Prototipo Web de una calculadora paso a paso del algoritmo AES para el apoyo del aprendizaje y evaluación de estudiantes de criptografía

Trabajo Terminal No._____

*Alumno: *Franco Aguilar Lenin Eduardo*

Directores: Cortez Duarte Nidia Asunción

*e-mail: *lfrancoa1600@alumno.ipn.mx*

Resumen: El presente documento establece las bases de la propuesta de un Prototipo Web de una calculadora del algoritmo AES con el procedimiento paso a paso de cifrado y descifrado de un bloque, con objeto principal de apoyar del aprendizaje, comprensión y evaluación de resultados a través de tutoriales visuales a los alumnos de la Escuela Superior de Cómputo que cursan la unidad de aprendizaje Criptografía.

Palabras clave: Prototipo Web, Criptografía, Programación Modular, Algoritmo AES.

1. Introducción

El aprendizaje es una parte fundamental del desarrollo humano y se produce a lo largo de toda la vida. Es esencial para adaptarse y prosperar en un mundo en constante cambio y para enfrentar nuevos desafíos y oportunidades. Existen muchas definiciones de aprendizaje otorgadas por diversos autores dedicados al área de estudio. Meza Anibal en [1] generalizo todas las definiciones en una sola, la cual es la siguiente: *"El aprendizaje se puede definir como el proceso por el cual adquirimos conocimientos, habilidades, valores, actitudes y comportamientos a través de la experiencia, la instrucción y la práctica. Es un proceso continuo y dinámico que implica la adquisición de información nueva y la capacidad de aplicarla en situaciones futuras"* ***(Meza, 2013)***.

Pero no todas las personas, específicamente estudiantes, aprenden de la misma forma ya que como seres humanos somos diferentes y poseemos características que nos diferencia de los demás. Entonces, la autora Elena Mosquera en [2] nos define los diferentes estilos de aprendizaje que se pueden presentar y que son estudiadas en la psicología. Estos estilos son: El aprendizaje visual, el aprendizaje auditivo, el aprendizaje verbal y el aprendizaje kinestésico.

En la era moderna los estilos de aprendizaje han ido cambiando en los jóvenes estudiantes, se ha observado que existe una gran mayoría de estudiantes con estilos de aprendizaje más visual y kinestésico, esto ha hecho que muchos educadores y empresas creen las llamadas plataformas educativas, las cuales ayudan a potenciar el aprendizaje de uno o muchos temas de estudio y, ser una alternativa a estudio en las instituciones educativas. Hablemos brevemente de las plataformas educativas y cómo estas han impactado en el desarrollo del estudiante de los jóvenes de esta era.

Según Mariela Viñas en su artículo [3] las plataformas educativas son sistemas informáticos diseñados para facilitar el proceso de enseñanza y aprendizaje. Estas plataformas pueden ofrecer una amplia variedad de herramientas y recursos educativos, como materiales didácticos, actividades interactivas, foros de discusión, tutorías en línea y evaluaciones.

La autora Mariela Viñas en su mismo artículo [3] menciona lo que debe contener una plataforma educativa para que esta sea funcional. Primero, tenemos el acceso a recursos multimedia educativos, que sea flexible, que cuente con un sistema de interacción y comunicación, evaluación y retroalimentación, seguridad y, lo que nos interesa, una herramienta de cálculo.

El uso de estas plataformas puede mejorar significativamente el aprendizaje de los estudiantes, ya que ofrecen una variedad de recursos y herramientas que se adaptan a diferentes estilos de aprendizaje y fomentan la interacción y colaboración entre los estudiantes y el profesor. Además, el uso de plataformas educativas aumenta la motivación y el compromiso de los estudiantes al permitirles acceder a los recursos educativos en cualquier momento y lugar, y aprender a su propio ritmo.

La Escuela Superior de Cómputo ofrece en su Plan de Estudios de la carrera de Ingeniería en Sistemas Computacionales 4 optativas en la que el estudiante tiene la capacidad de escoger 4 unidades de aprendizaje que contienen conocimientos que constituyen un valor agregado a la formación académico-profesional de los estudiantes. Una de las unidades de aprendizaje más demandadas es la criptografía.

En esta unidad de aprendizaje se enseñan diferentes algoritmos para el cifrado y descifrado de la información, desde simples sustituciones de letras hasta complejos sistemas de clave pública. Estos algoritmos fueron estandarizados por varios matemáticos y expertos en el área. Dichos algoritmos están, principalmente, documentados de manera técnica y formas en inglés. Esta documentación suele ser muy abrumadora para aquellas personas que son nuevas en esta disciplina, además de que, al estar en el idioma inglés, puede ser difícil comprender para esos estudiantes que no tienen práctica en el idioma.

Uno de los temas importantes de la unidad de aprendizaje son los cifradores de bloque [4], los cuales son algoritmos de cifrado que operan en bloques de datos fijos de un tamaño determinado y transforman cada bloque de datos de entrada en un bloque de datos cifrado de salida correspondiente. Uno de los algoritmos más importantes de este tipo de cifrado es el AES y DES, pero para este caso vamos a hablar del AES. En [5] lo define como un algoritmo de cifrado simétrico ampliamente utilizado en todo el mundo para proteger la información confidencial. AES es un estándar de cifrado del gobierno de los Estados Unidos y se considera uno de los algoritmos de cifrado más seguros disponibles en la actualidad.

Cuando un estudiante empieza a entender estos algoritmos y los analiza paso a paso puede basarse en los vectores de prueba de la documentación existente para saber si el resultado es correcto, esta se encuentra en la documentación oficial del AES conocido como RFC FIPS 197 AES [6]. Sin embargo, la matemática utilizada en este cifrador suele ser compleja para el alumno para el manejo de datos hexadecimales y binarias, además del manejo de matrices que simulan los bloques. También hay que tener en cuenta que el AES cuenta con 10 rondas intermedias, y los resultados parciales no están disponibles y es difícil identificar en dónde puede estar un posible error.

Para ayudar en esta problemática, existen diversas herramientas digitales que pueden apoyar a los estudiantes en el cálculo manual o implementación del algoritmo AES. Ahora bien, estas herramientas son muy útiles para las personas que utilizan el algoritmo AES para su aplicación, sin embargo, estos no necesitan los pasos intermedios y solo desean la salida, en cambio los estudiantes que aprenden este cifrador, necesitan los resultados intermedios para comprender como es el proceso de cifrado.

Tenemos como primer problema que estas herramientas digitales y librerías de lenguajes de programación no presentan los pasos tomados por el cifrador para llegar al mensaje codificado, es decir, estas herramientas trabajan como un sistema de caja negra, la cual solo presentan el resultado final sin mostrar el proceso que se tuvo que realizar. Aunque existan diversas calculadoras del algoritmo AES donde se muestran los pasos y resultados parciales que toma en cada ronda del cifrador, lamentablemente no siguen el estándar del RFC FIPS 197 AES [6] ofrecida por el gobierno de Estados Unidos, dando una mala práctica para los estudiantes al implementar este cifrador, a pesar de aumentar su seguridad, castiga la eficiencia.

Finalmente, existe una poca variedad de contenido multimedia que puede auxiliar a los alumnos en su estudio del algoritmo AES. Debido a esto, muchos alumnos no llegan a comprender el procedimiento manual del cifrador recurriendo a calculadores que solo les muestra el resultado sin mostrar los pasos para llegar a ese resultado.

Como Estado del Arte, se visualiza a continuación, una tabla comparativa de algunos sistemas implementados similares al que se propone. Los sistemas similares implementados han sido integrados en la categoría de **sistemas Web**.

Tabla 1 de Resumen de Aplicaciones Similares, donde se enfatiza tanto las características como el precio de mercado.

Tabla 1. Resumen de Aplicaciones Similares (elaboración propia)

No.	Software	Características	Precio en el Mercado
1	**Online AES Calculator**	Este sitio Web muestra el resultado de cifrado y descifrado de un bloque usando AES de 128 bits en entrada hexadecimal. Solo muestra el resultado en hexadecimal. La llave es en hexadecimal. Sitio Web disponible en [7].	Gratuito
2	**AES Encryption and Decryption Online Tool**	Permite cifrar y descifrar texto plano usando AES en todas sus versiones, mostrando el resultado del cálculo final ya sea en Base 64 o Hexadecimal. Permite seleccionar el modo de operación de cifrado y descifrado. Sitio Web disponible en [8].	Gratuito Tiene opción de donación
3	**Cifrador Online**	Muestra en un cuadro de texto el cifrado y descifrado de un texto plano usando AES de 128 bits. Solo muestra el resultado del cifrado y descifrado con una pequeña animación. La llave es en decimal. Sitio Web disponible en [9].	Gratuito Tiene opción de donación
4	**CrypTool Online**	Este sitio Web tiene una calculadora paso a paso en formato Hexadecimal de AES en todas sus versiones, mostrando los resultados parciales de cada operación del algoritmo de cifrado y descifrado. La entrada debe hacerse en Hexadecimal. Sitio Web disponible en [10].	Gratuito
5	**Prototipo Web de una calculadora paso a paso del algoritmo AES de un bloque para el apoyo del aprendizaje y evaluación de estudiantes de criptografía**	Busca mostrar visualmente los pasos de cifrado y descifrado del algoritmo AES con los resultados parciales en formato hexadecimal. Permite introducir una entrada en texto plano. Esto, implementando manualmente el algoritmo con uso de programación modular.	En fase de desarrollo

Cabe mencionar que el sitio Web **CrypTool Online** no cumple con el estándar RFC FIPS 197 AES ofrecido por el gobierno de los Estados Unidos, ya que este sitio agrega pasos extras que no se encuentran en el estándar, por lo tanto, no cumple los vectores de prueba. Los desarrolladores afirman que estos pasos extras aumentan la

seguridad del AES, sin embargo, castiga a la eficiencia del algoritmo, así como no mostrar los resultados correctos de un cálculo, esto afecta a la evaluación de un alumno que usa los pasos establecidos por el estándar.

2. Objetivos

Objetivo General.

Desarrollar un prototipo Web de una calculadora del algoritmo AES con el procedimiento paso a paso de cifrado y descifrado de un solo bloque para el apoyo del aprendizaje, comprensión y evaluación de resultados a través de tutoriales visuales, con base al estándar RFC FIPS 197 AES y con uso de la programación modular.

Objetivos Específicos

- Analizar, diseñar e implementar la calculadora y el prototipo Web para facilitar su uso a los usuarios con estilo de aprendizaje visual y kinestésico.
- Implementar el algoritmo AES para un solo bloque sin necesidad de bibliotecas externas y usando la programación modular, con el fin de obtener los resultados parciales de cada paso del algoritmo AES.
- Crear una API para obtener todos los resultados parciales del algoritmo AES usando librerías Web de Python.
- Corroborar los resultados de la implementación del algoritmo AES usando los vectores de prueba del RFC FIPS 197 AES.

3. Justificación

La realización del prototipo tiene como primordial objetivo beneficiar al sector educativo en el área de la seguridad informática; debido que su principal población objetivo son alumnos de la Escuela Superior de Computo que estén cursando la unidad de aprendizaje de la criptografía y requieran de un recurso de apoyo confiable para el aprendizaje, comprensión y evaluación del algoritmo AES. El Prototipo de Aplicación Web posee como objetivo principal, ayudar y apoyar en generar un cambio en favorecer el aprendizaje de los estudiantes sobre el algoritmo AES para su implementación en futuros proyectos.

En el desarrollo del prototipo Web de una calculadora del algoritmo AES con el procedimiento paso a paso de cifrado y descifrado de un bloque, se busca mostrar al estudiante los resultados parciales de cada uno de los pasos que toma el algoritmo en el cifrado y descifrado del bloque, para que el alumno pueda observar cómo se opera el bloque en cada uno de las operaciones que usa el algoritmo en su estándar oficial. Esto se llevará a cabo implementado el algoritmo manualmente para lograr obtener los resultados parciales, debido a que las bibliotecas y software externo solo ofrece el resultado final.

El prototipo Web plantea permitir la práctica del algoritmo AES usando el estándar oficial ofrecida por el Gobierno de los Estados Unidos en su documento RFC FIPS 197 AES, para que los alumnos no realicen pasos extras que afecten al rendimiento del algoritmo en sus implementaciones.

La implementación manual del algoritmo AES para un solo bloque, tiene como objetivo la correcta codificación del algoritmo para obtener los pasos intermedios que permite al prototipo Web mostrar visualmente los cálculos a los estudiantes. Además, convertir esta calculadora en una API, beneficia positivamente a los desarrolladores, empresas y usuarios finales en la implementación del algoritmo en sus sistemas, proporcionando integración, automatización, flexibilidad, escalabilidad y fomentar el desarrollo de ecosistemas de aplicaciones y servicios. Incluso, Los profesionales de la seguridad informática también pueden beneficiarse de una calculadora Web de AES. Pueden utilizarla para realizar pruebas y experimentos de cifrado, y para asegurarse de que están utilizando correctamente el algoritmo en sus sistemas. El área de aplicación permite mejorar el proyecto para que pueda implementar nuevos algoritmos criptográficos como el DES, RES, SHA y otros algoritmos cuyo aprendizaje sea difícil para los estudiantes. De igual forma, existen distintos tipos que, en conjunto con la

aplicación por desarrollar, posibilitan el trabajo a otras áreas del conocimiento formales como las Matemáticas, la Física y diferentes ciencias de la computación como la Inteligencia Artificial. Es un trabajo complejo en términos de Ingeniería en Sistemas.

Los recursos que se cuentan para llevar a cabo dicha idea, es el equipo o talento humano, que en este caso es solamente un integrante, la proyección de tiempo de desarrollo trabajo es de 10 meses aproximadamente, siendo las herramientas con las que se poseen equipos de escritorio, con un ISP (Proveedor de Servicios de Internet) y software dedicado para el desarrollo de un prototipo Web funcional y estable, como también el antecedente necesario en conceptos e información de la criptografía. Al implementar el prototipo Web, se espera facilitar la tarea del estudiante al momento de estudiar la práctica del algoritmo AES y, principalmente, brindar una herramienta a todas las personas que desean adentrarse al campo de la criptografía y la seguridad informática, la cual actualmente es muy requerido en un mundo globalizado y conectado a través del Internet.

4. Productos o Resultados Esperados

A continuación, se enlistan los productos esperados del "Trabajo Terminal", los cuales se trabajará y tomará en cuenta, al momento de implementar el Prototipo Web, para contribuir al aprendizaje, comprensión y evaluación de resultados del algoritmo AES.

1) Prototipo Web
2) Documentación técnica del sistema
3) Manual de usuario

Anexado a los productos se visualiza ***la Arquitectura del Sistema Imagen 1,*** el cual ilustra de manera sintetizada la estructura del Prototipo en cuestión.

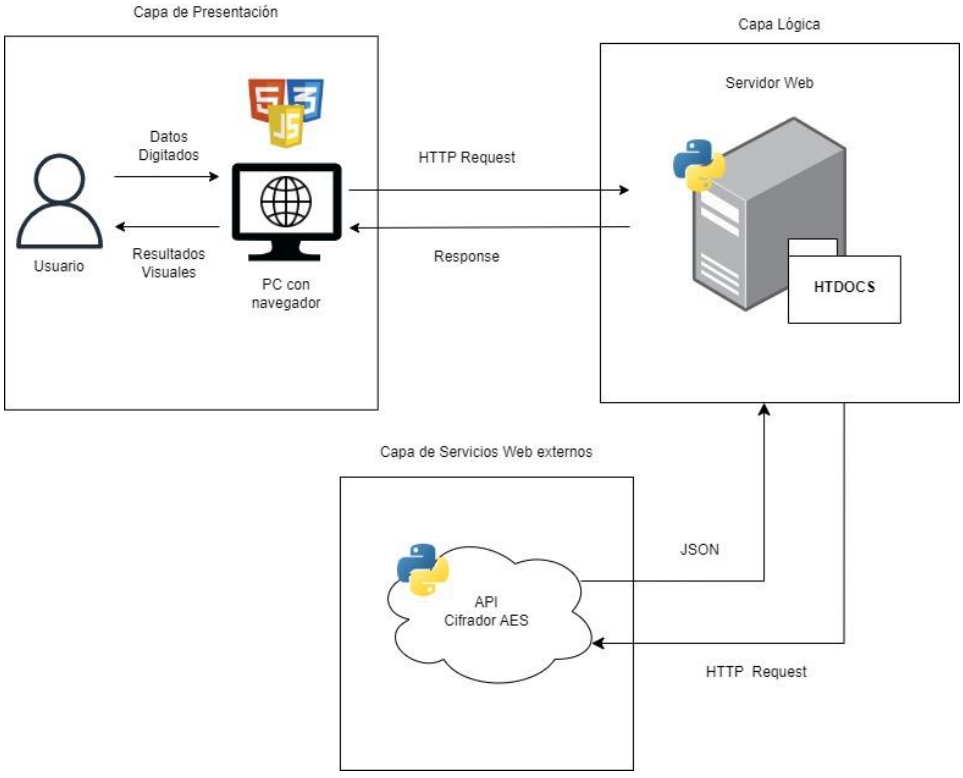

Imagen 1: Diagrama de la Arquitectura del Sistema (elaboración propia)

En el diagrama se plantean 3 actores principales;

- **Usuario**

  Sera el alumno que se encargará de introducir la información como el texto a cifrar y la llave, por lo que recibirá el procedimiento del cifrado y descifrado en la pantalla de su computador. Este agente, dada la posible escalabilidad del proyecto después de concluido, no se limita docentes, también pueden ser docentes o profesionales.

- **Servidor Web**

  Este servidor será el encargado de cargar todos los recursos Web para mostrarlos al usuario, este servidor será programado en el lenguaje Python que facilita la implementación del Back-End. Además, se usará diferentes frameworks Front-End para diseñar una interfaz adecuada y animaciones en la calculadora.

- **API o Servicio Web Externo**

  Será un servicio externo que recibirá peticiones HTTP GET por parte del Servidor o usuarios externos para ofrecer una respuesta en formato JSON de todos los cálculos realizados por el algoritmo, con el fin de ofrecer una fácil lectura de los datos y resultados obtenidos.

5. Metodología

Para el presente desarrollo del Proyecto (Prototipo), se ha seleccionado la metodología en cascada, esta consiste en una secuencia lineal en la que cada paso realiza una tarea en específica. El modelo en cascada es una metodología muy estructurada que se utiliza comúnmente en proyectos donde los requisitos del cliente están bien definidos y no se espera que cambien significativamente a lo largo del proyecto. Como nuestro sistema Web se trata de una calculadora Web paso a paso del cifrador AES, tenemos ya nuestros requisitos del sistema bien definidos y con poca probabilidad de cambios, además que se tiene los plazos de tiempo definidos para la implementación de nuestro sistema.

Por otra parte, se pretende tomar como referencia el siguiente estándar **ISO/IEC-9126, "Modelo de calidad del producto de software"**. En esta norma, se establecen atributos que permiten calificar si un producto de software maneja de manera adecuada y eficiente, el conjunto de funciones que satisfagan las necesidades para las cuales fue diseñado. Con respecto a nuestro Prototipo Web, será usada hacia un universo en particular de usuarios (alumnos que cursan la Unidad de Aprendizaje de Criptografía en la Escuela Superior de Cómputo).

Vamos a describir qué actividades realizaremos en cada una de las fases de la metodología para nuestro Trabajo Terminal:

- Análisis de Requisitos: En esta fase vamos a recopilar todos los requerimientos del sistema, definiendo todas las funcionalidades de nuestro prototitpo Web. Además, tomaremos en cuenta la opinión de diferentes alumnos de la Escuela Superior de Cómputo para complementar los requerimientos del sistema.
- Diseño del sistema: En esta sección elegiremos nuestro paradigma de programación para diseñar nuestro prototipo Web y definir la arquitectura de nuestro sistema para tener una presentación más visual para el desarrollo.
- Implementación: Vamos a codificar nuestro servidor Web con el lenguaje de programación Python y diseñar nuestro Front-End para tener un sitio Web funcional. Posteriormente, implementamos nuestra API del cifrador AES para obtener los resultados del cálculo y mostrarlo en pantalla al usuario final.
- Pruebas: Realizaremos diferentes técnicas de pruebas de un prototipo Web para experimentar el funcionamiento del sistema y posible corrección de errores previo a la entrega del producto final a los usuarios finales.

- Mantenimiento: Esta fase se realizará de manera semestral para poder mantener el sistema funcional en la Web, esto incluye corrección de errores y añadido de nuevas funcionalidades a largo plazo.

A continuación, se presenta un pequeño diagrama que representa la metodología a usar para el Trabajo Terminal.

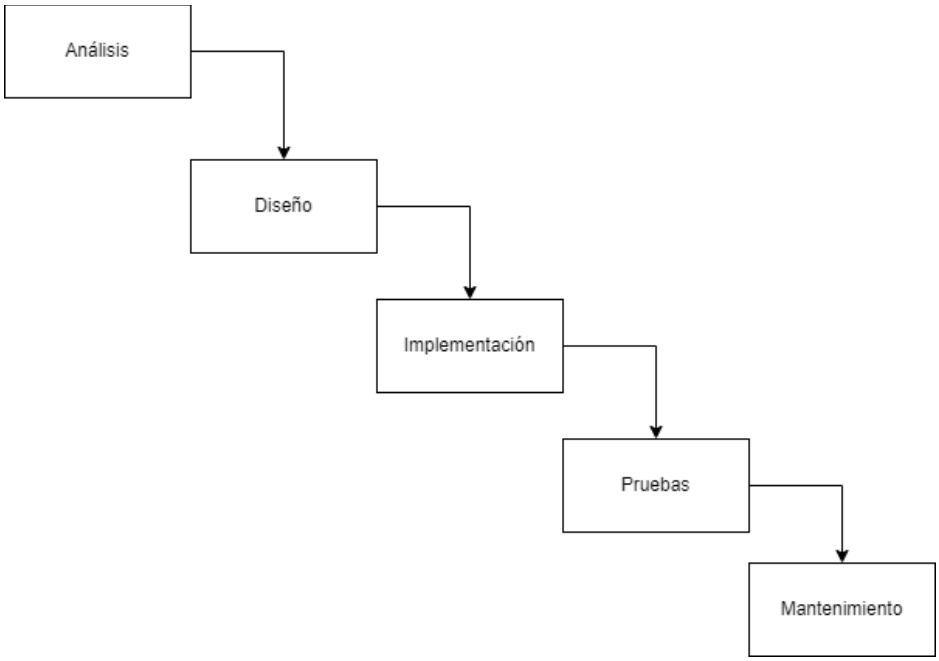

Imagen 2: Diagrama de la metodología en cascada (elaboración propia)

Las características que requiere la aplicación, como lo marca la norma son:

1) Funcionalidad
2) Confiabilidad
3) Usabilidad
4) Eficiencia
5) Mantenibilidad
6) Portabilidad
7) Satisfacción

6. Cronograma

Nombre del Alumno: Franco Aguilar Lenin Eduardo TT No.:

Título del TT: Prototipo Web de una calculadora paso a paso del algoritmo AES de un bloque para el apoyo del aprendizaje y evaluación de estudiantes de criptografía.

Actividad	SEP	OCT	NOV	DIC	ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO
Planeación del Trabajo Terminal												
Elaboración del Marco Teórico												
Indagación de Técnicas de implementación del algoritmo AES												
Planeación del Estado del Arte												
Indagación de la Metodología en Cascada												
Análisis del prototipo Web y calculadora												
Análisis de Riesgos												
Diseño del prototipo Web y calculadora												
Retroalimentación												
Evaluación TT1												
Implementación de la API del algoritmo AES												
Implementación del prototipo Web												
Pruebas unitarias de la API												
Pruebas del Servidor												
Dar de alta el prototipo Web en Internet												
Pruebas con Alumnos de la ESCOM.												
Manual de Usuario												
Documentación Técnica del Sistema												
Retroalimentación												
Evaluación TT2												

7. Referencias

[1] A. Meza, "Learning strategies. Definitions, classifications and measuring instruments," Propósitos y Representaciones, vol. 1, no. 2, pp. 193–213, 2013. [En línea]. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=5475212. [Ultimo acceso: 1 marzo 2023].

[2] Elena Díaz Mosquera, "Estilos de Aprendizaje," EÍDOS, no. 5, pp. 5–11, 2023. [En línea]. Disponible en: https://es.scribd.com/document/456308583/66ab7790-1068-4ab5-8b3f-56a4925af3bd-pdf#. [Ultimo acceso: 3 marzo 2023].

[3] M. Viñas, "La importancia del uso de plataformas educativas," Letras, vol. 1, no. 6, pp. 157–169, 2017. [En línea]. Disponible en: https://www.memoria.fahce.unlp.edu.ar/art_revistas/pr.8497/pr.8497.pdf. [Ultimo acceso: 8 marzo 2023].

[4] Gibrán Granados Paredes, 3150954, and rn, "Introducción a la Criptografía," Unam.mx, 2015. [En línea]. Disponible en: https://www.revista.unam.mx/vol.7/num7/art55/jul_art55.pdf. [Ultimo acceso 12 marzo 2023].

[5] A. Pousa, "Algoritmo de cifrado simétrico AES," Unlp.edu.ar, Dec. 2011. [En línea]. Disponible en: https http://sedici.unlp.edu.ar/handle/10915/4210. [Último acceso: 12 marzo 2023].

[6] "Federal Information Processing Standards Publication 197 Announcing the ADVANCED ENCRYPTION STANDARD (AES)," 2001. [En línea]. Disponible en: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf. [Último acceso: 15 marzo 2023].

[7] "Online AES Calculator," Testprotect.com, 2023. http://testprotect.com/appendix/AEScalc. [Ultimo acceso: 24 de marzo de 2023].

[8] DevGlan, "AES Encryption and Decryption Online Tool," devglan, 2021. https://www.devglan.com/online-tools/aes-encryption-decryption. [Ultimo acceso: 24 de marzo de 2023].

[9] C. Tech, "Cifrar Online - Encriptar y desencriptar texto con AES," Cifraronline.com, 2023. https://cifraronline.com/descifrar-aes. [Ultimo acceso: 24 de marzo de 2023].

[10] "CrypTool Portal," CrypTool Portal, 2023. https://www.cryptool.org/en/cto/aes-step-by-step. [Ultimo acceso: 24 de marzo de 2023].

8. Alumnos y Directores:

CARÁCTER: Confidencial
FUNDAMENTO LEGAL: Artículo 11 Fracc. V y Artículos 108, 113 y 117 de la Ley Federal de Transparencia y Acceso a la Información Pública.
PARTES CONFIDENCIALES: Número de boleta y teléfono.

Franco Aguilar Lenin Eduardo. - Alumno de la Carrera de Ing. En Sistemas Computacionales en ESCOM, Especialidad Sistemas, Boleta: 2020630106, Tel: 5619003786, email: lfrancoa1600@alumno.ipn.mx

Firma: _____

Nidia Asunción Cortez Duarte. - Doctora en Educación UEM 2021, Maestra en Ciencias en Computación CINVESTAV-IPN 2009, Ing. en Sistemas Computacionales ESCOM-IPN 2006, Profesora titular en ESCOM Depto. de Ingeniería en Sistemas Computacionales desde 2010. **Áreas de interés**: criptografía, seguridad de información, hardware reconfigurable, aritmética computacional, diseño digital y redes de computadoras.
Contacto: Teléfono: 57-29-6000 ext. 52032, email: ncortezd@ipn.mx

Firma: _____