APLICACIONES CRIPTOGRÁFICAS

Integrantes Grupo 2:

Hurtado Alexis
Quinatoa John
Rodríguez Gabriela
Vergara Dario

1. Definición y Principios Fundamentales de la Firma Digital

La firma digital es una tecnología criptográfica que permite verificar la autenticidad y la integridad de los mensajes digitales, así como garantizar el principio de no repudio. A través del uso de claves criptog

ráficas asimétricas, se consigue que un mensaje firmado digitalmente pueda ser verificado por cualquier receptor, quien a su vez puede confirmar que la firma fue efectuada por el titular de la clave privada correspondiente [1].

Este tipo de firma tiene como objetivo principal proporcionar confianza en entornos digitales, eliminando la ambigüedad sobre la identidad del remitente y sobre la integridad de los datos enviados [1].

Uno de los principios fundamentales que rige esta tecnología es la autenticidad, la cual garantiza que el firmante es quien dice ser; la integridad asegura que el contenido del mensaje no ha sido alterado desde su creación y firma; mientras que el no repudio impide que el firmante niegue posteriormente la autoría de la firma digital [2].

Estos principios son esenciales en procesos electrónicos sensibles como transacciones financieras, contratos electrónicos o procesos de votación digital, donde la seguridad y confianza son imprescindibles [2].

La firma digital también forma parte integral de muchos protocolos modernos de seguridad, como TLS/SSL y sistemas de gestión de identidad digital, consolidando su rol esencial en las infraestructuras de clave pública (PKI) que son la base de la confianza en sistemas distribuidos [3].

2. Algoritmos Criptográficos Utilizados en la Firma Digital

Diversos algoritmos criptográficos sustentan la tecnología de firma digital. Uno de los más antiguos y ampliamente utilizados es el algoritmo RSA (Rivest-Shamir-Adleman), que se basa en la dificultad de factorizar grandes números primos. RSA proporciona tanto firma como cifrado, y ha sido un estándar durante décadas [4].

El DSA (Digital Signature Algorithm), por otro lado, fue propuesto por la NSA como estándar para firmas digitales. A diferencia de RSA, que se basa en el problema de factorización, DSA utiliza la dificultad del problema del logaritmo discreto en grupos multiplicativos finitos, ofreciendo un enfoque diferente pero igualmente seguro para la firma digital [4].

ECDSA (Elliptic Curve Digital Signature Algorithm) representa una evolución de DSA que utiliza criptografía de curvas elípticas. Este algoritmo ofrece la misma seguridad que RSA o DSA pero con claves mucho más cortas, lo que se traduce en

mayor eficiencia, especialmente en dispositivos con recursos limitados como smartphones o tarjetas inteligentes [5].

Finalmente, los algoritmos hash como SHA-256 (parte de la familia SHA-2) son indispensables en el proceso de firma digital. Antes de firmar un mensaje, este es reducido a un resumen de longitud fija mediante un algoritmo hash. Este resumen, al ser firmado, garantiza que incluso un pequeño cambio en el mensaje original invalidará la firma [5].

3. Protocolos de Comunicación y Seguridad en la Implementación de Firmas Digitales

En un entorno digital donde la seguridad y confianza son imperativas, las firmas digitales emergen como un mecanismo crucial. Se fundamentan en criptografía asimétrica y requieren protocolos de soporte que garanticen la correcta emisión, validación y revocación de los certificados digitales, por ello dependen de varios protocolos de comunicación y seguridad que garantizan su correcta implementación en sistemas modernos. A continuación, se detallan los principales protocolos involucrados:

PKCS (Public Key Cryptography Standards): Es una colección de estándares desarrollados por RSA Laboratories para la criptografía de clave pública. Algunos de los más relevantes incluyen:

- **PKCS #1:** Define el estándar de cifrado y firma con RSA, estableciendo formatos para claves y firmas digitales.
- **PKCS #7:** Especifica la estructura para mensajes criptográficos, utilizados en la firma digital y cifrado de datos.
- **PKCS #12:** Define el formato para almacenar y transportar certificados digitales y claves privadas, asegurando la integridad de la autenticación.

X.509 (Certificados Digitales y PKI): Es el estándar que define la estructura de los certificados digitales utilizados en Infraestructuras de Clave Pública (PKI)[6]. Se compone de:

- **Formato del Certificado:** Contiene el número de serie, entidad emisora, clave pública del titular y firma de la autoridad de certificación.
- **Validación y Revocación:** Incluye métodos como CRL (Certificate Revocation List) y OCSP (Online Certificate Status Protocol) para verificar el estado de los certificados.

SSL/TLS (Protocolos de Comunicación Segura): Garantizan la transmisión segura de datos sobre redes inseguras mediante cifrado y autenticación [7]. Sus aspectos más relevantes incluyen:

- **Handshake TLS:** Intercambio de claves entre cliente y servidor, asegurando autenticación mutua.
- **Versiones:** Evolución desde SSL 3.0 hasta TLS 1.3, mejorando seguridad y eliminando algoritmos vulnerables como MD5 y SHA-1.
- **Aplicaciones:** Implementación en HTTPS, VPNs y sistemas de autenticación para proteger información confidencial.

OCSP (Online Certificate Status Protocol): Es un protocolo que permite verificar la validez de certificados en tiempo real sin necesidad de descargar CRLs completas. Sus características clave incluyen:

- **Interacción Cliente-Servidor:** Permite la verificación de certificados digitales con una autoridad de certificación sin necesidad de listas extensas.
- **Comparación con CRL: OCSP** ofrece tiempos de respuesta más rápidos y menor consumo de ancho de banda en comparación con las listas de revocación tradicionales.

4. Esquema de Funcionamiento de la Firma Digital: Proceso de Generación y Verificación

4.1. Proceso de Generación de la Firma Digital

Documento original: El usuario tiene un documento o mensaje que desea firmar digitalmente.

Hash del documento: Se aplica una función hash criptográfica al documento, generando un resumen o huella digital única (hash).

Encriptación del hash con clave privada: El hash se cifra usando la clave privada del firmante, generando la firma digital.

Envío del documento + firma digital: El documento original y la firma digital se envían juntos al receptor.

4.2. Proceso de Verificación de la Firma Digital

Recepción del documento + firma digital: El receptor recibe el documento junto con la firma digital.

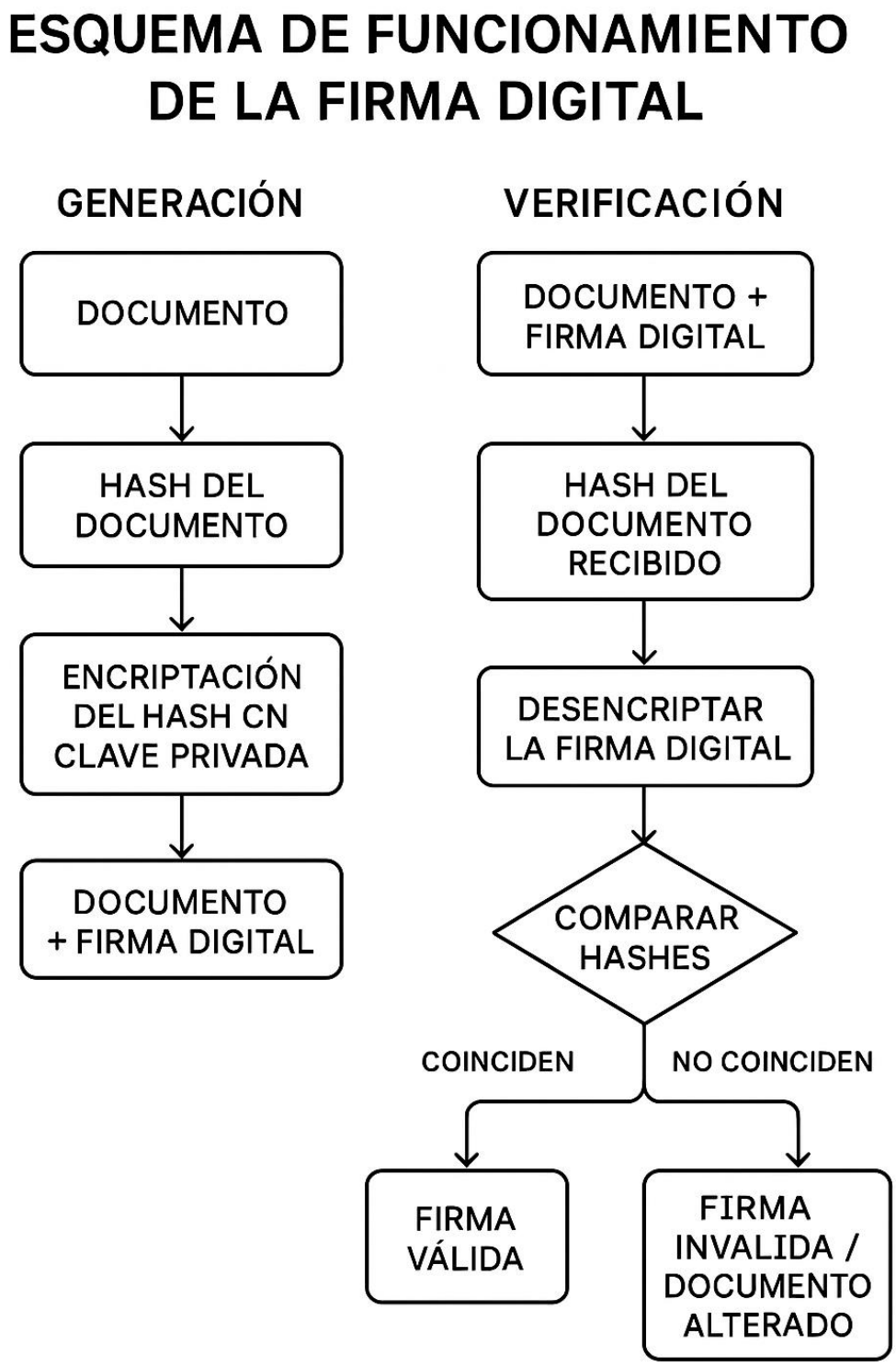
Hash del documento recibido: El receptor aplica la misma función hash al documento recibido para obtener un hash.

Desencriptar la firma digital: Se desencripta la firma digital usando la clave pública del firmante, recuperando el hash original firmado.

Comparar hashes: Se comparan el hash generado por el receptor con el hash recuperado al desencriptar la firma.

Si coinciden, la firma es válida y el documento no ha sido modificado.

Si no coinciden, la firma es inválida o el documento fue alterado.



5. Estructura Técnica de un Sistema de Firma Digital

Un sistema de firma digital se fundamenta en la Infraestructura de Clave Pública (PKI), que permite garantizar la autenticidad, integridad y no repudio de los

documentos electrónicos mediante el uso de criptografía asimétrica y certificados digitales emitidos por entidades confiables [8]

1. Criptografía Asimétrica

La base técnica de la firma digital es la criptografía asimétrica, que utiliza un par de claves:

- Clave privada: conocida solo por el firmante, se utiliza para generar la firma digital.
- Clave pública: disponible para cualquiera, se utiliza para verificar la validez de la firma.

Este esquema garantiza que solo el propietario legítimo pueda generar la firma y que cualquiera pueda verificarla, garantizando así la seguridad y confianza del sistema [8]

2. Certificados Digitales

Los certificados digitales son documentos electrónicos que vinculan una clave pública con la identidad de su propietario, emitidos por una Autoridad Certificadora (CA) confiable. Contienen información como:

- Nombre del titular,
- Clave pública,
- Período de validez,
- Firma digital de la CA.

Estos certificados aseguran la validez y autenticidad de las claves utilizadas en la comunicación [9]

3. Autoridad de Certificación (CA)

La CA es la entidad responsable de emitir y revocar certificados digitales. Para ello, verifica la identidad del solicitante antes de emitir un certificado, garantizando así que las claves públicas estén correctamente asociadas con sus titulares [8]

4. Autoridad de Registro (RA)

La RA actúa como un intermediario entre el usuario y la CA. Se encarga de verificar la identidad del solicitante y aprobar las solicitudes de certificados digitales antes de que la CA los emita [8]

5. Listas de Revocación de Certificados (CRL)

Las CRL son listas mantenidas por la CA donde se enumeran los certificados que han sido revocados antes de su fecha de expiración, ya sea por compromiso de la clave o por cambio de estado del firmante. Esto permite mantener actualizado el estado de validez de los certificados [9]

6. Proceso de Firma Digital

El proceso técnico incluye:

1. Aplicar una función hash al documento para obtener un resumen único.

2. Cifrar el resumen con la clave privada del firmante, generando la firma digital.

3. Adjuntar la firma digital al documento.

4. El receptor utiliza la clave pública del firmante para descifrar la firma y verificar que el resumen coincida, validando así integridad y autenticidad [8]

6. Aplicaciones Prácticas de la Firma Digital: Escenarios Comunes de Uso

1. Firma de Documentos Electrónicos

La firma digital se ha implementado exitosamente en el ámbito académico para la emisión de documentos oficiales. Por ejemplo, en la Universidad Nacional de Barranca, Perú, la adopción de una plataforma de firma digital redujo significativamente el tiempo de entrega de documentos académicos, pasando de 10 días a un máximo de 2 días, mejorando la eficiencia y satisfacción estudiantil [10]

2. Trámites Gubernamentales en Línea

En Ecuador, la implementación del Documento Nacional de Identidad Electrónico ha facilitado el acceso a servicios electrónicos públicos y privados. Este documento, respaldado por certificados digitales, permite validar la identidad de los ciudadanos en línea, mejorando la seguridad y eficiencia de los trámites gubernamentales [9]

3. Transacciones Bancarias Seguras

La firma digital cualificada se utiliza en el sector financiero para autenticar transacciones, firmar contratos y abrir cuentas de forma remota. Esto mejora la eficiencia operativa y la seguridad en las operaciones bancarias. Aunque no se identificó un estudio académico específico con DOI, diversas entidades financieras en América Latina han documentado su implementación en informes técnicos y normativas sectoriales.

Bibliografía

[1] A. Dasgupta, A. Roy y S. Saha, "A comparative study of digital signature algorithms", *Procedia Computer Science*, vol. 167, pp. 2344–2353, 2020. doi: https://doi.org/10.1016/j.procs.2020.03.289

[2] T. Khovratovich, J. Mennink, y L. Reyzin, "A formal treatment of the leakage resilience of the sponge construction", *Advances in Cryptology – EUROCRYPT 2014*, pp. 512–531, 2014. doi: https://doi.org/10.1007/978-3-642-55220-5_29

[3] S. S. Al-Riyami y K. G. Paterson, "Certificateless Public Key Cryptography", *Advances in Cryptology – ASIACRYPT 2003*, pp. 452–473, 2003. doi: https://doi.org/10.1007/978-3-540-40061-5_29

[4] J. Katz y Y. Lindell, *Introduction to Modern Cryptography*, 2nd ed., Chapman and Hall/CRC, 2014. doi: https://doi.org/10.1201/b17668

[5] Y. Liu, Y. Li, C. Xu y J. Hu, "An overview of security and privacy in smart devices", *Future Generation Computer Systems*, vol. 92, pp. 1164–1179, 2019. doi: https://doi.org/10.1016/j.future.2018.06.037

[6] M. Mladenov, T. Truderung, and R. Schmitz, "On the Validation of Web X.509 Certificates by TLS Interception Products," *IEEE Transactions on Dependable and Secure Computing*, vol. PP, no. 99, pp. 1-1, Jun. 2020, doi: https://ieeexplore.ieee.org/document/9110796

[7] J. E. Pino, R. G. Carrión, and D. C. Navas, "Análisis de Certificados SSL/TLS gratuitos y su implementación como Mecanismo de seguridad en Servidores de Aplicación," *Enfoque UTE*, vol. 8, supl. 1, Quito, Ecuador, pp. 128-138, Feb. 2017, doi: https://doi.org/10.29019/enfoqueute.v8n1.128.

***Blibliografias Dario

[8] A. J. Jiménez Alfaro, E. Corona-Organiche, G. Cortés-Barrera, e I. C. Alcocer-Guillermo, “Un protocolo criptográfico de firma digital para el signado de documentos digitales con criptografía asimétrica para el intercambio seguro de información en la empresa CDS, S.C.,” *Revista de Investigación Científica, Tecnológica e Innovación*, vol. 2, no. 3, 2024. [En línea]. Disponible en: https://revista.ccaitese.com/index.php/ridt/article/view/43

[9] C. F. Cedeño Sarmiento, A. G. Mendoza Arteaga, G. I. Mendoza Cedeño, y E. J. Macías Arias, “Aplicaciones de la firma electrónica mediante certificados digitales: El Documento Nacional de Identidad Electrónico en el Ecuador,” *Revista Científica Sinapsis*, vol. 1, no. 8, 2016. [En línea]. Disponible en: https://doi.org/10.37117/s.v1i8.78

[10] R. M. Ampuero Herrera, “Aplicación de la plataforma de firma digital en la emisión de los documentos académicos de una Universidad Pública,” *Alpha Centauri*, vol. 5, no. 3, 2024. [En línea]. Disponible en: https://journalalphacentauri.com/index.php/revista/article/view/176