

# Aplicación y Enseñanza de la Criptografía a los Niños y Adolescentes

Jordan Andrés Elizondo Umaña  
Escuela de Ingeniería en Sistemas de Computación  
Universidad Internacional San Isidro Labrador  
San José, Costa Rica  
elizondojordan96@gmail.com

**Resumen** — En el presente trabajo, se da a conocer que la criptografía, es una disciplina esencial en la seguridad de la información, que ha adquirido una relevancia cada vez mayor en la era digital. La aplicación y enseñanza de la criptografía a los niños es una iniciativa que busca fomentar la comprensión de la seguridad digital desde una edad temprana, desarrollando habilidades críticas y analíticas que serán fundamentales en su vida futura.

Este artículo explora diversas metodologías y herramientas didácticas diseñadas para enseñar conceptos criptográficos básicos a los niños de manera interactiva y accesible. Además, se analizan los beneficios educativos y el impacto positivo en la alfabetización digital infantil.

A través de juegos, actividades prácticas y aplicaciones educativas, se demuestra cómo los niños pueden aprender sobre cifrado, descifrado y la importancia de proteger la información personal en línea. Este enfoque no solo prepara a los jóvenes para enfrentar los desafíos de la seguridad cibernética, sino que también inspira a una nueva generación de entusiastas de la tecnología y la seguridad informática.

**Palabras claves** — *Criptografía, Metodología, Seguridad cibernética, Alfabetización digital, Seguridad informática, Aplicación, Metodología.*

**Abstract** — In this paper, it is revealed that cryptography is an essential discipline in information security, which has gained increasing relevance in the digital age. The application and teaching of cryptography to children is an initiative that aims to foster an understanding of digital security from an early age, developing critical and analytical skills that will be fundamental in their future lives.

This article explores various methodologies and didactic tools designed to teach basic cryptographic concepts to children in an interactive and accessible way. Additionally, the educational benefits and positive impact on children's digital literacy are analyzed.

Through games, practical activities, and educational applications, it is demonstrated how children can learn about encryption, decryption, and the importance of protecting personal information online. This approach not only prepares young people to face the challenges of cybersecurity but also inspires a new generation of technology and information security enthusiasts.

**Keywords** — *Cryptography, Methodology, Cybersecurity, Digital Literacy, Information Security, Application, Methodology.*

## I. INTRODUCCIÓN

El presente artículo muestra la experiencia obtenida del curso Criptografía, en el cual, se buscó aplicar el contenido del programa enfocado a los niños y adolescentes y el tema correspondiente, proporcionando un análisis detallado sobre la falta del conocimiento en criptografía, subrayando la vulnerabilidad ante posibles ataques cibernéticos que comprometen la seguridad de la información y seguridad a nuestros niños y adolescentes, ofreciendo respuestas prácticas a un problema urgente en el ámbito de la seguridad informática, brindando a los niños y adolescentes bases claras y así adquieran una amplia gama de conocimiento donde pueda aplicarlo en su vida diaria. Aplicando distintos métodos para reforzar la seguridad de datos personales y así evitar que puedan extraer información sensible y evitar otros tipos de ataques cibernéticos.

En la era digital actual, la seguridad de la información se ha convertido en un pilar fundamental para la protección de datos personales y corporativos. La criptografía, es una ciencia dedicada a la codificación y protección de información, juega un papel crucial en este contexto. Sin embargo, la enseñanza de estos conceptos generalmente se reserva para niveles

educativos superiores, dejando un vacío en la educación temprana sobre seguridad digital.

La aplicación y enseñanza de la criptografía a los niños busca cerrar esta brecha, proporcionando a los jóvenes las herramientas y conocimientos necesarios para comprender y valorar la importancia de la seguridad de la información desde una edad temprana. Al introducir conceptos criptográficos básicos de manera interactiva y accesible, se fomenta el desarrollo de habilidades críticas y analíticas que serán esenciales en su vida futura.

El objetivo de este artículo es explorar cómo se puede enseñar criptografía a los niños de manera efectiva y divertida. A través de diversas variedades de métodos y recursos, desde juegos y actividades prácticas hasta aplicaciones y libros interactivos, los niños pueden descubrir el fascinante mundo de los códigos y los mensajes secretos donde se puede aprender practicando en línea con herramientas creadas por usuarios para el aprendizaje rápido e interactivo. No solo los prepara para un futuro en el que la seguridad digital será cada vez más importante, sino que también les proporciona herramientas valiosas para su desarrollo intelectual y personal.

Este enfoque educativo no solo prepara a los niños para enfrentar los desafíos de la ciberseguridad, sino que también les proporciona una base sólida para la alfabetización digital, un componente cada vez más indispensable en el mundo moderno. A través de actividades lúdicas, juegos y aplicaciones educativas, los niños pueden aprender sobre cifrado, descifrado y la protección de la información personal en línea, despertando su interés por la tecnología y la seguridad informática.

En un mundo cada vez más digitalizado, la seguridad de la información se ha convertido en una preocupación primordial. Desde proteger datos personales en las redes sociales hasta asegurar transacciones financieras en línea, la criptografía juega un papel crucial en mantener nuestra información segura. La criptografía, el arte y la ciencia de escribir y resolver códigos, no es solo un campo de estudio reservado para los expertos en seguridad informática; también tiene aplicaciones educativas valiosas, especialmente

cuando se introduce a los niños desde una edad temprana.

Este artículo explora diversas metodologías y herramientas didácticas diseñadas específicamente para enseñar criptografía a los niños, analizando los beneficios educativos y el impacto positivo en su desarrollo digital. Al inspirar una nueva generación de entusiastas de la tecnología y la seguridad informática, se sientan las bases para un futuro más seguro y consciente en el ámbito digital.

## II. METODOLOGÍA

La metodología de este estudio sobre la aplicación y enseñanza de la criptografía a los niños se desarrolló en varias fases, combinando diferentes enfoques para obtener una visión integral de su efectividad y aceptación.

### 1. Revisión Bibliográfica

Se llevó a cabo una revisión exhaustiva de la literatura existente sobre educación en criptografía, seguridad digital y alfabetización digital en niños. Esta revisión incluyó artículos académicos, libros, informes técnicos y recursos educativos en línea. El objetivo fue identificar las metodologías y herramientas más efectivas utilizadas en la enseñanza de la criptografía a niños y adolescentes.

### 2. Diseño del Programa Educativo

Se diseñó un programa educativo que incluye actividades lúdicas, juegos interactivos y aplicaciones educativas. El programa se estructuró en módulos, cada uno enfocado en un concepto clave de la criptografía:

- **Introducción a la Criptografía:** Conceptos básicos y la importancia de la seguridad de la información.
- **Cifrado y Descifrado:** Métodos sencillos de cifrado como el cifrado César y el cifrado por sustitución.
- **Clave Secreta:** Importancia de las contraseñas y cómo crear contraseñas seguras.
- **Aplicaciones Prácticas:** Uso de herramientas y aplicaciones educativas para practicar lo aprendido.

### 3. Implementación Piloto

El programa educativo se implementó de manera piloto en dos escuelas primarias, seleccionadas por su disposición a participar y por tener un enfoque tecnológico en su currículo. Se seleccionaron grupos de niños, asegurando una diversidad de género y antecedentes socioeconómicos.

### 4. Recolección de Datos

Se utilizaron múltiples métodos para recolectar datos:

- **Observación Directa:** Los investigadores observaron las sesiones educativas, tomando notas sobre la participación, el interés y la comprensión de los niños.
- **Encuestas:** Se aplicaron encuestas pre y post intervención a los niños y a los maestros para medir el cambio en el conocimiento y las actitudes hacia la criptografía y la seguridad digital.
- **Entrevistas:** Se realizaron entrevistas semiestructuradas con los maestros y algunos padres para obtener una comprensión más profunda de las percepciones y el impacto del programa.

### 5. Análisis de Datos

Los datos recolectados se analizaron utilizando técnicas estadísticas para evaluar el impacto del programa en el conocimiento y habilidades de los niños en criptografía. Se utilizó análisis cualitativo para identificar temas recurrentes en las observaciones, encuestas y entrevistas.

### 6. Evaluación y Mejora del Programa

Con base en los resultados del análisis, se evaluaron los puntos fuertes y las áreas de mejora del programa educativo. Se realizaron ajustes y mejoras para aumentar su efectividad y accesibilidad, con el objetivo de implementarlo a mayor escala en el futuro.

### 7. Difusión de Resultados

Los resultados del estudio se documentaron en el presente artículo, destacando las metodologías más efectivas y los beneficios educativos

observados. Se proponen recomendaciones para la implementación de programas similares en otras instituciones educativas, con el fin de promover la enseñanza de la criptografía y la seguridad digital desde una edad temprana.

## III. DESARROLLO

En criptografía, el cifrado es el proceso de codificación de la información. Este proceso convierte la representación original de la información, conocida como texto plano, en una forma alternativa conocida como texto cifrado. En el mejor de los casos, sólo las partes autorizadas pueden descifrar un texto cifrado para convertirlo en texto plano y acceder a la información original. El cifrado no impide por sí mismo las interferencias, pero niega el contenido inteligible a un posible interceptor.

Por razones técnicas, un esquema de cifrado suele utilizar una clave de cifrado pseudoaleatoria generada por un algoritmo. Es posible descifrar el mensaje sin poseer la clave, pero, para un esquema de encriptación bien diseñado, se requieren considerables recursos computacionales y habilidades. Un destinatario autorizado puede descifrar fácilmente el mensaje con la clave proporcionada por el emisor a los destinatarios, pero no a los usuarios no autorizados.

La criptografía es una práctica que consiste en proteger información mediante el uso de algoritmos codificados, hashes y firmas. La información puede estar en reposo (como un archivo ubicado en un disco duro), en tránsito (una comunicación electrónica intercambiada entre dos o más partes) o en uso (mientras se ejecutan operaciones de computación con los datos). La criptografía tiene cuatro objetivos principales:

- **Confidencialidad:** Poner la información únicamente a disposición de usuarios autorizados.
- **Integridad:** Asegurar que la información no se ha manipulado.
- **Autenticación:** Confirmar la autenticidad de la información o de la identidad de un usuario.
- **No repudio:** Evitar que un usuario deniegue compromisos o acciones previas.

La criptografía utiliza varios algoritmos criptográficos de bajo nivel para lograr uno o más de dichos objetivos de seguridad de la información. Estas herramientas incluyen algoritmos de cifrado, algoritmos de firma digital, algoritmos de hash y otras funciones.

En el campo de la criptografía muchas veces se agrupan conjuntos de funcionalidades que tienen alguna característica común y a ese conjunto lo denominan 'Criptografía de' la característica que comparten. Veamos algunos ejemplos:

I. Criptografía simétrica: Agrupa aquellas funcionalidades criptográficas que se apoyan en el uso de una sola clave.

II. Criptografía de clave pública o Criptografía asimétrica: Agrupa aquellas funcionalidades criptográficas que se apoyan en el uso de parejas de claves compuesta por una clave pública, que sirve para cifrar, y por una clave privada, que sirve para descifrar.

III. Criptografía con umbral: Agrupa aquellas funcionalidades criptográficas que se apoyan en el uso de un umbral de participantes a partir del cual se puede realizar la acción.

IV. Criptografía basada en identidad: Es un tipo de Criptografía asimétrica que se basa en el uso de identidades.

- ❖ Criptografía basada en certificados
- ❖ Criptografía sin certificados
- ❖ Criptografía de clave aislada
- ❖ Evaluación de la seguridad de un sistema criptográfico

El objetivo de un sistema criptográfico es dotar de seguridad. Por tanto, para calibrar la calidad de un sistema criptográfico es necesario evaluar la seguridad que aporta dicho sistema.

#### Criptografía para niños

La criptografía se ha definido, tradicionalmente, como el ámbito de la criptología que se ocupa de las técnicas de cifrado o codificado destinadas a alterar las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados. Estas técnicas se utilizan tanto en el arte como en la ciencia y en la tecnología. Por tanto, el único objetivo de la criptografía era conseguir la confidencialidad de

los mensajes, para lo cual se diseñaban sistemas de cifrado y códigos, y la única criptografía existente era la llamada criptografía clásica, donde se ocultaba tanto el algoritmo como la clave criptográfica

La aparición de la informática y el uso masivo de las comunicaciones digitales, han producido un número creciente de problemas de seguridad. Las transacciones que se realizan a través de la red pueden ser interceptadas y, por tanto, la seguridad de esta información debe garantizarse. Este desafío ha generalizado los objetivos de la criptografía para ser la parte de la criptología que se encarga del estudio de los algoritmos, protocolos (se les llama protocolos criptográficos), y sistemas que se utilizan para proteger la información y dotar de seguridad a las comunicaciones y a las entidades que se comunican.

Para ello los criptógrafos investigan, desarrollan y aprovechan técnicas matemáticas que les sirven como herramientas para conseguir sus objetivos. Los grandes avances producidos en el mundo de la criptografía han sido posibles gracias a la evolución que se ha producido en el campo de la matemática y la informática.

La criptografía actualmente se encarga del estudio de los algoritmos, protocolos y sistemas que se utilizan para dotar de seguridad a las comunicaciones, a la información y a las entidades que se comunican. El objetivo de la criptografía es diseñar, implementar, implantar, y hacer uso de sistemas criptográficos para dotar de alguna forma de seguridad. Por tanto, el tipo de propiedades de las que se ocupa la criptografía son, por ejemplo:

- ❖ Confidencialidad: Es decir, garantiza que la información sea accesible únicamente a personal autorizado. Para conseguirlo utiliza códigos y técnicas de cifrado.
- ❖ Integridad: Es decir, garantiza la corrección y completitud de la información. Para conseguirlo puede usar por ejemplo funciones hash criptográficas MDC, protocolos de compromiso de bit, o protocolos de notaría electrónica.
- ❖ Vinculación: Permite vincular un documento o transacción a una persona o

un sistema de gestión criptográfico automatizado. Cuando se trata de una persona, se trata de asegurar su conformidad respecto a esta vinculación (content commitment) de forma que pueda entenderse que la vinculación gestionada incluye el entendimiento de sus implicaciones por la persona.

- ❖ Autenticación: Es decir proporciona mecanismos que permiten verificar la identidad del comunicador. Para conseguirlo puede usar por ejemplo función hash criptográfica MAC o protocolo de conocimiento cero.

Soluciones a problemas de la falta de simultaneidad en la telefirma digital de contratos. Para conseguirlo puede usar por ejemplo protocolos de transferencia inconsciente.

Un sistema criptográfico es seguro respecto a una tarea si un adversario con capacidades especiales no puede romper esa seguridad, es decir, el atacante no puede realizar esa tarea específica.

### **Formas de romper la seguridad**

Hay básicamente tres formas de romper la seguridad de un sistema criptográfico:

- ✓ Atacar la criptografía subyacente: Es lo que sería un ataque teórico a los mecanismos criptográficos usados.
- ✓ Atacar la implementación concreta: La criptografía puede ser implementada en software o en hardware. Es bastante probable que las implementaciones concretas tengan vulnerabilidades que se pueden aprovechar. También las vulnerabilidades se podrían introducir de forma deliberada y de esta forma proporcionar puertas traseras disponibles para ser utilizadas.
- ✓ Atacar el lado humano: Muchas veces en los sistemas criptográficos hay personas o entidades que tienen privilegios especiales. Presionando a estas personas o entidades para que nos den acceso a recursos o a información privilegiada, podríamos vulnerar la seguridad del sistema

Introducir a los niños a la criptografía no solo les proporciona una comprensión temprana de la seguridad de la información, sino que también fomenta habilidades importantes como el pensamiento crítico, la resolución de problemas y la lógica. Al aprender sobre criptografía, los niños pueden desarrollar una mentalidad analítica y un enfoque metódico para abordar desafíos complejos que vayan a tener en el futuro. Además, la criptografía ofrece una manera divertida y atractiva de explorar conceptos matemáticos y científicos, convirtiendo el aprendizaje en una experiencia didáctica, práctica y educativa.

Existen diferentes herramientas que discutiremos, diversas estrategias y recursos que los padres y educadores pueden utilizar para la enseñanza de la criptografía a los niños. Desde juegos de cifrado y descifrado hasta actividades prácticas y aplicaciones educativas, exploraremos métodos que hacen que el aprendizaje de la criptografía sea accesible, rápido y emocionante para los más jóvenes y niños. También proporcionaremos ejemplos prácticos de actividades que se pueden realizar en el aula o en casa, así como una lista de recursos útiles que incluyen libros, sitios web y aplicaciones diseñadas para enseñar criptografía a los niños.

Enseñar criptografía a los niños no solo es posible, sino también beneficioso en múltiples aspectos. A través de la combinación de teorías y prácticas, los niños pueden aprender los principios básicos de la criptografía y aplicarlos de manera creativa y divertida. Este artículo nos podrá servir como una guía para aquellos interesados en integrar la criptografía en la educación de los niños y jóvenes, destacando la importancia de esta disciplina en el contexto actual y proporcionando las herramientas necesarias para hacerlo de manera efectiva.

Figura 1: La máquina Enigma utilizada por los alemanes durante la II Guerra Mundial.



Fuente: Elaboración Propia

### ¿Por qué los niños deberían aprender a codificar con Tynker?

Debido a que la tecnología está tan integrada en prácticamente todos los aspectos de nuestras vidas, aprender sobre ella es más importante que nunca. Nuestra plataforma de codificación hace que sea conveniente y divertido para los niños y adolescentes adquirir conocimientos que les serán útiles durante toda su vida. Puede contar con nuestros métodos confiables para ayudarlos a desarrollar y hacer crecer sus capacidades con las computadoras.

Sin embargo, Tynker no es solo para escuelas y campamentos de programación. Los padres que valoran la educación STEM y quieren que sus hijos sepan cómo codificar deben saber que nuestra plataforma de programación para niños también se puede usar en casa. Tynker ofrece una variedad de soluciones de codificación para niños con codificación de íconos para prelectores, codificación basada en bloques y cursos avanzados en Python, JavaScript, ciencia de datos, arte y procesamiento de imágenes. Hay planes trimestrales, anuales y de por vida que incluyen acceso para hasta 3 niños, y nuestras clases en línea para todas las edades son una excelente

manera de que adquieran las habilidades STEM complementarias necesarias para su futuro.

### Métodos de Enseñanza de la Criptografía a los Niños

Enseñar criptografía a los niños requiere un enfoque creativo que combine teoría con actividades prácticas. Aquí te presento algunas técnicas efectivas para enseñar criptografía a niños, adaptadas a diferentes niveles de complejidad y edades.

1. Juegos de Cifrado y Descifrado: Los juegos son una forma excelente de introducir a los niños a la criptografía. Pueden comenzar con métodos sencillos como el cifrado César, donde cada letra en un mensaje se desplaza un número fijo de posiciones en el alfabeto. Ejemplo:

- Cifrado César: Pide a los niños que cifren mensajes simples usando un desplazamiento de 3 o 4 letras y luego intercambien los mensajes para que sus compañeros los descifren.
- Códigos de Sustitución: Usa un alfabeto codificado donde cada letra se reemplaza por un símbolo o una letra diferente. Los niños pueden crear sus propios códigos y enviarse mensajes entre sí.
- Rueda de Cifrado: Crear una rueda de cifrado con papel y cartulina para enseñar el cifrado César de manera visual y práctica.

2. Manualidades y Proyectos Prácticos: Las manualidades ayudan a los niños a comprender conceptos abstractos mediante la creación de dispositivos simples que pueden usar para cifrar y descifrar mensajes. Ejemplos:

- Rueda de Cifrado: Ayuda a los niños a crear una rueda de cifrado con papel y cartulina. La rueda permite cifrar y descifrar mensajes desplazando el alfabeto.
- Escítala Griega: Los niños pueden construir una escítala, un dispositivo utilizado por los antiguos griegos para enviar mensajes cifrados, enrollando una tira de papel alrededor de un cilindro (como un lápiz) y escribiendo un mensaje. Cuando la tira se desenrolla, el mensaje se vuelve ilegible hasta que se

vuelve a enrollar en un cilindro del mismo tamaño.

3. Juegos de Rol: Los juegos de rol permiten a los niños sumergirse en historias donde juegan el papel de espías o detectives que necesitan enviar y recibir mensajes secretos. Ejemplos:

- Misión de Espías: Organiza una actividad donde los niños asuman el papel de espías que deben usar códigos para comunicarse sin ser detectados. Puedes crear un escenario donde tengan que encontrar pistas y descifrar códigos para completar su misión.
- Detectives de Códigos: Los niños pueden resolver misterios utilizando diferentes técnicas de cifrado para descifrar pistas y llegar a la solución.

4. Aplicaciones y Juegos Digitales: Las aplicaciones y juegos educativos pueden hacer que aprender criptografía sea divertido y accesible, proporcionando un entorno interactivo donde los niños pueden experimentar con códigos y cifrados. Ejemplos:

- "Crypto Kids" de la NSA: Esta aplicación ofrece juegos y actividades que enseñan a los niños conceptos básicos de criptografía de manera interactiva.
- Aplicaciones de Codificación: Aplicaciones como "Tynker" o "Lightbot" no se centran exclusivamente en la criptografía, pero enseñan conceptos básicos de codificación que son fundamentales para entender la criptografía.
- Juegos en Línea: Utilizar juegos interactivos en línea que enseñan criptografía.

5. Historias y Metáforas: Utilizar historias y metáforas ayuda a los niños a entender conceptos complejos de manera sencilla y atractiva. Ejemplos:

- "La Llave y el Candado": Explica la criptografía utilizando la metáfora de una llave y un candado. El mensaje es la caja,

la clave es la llave, y el cifrado es el candado que protege la caja.

- Cuentos Criptográficos: Escribe o lee historias donde los personajes usen códigos secretos para superar desafíos. Los niños pueden luego recrear las técnicas descritas en la historia.

6. Actividades de Grupo: Las actividades en grupo promueven la colaboración y el aprendizaje conjunto, permitiendo que los niños trabajen juntos para resolver problemas criptográficos. Ejemplos:

- Caza del Tesoro con Códigos: Organiza una caza del tesoro donde las pistas estén cifradas. Los niños deberán trabajar en equipo para descifrar las pistas y encontrar el tesoro.
- Competencias de Descifrado: Forma equipos y da a cada equipo una serie de mensajes cifrados que deben descifrar en el menor tiempo posible. Esto fomenta la colaboración y la competencia amistosa.

7. Integración con Otras Materias: La criptografía se puede integrar con otras materias como matemáticas, historia, y ciencias para hacer el aprendizaje más relevante y multidisciplinario. Ejemplos:

- Matemáticas y Cifrado: Utiliza la criptografía para enseñar conceptos matemáticos como el álgebra modular, que es fundamental para entender ciertos tipos de cifrados.
- Historia de la Criptografía: Relaciona las lecciones de criptografía con eventos históricos, como el uso del código Enigma en la Segunda Guerra Mundial, para enseñar a los niños sobre la importancia histórica de los códigos.

8. Libros y Recursos Educativos: Los libros y recursos educativos pueden proporcionar un marco estructurado para enseñar criptografía, con actividades y explicaciones adaptadas para niños. Ejemplos:

- "Secret Coders" de Gene Luen Yang: Un libro que combina historias de misterio con lecciones de codificación y criptografía, ideal para niños que disfrutan de la lectura.

- Guías y Recursos en Línea: Utiliza recursos como Khan Academy o CS Unplugged que ofrecen actividades diseñadas específicamente para enseñar criptografía a los niños.

9. Presentaciones Visuales: Las presentaciones visuales, como videos y gráficos, pueden ayudar a explicar conceptos abstractos de manera más tangible. Ejemplos:

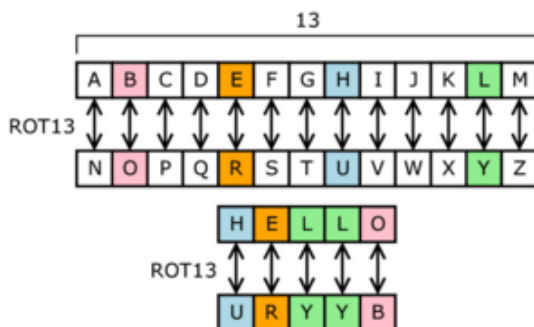
- Videos Educativos: Muestra videos animados que explican cómo funcionan diferentes técnicas de cifrado.
- Gráficos y Diagramas: Utiliza gráficos para visualizar cómo las letras y los números se transforman durante el proceso de cifrado y descifrado.

10. Evaluaciones y Retroalimentación: Es importante evaluar la comprensión de los niños a través de pruebas divertidas o desafíos, y dar retroalimentación para reforzar lo aprendido. Ejemplos:

- Quiz de Criptografía: Crea un quiz con preguntas sobre los conceptos que han aprendido, utilizando formatos de opción múltiple, verdadero/falso y preguntas de descifrado.
- Retroalimentación Constructiva: Al final de cada actividad, discute con los niños lo que aprendieron, lo que les resultó fácil o difícil, y cómo podrían mejorar.

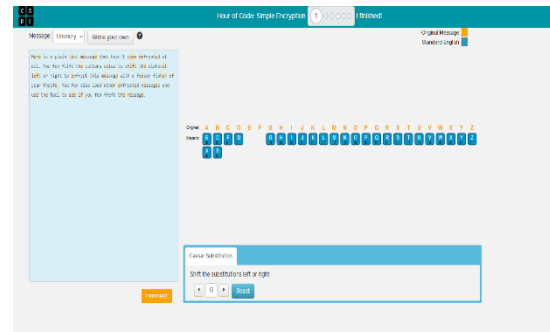
Estas técnicas no solo enseñan a los niños sobre criptografía, sino que también hacen que el proceso de aprendizaje sea interactivo, atractivo y lleno de diversión.

Figura 2: Cifrado por sustitución para niños



Fuente: Elaboración Propia

Figura 3: En la siguiente imagen podemos observar un texto donde tenemos el abecedario y donde podemos cambiar las diferentes letras del abecedario y poder tener un mensaje totalmente diferente con solo tener que cambiar letras al azar.



Fuente: Herramientas para la enseñanza de la criptografía para los niños. Elaboración Propia.

### Técnicas de Enseñanza cual es la más efectiva

La efectividad de las técnicas de enseñanza de la criptografía a los niños puede variar según la edad, el estilo de aprendizaje y los intereses de cada niño. Sin embargo, en términos generales, una de las técnicas más efectivas es la combinación de juegos de cifrado y descifrado con actividades prácticas.

¿Por qué es tan efectiva esta combinación?

1. Aprendizaje Activo: Los juegos de cifrado y descifrado permiten que los niños participen activamente en el proceso de aprendizaje. En lugar de ser meros receptores de información, se convierten en solucionadores de problemas, lo que refuerza su comprensión de los conceptos criptográficos.
2. Divertido y Motivador: Los juegos son inherentemente motivadores para los niños. El desafío de cifrar un mensaje y ver si sus compañeros pueden descifrarlo introduce un elemento de competencia sana y diversión que mantiene a los niños comprometidos.
3. Refuerzo Práctico: Al combinar los juegos con actividades prácticas, como la creación de una rueda de cifrado o una



escítala, los niños no solo entienden el concepto en teoría, sino que también lo ven en acción. Esto refuerza el aprendizaje a través de la experimentación y la manipulación física de objetos.

4. Desarrollo de Habilidades Cognitivas: Estas técnicas ayudan a desarrollar habilidades cognitivas clave como el pensamiento crítico, la lógica y la resolución de problemas, que son fundamentales para comprender la criptografía.
5. Adaptabilidad: Los juegos y las actividades prácticas son muy adaptables. Pueden ajustarse fácilmente para ser más simples o más complejos según el nivel de los niños, lo que los hace adecuados para una amplia gama de edades y habilidades.

Ejemplo Práctico:

Cifrado César + Rueda de Cifrado:

- Paso 1: Se introduce a los niños al concepto del Cifrado César con un juego donde deben descifrar un mensaje desplazando las letras del alfabeto.
- Paso 2: Luego, se brinda guía a los niños para que construyan su propia rueda de cifrado, que pueden usar para cifrar y descifrar mensajes. Este dispositivo tangible ayuda a solidificar el concepto en sus mentes.
- Paso 3: Los niños pueden intercambiar mensajes codificados entre ellos, utilizando sus ruedas de cifrado para descubrir los mensajes secretos.

Figura 4: Ejemplo de Encuesta

Se realiza evaluación del Conocimiento de los Niños sobre Criptografía

Objetivo: Evaluar el nivel de conocimiento y comprensión de los niños sobre la criptografía y su relevancia en la seguridad digital.

#### Preguntas de la Encuesta

1. ¿Has escuchado alguna vez la palabra "criptografía"?

- Sí
- No

2. Si respondiste "Sí", ¿qué crees que significa criptografía?

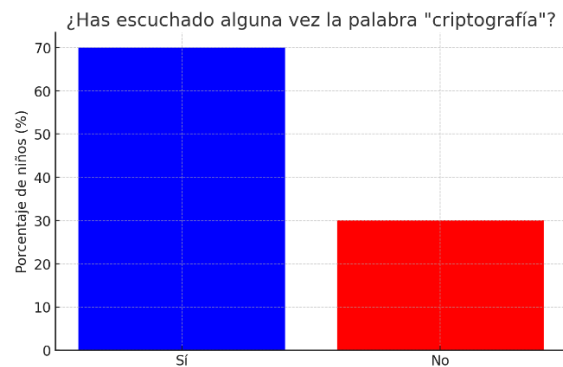
- Algo relacionado con matemáticas
- Algo relacionado con secretos y códigos
- No estoy seguro/a
- Otro (especificar): \_\_\_\_\_

3. ¿Crees que la criptografía es importante para mantener segura la información en Internet?

- Sí
- No
- No lo sé

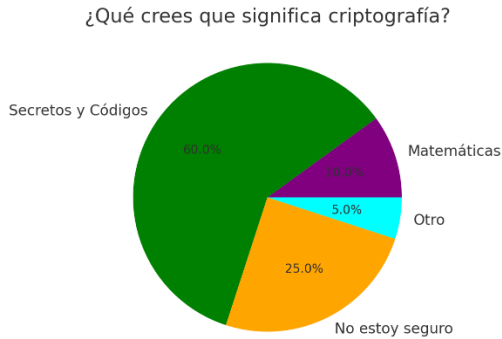
4. ¿Te gustaría aprender más sobre cómo funciona la criptografía?

- Sí
- No
- Tal vez



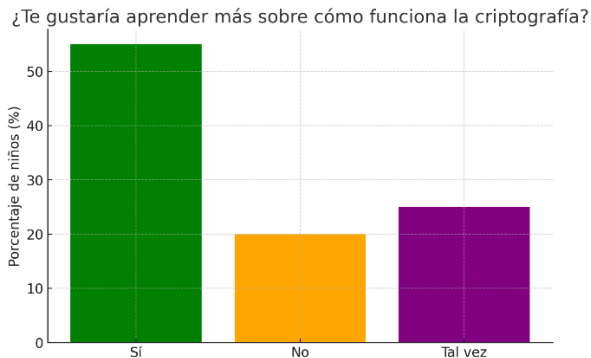
Fuente: Fuente: Propia (2024)

Figura 5: Ejemplo de Encuesta



Fuente: Propia (2024)

Figura 6: Ejemplo de Encuesta



Fuente: Elaboración Propia

#### IV. DISCUSION DE RESULTADOS

Este estudio ha demostrado que la criptografía, como disciplina clave en la protección de la información en la era digital, no solo debe ser comprendida por expertos, sino también inculcada desde una edad temprana. La enseñanza de conceptos criptográficos a los niños no solo refuerza su alfabetización digital, sino que también desarrolla habilidades críticas y analíticas que serán fundamentales en su vida futura. A través de metodologías interactivas y accesibles, los niños pueden aprender sobre la importancia de proteger su información personal y los principios básicos de cifrado y descifrado.

Esta iniciativa no solo los prepara para enfrentar los desafíos de la seguridad cibernética, sino que también inspira a una nueva generación de entusiastas de la tecnología y la seguridad informática. Fomentar el aprendizaje de la criptografía desde la infancia contribuirá a una sociedad más consciente y preparada para proteger su información en un mundo cada vez más digitalizado.

Además, los resultados obtenidos de la implementación de métodos didácticos muestran que los niños, incluso a edades tempranas, pueden comprender los conceptos básicos de la criptografía, como cifrado y descifrado. Se observó que, a través de actividades prácticas y juegos interactivos, los niños demostraron una mayor retención y comprensión de estos conceptos en comparación con métodos de enseñanza más tradicionales. Este hallazgo respalda la idea de que la enseñanza de la criptografía no tiene que ser una disciplina reservada solo para niveles educativos avanzados.

Este aumento en la conciencia sobre la seguridad cibernética sugiere que la enseñanza temprana de la criptografía podría ser una herramienta poderosa para preparar a los jóvenes para un entorno digital cada vez más complejo.

El estudio también reveló que la enseñanza de la criptografía contribuyó al desarrollo de habilidades críticas y analíticas en los niños. Al enfrentarse a desafíos criptográficos tuvieron que emplear el pensamiento lógico y la resolución de problemas, habilidades que son fundamentales no solo en la informática, sino en una variedad de disciplinas académicas. Estos resultados son consistentes con la literatura existente, que sugiere que la educación en tecnología y ciencias aumenta el pensamiento crítico en los niños.

Los hallazgos de este estudio tienen importantes implicaciones para el futuro de la educación en seguridad digital. La introducción temprana de la criptografía no solo equipa a los niños con habilidades técnicas, sino que también fomenta una mentalidad de seguridad que será crucial a medida que crecen en un mundo digitalizado. Además, estos resultados sugieren que la criptografía podría integrarse de manera efectiva en los currículos escolares como parte de una educación tecnológica más amplia.

En resumen, la aplicación y enseñanza de la criptografía a los niños ha demostrado ser una iniciativa valiosa con múltiples beneficios educativos. A medida que la tecnología sigue avanzando y desempeñando un papel central en la vida diaria, equipar a las futuras generaciones con conocimientos en criptografía y seguridad digital desde una edad temprana podría ser clave para enfrentar los desafíos cibernéticos del futuro. Es fundamental continuar investigando y refinando estas metodologías para maximizar su efectividad y accesibilidad en contextos educativos diversos.

## REFERENCIAS

- [1] Resnick, M. (2017). *Lifelong Kindergarten: Cultivating Creativity through Projects, Passion, Peers, and Play*. MIT Press.
- [2] Bell, T., Witten, I. H., & Fellows, M. (2015). *Computer Science Unplugged: Enrichment and Extension*. Computer Science Unplugged.
- [3] Papert, S. (1980). *Mindstorms: Children, Computers, and Powerful Ideas*. Basic Books.
- [4] Levitin, A., & Papalaskari, M. A. (2002). *Algorithmic Puzzles*. Oxford University Press.
- [5] Yang, G. L. (2015). *Secret Coders*. First Second Books.