IMPLEMENTACIÓN DE CRIPTOGRAFÍA ASIMÉTRICA DE FIRMA ELECTRÓNICA MEDIANTE SISTEMA WEB

Viramontes Rodríguez Luis Alfonso[1], García Castañón Alfredo[2], Torres Hernández Luis Eduardo[3], Márquez Martínez Luis Enrique[4], Reyes Rodríguez José Antonio[5]*
[1]Instituto Tecnológico de Zacatecas, alfredo.garcia@itz.edu.mx, [2]Instituto Tecnológico de Zacatecas, alfredo.garcia@zacatecas.tecnm.mx, [3] Instituto Tecnológico de Zacatecas, luis.torres@zacatecas.tecnm.mx, [4]Instituto Tecnológico de Zacatecas, luise.mm@zacatecas.tecnm.mx, [5]Instituto Tecnológico de Zacatecas, jose.rr@zacatecas.tecnm.mx

Área de participación: **Sistemas Computacionales**

Resumen

Los sistemas de información han cambiado de manera significativa el proceso de validar y autenticar documentos electrónicos directamente con el firmante. La firma electrónica es un concepto legal, que equivale electrónicamente al de la firma manuscrita, donde una persona física o moral acepta y da por validado el contenido de un mensaje o documento electrónico a través de cualquier medio digital que sea legítimo y permitido según las leyes de cada estado o país, sustituyendo así los mecanismos de firma autógrafa que han prevalecido por años. En la presente investigación se muestra la implementación de un sistema web de firma electrónica de documentos, analizando distintos tipos de procesos, modelos y algoritmos criptográficos asimétricos para la correcta operación del mismo y así poder garantizar aspectos de seguridad y confidencialidad de los datos.

Palabras clave: *Firma electrónica, Criptografía, Criptografía Asimétrica, Algoritmos de encriptación.*

Abstract

Information systems have significantly changed the process of validating and authenticating electronic documents directly with the signer. The electronic signature is a legal concept, which is electronically equivalent to that of the handwritten signature, where a natural or legal person accepts and validates the content of an electronic message or document through any digital means that is legitimate and permitted according to the laws. of each state or country, thus replacing the handwritten signature mechanisms that have prevailed for years. This research shows the implementation of a web system for electronic signature of documents, analyzing different types of processes, models and asymmetric cryptographic algorithms for its correct operation and thus being able to guarantee aspects of security and confidentiality of the data.

Key words: *Electronic signature, Cryptography, Asymmetric Cryptography, Encryption algorithms.*

Introducción

La transformación digital ha cambiado la dinámica del mundo de los negocios, la mayoría de las empresas necesitan adaptarse para ganar mayor cuota de mercado. Y en este crecimiento de nuevas

tecnologías existe una que es fundamental para incrementar la productividad como lo es la firma electrónica.

Con la implementación de un sistema web, es posible firmar contratos en línea, legalmente vinculantes, sin imprimir en papel o tomar un bolígrafo, obteniendo resultados tales como mayor aumento en la rentabilidad, productividad, adaptabilidad y escalabilidad en un mercado en constante desarrollo. Es por ello que la firma electrónica se ha vuelto imprescindible para muchas empresas aumentando su productividad en México [1] hasta en un 25% implementando estas herramientas en su flujo de trabajo.

Según la ley de firma electrónica avanzada, se define como el conjunto de datos y caracteres que permiten la identificación del firmante, que ha sido creada por medios electrónicos bajo su control exclusivo, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación interior de éstos, la cual produce los mismos efectos jurídicos que la firma autógrafa [2], en consecuencia, tendrán el mismo valor probatorio que las disposiciones legales que se otorguen a éstos. Se debe entender que dentro de la firma electrónica se realiza un proceso de encriptación de la información que se desea enviar o firmar según sea el caso, pero no es con el fin de ocultar los datos, sino garantizar la identidad del emisor.

Marco Teórico

2.1 Criptografía

La criptografía es una disciplina que hace uso de métodos y técnicas [3] con el objetivo principal de codificar y proteger un conjunto de datos mediante el uso de algoritmos. La protección de datos, se ha convertido en una tarea indispensable para las operaciones que se realizan en internet, esto debido al crecimiento y auge de sistemas y aplicaciones web. Sin el uso de algoritmos criptográficos la información que viaja en la red, sería vulnerable a ataques y robo de información. Es por ello, que la mayoría de los datos que recorren el internet se encuentran cifrados, pero esto no garantiza que estén totalmente seguros, por lo que es necesario implementar infraestructuras de políticas, recursos de hardware y software para asegurar altos niveles de certeza y confiablidad para los usuarios.

2.2 Tipos de algoritmos criptográficos

Un algoritmo criptográfico es aquel que partiendo de un documento original o un conjunto de datos aplica un algoritmo que utiliza una clave secreta como argumento [4], con el objetivo de obtener características de seguridad, existen dos tipos de algoritmos de cifrado, algoritmo asimétrico o de clave pública y algoritmo simétrico o de clave secreta.

2.3 Criptografía Simétrica

La criptografía simétrica se define como el conjunto de técnicas y algoritmos para descifrar y encriptar un conjunto de datos [5]. Son grupos de algoritmos distintos que se relacionan unos con otros para mantener la conexión confidencial de la información, algunas características de este tipo de cifrado son las siguientes:

- A partir del mensaje o documento cifrado no se puede obtener el mensaje original ni la clave secreta que se ha utilizado, aunque se conozcan todos los detalles del algoritmo criptográfico.
- Utiliza la misma clave para cifrar el mensaje original que para descifrar el mensaje codificado.
- Emisor y receptor deben haber acordado una clave común por medio de un canal de comunicación confidencial antes de poder intercambiar información.

En la figura 1 se muestra un ejemplo del uso de criptografía simétrica donde el mensaje original “Hola alumnos del ITZ” se cifra mediante una clave conocida por todos los interlocutores, y como resultado arrojara en conjunto de caracteres, que se enviarán mediante un canal de combinación inseguro, como resultado el destinatario podrá descodificar el mensaje mediante la clave que el remitente debió proporcionar.

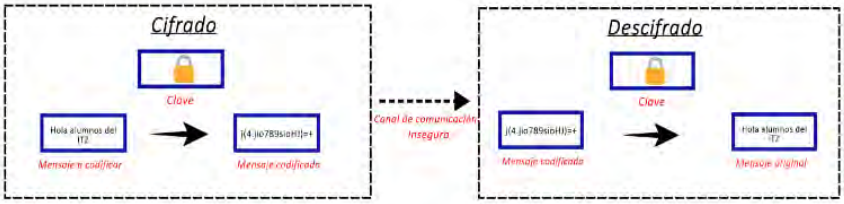


Figura 1. Ejemplo del uso de criptografía simétrica. Fuente propia.

2.4 Criptografía asimétrica

El método criptográfico asimétrico [6] utiliza dos claves, clave privada de uso exclusivo del usuario, esta clave permitirá cifrar y descifrar mensajes de manera completamente segura, la segunda clave se denomina clave pública, la cual es un clave que el usuario puede compartir a terceras personas, el funcionamiento de este método dependerá del origen del mensaje, por ejemplo si el usuario con la clave pública cifra un mensaje, solamente el usuario con la llave privada podrá descifrar dicho mensaje, en cambio si el usuario con su llave privada cifra un mensaje, solamente aquellas personas que haya proporcionado su clave pública podrán descifrar el mensaje, es extremadamente difícil que lo descifre alguien salvo el destinatario. En la figura 2 se observa el uso de la criptográfica asimétrica.

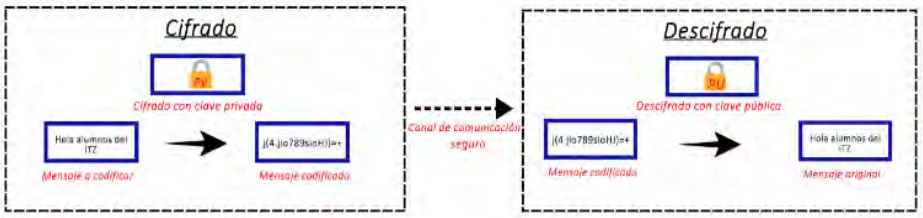


Figura 2. Ejemplo del uso de criptografía asimétrica. Fuente propia.

Los métodos criptográficos garantizan que cada pareja de llaves sólo se puede generar una vez, de modo que no es posible que dos personas obtengan la misma pareja de llaves, todo el proceso de cifrado asimétrico se considera el núcleo de la firma electrónica digital.

2.5 Análisis comparativo de tipos de criptografía

Una vez que se conocen los dos tipos de criptografía se realizó la siguiente tabla comparativa [7], para analizar los principales atributos y diferencias de los tipos de cifrado, se observa que los algoritmos asimétricos están enfocados a firmas digitales esto debido al grado de complejidad, seguridad y longitud de claves que se aplican, en cambio el cifrado simétrico es utilizado principalmente en grandes volúmenes de datos como se muestra en la tabla 1.

Tabla1. Análisis comparativo de tipos de criptografía. Fuente propia.

Atributo	Clave simétrica	Clave asimétrica
Años en uso	Mas de 50 años	Menos de 50 años
Velocidad	Rápida	Lenta
Uso principal	Cifrado de grandes volúmenes de datos	Intercambio de Claves y Firma digital
Claves	Compartidas entre el emisor y receptor	Privada; sólo conocida por 1 persona, Pública: conocida por todos
Intercambio de claves	Difícil de intercambiar por un canal inseguro	La Clave pública se comparte por cualquier canal. La privada nunca se comparte
Longitud de claves	56 bits (Vulnerable) 256 bits(seguro)	1024 bits mínimo
Algoritmos	DES, 3DES, Blowfish, IDEA, AES	RSA, DSA, Elgamal
Servicio de seguridad	Confidencialidad Integridad Autenticación	Confidencialidad Integridad Autenticación No repudio

2.6 Tipos de algoritmos criptográficos

Los algoritmos simétricos están enfocados en el cifrado de grandes volúmenes de datos [8], en caso contrario la aplicación de los algoritmos asimétricos se enfoca principalmente en firmas digitales e intercambio de claves mediante un canal seguro como se muestra en la tabla 2.

Tabla 2. Análisis comparativo de algoritmos simétricos y asimétricos. Fuente propia.

Algoritmo	Fecha de creación	Tipo de Encriptación	Longitud de claves	Estructura o modelo	Velocidad	Seguridad	Actualmente se utiliza	Recursos necesarios de hardware
RSA	1977	Asimétrica	1024-2048 bits	Llave pública	Lento	Seguro	SI	Alto
DSA	1991	Asimétrica	2048 bits	Llave pública	Lento	Seguro	SI	Medio
EdSA	2011	Asimétrica			Rápido		SI	
ElGamal	1984	Asimétrica	1024 bits	Llave pública	Lento	Seguro	SI	Bajo
DES	1976	Simétrica	56 bits a 64	-	Lento	Inseguro	NO	
ECC	1985	Asimétrica	3072 bits	Llave pública	Lento	Seguro	SI	Bajo
AES	1997	Simétrica	128 bits		Rápido	Seguro	SI	

2.7 Funciones Hash

Es un proceso criptográfico el cual se realiza sobre un conjunto de datos de determinado tamaño [9], que nos regresa como resultado otro conjunto de datos que se le llama digest o resumen de los datos originales, que a diferencia de los algoritmos de cifrado simétricos, el resultado del proceso es de un tamaño fijo independiente del tamaño original, de tal forma que tiene la característica de encontrarse asociado unívocamente a los datos iniciales, con este proceso es prácticamente imposible encontrar dos mensajes que tengan el mismo hash, como se muestra en la figura 3.

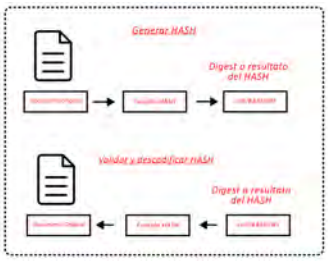


Figura 3. Ejemplo de una función Hash. Fuente propia

2.8 Firma electrónica digital

Método criptográfico que asocia la identidad de una persona a un mensaje, documento o dato [10], la firma electrónica digital se utiliza con el principal objetivo de garantizar la integridad del documento o mensaje que se desea firmar, mientras no se comprometa la llave privada del firmante, es prácticamente imposible falsificar una firma electrónica digital, en la Figura número 4 se puede observar el proceso de firma electrónica digital.

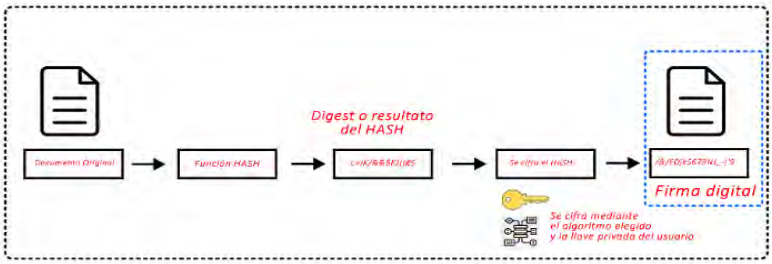


Figura 4. Firma electrónica digital

Metodología

3.1 Tipos de algoritmo de cifrado

En la presente metodología se implementó una investigación descriptiva con el fin de estudiar las técnicas y modelos basados en la criptografía asimétrica [11], el objetivo principal es analizar, comprender y demostrar cuales son los algoritmos y técnicas más efectivas en la protección, integridad y no repudio de la información. Se analizaron los siguientes factores: algoritmo y curva de cifrado o curva elíptica, longitud de claves, intercambio de claves, años en uso, velocidad y métodos de propagación de confianza. Una vez analizados los tipos de algoritmos criptográficos se procede a la generación de claves en el cifrado de clave pública, se utilizan dos claves, privada y pública de forma enlazada en parejas de claves que se encargan de una función específica para que el sistema criptográfico funcione de manera correcta. Si la llave pública es utilizada para cifrar datos, la correspondiente llave privada es la única que se podrá utilizar para descifrarlos como se muestra en la figura 5.

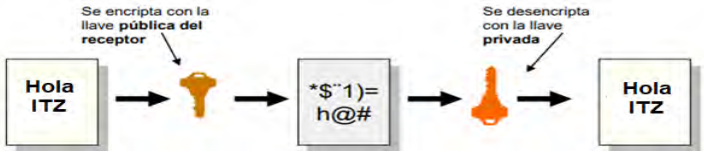


Figura 5. Llave privada y llave pública. Fuente propia.

Una vez realizado este proceso se puede concluir que se garantiza la identidad del emisor y autenticidad del mensaje. Sin embargo, existe un inconveniente como se demuestra en la Tabla 1, donde la principal desventaja de utilizar el algoritmo de clave pública RSA es su lentitud, ya que el algoritmo crece con el tamaño de mensaje a cifrar. Después de seleccionar el algoritmo criptográfico se analizó el funcionamiento de las llaves privadas, públicas y funciones hash, se procede a firmar un documento el cual junto con todos los procesos anteriores se puede realizar el proceso de firmado, en cual se define como el método criptográfico que asocia la identidad de una persona a un mensaje, documento o dato, la firma electrónica digital se utiliza con el principal objetivo de garantizar la integridad del documento o mensaje que se desea firmar, mientras no se comprometa la llave

privada del firmante, es prácticamente imposible falsificar una firma electrónica digital, en la figura 6 se muestra el proceso de firma electrónica digital.

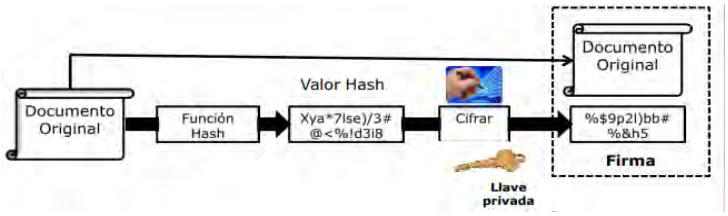


Figura 6. Firma electrónica de un documento. Fuente propia.

La eficacia de las operaciones de cifrado y firma electrónica basadas en criptografía de llave pública se fundamenta en tener certeza que la llave privada de una persona únicamente es conocida por ella. Cualquier individuo o institución pública puede generar un certificado digital y disponer a fungir como autoridad certificadora, por lo que si el emisor no es reconocido por quienes interactúen con el propietario del certificado, el valor del mismo es prácticamente nulo. Por ello, los emisores de certificados de seguridad deben acreditarse mediante el proceso por el cual la entidad reconocida, generalmente pública, otorga validez a la institución certificadora, de forma que su firma pueda ser reconocida como fiable, transmitiendo esa fiabilidad a los certificados que emite, para lo cual se aplican una serie de procesos para autenticar a las autoridades certificadoras como se muestra en la figura 7.

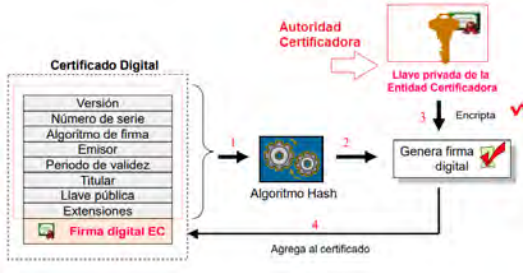


Figura 7. Componentes principales de un Certificado de Seguridad. Fuente propia.

Una vez validada la identidad de la persona se podrán generar las llaves privadas, llaves públicas y certificado de seguridad del solicitante. La emisión se realizará en forma descentralizada a través de "Entidad de Registro" que será la encargada de verificar la identidad de los titulares o solicitantes. La entidad de registro será la responsable de registrar las peticiones que hagan los usuarios para obtener un certificado de seguridad y llaves privada y pública para comprobar la veracidad de los datos que aportan los usuarios en las solicitudes para ser enviadas a una ER y que sean procesadas como se muestra en la figura 8.



Figura 8. Entidad de registro. Fuente propia.

El proceso para el firmado de documentos comprende los siguientes pasos:

- Elegir un documento o conjunto de datos a firmar.
- Validar identidad del firmante mediante el Certificado de Seguridad.

- Aplicar función Hash al documento como se muestra en la figura 9.

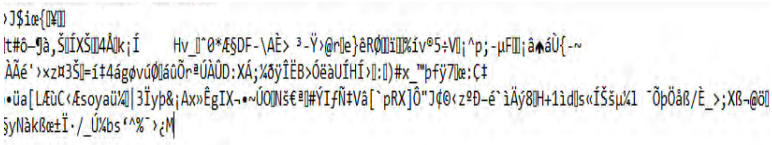


Figura 9. Digest o resumen de datos resultante. Fuente propia.

El resultado codificado anexará al documento un código QR de validación para verificar el contenido de la firma electrónica como se puede observar en la figura 10 y le permitirá al usuario descargar un archivo comprimido zip el cual contendrá la firma electrónica emitida, el documento original, el documento con la firma incrustada, y un archivo XML con la información del documento y datos del firmante.



Figura 10. Ejemplo del resumen de datos en Base 64. Fuente propia.

El siguiente paso será aplicar una función hash al documento original lo cual arrojará un resultado al cual llamaremos resumen de datos 2 o digest 2. Si los resúmenes de datos son iguales, la firma electrónica es válida y el documento no ha sido alterado o modificado, en caso de que los resumes de datos no coincidan la firma electrónica no será válida y es probable que el documento haya sido alterado o modificado. En la figura 11, se puede ver un ejemplo de verificación de firma electrónica:



Figura 11. Ejemplo de una verificación de firma electrónica. Fuente propia.

3.2 Implementar una infraestructura de clave pública o PKI

Se realizó la implementación de la estructura de hardware y software en Amazon Elastic Compute Cloud EC2, que permite alquilar una computadora virtual con sistema operativo Ubuntu y los servicios de DNS con Amazon Route y equilibrio de carga que se utiliza para distribuir automáticamente el tráfico entrante entre varios destinos y un servidor de correo que permita enviar correos desde la aplicación a los usuarios.

Resultados

El rendimiento de estos algoritmos criptográficos se basa en: estructura, clave longitud, tamaño del bloque, número de rondas utilizadas y tiempo criptográfico. En última instancia, estos son los factores que afectan la seguridad de un algoritmo en particular, el tamaño del bloque juega un papel vital en el cifrado y descifrado, que es la unidad básica de datos.

4.1 Implementación del sistema

A continuación, se presenta el funcionamiento del sistema web de firma electrónica para documentos mediante criptografía asimétrica que cuenta con una interfaz amigable para el usuario, como se muestra en la figura 12.

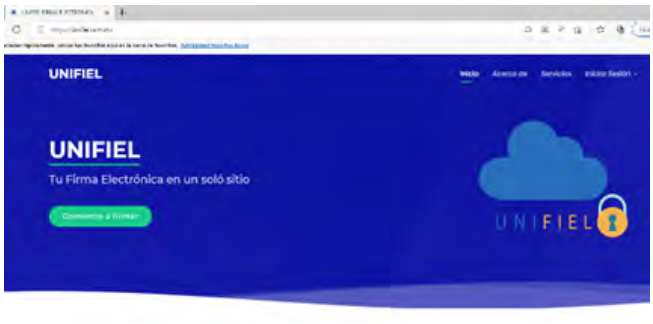


Figura 12. UNIFIEL. Fuente propia.

4.2 Registro de usuarios

Para hacer uso del sistema, una vez realizado el registro llegará una confirmación de email para activar la cuenta, el usuario deberá ingresar datos y documentos para validar su cuenta y hacer uso de las funciones criptográficas, como se muestra en la figura 13.

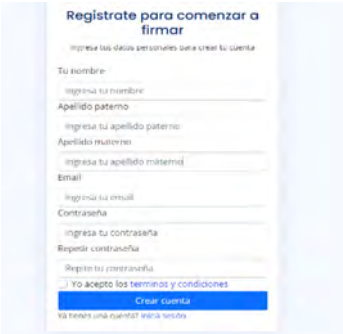


Figura 13. Registro de usuarios. Fuente propia.

Creación de llave privada y llave publica

Para generar el par de llaves pública y privada, se deberá seleccionar el tipo de función hash, el tamaño de clave bits y el tipo de algoritmo para cifrar el par de llaves como se muestra en la figura 14.



Figura 14. Creación de llave privada y llave publica

4.3 Encriptar mensajes

Una vez que se tenga la pareja de llaves se podrá hacer uso de las funciones de encriptar y desencriptar datos, el proceso para encriptar mensajes consistirá en cargar la llave publica del usuario, y se ingresará el mensaje o conjunto de datos a cifrar, una vez que se carguen los datos, se presiona sobre el botón de encriptar como se muestra en la figura 15.

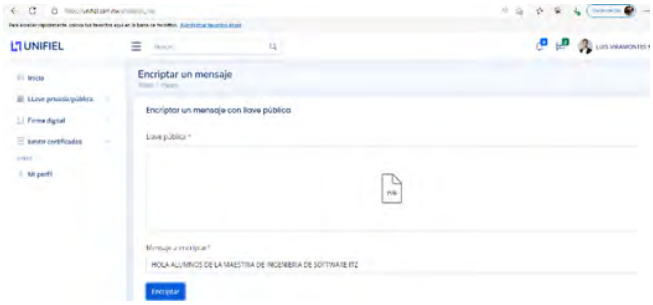


Figura 15. Encriptar mensaje (fuente propia)

Si el sistema no arroja error se descarga automáticamente el mensaje cifrado como se muestra en la figura 16.

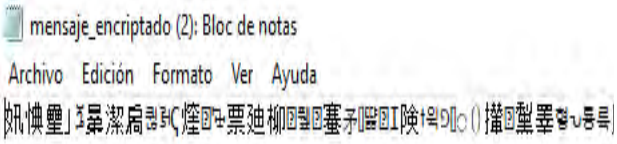


Figura 16. Mensaje codificado. Fuente propia.

4.4 Desencriptar mensaje con llave privada

Para poder visualizar el mensaje, el usuario deberá cargar su llave privada y el mensaje codificado, una vez realizado este paso, simplemente seleccionara la opción de desencriptar y si la llave privada coincide con la llave publica que fue cifrado dicho mensaje, el sistema descargará automáticamente el mensaje descifrado como se puede observar en figura 17.

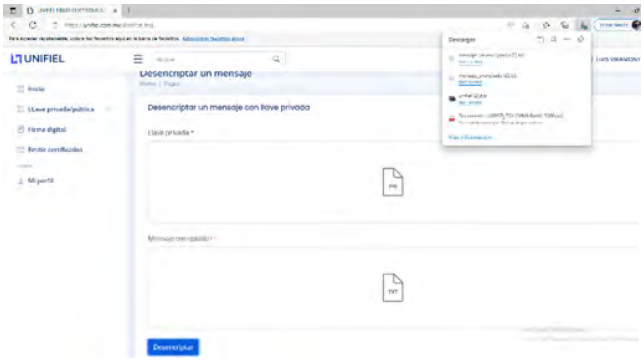


Figura 17. Desencriptar mensaje. Fuente propia.

4.5 Firma digital

Para poder realizar firmas digitales el usuario deberá cargar su llave privada y el documento a firmar, puede ser cualquier archivo de texto, una vez realizado este paso selecciona la opción de firmar y se genera un archivo comprimido como se muestra en la figura 18.

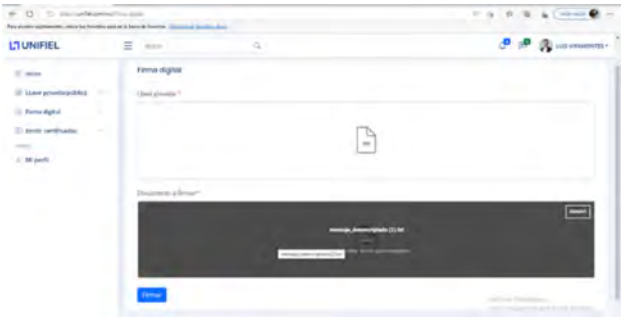


Figura 18. Generar firma digital (fuente propia)

4.6 Verificación de firma

Para verificar que dicha firma corresponde con el documento, el proceso de validación de firma consiste en cargar la llave publica del usuario, el documento original que se firmó y la firma que anteriormente descargó el sistema se selecciona la opción de validar, si la firma coincide con el documento mostrará un mensaje donde la firma corresponde con el documento como se muestra en la figura 19



Figura 19. Validar firma digital. Fuente propia.

Conclusiones

Después de haber analizado diferentes trabajos relacionados con el tema, se pudo definir que los beneficios de implementar una herramienta tecnológica como lo es la firma electrónica son innumerables ya que agiliza los procesos de las organizaciones, permitiendo no tener que estar presente físicamente para poder firmar un documento, esto contribuye al cuidado del medio ambiente al no utilizar papel, garantizando la integridad, protección y fiabilidad de todos los datos que cuenten con firma electrónica que las disposiciones legales les otorgan.

Referencias

[1] M. Morales, "Firmas digitales en México: conceptos, oportunidades y desafíos". 2022.

[2] Unión, C. D. Ley de firma electrónica avanzada. Obtenido de cámara de diputados del H. Congreso de la unión: https://www.diputados.gob.mx/leyesbiblio/pdf/LFEA_200521.pdf. 20/05/2021.

[3] R.D. Velasco. Criptografía, una necesidad moderna. Revista Digital Universitaria, vol. 9. 2006.
[4] Sánchez Muñiz. "Analysis of modern cryptographic algorithms and their effectiveness in protecting personal data". 2023.

[5] A.D. Hering & J.P. Espinoza. "Uso de la criptografía simétrica para la comunicación de mensajes cortos en dispositivos móviles. COMTEL", 5. 2014.

[6] T. Cisneros, V. T., & Hernández. "Análisis Comparativo de Cifrado Asimétrico algoritmos RSA y elgamal". Revista de Sistemas Computacionales y TIC's, Vol 8. 2017.

[7] L. Centellas. "Comparative study of the symmetric cryptography algorithms AES, 3DES and ChaCha20". 2022.

[8] L. Espinoza. Light cryptography algorithms for security applications in electronic clinical records. 2019.

[9] V. Valenzuela," Manual Análisis de Algoritmos". [Online].Available:http://colabora.inacap.cl/sedes/ssur/Asignatura%20Indtroduccion%20a%20la%20Programacn/An%C3%A1lisis%20de%20Algoritmo/Manual-Analisis%20de%20Algoritmos_v1.pdf. 05/05/2023.

[10] F. Morales-Sánchez. "Validez de la prueba electrónica: un estudio sobre la firma digital y electrónica". Trabajo de Grado. Universidad Católica de Colombia. Facultad de Derecho. Bogotá, Colombia. 2016.

[11] F. Penares. "Estudio y caracterización de los diferentes modelos de algoritmos de encriptación".2022.