CryptoPlayground: plataforma interactiva para aprender sobre fundamentos y esquemas de cifrado criptográficos

Edgar Andres Torres Perez, Juan Pablo Vargas Rodriguez
edgarat@uninorte.edu.co, vargasjp@uninorte.edu.co,

I. Introducción

Durante los últimos años, el campo de la criptografía se ha vuelto esencial para garantizar la seguridad de la información y las comunicaciones. Lo que antes era visto como un conocimiento reservado para especialistas, hoy es una competencia fundamental para cualquier profesional de la informática. Sin embargo, su enseñanza sigue representando un desafío, ya que muchos de sus fundamentos se basan en matemáticas avanzadas. Para los estudiantes con poca formación en esta área, el aprendizaje de la criptografía puede resultar intimidante.

A partir del desarrollo de nuevas amenazas cibernéticas, los enfoques didácticos basados en la experimentación y el uso de herramientas interactivas pueden hacer que los conceptos sean más accesibles y comprensibles (Adamovic et al., 2011).

Recientemente, a medida que los ataques cibernéticos se vuelven más frecuentes y sofisticados, la necesidad de expertos en seguridad informática es más urgente que nunca. Las universidades y centros de formación tienen la responsabilidad de integrar la criptografía en sus planes de estudio, asegurando que los futuros profesionales desarrollen las habilidades necesarias para proteger sistemas y datos sensibles. Al hacerlo, no solo fortalecen la formación académica, sino que también contribuyen a la creación de un entorno digital más seguro y resistente a amenazas (Gavirova, 2024).

Varios trabajos se han desarrollado en el campo de la educación criptográfica, y la revisión de la literatura extraída desde las bases de datos da cuenta de que la enseñanza de la criptografía enfrenta el reto de mantenerse al día con el avance de las amenazas cibernéticas y la creciente necesidad de profesionales capacitados. Es por ello que la integración de gamificación y herramientas interactivas en la educación ha demostrado ser una estrategia efectiva para mejorar el compromiso de los estudiantes y fomentar una comprensión más profunda de los conceptos criptográficos. Incorporar tecnologías como la simulación y el aprendizaje basado en la práctica puede hacer que estos temas sean más accesibles y aplicables en escenarios reales, promoviendo un enfoque más dinámico e intuitivo del aprendizaje (Huitema & Wong, 2025).

El propósito se centra en encontrar alternativas para facilitar el proceso de enseñanza y aprendizaje de la criptografía mediante la integración de tecnologías emergentes y el desarrollo de sistemas inteligentes que permitan a los estudiantes experimentar con conceptos complejos de manera intuitiva.

Con esto en mente, el presente proyecto tiene como propósito desarrollar un prototipo de aplicación web llamado CryptoPlayground, un entorno interactivo diseñado para enseñar criptografía de forma práctica y accesible. A través de una experiencia dinámica y ejercicios, los usuarios podrán experimentar con algoritmos de cifrado, logrando un aprendizaje más profundo y significativo.

II. Descripción del Problema

La criptografía es un componente esencial en la protección de los sistemas de información modernos, y comprender los algoritmos, sistemas y protocolos criptográficos actuales es una habilidad fundamental en la era digital (Percival, Narain, & Lee, 2023). Sin embargo, la enseñanza de la criptografía enfrenta diversos desafíos, especialmente en la aplicación práctica de conceptos teóricos. Muchas universidades y programas educativos carecen de enfoques experimentales y herramientas interactivas que permitan a los estudiantes aplicar y comprender mejor los principios criptográficos (Adamovic, Sarac, Stamenkovic, & Radovanovic, 2018).

El aprendizaje activo, facilitado a través de visualizaciones interactivas, se ha identificado como un método eficaz para mejorar la comprensión de los conceptos criptográficos (Simms & Chi, 2011). No obstante, muchos programas educativos aún dependen

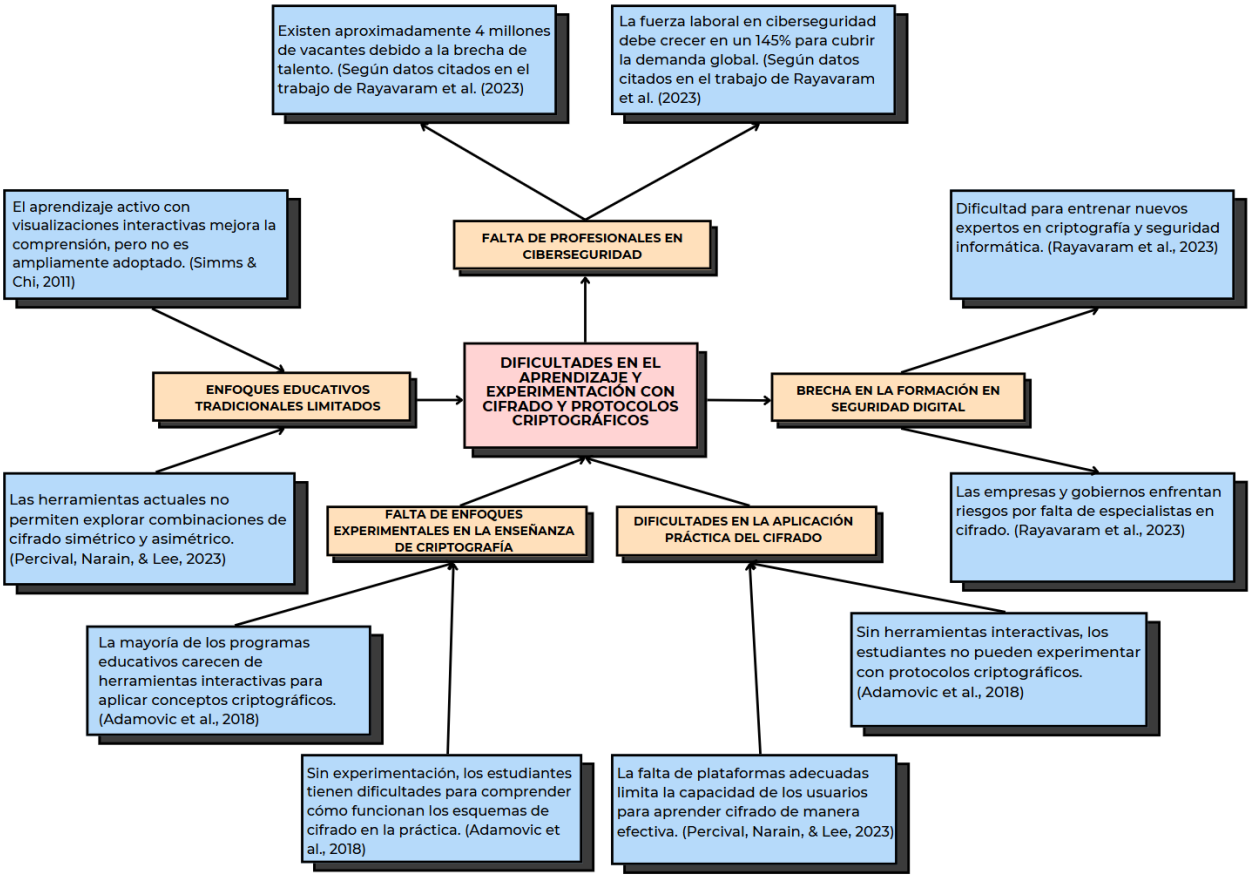

Figura 1: Árbol del problema

de enfoques tradicionales que no aprovechan plenamente estas herramientas. Por ejemplo, Lodi et al. (citado en Percival, Narain, & Lee, 2023) implementaron entornos de experimentación basados en Snap! para enseñar cifrados como el Cifrado César, Diffie-Hellman, DES y AES, permitiendo que los estudiantes interactuaran con animaciones para aprender sobre el cifrado de clave pública. Sin embargo, el estudio también señala que los estudiantes no implementaron combinaciones de cifrado simétrico y asimétrico en este entorno, lo que sugiere la necesidad de herramientas más completas y flexibles.

La escasez de profesionales en ciberseguridad también plantea un problema significativo. Según datos citados en el trabajo de Rayavaram et al. (2023), el International Information System Security Certification Consortium (ISC)² estima que la fuerza laboral en ciberseguridad debe aumentar en un 145 % para satisfacer la demanda global, con aproximadamente 4 millones de vacantes debido a la brecha de talento. Abordar esta carencia requiere enfoques innovadores en la educación de la criptografía, incluyendo la implementación de entornos de aprendizaje interactivo que fomenten una comprensión práctica y efectiva de los sistemas criptográficos.

Dado el crecimiento del uso del cifrado en la vida cotidiana y la importancia de la seguridad de la información, es fundamental diseñar herramientas educativas que permitan a los usuarios experimentar con esquemas de cifrado en un entorno interactivo. La falta de experimentación en los cursos de criptografía puede limitar la comprensión de los estudiantes y su capacidad para aplicar estos conocimientos en situaciones del mundo real (Adamovic et al., 2018). Por lo tanto, es necesario desarrollar una plataforma que ofrezca un espacio de experimentación interactiva, permitiendo a los estudiantes aprender sobre criptografía de una manera práctica, visual y accesible.

III. Justificación

El aprendizaje de la criptografía enfrenta múltiples barreras que dificultan su comprensión y aplicación. Para muchas generaciones, los requisitos matemáticos avanzados y la falta de herramientas accesibles pueden convertirse en obstáculos significativos para adquirir conocimientos sobre esta disciplina (Abdelhamid, Patterson & Patterson, 2022). Aunque los estudios en educación criptográfica han abordado estrategias para simplificar conceptos matemáticos complejos, pocas investigaciones han analizado los desafíos que implica la implementación práctica de algoritmos de cifrado (Abdelhamid et al., 2022).

Diversas investigaciones han explorado métodos efectivos para la enseñanza de seguridad y criptografía. Una de las estrategias consiste en integrar conceptos de seguridad en cursos existentes de ciencias de la computación (Abdelhamid et al., 2022). Otra opción es desarrollar cursos y programas específicos sobre criptografía y ciberseguridad (Rayavaram et al., 2025). Además, técnicas de aprendizaje activo han demostrado ser efectivas para motivar a los estudiantes y mejorar la asimilación de conceptos criptográficos, incluyendo el uso de software de código abierto y escenarios del mundo real ilustrados mediante animaciones (Abdelhamid et al., 2022).

Actualmente, la enseñanza de la criptografía se enfoca en matemáticas avanzadas y seguridad informática, lo que ha llevado a su exclusión de los currículos educativos en niveles tempranos de formación (Rayavaram et al., 2025). Aunque herramientas como Visual CryptoED han tratado de abordar esta brecha mediante visualizaciones interactivas, su nivel de interactividad sigue siendo limitado y no proporciona una experiencia práctica de codificación, elemento clave para la comprensión de los conceptos más complejos (Rayavaram et al., 2025).

Con este contexto, la aplicación propuesta responderá a las limitaciones de los métodos actuales de enseñanza criptográfica al proporcionar un entorno interactivo, accesible y práctico para la exploración y experimentación de técnicas criptográficas.

IV. Objetivos

IV-A. Objetivo general

Desarrollar, modelar, diseñar e implementar una aplicación interactiva denominada CryptoPlayground, que permita a los estudiantes explorar, simular y aprender sobre fundamentos y esquemas de cifrado criptográficos, a través de módulos y retos dinámicos, con el fin de fortalecer el aprendizaje práctico y experimental de conceptos de seguridad informática.

IV-B. Objetivos específicos

- Elaborar la revisión sistemática de la literatura relacionada con esquemas de cifrado y técnicas de enseñanza de criptografía y enfoques de aprendizaje activo.
- Diseñar la arquitectura de la solución asociada con CryptoPlayground, definiendo los módulos funcionales, mecanismos de interacción y recursos didácticos para la exploración y simulación de algoritmos criptográficos.
- Implementar el prototipo funcional de la solución asociada con CryptoPlayground, integrando las funcionalidades de selección de modulos de aprendizaje y desafios criptográficos dinámicos.
- Validar el prototipo de la solución CryptoPlayground a través de pruebas de usabilidad, experiencia de usuario y evaluación educativa con una muestra representativa de estudiantes, con el propósito de medir su efectividad en el aprendizaje de conceptos criptográficos.

V. Marco Teórico

Percival et al. (2023) señalan que diversas organizaciones han desarrollado recursos para introducir conceptos básicos de criptografía en aulas de educación secundaria, como el Museo Criptológico Nacional, el Apoyo al Aula K-12 de la NSA y CYBER.org. También existen iniciativas extracurriculares como CryptoClub de la Universidad de Chicago y PLTW que proporcionan recursos adicionales. Sin embargo, aunque estos autores advierten que esta introducción es un gran comienzo, no da una comprensión adecuada de los tipos de criptografía utilizados hoy en día.

Percival et al. (2023) destacan que las técnicas criptográficas clásicas solo proporcionan una protección débil de los datos, mientras que las técnicas criptográficas modernas como la criptografía simétrica, la criptografía asimétrica, los algoritmos de hash seguros y las combinaciones de sistemas criptográficos pueden proporcionar confidencialidad de los datos, autenticación del remitente y el receptor, protección de integridad, no repudio y sistemas de confianza.

Lodi et al. (2022) desarrollaron actividades interactivas basadas en Snap!, un lenguaje de programación visual con bloques, para que los estudiantes experimentaran con sistemas criptográficos clásicos. Los autores crearon una progresión de entornos para las actividades prácticas. Estos entornos

permiten a los estudiantes experimentar con sistemas criptográficos (por ejemplo, cifrado César, One-time pad) y sus limitaciones. Estos entornos de aprendizaje o "playgrounds"son proyectos de Snap! con un conjunto limitado de instrucciones visibles, aprovechando la capacidad de Snap! para crear bloques personalizados y ocultar los existentes.

La intervención de Lodi et al. (2022) se diseñó para enseñar ideas fundamentales de criptografía haciendo que los estudiantes encuentren algunos sistemas criptográficos representativos (desde clásicos hasta modernos) y experimenten sus limitaciones (a través de actividades prácticas), así como la necesidad de superar esas limitaciones (hacia sistemas más seguros). Los conceptos abordados incluyeron el cifrado César, el cifrado One-time pad, redes simples de sustitución-permutación, el protocolo de acuerdo de claves Diffie-Hellman, la idea de secreto y autenticación de clave pública, y la idea de sistemas criptográficos híbridos.

Rayavaram et al. (2023) diseñaron un plan de estudios utilizando una extensión de Scratch llamada CryptoScratch que implementa algoritmos criptográficos modernos como AES y RSA para cifrado/descifrado y el algoritmo SHA-256 para el hash de mensajes. Los autores eligieron Scratch debido a su capacidad para demostraciones visuales y una interfaz de usuario que permite a los niños interactuar fácilmente con los bloques.

A diferencia de los creadores de CryptoScratch, que se centraron principalmente en el desarrollo de herramientas, Rayavaram et al. (2023) se enfocaron en enseñar cómo usar los bloques algorítmicos mencionados para proporcionar servicios de seguridad como confidencialidad, protección de integridad y autenticación. Su estudio involucró a 18 participantes de entre 10 y 15 años, quienes encontraron unánimemente que los conceptos de ciberseguridad del plan de estudios eran fáciles de aprender.

Adamovic et al. (2014) presentaron una solución para el trabajo interactivo y colaborativo de los estudiantes en la adopción del material de criptología basada en Cryptool, un paquete de software que ofrece una interfaz gráfica para el modelado y la simulación de escenarios criptológicos con la capacidad de utilizar algoritmos populares. Los autores desarrollaron extensiones de programa apropiadas para facilitar el trabajo colaborativo de los estudiantes, específicamente un servidor TCP y un cliente TCP.

Según Adamovic et al. (2014), el uso de Cryptool permite un trabajo estudiantil más interactivo con métodos criptográficos. Esta herramienta proporciona el nivel adecuado de abstracción y visualización en el trabajo con métodos criptográficos, con todos los algoritmos de cifrado populares disponibles como componentes integrados.

Adamovic et al. (2014) afirman que la solución ha resultado en un ahorro tremendo de tiempo necesario para implementar procedimientos criptográficos en lenguajes de programación clásicos, con particular énfasis en el tiempo ahorrado en depuración. El enfoque cambió de la comprensión de los fundamentos matemáticos de los algoritmos criptográficos y su implementación en lenguajes de programación a la comprensión de la arquitectura y los puntos débiles de sistemas complejos.

Rayavaram et al. (2025) desarrollaron CryptoEL, una herramienta basada en web diseñada para enseñar conceptos complejos de criptografía a través de las cuatro etapas del modelo de Aprendizaje Experiencial (EL) de Kolb. Los autores eligieron el modelo EL por su énfasis en el aprendizaje a través de la experiencia directa, integrando conceptos teóricos con aplicaciones del mundo real, crucial para la educación en ciberseguridad.

La herramienta CryptoEL fue desarrollada utilizando el framework web Django para gestionar la funcionalidad de la aplicación y el flujo de datos. Los escenarios del mundo real, creados con HTML, CSS y JavaScript, hacen que el aprendizaje sea relevante y atractivo. El estudio involucró a 51 estudiantes de secundaria y preparatoria, incluyendo 18 estudiantes de secundaria (5 mujeres, 13 hombres) y 33 estudiantes de preparatoria (15 mujeres, 18 hombres).

Los resultados recopilados por Rayavaram et al. (2025) mostraron que la herramienta CryptoEL fue altamente calificada por su compromiso, efectividad y beneficio educativo, con casi el 93 % de los estudiantes de secundaria y preparatoria calificándola con 4 o más en una escala Likert de 5 puntos. Aproximadamente el 87 % de los estudiantes de secundaria y el 79 % de los estudiantes de preparatoria dieron retroalimentación positiva sobre la naturaleza práctica de la herramienta.

Las investigaciones revisadas demuestran la efectividad de los enfoques interactivos y experienciales para la enseñanza de la criptografía. Las plataformas basadas en programación visual como Snap! y Scratch, junto con herramientas específicas como Cryptool y

CryptoEL, proporcionan entornos de aprendizaje que facilitan la comprensión de conceptos criptográficos complejos. Estos enfoques no solo hacen que el aprendizaje sea más accesible y atractivo, sino que también permiten a los estudiantes experimentar directamente con algoritmos criptográficos y comprender sus aplicaciones prácticas en la seguridad de la información.

Basándonos en estos antecedentes, nuestro proyecto busca aprovechar estrategias de aprendizaje interactivo y basado en experiencias para acercar la criptografía a estudiantes. Al emplear herramientas digitales y actividades prácticas, pretendemos mejorar la comprensión de los sistemas criptográficos y su aplicación en la seguridad de la información, abordando las limitaciones identificadas en los enfoques anteriores.

VI. Metodología del proyecto

Para garantizar la ejecución del proyecto de una forma organizada y estructurada, se implementará una metodología que dividirá el proceso en varias fases claramente definidas: Planeación, Modelado, Prototipado, y Análisis de Resultados y Conclusiones.

VI-A. Planeación

En la fase de Planeación se llevará a cabo una revisión exhaustiva de literatura, consultando artículos científicos, libros especializados y recursos académicos provenientes de bases de datos reconocidas como IEEE Xplore, Scopus y Google Scholar. El objetivo de esta etapa será identificar las principales dificultades asociadas al aprendizaje de la criptografía, así como explorar las estrategias didácticas y herramientas tecnológicas emergentes utilizadas en contextos educativos. Este análisis permitirá definir los lineamientos teóricos y prácticos que fundamentarán el desarrollo del proyecto.

VI-B. Modelado

La fase de Modelado consistirá en el diseño conceptual de los recursos didácticos que se utilizarán para facilitar la enseñanza de los contenidos criptográficos. En esta etapa se definirán las características principales de las herramientas educativas, estableciendo aspectos como la interactividad, la integración de editores de código, la incorporación de actividades gamificadas, y el diseño de módulos de aprendizaje.

VI-C. Prototipado

Posteriormente, en la fase de Prototipado, se procederá a la construcción y desarrollo de los recursos diseñados. Esta etapa contemplará la implementación de una ruta de aprendizae criptográfica, la creación de retos y dinámicas basadas en gamificación, y el desarrollo de entornos virtuales de práctica orientados a la resolución de problemas reales.

VI-D. Análisis de Resultados y Conclusiones

Finalmente, en la fase de Análisis de Resultados y Conclusiones, se realizará una prueba piloto con estudiantes de carreras afines a la informática y la seguridad de la información. En esta etapa se aplicarán talleres prácticos y cuestionarios que permitirán evaluar tanto el nivel de comprensión de los conceptos criptográficos como el grado de motivación y participación de los estudiantes.

VII. Marco Conceptual

VII-A. Criptografía

La criptografía es la disciplina que estudia los principios, medios y métodos para transformar datos con el fin de ocultar su contenido semántico, evitar su uso no autorizado o impedir su modificación sin ser detectada (Barker, 2003).

VII-B. Funciones criptográficas

Las funciones criptográficas comprenden los algoritmos criptográficos junto con sus modos de operación, en caso de ser aplicables. Ejemplos de estas funciones incluyen cifradores de bloque, algoritmos de firma digital, algoritmos de establecimiento de claves asimétricas, códigos de autenticación de mensajes (MAC), funciones hash y generadores de bits aleatorios (Barker & Dang, 2016).

VII-C. Algoritmos criptográficos de clave pública (asimétricos)

Un algoritmo criptográfico de clave pública emplea dos claves relacionadas: una clave pública y una clave privada. La seguridad de este esquema se basa en la imposibilidad práctica de deducir la clave privada a partir de la clave pública mediante un proceso computacionalmente factible (Barker & Dang, 2016).

VII-D. Algoritmos criptográficos de clave simétrica

A diferencia de los algoritmos asimétricos, los algoritmos de clave simétrica emplean la misma clave secreta tanto para el cifrado como para el descifrado. Este tipo de criptografía es altamente eficiente en términos de velocidad y consumo de recursos computacionales, lo que la hace ideal para el cifrado de grandes volúmenes de datos (Barker & Dang, 2016).

VII-E. *Protocolos de gestión de claves*

Los protocolos de gestión de claves son un conjunto de reglas documentadas y coordinadas para el intercambio de claves y metadatos asociados, como los certificados X.509. Estos protocolos son esenciales para garantizar la seguridad en las comunicaciones cifradas y la correcta distribución de claves en entornos seguros (Barker & Dang, 2016).

VII-F. *Ataque de hombre en el medio (Man-in-the-Middle, MITM)*

Un ataque de hombre en el medio es una vulnerabilidad en la seguridad informática y criptográfica en la que un atacante intercepta, modifica o retransmite la comunicación entre dos partes sin que estas lo adviertan. En este tipo de ataque, el atacante puede escuchar o suplantar a una de las partes, generando la impresión de que se trata de una comunicación legítima cuando en realidad la información está comprometida (Mallik, 2019).

VIII. Arquitectura de la Solución

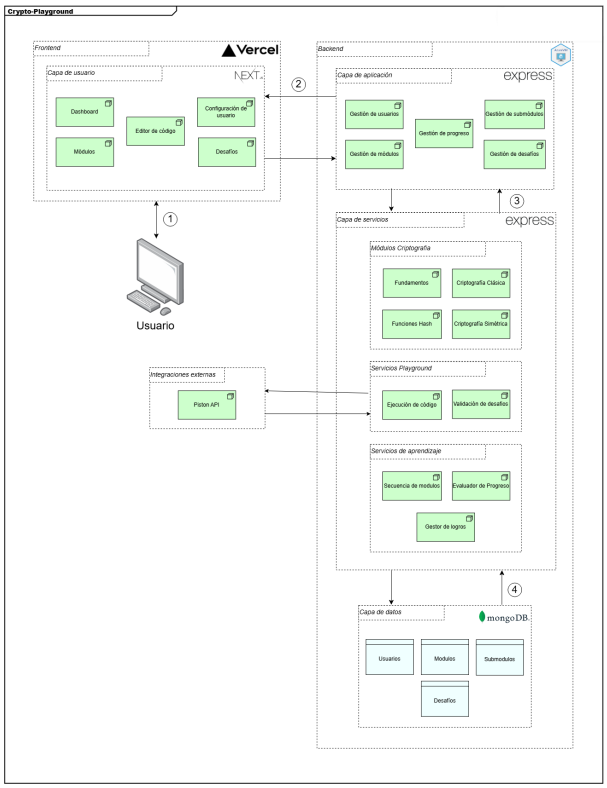

Figura 2: Diagrama de la arquitectura del sistema.

La arquitectura se encuentra estructurada de la siguiente forma:

- Frontend (Vercel + Express.js): Interfaz de usuario que incluye dashboard de progreso, módulos educativos, editor de código, configuración de usuario y desafíos.
- Backend (Express.js): Dividido en dos subcapas:
  - Capa de Aplicación: Controladores para gestión de usuarios, módulos, submódulos, desafíos y progreso.
  - Capa de Servicios: Implementa módulos criptográficos (fundamentos, criptografía clásica, funciones hash y criptografía simétrica), servicios de playground (ejecución de código y validación de desafíos) y servicios de aprendizaje (secuenciación, evaluador de progreso, gestión de logros).
- Capa de Datos (MongoDB): Almacena información de usuarios, contenido educativo y desafíos.
- Integraciones Externas: Piston API para ejecución segura de código en entorno aislado.

IX. Ruta de Aprendizaje

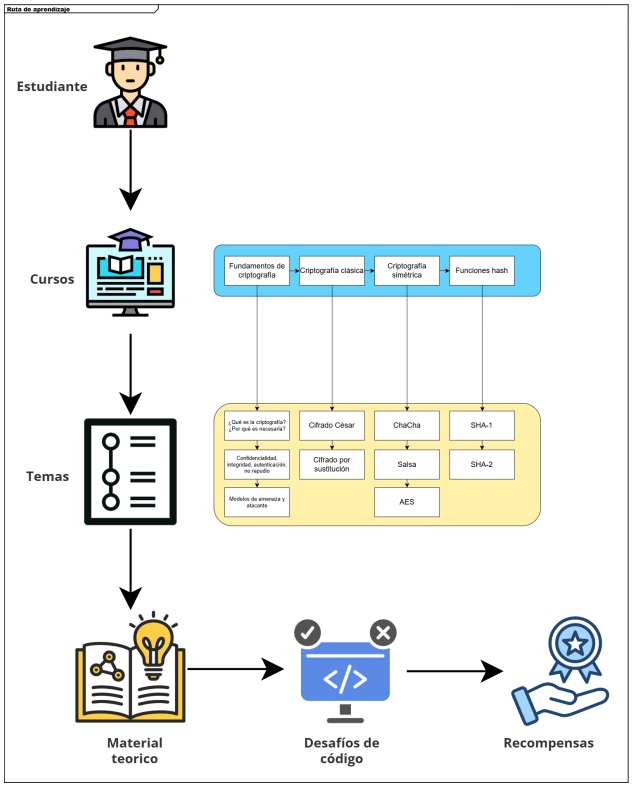

Figura 3: Ruta de aprendizaje.

La ruta de aprendizaje está estructurada para que los estudiantes avancen de manera progresiva desde los conceptos básicos hasta los más avanzados de criptografía, de forma práctica y aplicada. Cada curso se organiza en

módulos temáticos que combinan teoría, implementación y uso real.

- Material teórico: Cada módulo comienza con una explicación teórica clara y accesible, complementada con ejemplos.
- Desafíos de implementación: Tras adquirir la teoría, los estudiantes enfrentan desafíos prácticos de codificación, donde implementan lo aprendido.
- Recompensas: Al superar los desafíos de codificación, el estudiante obtiene recompensas simbólicas, como logros y puntos, que marcan su progreso.

X. Prototipo

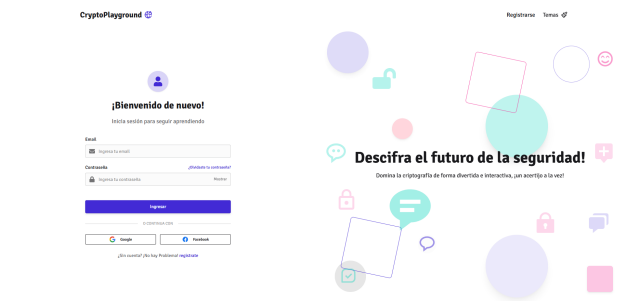

Figura 4: Login

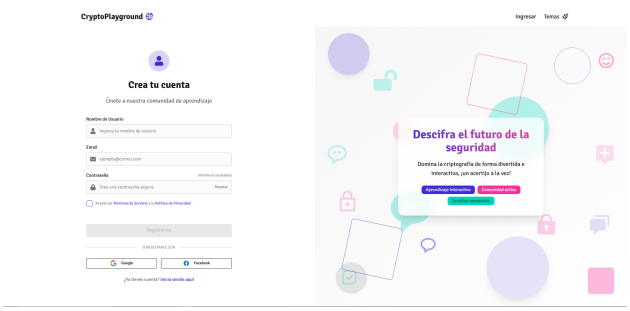

Figura 5: Registro

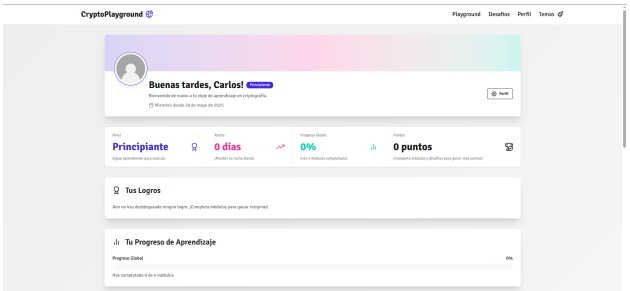

Figura 6: Dashboard

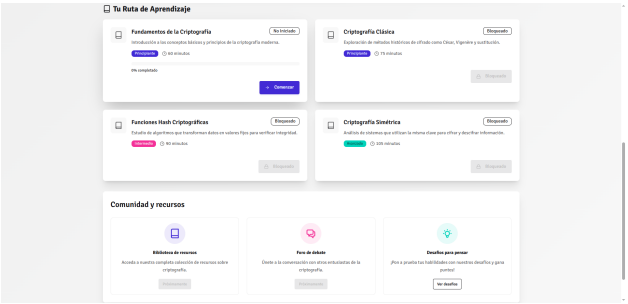

Figura 7: Dashboard

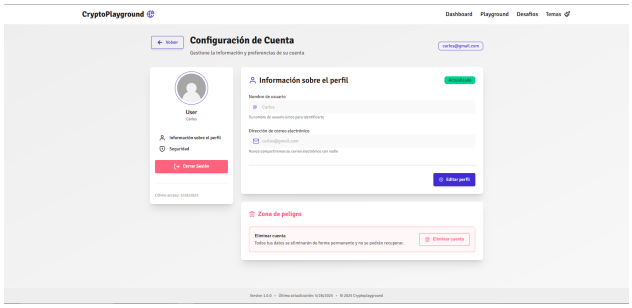

Figura 8: Configuración de usuario

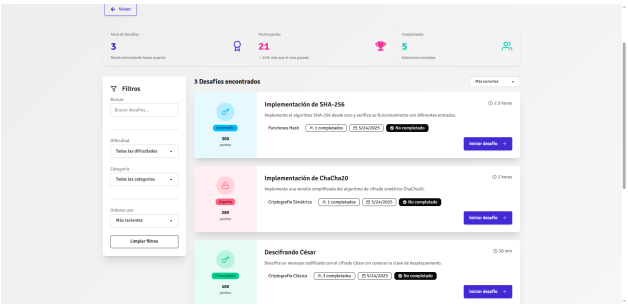

Figura 9: Desafíos

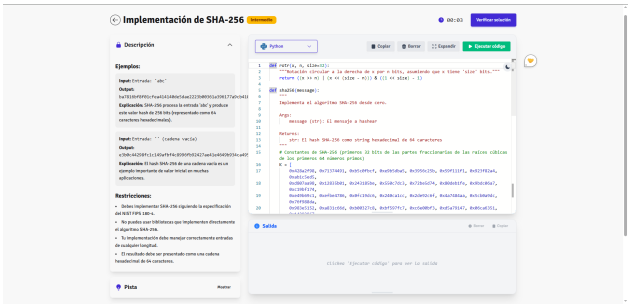

Figura 10: Desafío

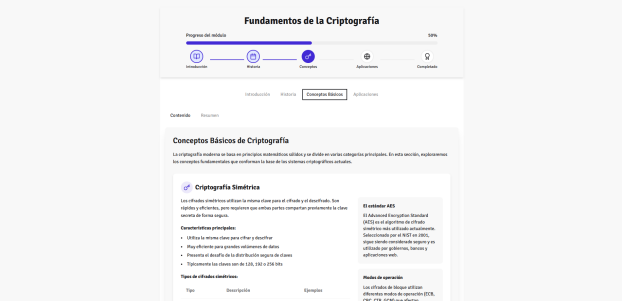

Figura 11: Ejemplo de módulo

Figura 12: Ejemplo de prueba conceptual

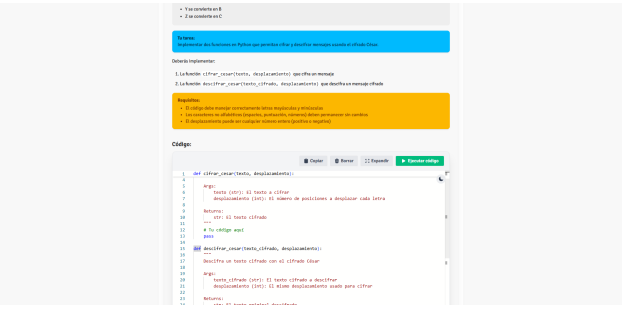

Figura 13: Ejemplo de prueba práctica

XI. Tabla de Evaluación

Caracteristica	Definición o descripción	1	2	3	4	5
Understandability	¿Facil de comprender?					5
Documentation	¿Documentación de usuario completa, apropiada y bien estructurada?					5
Buildability	¿Fácil de construir en un sistema compatible? (Close-Open)					5
Installability	¿Fácil de instalar en un sistema compatible?					5
Learnability	¿Facil de aprender a usar sus funciones?					5
Identity	¿La identidad del proyecto / software es clara y única?				4	
Copyright	¿Es fácil ver quién posee el proyecto / software?					
Licencing	¿Adopción de la licencia apropiada?					
Governance	¿Fácil de entender cómo se ejecuta el proyecto y cómo se gestiona el desarrollo del software?					
Community	¿Evidencia de comunidad actual / futura?					5
Accessibility	¿Evidencia de capacidad de descarga actual / futura?					
Testability	¿Fácil de probar la corrección del funciones caja negra?			3		
Portability	¿Utilizable en múltiples plataformas?				4	
Supportability	¿Evidencia de soporte para desarrolladores actuales / futuros?					5
Analysability	¿Fácil de entender a nivel fuente?				4	
Changeability	¿Fácil de modificar y aportar cambios a los desarrolladores?				4	
Evolvability	¿Evidencia de desarrollo actual / futuro?					5
Interoperability	¿Interoperable con otro software requerido / relaciona					
modelo de evaluación basado en el estandar ISO 9126 ISO 15504 + ESCALA DE LIKERT						

Figura 14: Tabla de validación del prototipo

La tabla proporciona una evaluación numérica de varios criterios relacionados con el prototipo. Un grupo de control, que estaba trabajando en su propio proyecto de investigación, realizó esta valoración. Los aspectos analizados incluyen comprensión, documentación, portabilidad, modularidad, entre otros. Esta tabla facilita la identificación tanto de los puntos fuertes como de las áreas que requieren mejoras dentro del prototipo.

XII. Conclusiones

El presente trabajo desarrolló una herramienta interactiva para el aprendizaje de criptografía, con el fin de facilitar la comprensión de conceptos complejos relacionados con este campo. Al integrar estrategias de gamificación, visualización interactiva y práctica guiada, se busca aumentar la motivación y el compromiso de los estudiantes, promoviendo un aprendizaje significativo y accesible.

La revisión de la literatura permitió identificar las principales dificultades en la enseñanza de criptografía, así como las estrategias exitosas implementadas en iniciativas previas. Esta base teórica sólida orientó el diseño de CryptoPlayground, permitiendo consolidar una arquitectura técnica escalable y una experiencia de usuario centrada en la interactividad, la progresión modular del aprendizaje y la experimentación práctica con algoritmos reales.

Durante el desarrollo, se implementó un prototipo funcional compuesto por un sistema frontend desarrollado en Next.js, un backend en Express.js, y una base de datos en MongoDB, apoyado por la integración de Piston API para la ejecución segura de código. Esta arquitectura permitió ofrecer al usuario un entorno educativo robusto, donde el estudiante puede aprender haciendo, con retroalimentación inmediata y recompensas simbólicas que fomentan la continuidad del proceso de formación.

La validación del prototipo a través de pruebas con estudiantes demostró un impacto positivo en la comprensión de los temas abordados, destacando mejoras en aspectos como la motivación, la claridad conceptual y la facilidad de uso de la herramienta.

Es así como CryptoPlayground representa una solución educativa innovadora para la enseñanza de la criptografía. Su enfoque práctico e interactivo no solo mejora la experiencia de aprendizaje, sino que también contribuye al cierre de brechas en la formación de profesionales en ciberseguridad.

Referencias

[1] S. Adamovic, M. Sarac, D. Stamenkovic, and D. Radovanovic, "The importance of the using software tools for learning modern cryptography,"*Int. J. Eng. Educ.*, vol. 34, no. 1, pp. 256-262, 2018.

[2] N. Percival, S. Narain, and C. S. Lee, "Modern Cryptography Education of Middle School Students: A Review of Current Works,ïn *Proc. 24th Annu. Conf. Inf. Technol. Educ.*, Oct. 2023, pp. 33-38.

[3] P. Rayavaram, S. Sista, A. Jagadeesha, J. Marwad, N. Percival, S. Narain, and C. S. Lee, "Designing a Visual Cryptography Curriculum for K-12 Education,ïn *Proc. 2023 IEEE Global Eng. Educ. Conf. (EDUCON)*, May 2023, pp. 1-10, doi: 10.1109/EDUCON54358.2023.10114876.

[4] X. Simms and H. Chi, .Enhancing cryptography education via visualization tools,ïn *Proc. 49th Annu. ACM Southeast Conf.*, Mar. 2011, pp. 344-345.

[5] S. Adamović, I. Branović, D. Živković, V. Tomašević, and M. Milosavljević, "Teaching interactive cryptography: the case for CrypTool,ïn *Proc. IEEE Conf. ICEST*, vol. 1, no. 44006, pp. 3-5, Mar. 2011.

[6] O. Gavirova, "The importance of teaching cryptography and computer security in higher educational institutions," , no. 11-2-1, pp. 92-94, 2024.

[7] D. Huitema and A. Wong, .A Case Study in Gamification for a Cybersecurity Education Program: A Game for Cryptography,"*arXiv preprint arXiv:2502.06706*, 2025.

[8] S. Abdelhamid, S. Patterson, and B. Patterson, .Enhancing Cryptography Education Using Collaborative Visual Programming,ïn *Proc. Future Educ. Conf.*, July 2022.

[9] P. Rayavaram, O. Ukaegbu, M. Abbasalizadeh, K. Vellamchetty, and S. Narain, ÇryptoEL: A Novel Experiential Learning Tool for Enhancing K-12 Cryptography Education,ïn *Proc. 56th ACM Tech. Symp. Comput. Sci. Educ. V. 1*, Feb. 2025, pp. 980-986.

[10] M. Lodi, M. Sbaraglia, and S. Martini, Çryptography in Grade 10: Core Ideas with Snap! and Unplugged,ïn *Proc. 27th ACM Conf. Innov. Technol. Comput. Sci. Educ.*, vol. 1, July 2022, pp. 456-462.

[11] W. C. Barker, "SP 800-59. Guideline for Identifying an Information System as a National Security System,"*NIST Special Publication*, 2003.

[12] E. Barker and Q. Dang, "NIST Special Publication 800-57 Part 2, Revision 4,"*NIST Tech. Rep.*, vol. 16, p. 51, 2016.

[13] A. Mallik, "Man-in-the-middle-attack: Understanding in simple words,"*Cyberspace: J. Pendidikan Teknologi Informasi*, vol. 2, no. 2, pp. 109-134, 2019.

[14] D. Bohdanov, "Modern Web App Architectures,"*Tech Stack Blog*, May 30, 2024. [Online]. Available: https://tech-stack.com/blog/modern-application-development/. [Accessed: Apr. 2, 2025].