

Secretos y mensajes ocultos

Miriam Guadalupe Baéz Hernández^{1,2} CoDiCE

Jorge Luis Arroyo Neri ¹

¹ Universidad Anáhuac Veracruz-

² Colectivo de Divulgación de la Ciencia y la Educación CoDiCE

Resumen

Este juego de misterio desafía a los participantes a trabajar en equipo para resolver un caso mediante el uso de diversas técnicas de cifrado. Los equipos emplearán métodos como el cifrado César, el cifrado de Polibio y la Escítala Espartana para descifrar mensajes ocultos. El objetivo principal es descubrir la ubicación de un suceso y, a través del descifrado, llegar a la resolución del misterio planteado.

Tipo de público (marcar con X los que correspondan)

Estudiantes				
Preescolar	Primaria	Secundaria	Bachillerato	
	X	X		
Otros sectores				
Familias	Jóvenes adultos	Adultos mayores	Madres de familia	Otro (especificar)
X	X		X	
¿La actividad ofrece ajustes para trabajar con un enfoque inclusivo? Especificar casos				
No				

Área de la ciencia: Matemáticas

Literatura

Conceptos clave: Cifrado de César
Cifrado de Polibio
Escítala Espartana

Objetivo (s)

Mostrar a las y los jóvenes algunos de los cifrados que existen para ocultar mensajes, e incentivar su curiosidad para resolver situaciones que impliquen el método deductivo.

Tipo de actividad: juego

Duración sugerida: 45 minutos

Material	
Grupal	Tablero (Anexo) Tarjetas 6 listones 6 tubos de pvc o cartón de diferente tamaño y grosor. Sobres de misión Cifrados de César Cifrados de Polibio Cartas Plumón permanente
Por participante	Lápiz Goma Hojas
Requerimientos técnicos	
Mesa de trabajo. Se recomienda trabajar la actividad con 4 facilitadores; cada uno de ellos tendrá un caso diferente y ayudará a cada equipo a resolver su misterio.	
Factores de riesgo	
No se tienen.	

Marco teórico

La criptografía es un campo fascinante y fundamental en el ámbito de la seguridad de la información. En un mundo cada vez más digitalizado, es crucial comprender los principios y métodos detrás de los cifrados para proteger la confidencialidad, autenticidad e integridad de los datos. El presente marco teórico proporcionará una base sólida para el desarrollo de un taller de divulgación de cifrados, cuyo objetivo es introducir a los participantes en los conceptos y técnicas criptográficas de manera accesible y práctica.

La criptografía se encarga del cifrado de mensajes con la finalidad de ocultar su contenido a receptores no autorizados. A lo largo de la historia han existido diferentes métodos de cifrado: por ejemplo, en la antigua Roma era común utilizar un método por sustitución, donde cada letra del alfabeto era reemplazada por otra más mediante una técnica de corrimiento. Con la aparición de la informática y las computadoras, las técnicas de la criptografía se han vuelto cada vez más sofisticadas, empleándose en la mayoría de ellas la aritmética y los números primos. Tal es su relevancia actualmente, que es utilizada para encriptar datos de suma importancia como claves bancarias o mensajes de seguridad nacional.

Además de proteger la confidencialidad de la información, la criptografía también juega un papel crucial en la autenticación y la integridad de los datos. Junto con el cifrado, se utilizan técnicas de firma digital y funciones hash criptográficas para verificar la identidad de los remitentes y asegurarse de que los mensajes no hayan sido alterados durante la transmisión.

En el ámbito de la criptografía moderna, se han desarrollado algoritmos de cifrado simétrico y asimétrico. El cifrado simétrico utiliza una única clave para cifrar y descifrar los mensajes, lo que implica que tanto el emisor como el receptor deben conocer la misma clave secreta. Por otro lado, el cifrado asimétrico utiliza un par de claves: una pública y una privada. La clave pública se comparte ampliamente para cifrar los mensajes, mientras que la clave privada se mantiene en secreto y se utiliza para descifrarlos. Esta técnica permite una comunicación segura incluso cuando las claves públicas son conocidas por todos.

La criptografía moderna también se basa en problemas matemáticos difíciles de resolver, como la factorización de números grandes o el logaritmo discreto. Estos problemas proporcionan la base para los algoritmos criptográficos más utilizados, como el Rivest-Shamir-Adleman y el ElGamal. Además, los protocolos de clave pública, como el intercambio de claves de Diffie-Hellman, permiten a dos partes establecer de manera segura una clave compartida a través de un canal inseguro.

Por lo tanto, la comprensión de la criptografía es esencial para salvaguardar la información en un entorno digital cada vez más interconectado.

Flujo de la actividad

Antes de realizar la actividad.

El objetivo del juego es descifrar a través de diferentes tipos de cifrado quién cometió un asesinato, cómo y con qué. Para ello se proporcionan 4 diferentes casos: dos de ellos serán la versión fácil y los otros dos una versión más avanzada. Se pueden construir más.

Para ello, lo primero que se debe hacer es impirmir el material que aparece en las referencias, y familiarizarse con él, así como con los cifrados que se usarán. A continuación, se explicará a detalle cómo se deben usar algunos de los cifrados.

Cifrado Escítala Espartana

El facilitador debe construir los cifrados de la Escítala Espartana. El proceso consiste en lo siguiente:

1. **Obtención de los tubos:** Se buscan 6 tubos de diferentes grosores. No importa el tamaño exacto; lo crucial es que haya variedad.
2. **Preparación de los listones:** Se cortan listones de diferentes anchos. **El ancho de cada listón debe corresponder a la circunferencia de uno de los tubos.** Es decir, al enrollar el listón alrededor del tubo, debe cubrirlo completamente sin superponerse ni dejar espacios.

Este proceso de adaptación hace que cada juego de Escítala Espartana sea único. Las dimensiones exactas de los tubos y listones variarán según los materiales encontrados, pero la relación entre ellos (listón enrollado ajustando perfectamente al tubo) es lo que permite el cifrado y descifrado.

En resumen: No se proporcionan medidas específicas porque dependen del material disponible. La clave está en que el listón se ajuste perfectamente al tubo al enrollarlo.

3. Se escriben los mensajes verticalmente en los listones. Se sugieren los mensajes:

“FUE EN LA BIBLIOTECA MIENTRAS BUSCABA SU LIBRO FAVORITO”

“FUE EN EL COMEDOR. FUE EN EL COMEDOR”

“OCURRIÓ EN LA SALA DE MÚSICA. LO TOMÓ POR SORPRESA MIENTRAS ENSAYABA EL RECITAL”

“FUE EN LA TARDE. FUE EN LA COCINA. FUE EN LA COCINA”

4. Se pueden usar letras al azar o mensajes diferentes en los dos tubos restantes.
5. Se recomienda pintar los tubos para facilitar la identificación.
6. Se debe repartir a cada facilitador un sobre con las respuestas de cada caso; es decir, el tubo y el listón asignado para encontrar el mensaje.
7. Es muy importante dar un breve repaso del material a usar.



Cifrado Método Tablas

1. Las tarjetas mostradas están diseñadas para ser colocadas sobre un tarjetón de color café. Al superponerlas, ciertas letras se destacan y forman un mensaje.
2. Se presenta un conjunto de tarjetas que, al ser colocadas sobre un tarjetón café, revelan un mensaje oculto gracias a la superposición y la distinción de ciertas letras.

3. Para descifrar el mensaje, se deben superponer las siguientes tarjetas sobre un tarjetón de color café. La combinación de las letras visibles al superponerlas revelará el mensaje.

¡Qué ganas tenía de dejar la sombría sala y deambular por entre aquellos lechos de rutilantes flores y aquellas frescas fuentes!, pero ni siquiera le entraba la cabeza por el hueco de la puerta; “y en caso de que pasara —pensó Alicia— de poco me serviría sin los hombros. ¡Ah, cómo me gustaría plegarme como un telescopio! Creo que podría, si supiera cómo empezar”. Porque, ya ven, le habían ocurrido últimamente tantas cosas extraordinarias que Alicia empezaba a pensar que muy pocas eran realmente imposibles.
Era inútil quedarse allí plantada ante la puertecita, así que volvió a la mesa, con cierta esperanza de hallar encima otra llave o, al menos, un libro con las instrucciones para poder plegarse como un telescopio. Esta vez encontró una botellita (“que por cierto no estaba aquí antes”, se dijo Alicia); tenía atada alrededor del cuello una etiqueta de papel, en mayúsculas bellamente impresas, con la palabra: **Bébe me**.
Fragmento de Alicia en el País de las Maravillas

Bastían no sintió que las lágrimas le corrían por la cara. Casi sin darse cuenta gritó de pronto:
-¡Hija de la Luna! ¡Voy!
En ese mismo momento ocurrieron muchas cosas simultáneamente.
La cáscara del gran huevo fue rota en pedazos por una fuerza tremenda, mientras se oía el oscuro retumbar de un trueno. Comenzó a soplar un viento tempestuoso que surgió de las páginas del libro que Bastían tenía sobre las rodillas, de forma que esas páginas empezaron a revolotear desordenadamente. Bastían sintió la tormenta en el pelo y el rostro, se quedó casi sin aliento, las llamas de las velas del candelabro de siete brazos danzaron y se pusieron horizontales, y entonces un segundo viento tormentoso, más poderoso aún, agitó el libro y apagó todas las luces.
El reloj de la torre dio las doce.
Fragmento de la Historia Interminable



Cifrado De Polibio

Este cifrado utiliza una tabla (el área café del material impreso) donde cada letra del alfabeto tiene una posición única, como una dirección en un mapa. Esta "dirección" se compone de dos partes:

- **Horizontal (Columna):** Indica la posición de la letra de izquierda a derecha dentro de la tabla.
- **Vertical (Fila):** Indica la posición de la letra de arriba a abajo dentro de la tabla.

Proceso de Cifrado (Paso a Paso):

1. **Localizar la letra:** Busca la letra que quieres cifrar dentro de la tabla (área café).
2. **Anotar la coordenada horizontal:** Observa en qué columna se encuentra la letra y anota ese valor. Esta será la primera parte de la clave cifrada.
3. **Anotar la coordenada vertical:** Observa en qué fila se encuentra la letra y anota ese valor. Esta será la segunda parte de la clave cifrada.
4. **Repetir:** Repite los pasos 1 al 3 para cada letra del mensaje que quieres cifrar.

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

Mensaje Original: **HOLA**
 Cifrado de Polibio: **BCCDCAAA**

Cifrado de César

Este cifrado se basa en el Cifrado de César original, pero con una modificación importante: en lugar de una traslación fija, se utilizan todas las traslaciones posibles del alfabeto (27 en total, considerando que el alfabeto español incluye la Ñ, aunque una de ellas no modifica el mensaje, dejando 26 traslaciones útiles). Esto significa que cada letra se desplaza un número variable de posiciones.

Proceso de Cifrado (Paso a Paso):

1. **Seleccionar el número de traslación:** Se elige un número entre 1 y 26. Este número determinará cuántas posiciones se desplazarán las letras.
2. **Desplazar el alfabeto:** Se desplaza el alfabeto la cantidad de posiciones indicada por el número de traslación. Por ejemplo, si el número es 5:
 - A se convierte en F
 - B se convierte en G
 - C se convierte en H
 - ... y así sucesivamente.
3. **Cifrar el mensaje:** Se reemplaza cada letra del mensaje original por la letra correspondiente en el alfabeto desplazado.

Ejemplo de Cifrado:

Si el número de traslación es 3...

- La palabra "HOLA" se cifraría como "KROD" (H->K, O->R, L->O, A->D).

Proceso de Descifrado (Paso a Paso):

Este es el punto clave donde interviene el facilitador. Debido a las 26 posibilidades, se utiliza un método de prueba y error guiado. Se utilizan dos círculos concéntricos: uno grande con el alfabeto original y uno mediano con el alfabeto cifrado.

1. **Proponer un número de traslación:** Los participantes eligen un número entre 1 y 26 como posible número de traslación.
2. **Alinear los círculos:** Se sitúa el círculo de radio medio (con el mensaje cifrado) de forma que el número propuesto coincida con la letra A del círculo de radio mayor (alfabeto original). Por ejemplo, si proponen el número 5, la letra que esté en la posición 5 del círculo mediano se alinea con la A del círculo grande.
3. **Leer el mensaje descifrado:** Se lee el mensaje descifrado en el círculo de radio mayor, buscando las correspondencias de las letras del mensaje cifrado en el círculo mediano.
4. **Probar con otros números (hasta 3 intentos):** Se repiten los pasos 1 al 3 con diferentes números de traslación hasta que se encuentre un mensaje con sentido.
5. **Pista del facilitador:** Si después de tres intentos los participantes no han encontrado la solución, el facilitador les da la pista crucial: **la primera letra del mensaje cifrado corresponde a la letra S en el mensaje original.**
6. **Ajustar con la pista:** Con esta pista, los participantes deben buscar la letra S en el círculo grande y alinearla con la primera letra del mensaje cifrado en el círculo mediano. Esto les dará el número de traslación correcto y les permitirá descifrar el resto del mensaje.

Ejemplo de Descifrado con la Pista:

Supongamos que el mensaje cifrado comienza con la letra "V". El facilitador indica que la primera letra del mensaje original es "S". Los participantes buscan la "S" en el círculo grande y la alinean con la "V" del círculo mediano. La posición relativa de los círculos les indicará el número de traslación correcto.

Puntos importantes:

- El círculo de radio mayor contiene el alfabeto original.
- El círculo de radio medio contiene el mensaje cifrado.
- La pista de que la primera letra corresponde a la "S" es fundamental para guiar el descifrado.

Material

El juego contiene cuatro casos, dos de ellos en su versión fácil. Antes de iniciar, es importante organizar el material por casos; para ello, se sugiere usar sobres con las herramientas que ayudarán a los jugadores a resolver cada uno. Para diferenciar cada caso, se pueden usar sobres de cuatro colores diferentes: negro, amarillo, azul (versión fácil) y rojo (versión menos fácil). Estos colores ayudarán al facilitador a identificar qué caso se está abordando. Asimismo, el facilitador tendrá una tarjeta con las soluciones, como se muestra a continuación.

Respuestas Juego Negro-M

Lugar

Método Escítala Espartana
Tubo: Rojo-delgado-largo
FUE EN LA BIBLIOTECA MIENTRAS BUSCABA SU
LIBRO FAVORITO

Arma

Método Tablas
Fragmento de Alicia en el País de las Maravillas
dejó el tubo y tomó la llave de tuercas

Personaje

Método Cifrado de Polibio
BA DE AE DE CC AA CB DE BD AE DB
F U E U N A M U J E R

Método Cifrado de César
Traslación No 10
BJALJATXCT
SRACARLOTA

Solución: Biblioteca/Llave de tuercas/Sra.
Cariota



Respuestas Juego Amarillo-F

Lugar

Método Escítala Espartana
Tubo: Verde seco-delgado-mediano
FUE EN EL COMEDOR FUE EN EL COMEDOR

Arma

Método Tablas
Fragmento de Historia Interminable
gritó en ese momento atacó con el candelabro

Personaje

Método Cifrado de Polibio
BA DE AE DE CC BC CD CB AB DB AE
F U E U N H O M B R E

Método Cifrado de César
Traslación No 15
GFOYÑAPC
SRBLANCO

Solución: Comedor/Candelabro/Sr. Blanco



Respuestas Juego Azul-M

Lugar

Método Escítala Espartana
Tubo: Rosado-ancho-largo
OCURRIÓ EN LA SALA DE MÚSICA LO TOMÓ
POR SORPRESA MIENTRAS ENSAYABA EL
RECITAL

Arma

Método Tablas
Fragmento de Alicia en el País de las Maravillas
dejo el tubo y tomo la llave de tuercas

Personaje

Método Cifrado de Polibio
BA DE AE DE CC BC CD CB AB DB AE
F U E U N H O M B R E

Método Cifrado de César
Traslación No 20
LKIAEWFMD
SRPIMENTEL

Solución: Sala de Música/Llave de tuercas/Sr.
Pimentel



Respuestas Juego Rojo-F

Lugar

Método Escítala Espartana
Tubo: Rosado Oscuro-Delgado-Corto
FUE EN LA TARDE EN LA COCINA FUE EN LA
COCINA

Arma

Método Tablas
Fragmento de Historia Interminable
gritó en ese momento atacó con el candelabro

Personaje

Método Cifrado de Polibio
BA DE AE DE CC AA CB DE BD AE DB
F U E U N A M U J E R

Método Cifrado de César
Traslación No 5
WVEVSWW
SRAROSS

Solución: Cocina/Candelabro/Sra. Ross



Cada sobre deberá contener lo siguiente:

1. Juego de cartas de los personajes.
2. Juego de cartas de los utensilios.
3. Juego de cartas de los lugares.
4. Un cifrado de César.
5. Un cifrado de Polibio.
6. 3 tickets

Los sobres, distinguidos por colores, deberán contener lo siguiente:

Amarillo:

1. Fragmento de *La historia interminable*.
2. Hoja con este mensaje: BA DE AE DE CC BC CD CB AB DB AE
3. Hoja con este mensaje: GFOYÑAPC

Rojo:

1. Fragmento de *Alicia en el país de las maravillas*.
2. Hoja con este mensaje: BA DE AE DE CC BC CD CB AB DB AE
3. Hoja con este mensaje: GFOYÑAPC

Negro:

1. Fragmento de *Alicia en el país de las maravillas*.
2. Hoja con este mensaje: BA DE AE DE CC AA CB DE BD AE DB
3. Hoja con este mensaje: WVEVSWW

Azul:

1. Fragmento de *Alicia en el país de las maravillas*.
2. Hoja con este mensaje: BA DE AE DE CC BC CD CB AB DB AE
3. Hoja con este mensaje: LKIAEWMWD

Durante la actividad.

El tallerista ofrecerá una breve introducción a los métodos de cifrado.

A continuación, se formarán cuatro equipos.

Cada equipo recibirá un sobre con el caso a resolver. Dentro de cada sobre encontrarán la misión y una tarjeta con tres boletos. Estos boletos permitirán al equipo solicitar pistas adicionales. Para canjear una pista, el equipo deberá entregar un boleto al facilitador, quien proporcionará ayuda adicional sobre el cifrado adecuado o sugerencias para el uso de los cifrados.

Ejemplos de pistas:

En el caso de la Escítala Espartana: El facilitador guiará la búsqueda de tubos y proporcionará dos opciones al equipo. Para ello, consultará su sobre de facilitador.

En el caso del cifrado de César: El facilitador indicará que el número de traslación para descifrar el mensaje termina en 5 o en 0, según corresponda a la misión. El facilitador deberá consultar su sobre para determinar la pista correcta.

El facilitador comenzará guiando a los integrantes en la búsqueda del lugar del asesinato. Para ello, el método que usarán será la Escítala Espartana. Comenzará explicando el método.

El facilitador posteriormente, les proporcionará tres listones con letras, uno de los cuales contiene el mensaje que revela la ubicación. El desafío consiste en encontrar el tubo adecuado para leer el mensaje correctamente. Para lograrlo, todos los miembros del equipo se acercarán a la zona donde se encuentran los tubos y buscarán el que les permita leer el mensaje

En los espacios laterales del tablero se colocan los posibles lugares.



Una vez descifrado el lugar del asesinato, se coloca la tarjeta en alguno de los tres espacios que se encuentran en el centro del tablero.



Posteriormente, el facilitador instruirá a los jugadores para que procedan a la descripción del utensilio. Para esta tarea, se les proporcionarán tarjetas con fragmentos

literarios, y deberán seleccionar un tarjetón café cuya superposición revele un mensaje codificado. Y se colocarán las tarjetas en los laterales.



¡Qué ganas tenía de dejar la sombría sala y deambular por entre aquellos lechos de rutilantes flores y aquellas frescas fuentes!, pero ni siquiera le entraba la cabeza por el hueco de la puerta; “y en caso de que pasara —pensó Alicia— de poco me serviría sin los hombros. ¡Ah, cómo me gustaría plegarme como un telescopio! Creo que podría, si supiera cómo empezar”. Porque, ya ven, le habían ocurrido últimamente tantas cosas extraordinarias que Alicia empezaba a pensar que muy pocas eran realmente imposibles. Era inútil quedarse allí plantada ante la puertecita, así que volvió a la mesa, con cierta esperanza de hallar encima otra llave o, al menos, un libro con las instrucciones para poder plegarse como un telescopio. Esta vez encontró una botellita (“que por cierto no estaba aquí antes”, se dijo Alicia); tenía atada alrededor del cuello una etiqueta de papel, en mayúsculas bellamente impresas, con la palabra: **Bébe me**.

Fragmento de Alicia en el País de las Maravillas

Bastían no sintió que las lágrimas le corrieran por la cara. Casi sin darse cuenta gritó de pronto:
-¡Hija de la Luna! ¡Voy!
En ese mismo momento ocurrieron muchas cosas simultáneamente. La cáscara del gran huevo fue rota en pedazos por una fuerza tremenda, mientras se oía el oscuro retumbar de un trueno. Comenzó a soplar un viento tempestuoso que surgió de las páginas del libro que Bastían tenía sobre las rodillas, de forma que esas páginas empezaron a revolotear desordenadamente. Bastían sintió la tormenta en el pelo y el rostro, se quedó casi sin aliento, las llamas de las velas del candelabro de siete brazos danzaron y se pusieron horizontales, y entonces un segundo viento tormentoso, más poderoso aún, agitó el libro y apagó todas las luces. El reloj de la torre dio las doce.

Fragmento de la Historia Interminable



Una vez descifrada el arma del asesinato, se coloca la tarjeta en alguno de los dos espacios disponibles que se encuentran en el centro del tablero. Y se regresan las tarjetas descartadas al sobre.



Ahora se toman las tarjetas de los sospechosos y se colocan en los laterales del tablero.



El facilitador indica que tomen de su sobre las siguientes hojas, con el mensaje oculto.

¿Quién es el culpable?

BA DE AE DE CC AA CB DE BD AE DB

¿Quién es el culpable?

BA DE AE DE CC BC CD CB AB DB AE



Para descifrar la tercera pista el método que se usará será el cifrado de Polibio. El tallerista explicará el método. Con este mensaje los jugadores han acotado la búsqueda. Para finalizar se les indica a los jugadores que utilicen las siguientes hojas:

¿Quién es el culpable?

LKIAEFMWD



¿Quién es el culpable?

WVEVSWW



¿Quién es el culpable?

GFOYÑAPC

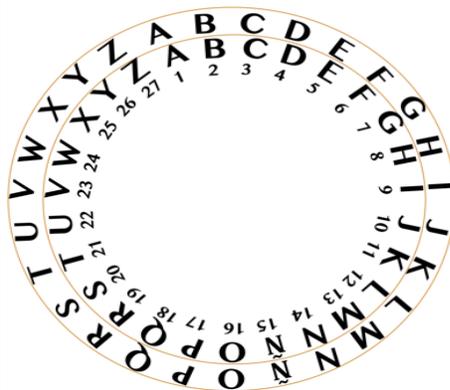


¿Quién es el culpable?

BJALJATXCT



Para descifrar la cuarta pista el método que se usará será Cifrado de César. El facilitador explicará el método.



Una vez descifrado el asesino, se coloca la tarjeta en el último lugar disponible del centro del tablero. Y se regresan las tarjetas descartadas al sobre.



El tallerista revela el misterio y verifica que cada equipo tenga la respuesta correcta. El tallerista concluye explicando métodos actuales de encriptación.

Observaciones:

1. Se pueden hacer variaciones del juego; la forma más sencilla de hacerlo es a través del cifrado de César y de Polibio.
2. Una segunda parte del juego es que los participantes ahora cifren los mensajes y creen un nuevo caso.

Bibliografía

- Teixes Argilés, F.(2016) Gamificación: Motivar jugando. Editorial UOC.
- García Lázaro, D. Jiménez Torres, A. I. (2016) *El proceso de gamificación en el aula: Las matemáticas en educación infantil*. GRIN Verlag.
- González Vasco, M.I. (2018) *Las matemáticas de la criptología. Secretos demostrables y demostraciones secretas..* Los libros de la Catarata.
- Báez Hernández, M. G. (2022). Anexo_Secretos y mensajes ocultos. https://drive.google.com/drive/folders/1dNcnod7Inp8_XIIXmzPrto-NZjuMz4Rz?usp=sharing