Instituto Tecnológico y de Estudios Superiores de Monterrey

Casa Monarca Ayuda Humanitaria al Migrante A.B.P.

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

Reto. ***Firmas solidarias: Tecnología criptográfica para los derechos humanos.***

Challenge. ***Solidary signatures: Cryptography technology for human rights.***

Profesores:

Luis Miguel Méndez Díaz

Daniel Otero Fadul

Integrantes:

Andrea Renata Garfias Núñez	| A01369860
Luis Roberto Garza Sánchez	| A00836982
Carol Jatziry Rendon Guerrero	| A01425341
Rolando Ruiz Martínez	| A00835733
Maritza Barrios Macías	| A00836821

16 de marzo de 2025

1. Resumen

Las firmas digitales y electrónicas desempeñan un papel crucial para garantizar la autenticidad e integridad de los documentos electrónicos hoy en día. Este informe presenta una revisión inicial del entorno tecnológico y organizacional de Casa Monarca con el objetivo de implementar algoritmos criptográficos para la firma de documentos. Explora la investigación e implementación de firmas electrónicas y digitales existentes en Python, priorizando aquellas que sean accesibles, seguras y de fácil implementación para identificar la opción más adecuada a las necesidades de la organización considerando factores como costos e infraestructura tecnológica. Los hallazgos de esta investigación servirán de base para implementar una solución criptográfica adecuada.

Digital and electronic signatures play a crucial role in ensuring the authenticity and integrity of electronic documents today. This report presents an initial review of Casa Monarca's technological and organizational environment with the goal of implementing cryptographic algorithms for document signing. It explores the research and implementation of existing electronic and digital signatures in Python, prioritizing those that are accessible, secure, and easy to implement to identify the most appropriate option for the organization's needs, considering factors such as costs and technological infrastructure. The findings of this research will serve as the basis for implementing an appropriate cryptographic solution.

2. Introducción

En la era digital, la seguridad de la información representa un desafío importante, especialmente en el manejo de documentos electrónicos con validez legal. La firma digital garantiza la autenticidad e integridad de estos archivos, previniendo fraudes, falsificaciones y modificaciones no autorizadas. Su implementación es fundamental en sectores donde la certificación de identidad y la validez documental son aspectos esenciales.

En este contexto, surge la necesidad de desarrollar un sistema confiable de firma digital adaptado a las necesidades de la organización social conocida como Casa Monarca, la cual se enfoca en apoyar a migrantes. Este tipo de instituciones emiten documentos clave, tales como constancias de residencia, permisos de trabajo y certificados de identidad, los cuales deben estar protegidos contra manipulaciones que puedan comprometer la seguridad y los derechos de las personas migrantes. La falta de mecanismos de validación confiables que

garanticen la autenticidad de estos documentos puede derivar en problemas legales, pérdida de oportunidades y una mayor vulnerabilidad ante fraudes.

El desarrollo de esta solución requiere un enfoque técnico sólido, donde se combinen conceptos de matemática abstracta con principios avanzados de criptografía. La optimización de recursos y la velocidad de procesamiento serán factores clave para garantizar un sistema seguro y funcional. Más allá de su impacto tecnológico, esta iniciativa representa una contribución significativa a la protección de los derechos humanos y la confianza en los entornos digitales, fortaleciendo la seguridad documental en un contexto de alta vulnerabilidad.

3. Marco referencial

Con el avance de la tecnología y su creciente uso, las firmas electrónicas se han convertido en una herramienta fundamental en la actualidad. Estas permiten confirmar de manera sencilla la identidad de una persona, confirmando su autorización sobre determinado documento. En este sentido, este mecanismo "brinda seguridad y certeza jurídica en transacciones electrónicas, facilitando la adopción de procesos digitales y contribuyendo al desarrollo de la economía digital en el país" (Tosca y Vidal, 2023, p. 247). Gracias a sus beneficios, la firma electrónica cuenta con reconocimiento legal, lo que permite su uso para la autenticación de documentos con validez jurídica, incluyendo aquellos relacionados con el gobierno (Tosca y Vidal, 2023).

Resulta relevante mencionar que la firma electrónica y la firma digital son conceptos relacionados pero con diferencias en su propósito y funcionamiento. Por un lado, la firma electrónica es un paquete de datos que vincula información del firmante, como la dirección IP, correo electrónico o número de móvil, aunque no necesariamente certifica su identidad. En contraste, la firma digital emplea tecnología criptográfica para garantizar la autenticidad e integridad del firmante mediante certificados digitales emitidos por entidades certificadoras. Ambas pueden usarse en diversos contextos, desde contratos hasta validaciones en SMS, WhatsApp o correos electrónicos, dependiendo de los requisitos legales y el acuerdo entre las partes (Adobe Latinoamérica, 2022)

En Latinoamérica, ambas tienen validez jurídica, aunque en algunos casos la ley exige específicamente la firma digital. La diferencia principal entre ambas radica en el nivel de autenticación e integridad de los datos: mientras que la firma digital asegura la identidad del

firmante desde el momento de la firma, la firma electrónica puede requerir un proceso adicional de verificación.

El aspecto legal en las firmas electrónicas ha sido objeto de discusión desde finales del siglo pasado, impulsando esfuerzos internacionales para su regulación. De acuerdo a Guzmán (2010), la regulación a nivel federal abarca el Código de Comercio, permitiendo usar la firma electrónica de manera similar a la manuscrita en transacciones comerciales y contratos electrónicos. Asimismo, el Código Civil Federal y el Código de Procedimientos Civiles reconocen la validez de los documentos firmados electrónicamente, otorgándoles valor en juicio. En el ámbito fiscal, el Código Fiscal de la Federación exige el uso de la firma electrónica avanzada (FIEL) en documentos digitales, asegurando su autenticidad y seguridad en trámites gubernamentales.

México ha adoptado los principios de la Ley Modelo de Firmas Electrónicas de la CNUDMI en Estados como Guanajuato, Sonora, Chiapas, Jalisco e Hidalgo, donde se han desarrollado leyes específicas para regular la firma electrónica. Estas regulaciones establecen el uso de la firma electrónica avanzada y el papel de los prestadores de servicios de certificación, que son los responsables de emitir los certificados digitales para validar la identidad de los firmantes. En cuanto a las firmas digitales, la Ley Modelo de Comercio Electrónico, redactada CNUDMI y aprobada por la asamblea general de las Naciones Unidas, busca una facilitación en el uso de nuevas tecnologías para la información mediante procedimientos y principios regulados (CNUDMI, s.f.). En cambio, para la Unión Europea (UE), las firmas digitales están reguladas por el Reglamento eIDAS, que entró en vigor en 2016 y busca garantizar las “interacciones electrónicas seguras y fluidas entre empresas, ciudadanos y autoridades públicas” para todos los miembros de la UE (Comisión Europea, s.f.).

Ante la creciente demanda y relevancia de esta tecnología, el gobierno mexicano también ha trabajado en el desarrollo de estándares que regulen su uso. Un ejemplo de ello es la Norma Oficial Mexicana NOM-151-SCFI-2016, conocida como NOM 151, la cual establece las condiciones que deben cumplir las constancias de conservación de mensajes de datos en documentos electrónicos. Además, define los requisitos para la digitalización de documentos físicos, regulando así la conservación de archivos electrónicos utilizados en procesos empresariales (DocuSign, 2025).

Con respecto a soluciones existentes, aparece DocuSign, empresa que gestiona servicios relacionados con firmas digitales, y que ha logrado ser válida ante cualquier

organismo legal en México, permitiendo certificar que “un documento electrónico fue remitido y aceptado por todos los intervinientes” (DocuSign, 2022).

Otra empresa centrada en brindar soluciones tecnológicas de firma digital y autenticación electrónica es Viafirma, fundada en Sevilla en el año 2000. Esta permite garantizar la autenticidad de documentos a partir de certificados digitales, facilitando el proceso de trámites en diversas áreas. En Colombia, ha implementado soluciones innovadoras que incluyen una red comercial con más de 5,000 puntos de atención al cliente. Su sistema trabaja con la firma biométrica y la validación de huella dactilar para la formalización de pólizas. Desde 2019, se convirtió en un prestador cualificado de servicios electrónicos de confianza en Europa, siendo de las primeras empresas en España en obtener esta acreditación (Poveda, 2025).

Funcionamiento de las firmas digitales

Una de las distintas formas de crear una firma digital para verificar la integridad de un documento consiste en utilizar el algoritmo propuesto en la Figura 1. De manera general, este procedimiento se basa en obtener el *hash* del documento a firmar, encriptar el resultado con una llave criptográfica privada del firmante y transmitir el documento original con este resultado (la *firma* obtenida) por separado. La verificación se basa entonces en calcular nuevamente el *hash* del documento recibido y desencriptar la firma digital con la llave pública del firmante; si ambos *hashes* coinciden, entonces es posible asegurar que fue el firmante el que emitió el documento y que, además, este no ha sido alterado en un paso intermedio de la comunicación al receptor.

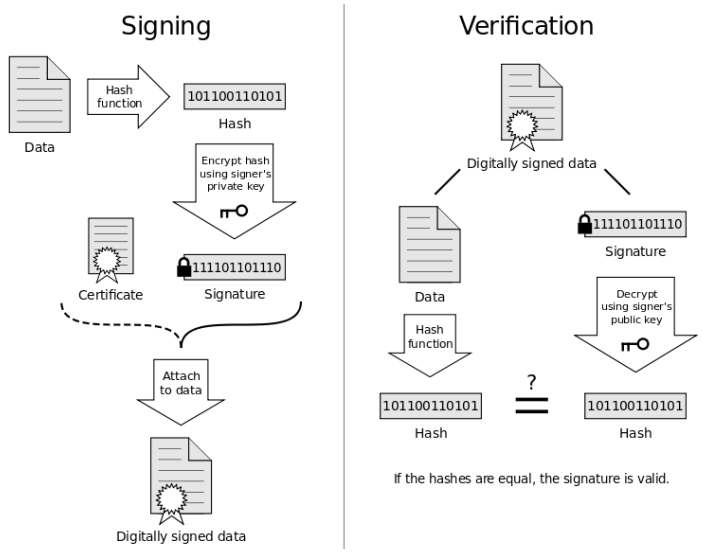

Figura 1. Proceso de firma y verificación de un documento con firma digital. Tomado de Salman, M. 2024.

La generación del par de llaves pública-privada es llevada a cabo usualmente mediante el algoritmo RSA basado en el problema de la factorización de enteros, el cual es computacionalmente costoso cuando los primos son lo suficientemente grandes (Cao y Fu, 2008). Alternativa y más recientemente se ha propuesto la utilización de algoritmos basados en curvas elípticas, los cuales proporcionan la misma seguridad de encriptación con una menor longitud de llaves y una mayor velocidad computacional de obtención (Koblitz et al., 2000, p. 103). De esta forma, el estado del arte de las firmas digitales mediante versiones ajustadas del algoritmo RSA y de curvas elípticas demuestra que es posible utilizarlas a gran escala en sistemas como estructuras *blockchain* para mantener un historial íntegro de transacciones entre usuarios con un costo computacionalmente bajo (Fang et al., 2020, pp. 10-12).

Implementación con Python

Para la implementación de estas y otras herramientas criptográficas, se encuentra disponible la librería *cryptography* para Python. En esta biblioteca se proporcionan una variedad de instrumentos que pueden ser aprovechados con fines que van desde el cifrado y descifrado de mensajes hasta la gestión de claves (Cryptography, 2025a). Por una parte, se encuentra un grupo de módulos y submódulos, denominados recetas, los cuales son facilidades que generalmente requieren un mínimo de configuración, lo que las hace sencillas de manejar. En este grupo se encuentra Fernet, caracterizado por trabajar con claves simétricas, efectivo para el cifrado y descifrado de mensajes con una misma clave (Cryptography, 2025b). Por otro lado, hay un grupo de *bajo nivel*, donde es crucial tener conocimiento de criptografía para aplicar correctamente estas herramientas y sin exponerse a errores; por lo mismo, este módulo es llamado *hazardous material*. Entre los recursos disponibles está la implementación de algoritmos asimétricos, como RSA, autenticación de doble factor o funciones de derivación de clave (Cryptography, 2025a).

Referencias

Adobe Latinoamérica . (2022). Diferencias entre firma digital y firma electrónica. https://blog.adobe.com/es/publish/2022/05/26/existe-alguna-diferencia-entre-firma-digital-y-firma-electronica

Cao, Y., & Fu, C. (2008). An Efficient Implementation of RSA Digital Signature Algorithm. 2008 International Conference on Intelligent Computation Technology and Automation (ICICTA), 2, 100–103. https://doi.org/10.1109/ICICTA.2008.398

CNUDMI. (s.f.). Ley Modelo de la CNUDMI sobre Comercio Electrónico (1996) con su nuevo artículo 5 bis aprobado en 1998. https://uncitral.un.org/es/texts/ecommerce/modellaw/electronic_commerce

Cryptography. (2025b). Fernet (symmetric encryption). https://cryptography.io/en/latest/fernet/

Cryptography. (2025a). Welcome to pyca/cryptography. https://cryptography.io/en/latest/

DocuSign. (2025). NOM 151: qué es y cómo se relaciona con las firmas electrónicas. https://www.docusign.com/es-mx/blog/nom-151

DocuSign. (2022). La validez jurídica de la firma electrónica en México. https://www.docusign.com/es-mx/blog/validez-juridica-de-la-firma-electronica-en-mexico

European Commission. (s.f.). What is an electronic signature?. https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/What+is+eSignature

Fang, W., Chen, W., Zhang, W., Pei, J., Gao, W., & Wang, G. (2020). Digital signature scheme for information non-repudiation in blockchain: a state of the art review. https://doi.org/10.1186/s13638-020-01665-w

Guzmán, A. (2010). La firma electrónica en México. Universidad de Extremadura. https://dehesa.unex.es/handle/10662/11349

Koblitz, N., Menezes, A., y Vanstone, S. (2000). The State of Elliptic Curve Cryptography. Designs, Codes and Cryptography, 19, 173–193.

Poveda, J. (20 de febrero de 2025). 500 millones de firmas digitales en 20 países y 4 millones de facturación. El Economista, Spain. https://link.gale.com/apps/doc/A828240970/IFME?u=itesmgic&sid=ebsco&xid=3b5085eb

Salman, M. (2024). Digital signatures: what are they and how to use them? Mailfence. https://blog.mailfence.com/how-do-digital-signatures-work/

Tosca, C. y Vidal, J. (2023). Impacto de la firma electrónica (E.FIRMA) dentro de la sociedad. UTAP, 2(1). https://revistap.ejeutap.edu.co/index.php/utap/article/view/68