas sería conveniente trabajar en conjunto con la Resolución de Problemas, Proyectos de Trabajo, Modelación Matemática, Historia de las Matemáticas y el uso de recursos tecnológicos.

La metodología de resolución de problemas es indicada porque permite desarrollar actividades que permitan a los estudiantes construir estrategias de resolución pertinentes para resolver el problema. Ya que la resolución de problemas permite un aprendizaje basado en la motivación, el interés, el trabajo grupal colaborativo, el intercambio de experiencias y una visión crítica del grupo. Por tanto, estos aspectos hacen posible que esta metodología sea adecuada para el trabajo por temas, posibilitando un trabajo autónomo, en el que el estudiante necesita encontrar formas de resolver la situación presentada, brindando momentos para pensar y repensar las estrategias adoptadas (Doll Jr., 1997).

Mora (2003) señala que la resolución de problemas permite a los profesores de matemáticas trabajar con problemas intramatemáticos (problemas de las propias matemáticas) y extramatemáticos (problemas de diferentes áreas). Tenreiro y Vieira (2001) afirman que esta metodología permite que el estudiante desarrolle el pensamiento crítico, ya que necesita formular, probar, analizar y evaluar hipótesis para determinar la solución de problemas, mejorando habilidades y destrezas en la resolución de problemas.

La metodología de Proyectos de Trabajo, asimismo, es adecuada para el desarrollo de temas, ya que la elección del tema puede surgir tanto del profesor como de los estudiantes. Para Mora e Rivera (2004), trabajar con Proyectos tiene diferentes etapas, a saber: elección del tema; discusión del tema; elaboración de un cronograma de acciones; desarrollo del proyecto y finalización del proyecto, que corresponde a la presentación de los resultados encontrados.

Por tanto, se indica el trabajo con Proyectos, porque a partir de un tema es posible explorar contenidos matemáticos durante el desarrollo del proyecto, pudiendo hacer que las Matemáticas sean atractivas y significativas para el estudiante, relacionando la teoría con temas de interés para el Currículo y los estudiantes.

A su vez, la historia de las Matemáticas puede ser un recurso facilitador en el proceso de enseñanza y aprendizaje de contenidos específicos de esta área, los que pueden ser explicados mediante la historia, mostrando su surgimiento, necesidad y aportes, considerando sus desaciertos y aciertos, para la construcción de conocimientos matemáticos actuales.

También se sugiere trabajar con Modelación Matemática para el desarrollo de temas relacionados con problemas que enfrenta la comunidad, es decir, problemas reales, buscando resolverlos con contenidos matemáticos. Se enfatiza que los problemas para el Modelado Matemático deben estar relacionados con situaciones reales o

fenómenos reales, debido a que, según los autores, las situaciones problemáticas deben ser claramente comprendidas por los estudiantes, no deben contener información difícil de entender y trabajar, las situaciones iniciales deben contener información rica en contenido interesante para los estudiantes e incluir varias preguntas, así como situaciones reales; deben, en la medida de lo posible, incorporar otras áreas del conocimiento científico, posibilitando una Educación Matemática holística y temática.

Para el desarrollo de contenidos matemáticos, a lo largo de la Educación Básica, es fundamental considerar los avances tecnológicos y dotar a los estudiantes del uso de instrumentos como computadoras, calculadoras, *software* educativo, etc. Para Ponte (2001), el docente necesita innovar sus clases, utilizando diversas posibilidades tecnológicas y metodológicas para potenciar el proceso de enseñanza y aprendizaje de contenidos matemáticos. Por tanto, se cree que, al elegir y seleccionar temas, es necesario tener en cuenta la importancia de trabajar con recursos tecnológicos y temas de actualidad, que forman parte del día a día de los estudiantes, ya que pueden estimular y facilitar la comprensión de los mismos –contenido dirigido–.

Según Toledo y Toledo (1997, p. 12):

[...] es imprescindible repensar los objetivos de las Matemáticas. Si antes era necesario hacer los cálculos de forma rápida y correcta, hoy es importante saber por qué funcionan los algoritmos, qué ideas y conceptos intervienen en ellos, qué orden de magnitud de resultados se pueden esperar de determinados cálculos y cuáles son los más eficientes, estrategias ante una situación problema, dejando a la máquina las actividades repetitivas, la aplicación de procedimientos estándar y operaciones rutinarias.

Así, el educador necesita proponer temas que fomenten el conocimiento así como el manejo de los recursos tecnológicos, llevando al estudiante a dedicar más tiempo a la reflexión y análisis para resolver las actividades que presenten los cálculos. El uso de recursos tecnológicos puede permitir a los estudiantes ser más autónomos en la resolución de actividades y trabajar con datos reales, por lo que es necesario el uso de dichos recursos en la Enseñanza de las Matemáticas.

En este contexto, se entiende que los temas, combinados con diferentes recursos didácticos, metodológicos y tecnológicos, pueden posibilitar que el profesor de Matemática desarrolle un trabajo en el que los contenidos se interrelacionen con cuestiones importantes de la realidad de los estudiantes y que abarquen los cambios de sociedad contemporánea.

3. La criptografía y su historia

El cifrado garantiza la confidencialidad de la información, utilizando diferentes técnicas. En el pasado, los griegos, hebreos, persas, árabes, entre otros, utilizaron la

criptografía para mantener en secreto el contenido de sus mensajes (Carneiro, 2017). Hoy, la criptografía se ha utilizado en muchas situaciones de la vida moderna, ya que permite realizar auditorías electrónicas, autenticación de órdenes de pago electrónico, transmisión digital de documentos legales, autenticación y privacidad de la información.

El nombre Criptografía proviene de las palabras griegas *kryptos*, que significa secreto, y *graphein*, que se refiere a la escritura (Singh, 2003). Según Tamarozzi (2001), la criptografía es conocida como el arte de escribir códigos. Sin embargo, Carneiro (2017) aclara que el propósito de la criptografía no es ocultar un mensaje, sino aclarar su contenido, y para ello utiliza diferentes estrategias.

Una de las primeras estrategias para codificar un mensaje se utilizó en la guerra entre Esparta y Atenas, cuyo mecanismo de codificación se denominó Citale Spartano (Singh, 2003; Urgellés, 2018), que consistía en un palo de madera y una correa de cuero. Al envolver la tira en el palo se escribía el mensaje a enviar, al estirar la tira se confundía el mensaje y se usaba esta tira como correa para mover el mensaje. Para descifrar el mensaje, el destinatario necesitaba un Citale del mismo diámetro para envolver la correa de cuero y leer el mensaje.

Otra forma de codificación ampliamente utilizada fue el cifrado de sustitución o cifrado monoalfabético, conocido como cifrado César. Este cifrado consistía en reemplazar cada letra del abecedario por otra que estuviera tres lugares por delante en el mismo abecedario, por ejemplo la letra A en el texto original corresponde a la D en el texto cifrado, la letra B corresponde a la E, y así sucesivamente (Singh, 2003). Según Urgellés (2018), este código es ampliamente estudiado en criptografía, ya que permite ilustrar los principios de la aritmética modular que es la base para el estudio de este tema.

Después de años de utilizar cifras monoalfabéticas, en 1586 apareció el tratado sobre cifras, publicado por el diplomático francés Blaise Vigenère, que presenta una nueva técnica, basada en la cifra polialfabética, que consistía en el uso de 26 alfabetos distribuidos en una matriz, para codificar y decodificar un texto y esta estrategia se conoció como el Cifrado Vigenère (Carneiro, 2017).

Años más tarde, en 1918, apareció un nuevo cifrado, denominado Cifra ADFGVX, que utilizaba los métodos de cifrado por sustitución y transposición, ya que se caracterizaba por la reorganización de las letras del texto, generando anagramas. Según Singh (2003), las letras ADFGVX fueron seleccionadas porque, al traducirse a puntos y rayas del código Morse, reduce la posibilidad de errores durante la transmisión del mensaje.

Con el avance de la tecnología, el arquitecto Alberti crea la primera máquina criptográfica, el Disco de Cifras, construido a partir de dos discos de cobre, con diferentes diámetros, cuyas letras del alfabeto estaban fijadas en el borde de los discos y había una aguja que atravesaba el centro de los discos, constituyendo un eje común, lo que permitió cambiar las posiciones de los alfabetos para la codificación (Carneiro, 2017).

Singh (2003) y Urgellés (2018) señalan que años después de la creación del Cipher Disk, el alemán Artur Scherbius desarrolló la versión eléctrica de este disco, a la que denominó máquina Enigma y este instrumento se convirtió en el sistema de cifrado más complejo del mundo y fue utilizado por los alemanes durante la Segunda Guerra Mundial. Para decodificar los textos cifrados por Enigma, se diseñó Colossus, que marcó el comienzo de la era moderna de la criptografía. Sin embargo, es oportuno señalar que fueron los estudios de Turing acerca de los números computables los que dieron origen a la máquina universal, denominada Máquina de Turing, que consistía en una máquina que podía realizar automáticamente los procesos desarrollados por los matemáticos, como sumar, dividir, elevar al cuadrado, y otros, este mecanismo fue la base para el desarrollo de las primeras computadoras (Carneiro, 2017).

Incluso con la llegada de la computadora, las técnicas de cifrado por sustitución y transposición eran muy simples, creando así la necesidad de cifrados complejos; y para resolver este problema, se introdujeron dos algoritmos de cifrado: DES (sistema de clave secreta) y RSA (sistema de clave pública). Con los avances tecnológicos y las técnicas de encriptación, la comunicación digital ha traído flexibilidad y eficiencia en el registro, recuperación y distribución de información, siendo utilizada en sistemas de transacciones bancarias en línea, sistema de compras a distancia, retiros y transferencias de fondos con tarjetas electrónicas.

De esta forma, se entiende que este tema también puede ser utilizado para potenciar la enseñanza de contenidos matemáticos en la Educación Secundaria, ya que favorece el desarrollo de actividades de codificación y decodificación, además de ser un elemento motivador en el aprendizaje de las Matemáticas. En este sentido, Tamarozzi (2001) menciona que este tema ayuda en la elaboración de actividades para ejercitar y fijar los contenidos matemáticos de funciones y matrices.

Por tanto, este artículo presentará ejemplos de actividades que combinan el tema de la criptografía con contenidos relacionados con la aritmética, función polinomial de primer grado y matrices, que pueden ser utilizados por profesores de Matemáticas.

4. Metodología de investigación

Esta investigación se desarrolló en tres etapas. El primero fue el estudio de los conceptos e historia de la Criptografía, ya que el estudio exploratorio de este tema permite a los investigadores comprender con mayor profundidad su objeto de estudio.

La segunda etapa fue la selección y elaboración de actividades didácticas para el Currículo de Matemáticas de Bachillerato, que combinaron la temática con los contenidos matemáticos. El último paso fue la organización de una secuencia didáctica para el desarrollo del trabajo con el tema “Criptografía en el aula”, esta secuencia asume la necesidad de un contacto inicial del estudiante con el tema, en la que se pondrán a disposición personajes históricos, para luego abordar el tema con el contenido matemático de aritmética, función y matrices.

5. Actividades didácticas que involucran el tema Criptografía

Esta sección presenta un conjunto de actividades didácticas (Figura 2) que abordan el conocido arte de escribir en clave (Tamarozzi, 2001; Singh, 2003) combinado con los contenidos de aritmética, funciones y matrices que pueden ser explorados por los profesores de Matemáticas.

Figura 2
Secuencia didáctica con el tema Criptografía

Actividad	Intención	Contenido
Cifra de César	Conocer y aprender a utilizar cifrados por sustitución monoalfabéticos.	Cifra histórica
Cifra ADFGVX	Conocer y aprender a utilizar los cifrados por sustitución y transposición.	Cifra histórica
Criptograma	Aplicar los conocimientos de Aritmética en situaciones que impliquen la sustitución de letras por números, con el objetivo de introducir el concepto de Criptografía.	Aritmética
Código con función polinomial de primer grado	Revisar, profundizar y reforzar el concepto de función, imagen de la función, cálculo de funciones inversas, buscando ampliar conocimientos en cuanto al contenido de Función Polinomial de Primer Grado.	Función polinomial de primer grado
Código con Matrices	Revisar el concepto de matriz, multiplicación de matrices, operaciones con matrices, matriz transpuesta, cálculo de matrices inversas, buscando profundizar en el estudio de estos contenidos.	Matrices

Fuente: Adaptado de Olgin (2011, 2015).

Cuando se trabaja un tema del Currículo de Matemáticas, se entiende que es necesario introducirlo mediante su historia y aplicaciones. En este sentido, se entiende que para la introducción de la criptografía es importante que el docente presente algunas formas de codificación utilizadas a lo largo de la historia, como el Cifrado César, el Cifrado Chiqueiro y el Cifrado ADFGVX. Para luego presentar actividades que involucren la relación entre el tema y las Matemáticas, tales como criptogramas, código con funciones y código con matrices.

La primera actividad involucra el Cifrado César, que era de uso militar y consistía en reemplazar letras del alfabeto (Figura 3). En esta actividad se pretende poner en contacto al alumno con una de las formas de codificación más antiguas y conocidas.

Figura 3

Exemplo da Cifra de César

Cifre la frase “MATEMÁTICA É PARA VIDA”, usando el cifrado César, usando la tabla a continuación.

Alfabeto Normal	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
Alfabeto encriptado	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Se espera que, en esta actividad, el alumno encuentre el valor de cada letra, según la codificación utilizada por Julio César, en donde reemplazará la letra del abecedario normal por la letra del abecedario cifrado, encontrando el cifrado mensaje: “PDWHPDWLFDHSDUDYLGD”.

Fuente: Olgin (2011, p. 55-56).

Otra actividad que involucra cifrados históricos que se puede explorar en el aula es el Cifrado ADFGVX, que utiliza el método de sustitución y transposición² (Figura 4).

Figura 4

Ejemplo que involucra el cifrado ADFGVX

Según Singh (2003), el Cifrado ADFGVX se utiliza para codificar una cuadrícula de 6x6, llena de 36 cuadrados, donde se colocan las 26 letras del alfabeto y 10 dígitos. En la primera fila y columna se colocan las letras A, D, F, G, V y X, como se muestra en la siguiente tabla.

	A	D	F	G	V	X
A	8	P	3	D	1	N
D	L	T	4	O	A	H
F	7	K	B	C	5	Z
G	J	U	6	W	G	M
V	X	S	V	I	R	2
X	9	E	Y	0	F	Q

Comienza la codificación, tomando cada letra del mensaje a enviar, ubicando su posición en la grilla y reemplazándola con las letras de la fila y columna. Por ejemplo, d será reemplazada por AG. Un mensaje codificado por este cifrado se parecerá a la siguiente tabla.

Palabra original	Lógica
Palabra codificada	DADGGVVGFGDV

Para encriptar la letra L, ubica su posición en la grilla y reemplázala con las letras que están en su fila y columna, correspondientes a DA.

Fuente: Olgin (2011, p. 22-23).

² El cifrado por transposición implica la reorganización de las letras del mensaje, creando anagramas (Singh, 2003).

Las actividades que involucran contenido matemático presentan inicialmente los Criptogramas que tienen como objetivo explorar operaciones aritméticas por medio de la resolución de problemas aritméticos (Olgin, 2011; Serrano, 2017). Según Lins e Giménez (1997, p. 39), los contenidos aritméticos ofrecen respuestas a diferentes problemas abiertos, “entre ellos, las llamadas matemáticas discretas, con criptografía, problemas de minimización y máxima explotación en economía, análisis numérico, interacción, etcétera.

En la Figura 5 se presenta un ejemplo de un problema abierto que involucra criptogramas, que son actividades en las que las letras se convierten en números.

Figura 5
Ejemplo de actividad de criptograma

Sabiendo que cada letra corresponde a un dígito diferente, resuelve el siguiente criptograma.

$$\begin{array}{r} \text{DOIS} + \text{SEIS} \\ \hline \text{OITO} \end{array}$$

Resolución de actividad

Esta actividad se puede resolver por prueba y error o mediante el conocimiento del contenido de la aritmética. Utilizando la última forma de resolución, se puede llevar al estudiante a sistematizar la información relevante, formular hipótesis y buscar formas de determinar la solución.

Esta actividad puede ser explorada por el maestro de la siguiente manera:

- 1) Identificar la información relevante: $D + S \leq 9$.
- 2) Desarrollar hipótesis: $S + S = O \quad 2S = O$. Logo, O es número par.
- 3) Predecir resultados: Si $O=0$ que $S = 0$ o $S=5$. Pero O no puede ser cero, porque $D+S$ no puede ser cero. Entonces, proposición falsa.

Si $O=2 \quad S=1$ o $S=6$, porque $S+S=O$. S no puede ser 1, porque $D+S=2$ y no cumple las condiciones. Entonces la proposición es falsa. S no puede ser 6, porque $D+S$ no puede ser 2. Entonces, proposición falsa.

Si $O=4 \quad S=2$ o $S=7$, porque $S+S=O$. S no puede ser 7, porque $D+S$ tiene que ser 4. Entonces la proposición es falsa. S puede ser 2, entonces: $D=1$ e $O+E \geq 10 \quad E \geq 6$. Entonces, $E=6$ o $E=7$ o $E=8$ o $E=9$. La única posibilidad viable es que $E=9$. Entonces: $I=3$ e $T=6$.

Si $O=6 \quad S=3$ o $S=8$, porque $S+S=O$. $S=8$ no puede, porque $D+S$ tiene que ser igual a 6. Proposición falsa. $S=3$ no puede, porque $D+S=6$. Entonces, proposición falsa.

Si $O=8 \quad S=4$ o $S=9$, porque $S+S=O$. $S=9$ no puede, porque $D+S=8$. Proposición falsa. S puede ser 4, entonces: $D=3$ y $O+E \geq 10 \quad E \geq 2$. La única posibilidad viable es que $E=7$. Entonces: $I=6$ y $T=0$.

Así que hay dos respuestas posibles:

- $\text{DOIS} + \text{SEIS} = \text{OITO} \quad 1432 + 2932 = 4364$.
- $\text{DOIS} + \text{SEIS} = \text{OITO} \quad 3864 + 4764 = 8628$.

Fuente: Olgin (2015, p. 148-149).

Otra actividad, explora el contenido de función polinomial de primer grado, esta actividad se denominó codificar con función (Figura 6), que consiste en codificar y decodificar mensajes, donde se invita a los estudiantes a investigar mediante contenidos matemáticos, pues para codificar es necesario conocer, interpretar y realizar procedimientos matemáticos para determinar la imagen de una función, así como profundizar en las nociones de dominio de una función. Para la decodificación, es necesario utilizar las nociones referentes al cálculo de la función inversa.

Figura 6
Actividad que involucra código con función

Considere la siguiente tabla que, para cada letra del alfabeto, asocia un número y codifica el texto “A VIDA É UM SEGREDO”, sabiendo que la clave de cifrado es la función $f(x) = 3x - 2$.

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
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

Resolución de actividad

- Relacionar cada letra del abecedario con un número, obteniendo del texto una secuencia numérica: 1 - 22 - 9 - 4 - 1 - 5 - 21 - 13 - 19 - 5 - 7 - 18 - 5 - 4 - 15.
- Se encripta el texto, calculando la imagen de la función para cada número de la secuencia numérica del texto:

$f(1) = 3 \cdot 1 - 2 = 1$	$f(4) = 3 \cdot 4 - 2 = 10$	$f(5) = 3 \cdot 5 - 2 = 13$
$f(7) = 3 \cdot 7 - 2 = 19$	$f(9) = 3 \cdot 9 - 2 = 25$	$f(13) = 3 \cdot 13 - 2 = 37$
$f(15) = 3 \cdot 15 - 2 = 43$	$f(18) = 3 \cdot 18 - 2 = 52$	$f(19) = 3 \cdot 19 - 2 = 55$
$f(21) = 3 \cdot 21 - 2 = 61$	$f(22) = 3 \cdot 22 - 2 = 64$	

- El texto codificado corresponde a la imagen de cada número que se encuentra en la función: 1 - 64 - 25 - 10 - 1 - 13 - 61 - 37 - 55 - 13 - 19 - 52 - 13 - 10 - 43.
- El receptor recibe la secuencia numérica del texto codificado y la clave de cifrado. Para decodificar, debes calcular la imagen de los elementos, usando la función inversa. Si la clave de cifrado es la función $f(x) = 3x - 2$, la clave de descifrado es la inversa de la función clave, tenga en cuenta: $f(x) = 3x - 2$ $f(x) - 2 = 3x$ $\frac{f(x)-2}{3} = x$. Por tanto, la función inversa que permite decodificar el texto corresponde a $f^{-1}(x) = \frac{x+2}{3}$.
- Descifrando el último número de la secuencia numérica, uno tiene $f^{-1}(43) = \frac{43+2}{3} = 15$. Posteriormente, se observa qué letra corresponde al número 15, en la tabla establecida. Por tanto, 15 corresponde a la letra O. Por consiguiente, debe hacerse para toda la secuencia numérica codificada.

Fuente: Adaptado de Olgin (2015).

La tercera actividad comprende códigos con matrices, en la que se invita a los estudiantes a estudiar la multiplicación de matrices y su inversa en actividades de codificación y decodificación (Figura 7).

Figura 7
Actividad que involucra código con matrices

Considere la siguiente tabla que, para cada letra del alfabeto, asocia un número y codifica la palabra "FELICIDADE", sabiendo que la clave de codificación es la matriz $A = \begin{pmatrix} 2 & 3 & 1 & 4 \end{pmatrix}$.

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
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

Resolución de actividad

- Cada letra del alfabeto está relacionada con un número, es decir, la secuencia numérica de la palabra es: 6 - 5 - 12 - 9 - 3 - 9 - 4 - 1 - 4 - 5.
- Construya una matriz con la secuencia numérica de la palabra: $M = \begin{pmatrix} 6 & 5 & 12 & 9 & 3 & 9 & 4 & 1 & 4 & 5 \end{pmatrix}$.
- Para codificar, multiplicar matrices en las que la matriz A se multiplicará por la matriz M:

$$AM = \begin{pmatrix} 2 & 3 & 1 & 4 \end{pmatrix} \cdot \begin{pmatrix} 6 & 5 & 12 & 9 & 3 & 9 & 4 & 1 & 4 & 5 \end{pmatrix}$$

$$AM = \begin{pmatrix} 27 & 51 & 33 & 11 & 23 & 33 & 39 & 11 & 8 & 23 & 24 \end{pmatrix}$$

Los elementos de la matriz AM corresponderán al mensaje codificado: 27 - 26 - 51 - 48 - 33 - 39 - 11 - 8 - 23 - 24.

- El receptor recibe la secuencia numérica de la palabra y la clave de cifrado. Para decodificar, multiplique la matriz (AM) por la inversa de la matriz A (A^{-1}). Si la clave de cifrado es la matriz A, la clave de descifrado es la inversa de la clave de matriz, tenga en cuenta:

$$A^{-1} = \begin{pmatrix} 2 & 3 & 1 & 4 \end{pmatrix} \cdot \begin{pmatrix} a & b & c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix} \rightarrow A^{-1} = \begin{pmatrix} \frac{4}{5} & -\frac{3}{5} & -\frac{1}{5} & \frac{2}{5} \end{pmatrix}$$

Para decodificar se realiza la multiplicación de matrices, en la que se multiplica la matriz AM por la matriz A^{-1} :

$$(AM)A^{-1} = \begin{pmatrix} 27 & 51 & 33 & 11 & 23 \\ 26 & 48 & 39 & 8 & 24 \end{pmatrix} \cdot \begin{pmatrix} \frac{4}{5} & -\frac{3}{5} \\ -\frac{1}{5} & \frac{2}{5} \end{pmatrix} = \begin{pmatrix} 6 & 12 & 3 & 4 & 4 \\ 5 & 9 & 9 & 1 & 5 \end{pmatrix}$$

Fuente: Olgin (2015, p. 154-155).

Asimismo, en actividades de codificación con funciones y matrices, se pueden explorar recursos tecnológicos como hojas de cálculo o calculadoras para facilitar la resolución de cálculos matemáticos, ya que las actividades que involucran estos contenidos

requieren una gran cantidad de cálculos. Y el foco está en entender, profundizar y reparar los contenidos de funciones y matrices y no en cálculos que involucren operaciones básicas.

Por esta razón, el tema de la criptografía puede ser desarrollado en el Currículo de Matemática, ya que es un tema actual que permite el desarrollo de actividades didácticas, en las que los estudiantes amplían su red de conocimientos históricos respecto del tema, se involucran en un conjunto de actividades de codificación y decodificación con los contenidos que se trabajan en Bachillerato. Los estudiantes también pueden resolver situaciones problemáticas, como criptogramas, por medio de prueba y error o evolucionando hacia la formulación, prueba y validación de hipótesis (Olgin, 2015).

6. Conclusión

El tema Criptografía puede ser incluido en los currículos de Matemáticas en la Enseñanza Media, siempre y cuando las actividades planificadas por el docente sean motivadoras y permitan la construcción del conocimiento matemático.

Aún así, este tema es adecuado para el desarrollo de actividades didácticas utilizando los contenidos matemáticos que se trabajan en la Secundaria, combinados con una estrategia de resolución de problemas. Las actividades de codificación y decodificación pueden brindar a los estudiantes la oportunidad de revisar y reforzar los contenidos de funciones y matrices y utilizar la calculadora o las hojas de cálculo electrónicas como recurso facilitador para la resolución de cálculos.

Por consiguiente, coincidimos con Olgin (2011) en que es importante trabajar con temas de interés y que posibiliten el desarrollo de actividades y la comprensión y aplicación de contenidos matemáticos, ya que el Currículo de Matemáticas que se debe desarrollar en la Educación Secundaria necesita ser contextualizado, buscando incentivar a los estudiantes a estudiar los contenidos.

Referencias

- Carneiro, F. J. F. (2017). *Criptografía y Teoría de Números*. Editora Ciência Moderna.
- Doll Jr, W. E. (1997). *Currículo: una perspectiva posmoderna*. Trad. Maria Adriana Veríssimo Veronese. Porto alegre: Artes Médicas.
- Groenwald, C. L. O. y Franke, R. (2007). Currículo de Matemáticas y Criptografía en Bachillerato. *Revisión de la Educación Matemática*, 10(1), 97-116.
- Lins, R. C. y Giménez, J. (1997). *Perspectivas en aritmética y álgebra para el siglo XXI*. Campinas, São Paulo: Papirus.
- Mora, C. D. (2003). *Aprendizaje y enseñanza: proyectos y estrategias para una educación matemática del futuro*. Campo Iris.
- Mora, C. D. y Rivera, A. (2004). *Temas en Educación Matemática*. GIDEM.

- Olgin, C. A. (2011). *Currículo en la Enseñanza Media: una experiencia con el tema de la criptografía* (136 f.). Trabajo Fin de Máster, Enseñanza de las Ciencias y las Matemáticas, Universidade Luterana do Brasil, Canoas.
- Olgin, C. A. (2015). *Criterios, posibilidades y desafíos para el desarrollo de temas en el Currículo de Matemáticas de Nivel Medio* (265 f.). Tesis Doctoral, Enseñanza De Las Ciencias y Las Matemáticas, Universidade Luterana do Brasil, Canoas.
- Ponte, J. P. (2001). *Investigaciones matemáticas en el aula*. Belo Horizonte: Autêntica.
- Selbach, S. (2010). *Historia y didáctica. Cómo enseñar la colección*. Vozes.
- Serrano, J. G. (2017). *Diversión con números*. Panamericana Editorial.
- Silva, M. A. (2009). *Currículo de Matemática en la Educación Secundaria: en busca de criterios para la elección y organización de contenidos*. Tesis (Doctorado en Educación Matemática). Pontificia Universidade Católica de São Paulo.
- Singh, S. (2003). *El libro de códigos: las ciencias del secreto - desde el antiguo Egipto hasta la criptografía cuántica*. Editora Record.
- Skovsmose, O. (2006). *Educación Matemática Crítica: la cuestión de la democracia*. Papyrus.
- Tamarozzi, A. C. (2011). Codificar y descifrar mensajes. *Revista del profesor de matemáticas*, 45.
- Tenreiro, C. V. y Vieira, R. M. (2001). Resolução de problemas e pensamento crítico em torno das possibilidades de articulação. *Revista da Associação dos Professores de Matemática*, Lisboa.
- Toledo, M. y Toledo, M. (1997). *Didática da Matemática: como dois e dois - a construção da matemática*. São Paulo: FTD.
- Urgellés, J. G. (2018). *Matemática y códigos secretos*. Barcelona: Editora RBA Libros.



Copyright © 2022. Clarissa de Assis Olgin. Esta obra está protegida por una licencia [Creative Commons 4.0. International \(CC BY 4.0\)](https://creativecommons.org/licenses/by/4.0/).

Usted es libre para Compartir —copiar y redistribuir el material en cualquier medio o formato — y Adaptar el documento —remezclar, transformar y crear a partir del material— para cualquier propósito, incluso para fines comerciales, siempre que cumpla la condición de:

Atribución: Usted debe dar crédito a la obra original de manera adecuada, proporcionar un enlace a la licencia, e indicar si se han realizado cambios. Puede hacerlo en cualquier forma razonable, pero no de forma tal que sugiera que tiene el apoyo del licenciante o lo recibe por el uso que hace de la obra.

[Resumen de licencia - Texto completo de la licencia](#)