Actividad 1 - Etapa 1 del Reto

Firmas digitales para Proteger vidas

Digital Signatures to protect lives

Equipo 4

Juan Pablo Guzmán Segura	A01039810
Valeria Mariane Cárdenas Rodríguez	A01721814
Rodrigo Leal Torres	A00836930
Máximo Caballero Vargas	A01571607
Pablo Pérez Sandoval	A01710355

Docentes

Luis Miguel Méndez Díaz

Daniel Otero Fadul

Sadam Hussain

16 de marzo del 2025

Uso de álgebras modernas para seguridad y criptografía (Grupo 603)

Liga a github: https://github.com/Rodri1255/Equipo4_Cripto

Índice

I. Resumen

Español

Este proyecto propone el diseño e implementación de un sistema de firma digital sencillo, seguro y eficiente para Casa Monarca, organización que brinda apoyo a personas migrantes y refugiadas. Actualmente, los documentos oficiales que emite la organización pasan por un proceso informal de validación, exponiendo la información a riesgos de manipulación, pérdida de integridad y falta de autenticidad en la aprobación. Por consiguiente, se propone establecer un flujo formal de revisión y firma digital, donde cada persona involucrada pueda aprobar o rechazar documentos de manera controlada, así como firmarlos cuando sea necesario para garantizar su validez. Además, se contempla el almacenamiento de los documentos firmados en una base de datos protegida con autenticación de doble factor. Esta iniciativa contribuirá a fortalecer la seguridad de documentos, proteger los derechos de las personas migrantes y mejorar la confianza en la gestión administrativa de Casa Monarca, alineándose con el ODS 9.

Inglés

This project proposes the design and implementation of a simple, secure and efficient digital signature system for Casa Monarca, an organization that provides support to migrants and refugees. Currently, the official documents issued by the organization go through an informal validation process, exposing the information to risks of manipulation, loss of integrity and lack of authenticity in the approval. Therefore, the proposal consists of establishing a formal review and digital signature flow, where each person involved can approve or reject documents in a controlled manner, as well as sign them when necessary to ensure their validity. In addition, the signed documents will be stored in a database protected by two-factor authentication. This

initiative will help strengthen document security, protect the rights of migrants, and improve trust in the administrative management of Casa Monarca, in line with SDG 9.

II. Introducción

Un documento es más que un simple pedazo de papel o un archivo digital. Aunque no se perciba a simple vista, en él se refleja una historia única que, en muchos casos, constituye una prueba clave de existencia dentro de un sistema que determina quién pertenece y quién no. Pero, ¿qué ocurre cuando esa identidad es falsificada o manipulada? Para una persona migrante, el impacto puede ser devastador, ya que su vida y futuro dependen, muchas veces, de un solo documento.

En un mundo cada vez más digitalizado, el resguardo de datos no puede depender únicamente de la buena voluntad de las personas, sino de sistemas inteligentes capaces de reconocer y verificar la identidad de cada individuo. Por ello, es imprescindible contar con herramientas que garanticen la autenticidad e integridad de documentos importantes.

Casa Moncara es una organización social que brinda apoyo a personas migrantes y refugiadas en situación de incertidumbre y vulnerabilidad, ofreciendo tanto asistencia legal como apoyo social. Sin embargo, esto puede implicar varios desafíos, pues trabaja con información sensible que puede ser fácilmente manipulada si no se cuenta con sistemas de seguridad adecuados. Esto afecta directa y gravemente a quienes buscan la oportunidad de construir un futuro prometedor.

En este contexto, el presente trabajo propone emplear un sistema de firma digital que priorice la protección de los derechos de las personas migrantes y refuerce la importancia del uso de la tecnología para proteger a quienes se encuentran en condiciones de mayor vulnerabilidad. Se espera que este sistema contribuya a prevenir fraudes por parte de terceros, falsificación de

documentos y pérdida de confianza en la organización y en las instituciones que trabajan con la población migrante en general.

Para lograr este objetivo, se propone el desarrollo de una tecnología basada en herramientas de firma digital y automatización de procesos, mediante el uso de algoritmos que prioricen la seguridad, integridad, autenticidad y no repudio de los documentos de los solicitantes. Con base en lo mencionado, el equipo se centrará en la implementación de un flujo automatizado de aprobación y seguimiento que permita gestionar de forma eficiente los documentos oficiales generados por Casa Monarca, desencadenando una optimización de tiempos y una organización efectiva para los trámites que se realicen dentro de la organización, todo esto tomando en cuenta plataformas actuales que utiliza la organización como Microsoft 365 y OneDrive. De la misma forma, este proyecto pretende diseñar un sistema accesible y manipulable para cualquier persona que tenga conocimientos básicos de la información desarrollada.

Además de generar un impacto positivo e inmediato, este proyecto se alinea con los Objetivos de Desarrollo Sostenible (ODS), específicamente con el Objetivo 9 (Industria, innovación e infraestructura), el cual impulsa el uso de la seguridad digital para crear un mundo más inclusivo y sostenible. La implementación efectiva de esta propuesta no solo fortalecerá la confianza en instituciones claves como Casa Monarca, sino también fomentará el acceso equitativo a oportunidades y contribuirá al uso y desarrollo de distintas tecnologías que protejan los derechos de las poblaciones vulnerables.

III. Marco referencial

A. Marco Teórico

"La privacidad es necesaria para una sociedad abierta en la era electrónica" (Hugues, 1993). La criptografía surge como respuesta a la necesidad de proteger los datos y garantizar su privacidad. Esta disciplina se fundamenta en cuatro pilares esenciales: confidencialidad, integridad, autenticación y no repudio.

La **confidencialidad** asegura que solo las personas autorizadas puedan acceder a la información. La **integridad** garantiza que la información permanezca sin alteraciones durante su almacenamiento o transmisión. Por su parte, la **autenticación** verifica la identidad de quienes acceden a los datos y la veracidad de la información que proporcionan. Finalmente, el no repudio impide que una persona niegue haber realizado una acción determinada, como enviar un mensaje o firmar un documento digital.

Estos cuatro principios son la base sobre la cual se desarrollan los algoritmos criptográficos, los cuales permiten cifrar información confidencial para mantenerla segura. Dichos algoritmos emplean técnicas matemáticas que transforman los datos de manera que solo quienes posean las claves correspondientes puedan revertir el proceso y acceder a la información original. Entre estos algoritmos se incluyen los algoritmos de cifrado, los algoritmos hash unidireccionales, los algoritmos de distribución de claves y los algoritmos de generación de números aleatorios.

La propuesta de este trabajo se enfoca particularmente en los algoritmos de cifrado, es decir, aquellos que convierten la información en un texto ininteligible que únicamente puede ser revertido por usuarios autorizados. Estos algoritmos pueden clasificarse en dos tipos: simétricos, donde se emplea una sola clave secreta compartida entre el emisor y el receptor para cifrar y

descifrar la información; y asimétricos, donde se utiliza un par de claves, una pública y una privada, exclusiva de cada usuario. Si bien el cifrado asimétrico es más lento que el simétrico, este ofrece un nivel superior de seguridad.

Una de las aplicaciones más eficaces de la criptografía asimétrica en la actualidad son las firmas digitales. Estas funcionan de manera similar a una firma manuscrita, pero en un entorno digital, y se utilizan como método de verificación de identidad en diversos procesos de transacción. La utilidad de las firmas digitales es tan amplia que se emplean en sectores clave de la sociedad. Por ejemplo, en el ámbito empresarial, permiten agilizar procesos legales al reducir tiempos y costos; en el sector gubernamental, facilitan la emisión de certificaciones digitales para verificar identidades; y en las instituciones financieras, refuerzan la seguridad de las transacciones electrónicas.

En nuestro caso específico, el uso de firmas digitales permitirá asegurar la autenticidad y acelerar los procesos legales de los documentos correspondientes a las personas migrantes. Esto no solo contribuirá a proteger su identidad y derechos, sino también a fortalecer la confianza en las instituciones que trabajan con esta población vulnerable.

B. Marco Contextual

La migración es un fenómeno global que cada año afecta a millones de familias. Tan solo en México, más de seis millones de personas se encuentran en situación migratoria. El número de personas que se ven obligadas a recurrir a la migración va en aumento debido a factores como los conflictos armados, crisis económicas, desastres naturales o persecución política, lo que hace indispensable abordar las problemáticas que acompañan este proceso (referencia).

Uno de los principales desafíos que enfrentan los migrantes al llegar a un nuevo país es la **regularización de sus documentos**, los cuales son fundamentales para obtener una residencia definitiva, acceder a empleos formales, recibir ayuda social o, incluso, recibir atención médica primaria. Sin la documentación adecuada, los migrantes quedan en una situación de vulnerabilidad que limita sus oportunidades y los expone a la explotación laboral, discriminación y dificultades para integrarse en la sociedad. Además, la regularización de documentos suele ser un proceso complejo, burocrático y propenso a diversos riesgos, lo que puede derivar en problemas legales, pérdida de derechos y en algunos casos, la deportación.

C. Estado del Arte

El uso de las tecnologías mencionadas anteriormente ha adquirido gran relevancia en los últimos años. La protección de documentos digitales en contextos donde se requiere resguardar información personal es fundamental, especialmente en el caso de personas migrantes. La necesidad de proteger su identidad e integridad aumenta a medida que estas personas enfrentan procesos complejos de registro y legalización, en los que su documentación es esencial para el acceso a derechos y servicios básicos.

Este desafío no es nuevo en la sociedad, pero ha adquirido un contexto global debido al incremento de los flujos migratorios y la creciente preocupación por la seguridad de los datos personales. En respuesta, se han adoptado metodologías tecnológicas como las firmas digitales y la tecnología blockchain, cuyo propósito es garantizar la autenticidad, integridad y confidencialidad de la información sensible.

Por ejemplo, las **firmas digitales** son un mecanismo basado en criptografía asimétrica, que permite verificar la autenticidad de documentos electrónicos y garantizar que no han sido alterados. Algunos de los algoritmos más utilizados para la implementación de firmas digitales son **RSA** (Rivest-Shamir-Adleman), **DSA** (Digital Signature Algorithm) y **ECDSA** (Elliptic Curve Digital Signature Algorithm). Cada uno tiene diferentes variantes y niveles de seguridad que permiten validar la información con base en las necesidades específicas del sistema.

Por otro lado, la tecnología **blockchain** ha sido implementada como una solución innovadora para el registro descentralizado y seguro de información. Uno de los primeros ejemplos destacados es **ID2020**, una iniciativa que promueve el uso de identidades digitales seguras, éticas y privadas para facilitar el acceso de las personas a servicios sociales, políticos y económicos. Esta organización, en colaboración con Microsoft y Accenture, desarrolló soluciones de identidad digital dirigidas a personas sin documentación oficial, como refugiados y desplazados. Gracias a estas tecnologías, ID2020 ha logrado ofrecer servicios de registro e incluso programas de salud a comunidades vulnerables en distintas partes del mundo.

Otro caso relevante es el proyecto **Worldcoin**, el cual combina el uso de firmas digitales y blockchain para la verificación de identidad mediante la biometría del iris. Esta iniciativa busca asegurar el resguardo y control de la información personal de los usuarios, garantizando al mismo tiempo la autenticidad de los documentos vinculados a dicha identidad digital.

A pesar de los avances, la implementación de estas tecnologías enfrenta importantes desafíos. Se requiere de una infraestructura robusta y la colaboración de gobiernos, organizaciones no gubernamentales e instituciones privadas para asegurar el correcto funcionamiento de los sistemas y garantizar el acceso equitativo a estas soluciones tecnológicas. La expansión de iniciativas de este tipo representa un esfuerzo coordinado que permita proteger

los datos personales y los derechos de las personas en situación de vulnerabilidad, como lo son las personas migrantes.

IV. Metodología

V. Resultados

VI. Conclusiones

VII. Referencias

¿Qué es la criptografía? - Explicación sobre la criptografía - AWS. (s.f.). Amazon Web Services. https://aws.amazon.com/es/what-is/cryptography/#:~:text=La%20criptograf%C3%ADa%20es%20una%20pr%C3%A1ctica,algoritmos%20codificados%2C%20hashes%20y%20firmas

¿Qué es la firma digital? (s.f.). Proofpoint. https://www.proofpoint.com/es/threat-reference/digital-signature

Conceptos de criptografía. (7 de octubre de 2024). IBM. https://www.ibm.com/docs/es/i/7.5?topic=cryptography-concepts

Hughes, E. (1993). A cypherpunk's manifesto. Retrieved from https://www.cypherpunks.to/manifesto/

ID2020 | GHPC | Digital Identity Alliance. (2020). ID2020. https://www.id2020.org/

Regresa la empresa que te daba dinero por tu iris: ahora quiere tu pasaporte. (24 de octubre de 2024). El HuffPost. https://www.huffingtonpost.es/tecnologia/regresa-empresa-te-daba-dinero-iris-quiere-pasaporte.html

VIII. Anexos