Firma Digital y DSA

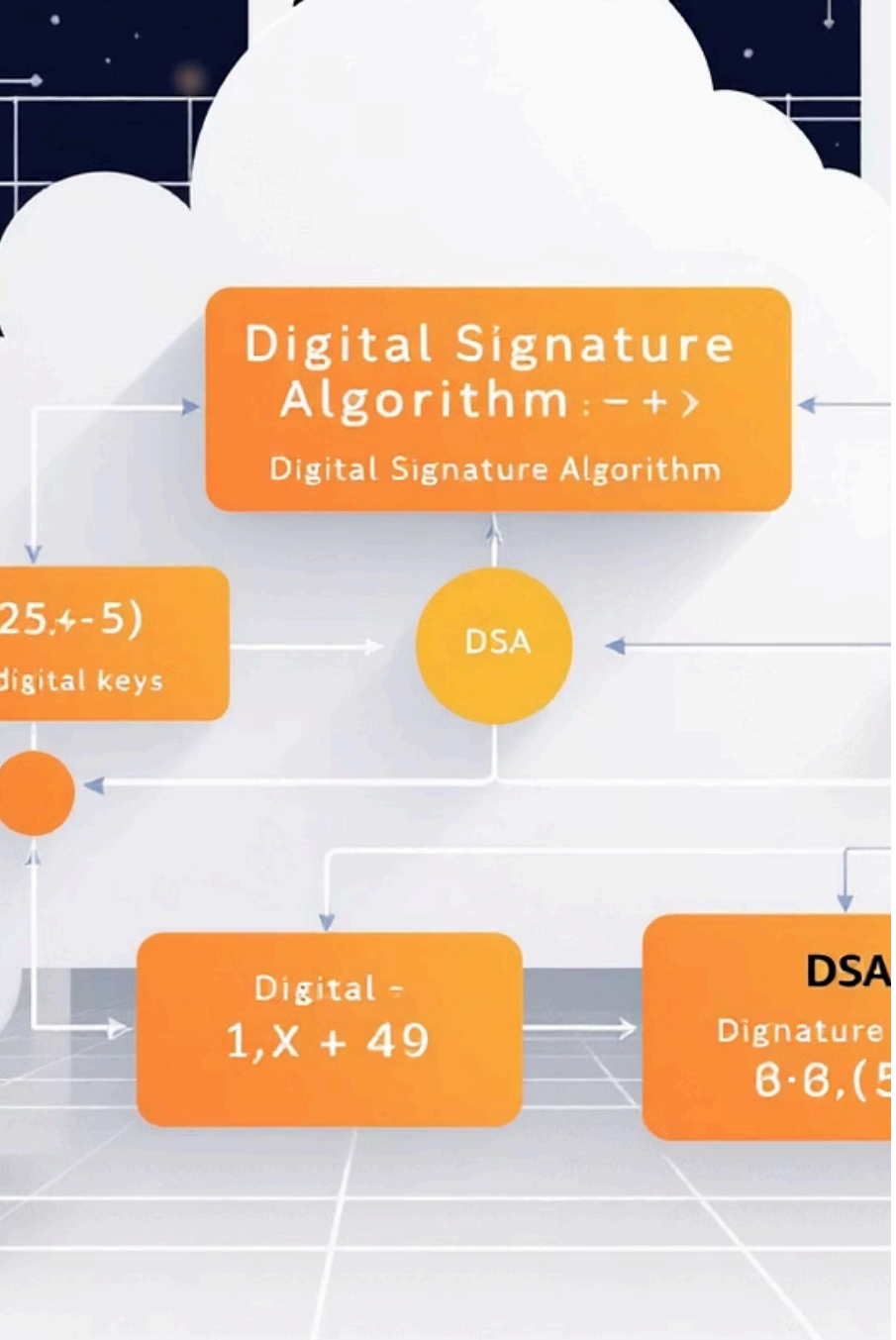
¿Qué es una Firma Digital?

Una **firma digital** es el equivalente electrónico de una firma manuscrita, pero mucho más segura. Es como un sello único e imposible de falsificar que garantiza:

- **Autenticidad**: Confirma quién envió el mensaje
- **Integridad**: Asegura que el mensaje no fue alterado
- **No repudio**: El firmante no puede negar que lo firmó

Definición de la tecnología

La *tecnología de firma digital* es un conjunto de métodos criptográficos que usa **criptografía de clave pública (asimétrica)** para producir y verificar firmas. Se basa en pares de claves (privada/pública), funciones hash y estándares que permiten asociar de forma verificable una identidad con un mensaje o documento digital.



¿Qué es DSA?

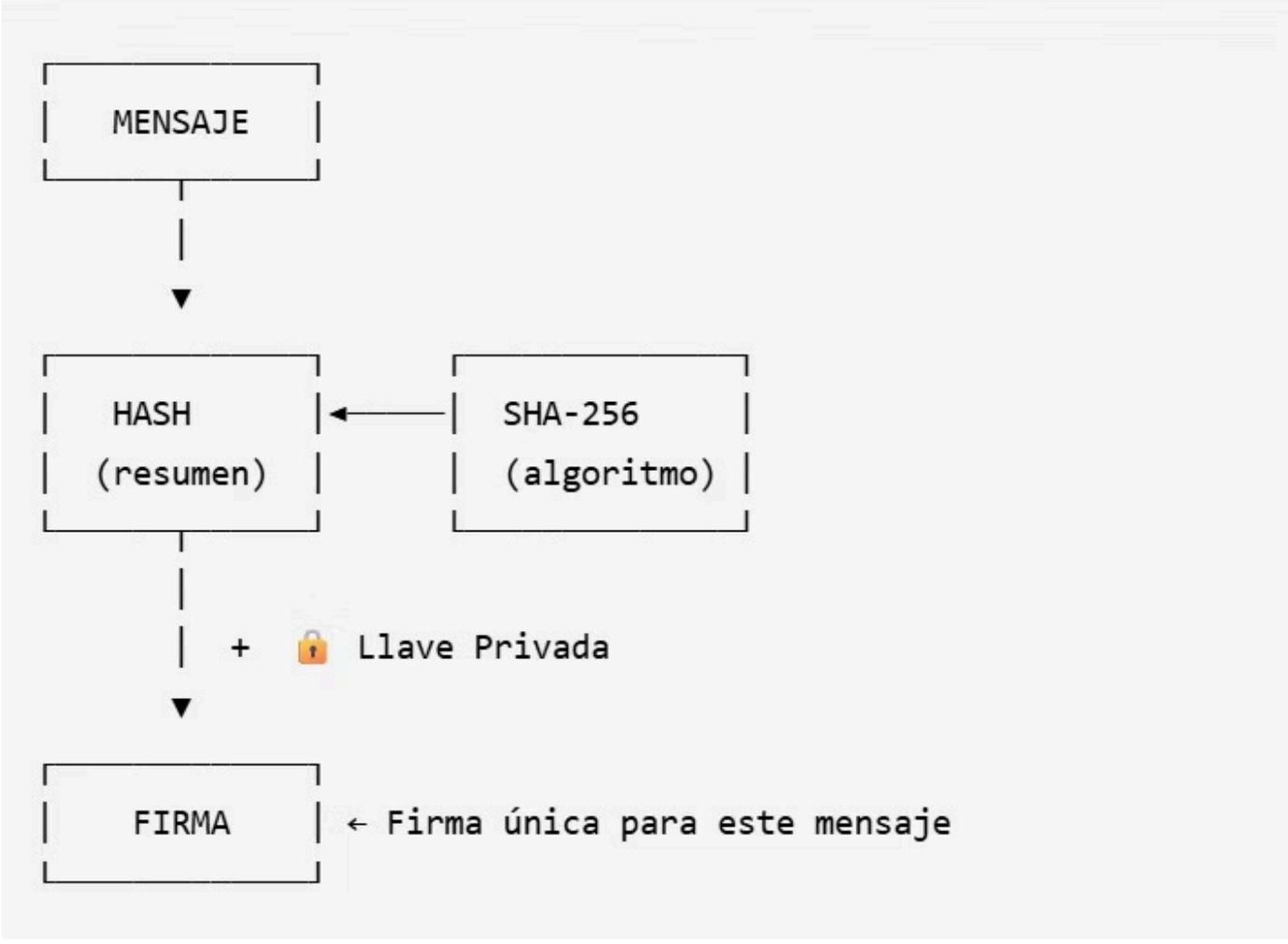
DSA (Digital Signature Algorithm) es un algoritmo matemático para crear firmas digitales. Fue desarrollado por el gobierno de EE.UU. y es un estándar federal.

¿Cómo funciona DSA? (Explicación simple)

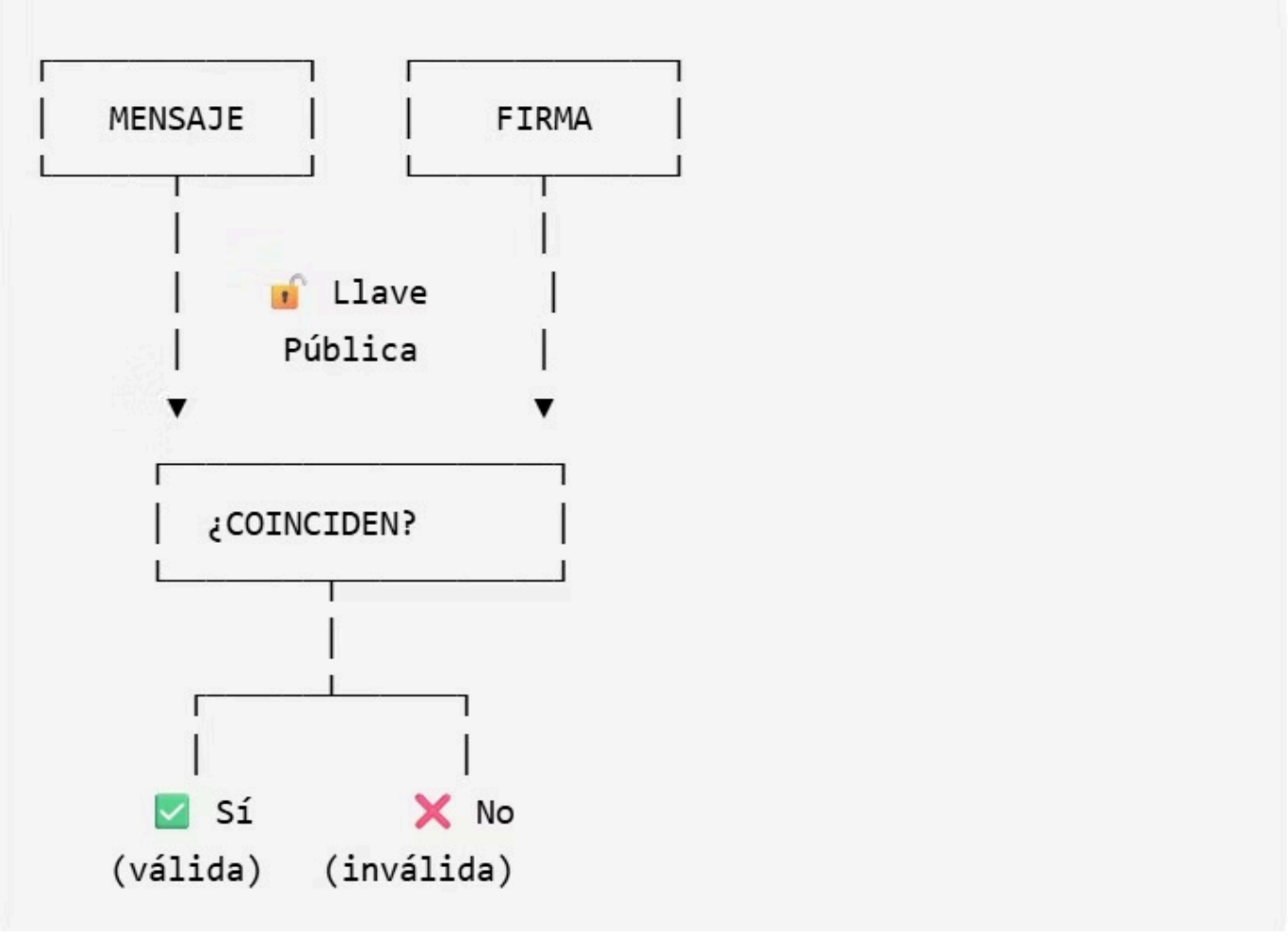
Imagina que tienes dos llaves:

1. **Llave Privada (secreta)**: Solo tú la tienes, NUNCA la compartes
2. **Llave Pública (compartida)**: La pueden tener todos

Proceso de firma:



Proceso de verificación:



Seguridad

¿Es seguro DSA?

- Sí, pero se recomienda usar **EdDSA** o **RSA-PSS** para nuevos proyectos
- DSA es seguro si se usa correctamente (claves de 2048+ bits)
- Nunca compartas tu clave privada

Conceptos Clave

Término	Significado
Hash	Un "resumen" único del mensaje (como una huella digital)
SHA-256	Algoritmo para crear el hash (256 bits de salida)
Clave Privada	Tu secreto, solo para ti
Clave Pública	Compartida con todos, usada para verificar
Firma	Resultado de aplicar tu clave privada al hash del mensaje

Algoritmos criptográficos involucrados

Los siguientes algoritmos son fundamentales para la implementación de la firma digital con DSA, como se observa en el código y su contexto matemático:

- **DSA (Digital Signature Algorithm)**

Algoritmo principal para generar el par de claves (pública/privada) y producir la firma.

- **SHA-256** (Secure Hash Algorithm - 256 bits)

Se utiliza para calcular el *resumen* (*message digest*) del mensaje. El código firma este resumen, no el mensaje completo, asegurando la integridad.

- **Generación de Números Aleatorios (RNG)**

- Cryptographically Secure Pseudo-Random Number Generator

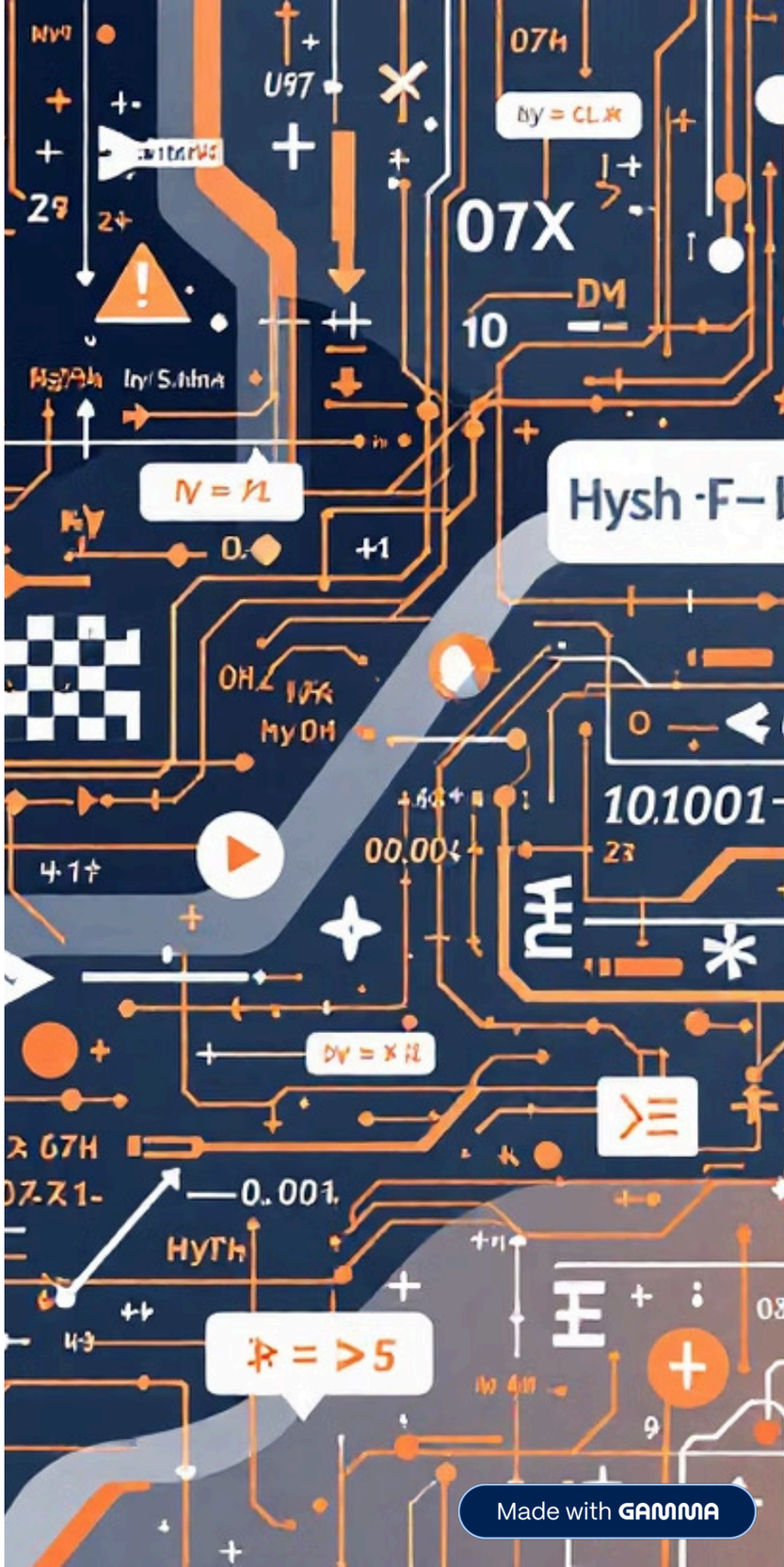
- Usado para generar claves privadas y valores "k" en el proceso de firma

- Crítico: Un RNG débil compromete toda la seguridad

- **Algoritmos de Generación de Claves**

- Generación de parámetros de dominio (p, q, g)

- Generación de pares de claves (privada/pública)}.



Protocolos criptográficos involucrados

DSA no es un protocolo de comunicación en sí mismo, sino un componente criptográfico que opera dentro de protocolos más grandes para proporcionar servicios de autenticación y seguridad:

1. FIPS / DSS (Digital Signature Standard) — definición normativa de DSA (generación de parámetros, formatos). (NIST FIPS 186 series).
2. RFC 6979 (Deterministic DSA/ECDSA) — procedimiento recomendado para generación determinística del nonce en DSA/ECDSA.
3. TLS (SSL/TLS) — en versiones históricas TLS/TLS 1.2 manejan DSA/DSS como uno de los algoritmos de firma aceptados (uso en certificados y en autenticación).
4. S/MIME / X.509 (PKI) — sistemas de firma de correo y certificados X.509 pueden contener claves DSA y usarlas para firmar/validar mensajes y certificados.
5. Implementaciones y librerías criptográficas (OpenSSL, cryptography, etc.) implementan DSA y/o sus variantes; en la práctica muchas migraciones han ido a ECDSA/EdDSA por eficiencia y tamaño de llave.

Escenarios donde se utiliza con frecuencia

Firma de Documentos Oficiales y Legales

Utilizado por gobiernos y empresas para aplicar la firma digital con valor legal, garantizando la identidad del firmante y la inalterabilidad del contenido, como en sistemas de historial clínico digital o contratos electrónicos.

Validación de Certificados Digitales (PKI)

Esencial en la Infraestructura de Clave Pública. Las Autoridades de Certificación (CA) firman los certificados X.509 utilizando DSA (o ECDSA/RSA) para establecer una cadena de confianza y validar la identidad de sitios web (HTTPS).

Integridad de Software y Distribución de Código

Utilizado por desarrolladores y distribuidores de software para firmar los ejecutables y las actualizaciones. Esto permite al usuario verificar que el software no ha sido manipulado por atacantes (malware) y que proviene de una fuente legítima.

Preguntas relacionadas

1. Verdadero o Falso:

SHA-1 es seguro para crear nuevas firmas digitales en aplicaciones modernas y se recomienda su uso para garantizar la integridad de mensajes a largo plazo.

2. Opción Múltiple (Una respuesta)

¿Cuál de los siguientes esquemas de firma se recomienda para nuevas implementaciones de firma con RSA?

a) RSASSA-PKCS1-v1_5

b) RSA-PSS

c) RSA-OAEP

d) RSA-ES

3. Opción Múltiple (Múltiples respuestas)

¿Al verificar una firma digital en un entorno con PKI, ¿cuáles de las siguientes comprobaciones son relevantes? (Selecciona 3)

a) Calcular localmente el hash del mensaje y compararlo con lo que verifica la firma.

b) Confirmar que el certificado del firmante no esté revocado (OCSP/CRL).

c) Comprobar que la clave privada del firmante esté almacenada en un HSM.

d) Verificar la cadena de confianza del certificado hasta una CA confiable.

e) Asegurarse de que el mensaje fue cifrado con AES.

4. Emparejamiento - Relaciona cada algoritmo con su característica principal.

DSA — a) Firma basada en curvas elípticas, tamaños de clave pequeños.

ECDSA — b) Estándar histórico de firma federal (originalmente FIPS 186).

Ed25519 — c) Proporciona resistencia y rendimiento con claves y firmas pequeñas (EdDSA).

RSA-PSS — d) Esquema de firma probabilístico recomendado para RSA.

5. Completar con una palabra

El estándar que define el formato para firmar objetos JSON en APIs y tokens (p. ej. tokens firmados en OAuth/OpenID) se denomina _____.

Referencias

[1] National Institute of Standards and Technology, *Digital Signature Standard (DSS)*, FIPS 186-5, 2023. [Online]. Disponible en: https://doi.org/10.6028/NIST.FIPS.186-5

[2] O. M. Semyonov, A. I. Chernykh, V. A. Evdokimov, y D. R. Tyncheva, "Eliminating Broadband Covert Channels in DSA-Like Signatures," en *Proc. IEEE Conf.*, 2021, pp. 1–6. doi: 10.1109/REDUNDANCY52534.2021.9606457

[3] M. Al-Haj y B. Tubaishat, "Using Digital Signature Standard Algorithm to Incorporate Non-invertibility in Private Digital Watermarking Techniques," en *Proc. ACIS Int. Conf. Softw. Eng., Artif. Intell., Netw. Parallel/Distrib. Comput.*, 2009, pp. 299–304. doi: 10.1109/SNPD.2009.89

[4] W. Li, S. Liu, y W. Liu, "Improved speed Digital Signature Algorithm based on modular inverse," en *Proc. Int. Conf. Inf. Sci. Technol.*, 2013, pp. 780–783. doi: 10.1109/MIC.2013.6758059

[5] H. Kaur, J. Singh, y J. Kaur, "Secure encryption with digital signature approach for Short Message Service," en *Proc. World Congr. Inf. Commun. Technol.*, 2012, pp. 1104–1108. doi: 10.1109/WICT.2012.6409184