Revista Digital del Departamento de Ingeniería e Investigaciones Tecnológicas de la Universidad Nacional de la Matanza
ISSN: 2525-1333
Vol.: 9 - Nro. 1 (JULIO 2024)

Sección de alumnos: artículo original

Criptografía: Autoridad Certificante

Cryptography: Certification authority

Integrantes:

Ramiro Alejo Acosta Bernascone[(1)]
Ingeniería Informática-Universidad Nacional de La Matanza
raacostabernascone@alumno.unlam.edu.ar

Octavio Dion Gemellaro[(2)]
Ingeniería Informática-Universidad Nacional de La Matanza
ogemellaro@alumno.unlam.edu.ar

Aylen Paula Gómez[(3)]
Ingeniería Informática-Universidad Nacional de La Matanza
aygomez@alumno.unlam.edu.ar

Franco My[(4)]
Ingeniería Informática-Universidad Nacional de La Matanza
frmy@alumno.unlam.edu.ar

Referentes Institucionales:

Alejandro Silvestri
Universidad Nacional de La Matanza
jasilvestri@unlam.edu.ar

Martín Zeballos
Universidad Nacional de La Matanza
mzeballos@unlam.edu.ar

Revista Digital del Departamento de Ingeniería e Investigaciones Tecnológicas de la Universidad Nacional de la Matanza
ISSN: 2525-1333
Vol.: 9 - Nro. 1 (JULIO 2024)

Resumen:

El siguiente artículo explora varios aspectos fundamentales de la seguridad en las comunicaciones digitales, enfocados en la autenticidad y confidencialidad de los mensajes. Comenzaremos dando una breve explicación acerca de la autenticidad en la comunicación digital, qué es y cómo se utiliza la firma digital. Luego desarrollaremos los conceptos algebraicos asociados, tales como Algoritmos Asimétricos, donde marcaremos las diferencias con los algoritmos simétricos. Analizaremos el algoritmo RSA, su funcionamiento y su fortaleza basada en la factorización de números primos. También explicaremos las funciones de Hash y su papel en la firma digital, importancia de los resúmenes de mensajes y la detección de colisiones en las funciones de hash. Aplicaciones principales de las funciones de hash en la seguridad digital. Certificados digitales y PKI. Definición y estructura de los certificados digitales. Descripción de la PKI y sus componentes clave, incluyendo las políticas y procedimientos para la gestión de claves y certificados. Aplicaciones prácticas de la PKI. Potenciales vulnerabilidades en los algoritmos y sistemas utilizados. Importancia de la gestión adecuada de las claves privadas y la confianza en las Autoridades Certificantes. Haremos una implementación de la firma de un documento y por último una conclusión de todo el trabajo.

Abstract:

This article explores fundamental aspects of digital communication security, focusing on message authenticity and confidentiality. We begin with a brief explanation of digital communication authenticity and the use of digital signatures. Then, we delve into algebraic concepts such as asymmetric algorithms, highlighting their differences from symmetric algorithms. We analyze the RSA algorithm, its operation, and its strength based on the factorization of prime numbers. Additionally, we explain hash functions and their role in digital signatures, the importance of message digests, and collision detection in hash functions. We discuss the main applications of hash functions in digital security, digital certificates, and PKI. This includes definitions and structures of digital certificates and the PKI's key components, such as policies and procedures

ISSN: 2525-1333
Vol.: 9 - Nro. 1 (JULIO 2024)

for managing keys and certificates, as well as the practical applications of PKI. We also examine potential vulnerabilities in the algorithms and systems used, emphasizing the importance of proper management of private keys and trust in Certification Authorities. Finally, we implement document signing and conclude the work.

Palabras Clave: *Criptografía, Firma digital, Algoritmo RSA, Funciones de hash, Certificados digitales*

Key Words: *Cryptography, Digital signatura, RSA algorithm, Hash functions, Digital certificates*

ISSN: 2525-1333. Vol.: 9 - Nro. 1 (JULIO-2024)

I. INTRODUCCIÓN

Antes de la aparición de Internet, los mensajes a los que accedía un individuo provenían de fuentes conocidas, por lo que no era necesario comprobar la autenticidad del emisor del mensaje. Esto cambió con la aparición de Internet y las nuevas tecnologías de la comunicación, donde los individuos se ven expuestos a una gran cantidad de mensajes que provienen de muy diversas fuentes y, en algunos casos, desconocidas. Previo a esta situación, el problema que enfrentaban las comunicaciones era la confidencialidad del mensaje, lo cual se solventó con los sistemas de cifrado simétrico y asimétrico, pero ahora el principal problema en las comunicaciones es la autenticidad del emisor del mensaje [1]. Para abordar este problema, surge el concepto de firma digital como solución fundamental.

La firma digital es una herramienta que autentica la identidad del remitente de un mensaje, asegurando que quien envía el mensaje es realmente quien dice ser. Esto se logra mediante un sistema de criptografía asimétrica, que utiliza un par de claves (una pública y una privada) y una infraestructura de verificación de claves [2].

El cifrado con la clave pública del receptor del mensaje permite proteger la confidencialidad e integridad de los datos transmitidos, ya que sólo el destinatario previsto puede acceder a la información descifrando el mensaje con la clave privada [3].

En cambio, el cifrado con la clave privada del emisor, permite garantizar que el mensaje fue emitido únicamente por la persona poseedora de dicha clave, y cualquier receptor puede verificarlo descifrando el mensaje con la clave pública del emisor.

La seguridad del sistema de firma digital se basa en la confianza mutua entre las partes que se comunican y las Autoridades Certificantes (AC), que son responsables de emitir y verificar los certificados digitales que asocian una clave pública a una entidad [4]. Estos certificados confirman la autenticidad de las claves públicas utilizadas en la comunicación.

La robustez de este esquema de seguridad depende tanto de la fiabilidad de las ACs como de la fortaleza de los algoritmos de cifrado asimétrico. En conjunto, la firma digital y el cifrado con clave pública proporcionan un marco sólido para proteger las comunicaciones en internet contra manipulaciones y suplantaciones, garantizando la autenticidad y privacidad de los mensajes.

II. CONCEPTOS ALGEBRAICOS

Algoritmos Asimétricos

La principal característica de los algoritmos asimétricos es que no utilizan una clave única compartida entre emisor y receptor, sino que utiliza un par de claves distintas. El algoritmo de cifrado asimétrico más popular es RSA. Si comparamos los algoritmos asimétricos de cifrado con los simétricos, veremos que la clave en aquellos asimétricos es mucho mayor que en los segundos. En los simétricos se considera como segura una clave de 128 bits y en los

ISSN: 2525-1333. Vol.: 9 - Nro. 1 (JULIO-2024)

asimétricos se recomiendan claves de al menos 1024 bits. La desventaja de los algoritmos asimétricos es la velocidad de cifrado, ya que es muy inferior a la velocidad de cifrado de un algoritmo simétrico.

En este tipo de algoritmos se utilizan un par de claves distintas: Una pública (la clave pública se puede compartir abiertamente sin comprometer la seguridad) y una privada (debe ser mantenida en secreto y bajo control exclusivo del propietario). Si utilizamos una para cifrar un bloque, debemos utilizar la otra para descifrarlo. Para que el sistema sea seguro, la tarea de calcular una de las claves a partir de la otra debe ser de complejidad no polinomial. Como vimos anteriormente en la introducción, los algoritmos simétricos tienen dos aplicaciones principales: la protección de la información y la autenticación del emisor. La primera consiste en cifrar el mensaje para poder transmitirlo por un canal inseguro. Para lograrlo el emisor obtiene la clave pública del receptor, cifra el mensaje y luego se lo envía al receptor. Éste último puede descifrar el mensaje con su clave privada. La segunda aplicación consiste en autenticar que el emisor del mensaje es quien realmente dice ser. El mecanismo consiste en que el emisor realiza un resumen del mensaje a través de una función de hash, luego cifra este resumen con su clave privada y envía tanto el mensaje como el resumen al receptor. Luego el receptor puede realizar su propio resumen del mensaje con la misma función de hash utilizada por el emisor, descifrar el resumen enviado por el emisor con la clave pública asociada a él y comparar los resúmenes. Si coinciden, el mensaje fue cifrado por la clave privada del emisor.

Si bien para firmar digitalmente un archivo podemos utilizar diferentes algoritmos simétricos de cifrado (DSA, RSA, ECDSA) pasaremos a explicar el funcionamiento de RSA que es el que utilizamos en la implementación [5].

RSA

RSA es un algoritmo de cifrado asimétrico que se basa en la dificultad de factorizar grandes números primos, tarea cuya complejidad computacional es no polinomial. Utiliza un par de claves que llamaremos ‘d’ y ‘e’. El mecanismo de cifrado consiste en elevar el bloque de mensaje a una de las claves (Por ejemplo ‘e’) en módulo ‘n’, y luego el descifrado consiste en elevar el bloque de criptograma a la otra clave (llamada ‘d’) en módulo ‘n’, para así obtener el mensaje original. Para que esto funcione, $e*d = 1 \bmod \varphi(n)$, ya que según el teorema de Euler $a\varphi^{(n)+1} = a \bmod n$.

ISSN: 2525-1333. Vol.: 9 - Nro. 1 (JULIO-2024)

3. **Demostración de $a^{\phi(n)+1} \equiv a \pmod{n}$:**

- Dado que a y n son coprimos, aplicamos el teorema de Euler:

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

- Multiplicamos ambos lados de esta congruencia por a:

$$a^{\phi(n)} \cdot a \equiv 1 \cdot a \pmod{n}$$

- Simplificando, obtenemos:

$$a^{\phi(n)+1} \equiv a \pmod{n}$$

Esta es la demostración de que $a^{\phi(n)+1} \equiv a \pmod{n}$, utilizando el teorema de Euler.

Fig. 1: Demostración del teorema de Euler

En cualquier caso, el bloque a cifrar debe ser menor que ‘n’.

Para generar el par de claves, el algoritmo debe obtener en primera instancia dos números primos grandes ‘p’ y ‘q’ distintos entre sí, luego calcula n = p * q y finalmente calcula φ(n) = (p-1)*(q-1). En siguiente instancia se genera un número ‘e’ que debe cumplir que ‘e’ sea primo relativo con φ(n) y gcd(φ(n),1)=1 con 1< e < φ(n). Finalmente, se calcula ‘d’ como e-1 mod φ(n) con el algoritmo extendido de Euclides. Por último, se descartan ‘p’ y ‘q’ y se elige una de las dos claves como pública y la otra como privada [6].

La fortaleza de RSA reside en que conociendo ‘e’ y ‘n’ calcular ‘d’ consiste en obtener e-1 mod φ(n), para lo cual debemos calcular φ(n). La forma de obtener φ(n) es encontrando ‘p’ y ‘q’ y para ello se debe factorizar ‘n’ lo cual tiene una complejidad no polinomial (siempre y cuando ‘p’ y ‘q’ y en consecuencia ‘n’ sean lo suficientemente grandes). Si se encontrase una técnica de factoreo con complejidad polinómica, la fortaleza de RSA desaparecería.

A pesar de su amplia adopción y robustez, el algoritmo RSA no está exento de vulnerabilidades y desafíos que pueden comprometer su seguridad [7]. A continuación, se detallan algunas de las principales vulnerabilidades de RSA:

1. Factorización de grandes números:
    - La seguridad de RSA se basa en la dificultad de factorizar grandes números compuestos por dos primos. Si un atacante puede factorizar eficientemente el número nnn (producto de los primos ppp y qqq), puede derivar la clave privada y descifrar los mensajes. Los avances en algoritmos de factorización y el aumento en el poder de computación pueden poner en riesgo la seguridad de RSA, especialmente con claves más cortas.

ISSN: 2525-1333. Vol.: 9 - Nro. 1 (JULIO-2024)

2. Ataques de criptoanálisis:
    - Ataque de texto cifrado elegido (CCA): Un atacante puede obtener textos cifrados y solicitar su descifrado (dentro de un entorno controlado), aprendiendo así información sobre la clave privada.
    - Ataque de clave privada pequeña: Si los exponentes de clave privada ddd son demasiado pequeños, los ataques como el ataque de Wiener pueden ser efectivos para recuperar la clave privada.
3. Ataques de canal lateral:
    - Estos ataques no se centran en debilidades matemáticas del algoritmo, sino en la implementación física. Ejemplos incluyen ataques de tiempo, donde se mide el tiempo que toma descifrar un mensaje, y ataques de análisis de potencia, donde se analiza el consumo de energía del dispositivo durante el proceso de descifrado.
4. Implementaciones defectuosas:
    - Las implementaciones incorrectas de RSA pueden introducir vulnerabilidades. Ejemplos incluyen la generación de claves defectuosas, la falta de relleno adecuado (padding) y la reutilización de claves.
5. Problemas con el relleno (padding):
    - RSA requiere técnicas de relleno seguras como OAEP (Optimal Asymmetric Encryption Padding) para prevenir ataques como el ataque de relleno de texto cifrado (Padding Oracle Attack). Implementaciones que no usan relleno seguro pueden ser vulnerables a este tipo de ataques.
6. Ataques basados en la estructura matemática:
    - Ataque de Hastad: Si el mismo mensaje es enviado a varios destinatarios usando el mismo exponente público pequeño (por ejemplo, e=3e = 3e=3), es posible recuperar el mensaje original mediante el teorema chino del resto.
    - Ataques de frecuencia de clave: Si la clave pública eee es común (como el valor 65537 que es ampliamente utilizado), y si la misma clave privada ddd se reutiliza con múltiples claves públicas nnn, la seguridad puede verse comprometida.
7. Uso de claves insuficientemente largas:
    - La fortaleza de RSA se debilita significativamente con claves de menor longitud. Se recomienda un tamaño de clave mínimo de 2048 bits para asegurar una protección adecuada, aunque para mayor seguridad, especialmente en el largo plazo, se recomienda el uso de claves de 3072 bits o mayores.

ISSN: 2525-1333. Vol.: 9 - Nro. 1 (JULIO-2024)

8. Algoritmos cuánticos:
    - Los avances en computación cuántica representan una amenaza potencial para RSA. El algoritmo de Shor, que puede ejecutarse en una computadora cuántica, puede factorizar grandes números en tiempo polinómico, lo que quebraría la seguridad de RSA. Aunque la computación cuántica todavía está en sus primeras etapas, es una preocupación futura significativa.

A partir de un algoritmo de cifrado asimétrico podemos ahora firmar nuestros mensajes cifrándolos con nuestra clave privada. El problema de este esquema es que el cifrado asimétrico requiere de una gran capacidad de cómputo y nuestro objetivo principal no es el de la confidencialidad, por lo que, en lugar de cifrar todo el mensaje, podríamos solamente cifrar un resumen del mismo. Por este motivo, para la firma digital se utilizan las funciones de hash [8].

Funciones de Hash

Estas funciones o algoritmos reciben como entrada un conjunto de datos de cualquier tamaño y devuelven otro conjunto de datos de tamaño fijo, independiente del tamaño del conjunto de entrada. Al resultado de esta función se lo denomina "Hash", "resumen" o "digesto". Idealmente, la función de Hash debe producir resúmenes que estén asociados unívocamente a los datos del archivo original. Sin embargo, es imposible que esto se cumpla, ya que el espacio de mensajes posibles es infinito y la cantidad de hashes no, debido a que su tamaño es finito. Como consecuencia de esto pueden producirse colisiones (Dos mensajes distintos que generen el mismo Hash). Dependiendo del algoritmo de Hash, es prácticamente imposible encontrar dos mensajes distintos que tengan un Hash idéntico.

Gracias a sus características, las aplicaciones principales de las Funciones de Hash, son las siguientes [9]:

- Contraseñas
- Firma Digital
- Sellado de Tiempo
- Integridad y Autenticación
- Autenticación usando MAC (Message Autentication Code)
- Blockchain

Entre las Funciones de Hash más utilizadas, encontramos:

- MD2 (RFC 1115)
- MD4 (RFC 1320)
- MD5 (RFC 1321)
- SHA-1 (NIST FIPS 180-2) y (RFC 3174)
- SHA-2 (SHA-224, SHA-256, SHA-384, y SHA-512)

ISSN: 2525-1333. Vol.: 9 - Nro. 1 (JULIO-2024)

Otras Funciones de Hash son:

- RIPEMD-160, RIPEMD-128, RIPEMD-256 y RIPEMD-320
- WHIRLPOOL-512 (ISO/IEC 10118-3)
- TIGER-192, TIGER-128 y TIGER-160HAVAL

Colisiones

En criptografía, una colisión de hash es una situación que se produce cuando dos entradas distintas a una función de hash producen la misma salida. Es matemáticamente imposible que una función de hash carezca de colisiones, ya que el número potencial de posibles entradas (X) es mayor que el número de salidas (Y) que puede producir un hash. Sin embargo, las colisiones se producen más frecuentemente en los algoritmos cuya salida es de menor cantidad de bits.

Funcionamiento

El mecanismo consiste en dividir el mensaje en bloques fijos de un tamaño ‘m’, luego estos bloques son comprimidos a través de un algoritmo que se repite ‘i’ veces y el resultado es un bloque de tamaño ‘n’ con ‘n’ < ‘m’. Luego el bloque resultado se vuelve a ingresar junto con el siguiente bloque de mensaje al algoritmo de compresión.

Pasaje

Con el conjunto de algoritmos asimétricos de cifrado, funciones de hash y autenticación de los mensajes cifrando con la clave privada y descifrando con la clave pública no solucionamos todos los problemas de la comunicación. Todavía queda un problema a solucionar, cómo puede un usuario saber que la clave pública de una entidad es efectivamente correcta. Es por este motivo que se crea la infraestructura de PK, las autoridades certificantes (AC) y los certificados.

Certificados

Un certificado contiene información sobre una entidad, una fecha de caducidad y la clave pública asociada a dicha entidad. Para que estos certificados tengan validez deben estar firmados digitalmente por una autoridad de certificación. Estos certificados, tienen una estructura jerárquica, donde un usuario puede verificar la autenticidad de un certificado comprobando la firma de la autoridad certificante que lo emitió, pero la autoridad certificante también posee un certificado que fue emitido por otra autoridad certificante. Esta cadena de certificados emitidos por otras autoridades finaliza en lo que se conoce como la autoridad certificante raíz. Todo este sistema de certificados se basa en la confianza que tenga el usuario sobre la autoridad certificante raíz que emitió el certificado que queremos verificar.
El mecanismo para conseguir un certificado consiste en enviar nuestra clave pública a una autoridad de certificación y seguir una serie de pasos para que la misma pueda certificar nuestra identidad.

ISSN: 2525-1333. Vol.: 9 - Nro. 1 (JULIO-2024)

También podemos crear nuestros propios certificados auto firmados, pero para poder utilizarlos es necesario que el mismo esté instalado en el sistema que utilicemos.

III. FUNCIONES PRINCIPALES DE LOS CERTIFICADOS DIGITALES

1. Autenticación: Verifica la identidad de una entidad (persona, organización o dispositivo) en una comunicación digital.
2. Cifrado: Permite el cifrado de datos para proteger la confidencialidad durante la transmisión.
3. Integridad: Asegura que los datos no han sido alterados durante la transmisión.

Componentes de un certificado digital

- Clave Pública: Utilizada para cifrar datos que sólo pueden ser descifrados por la clave privada correspondiente.
- Identidad del Propietario: Información sobre la entidad a la que pertenece la clave pública.
- Firma Digital de la Autoridad Certificante (CA): Verifica la autenticidad del certificado.
- Fecha de Expiración: Indica la validez temporal del certificado.
- Autoridad de Certificación (CA): La entidad que emite y firma el certificado.

Proceso de emisión de un certificado

1. Generación del Par de Claves: El solicitante genera un par de claves (pública y privada).
2. Solicitud de Firma de Certificado (CSR): Se envía a la CA junto con la clave pública y la información de identidad.
3. Verificación de Identidad: La CA verifica la identidad del solicitante.
4. Emisión del Certificado: La CA emite un certificado digital que incluye la clave pública del solicitante y firma digitalmente el certificado.

Jerarquía de certificados y cadena de confianza

- Certificados Intermedios: Emitidos por una CA raíz para delegar la autoridad de emisión de certificados a otras CAs.
- Certificados de Entidad Final: Emitidos para usuarios finales, dispositivos o servidores.
- Cadena de Certificados: Serie de certificados que se verifican unos a otros, comenzando por un certificado de entidad final y ascendiendo a un certificado raíz de confianza.

ISSN: 2525-1333. Vol.: 9 - Nro. 1 (JULIO-2024)

- Certificado Raíz: Certificado autofirmado de la CA raíz, que se incluye en los navegadores y sistemas operativos como entidad de confianza.

IV. APLICACIONES DE CERTIFICADOS DIGITALES

- TLS/SSL: Asegura conexiones web mediante el protocolo HTTPS.
- Firma de Código: Verifica la autenticidad del software y garantiza que no ha sido alterado.
- Cifrado de Correo Electrónico (S/MIME): Protege la confidencialidad y autenticidad de los correos electrónicos.
- Autenticación de Usuarios: Verifica la identidad de los usuarios en aplicaciones y sistemas.

V. INFRAESTRUCTURA DE PKI

PKI es un conjunto de políticas, procedimientos, hardware, software y personas necesarias para gestionar claves criptográficas y certificados digitales. Los componentes clave de una PKI incluyen:

- Autoridades de Certificación (CA): Entidades de confianza que emiten y gestionan certificados digitales. Un certificado digital vincula una clave pública con una identidad (persona, organización o dispositivo).
- Autoridades de Registro (RA): Verifican las identidades de las entidades antes de que una CA emita un certificado digital.
- Repositorio de Certificados: Almacena y distribuye certificados digitales y listas de revocación de certificados (CRL), asegurando que los certificados sean accesibles para los usuarios y sistemas que los necesitan.
- Políticas de Certificación: Conjunto de normas y procedimientos que determinan cómo se manejan las claves y los certificados.

PKI facilita la autenticación, confidencialidad, integridad y no repudio en las comunicaciones digitales. Permite a las organizaciones y a los individuos comunicarse de manera segura en un entorno en el que no se puede confiar completamente en todas las partes implicadas.

Algunos usos habituales de la PKI es la protección de páginas web, el cifrado de archivos, la autenticación y cifrado de correo electrónico, autenticación de nodos de redes inalámbricas y autenticación de conexiones VPN.

HTTPS: HyperText Transfer Protocol Secure

Si aparecen las letras HTTPS al principio de la dirección (URL) de un sitio web, dicho sitio está protegido por un certificado SSL o TLS. Además, en la barra de direcciones del navegador aparece un ícono de un candado y, al hacer clic sobre ese ícono, los usuarios pueden consultar los datos del certificado, como la autoridad emisora y el nombre de

ISSN: 2525-1333. Vol.: 9 - Nro. 1 (JULIO-2024)

la empresa propietaria del sitio web. La PKI permite al navegador y al servidor intercambiar claves públicas de forma segura, asegurando que los datos transmitidos están cifrados y que el sitio web es auténtico.

Autoridad certificante CA

Una Autoridad Certificadora (CA) es una entidad que valida identidades de entidades como sitios web, correos electrónicos, empresas o individuos mediante Certificados Digitales que vinculan a claves criptográficas.

Los Certificados Digitales tienen tres funciones principales: autenticación, cifrado e integridad. Sirven como credenciales para verificar la identidad de la entidad a la que se emiten, aseguran comunicaciones seguras a través de Internet y garantizan que los documentos firmados con ellos no sean alterados durante la transmisión.

Para obtener un certificado, el solicitante genera un par de claves públicas y privadas y envía una solicitud de firma de certificado (CSR) a la CA. La CA valida la identidad del solicitante y emite un certificado que incluye su clave pública, firmado digitalmente para asegurar su autenticidad. Las CA, como SSL.com, integran sus certificados raíz en sistemas operativos y navegadores para emitir certificados SSL/TLS, de correo electrónico, y de firma de código, entre otros, proporcionando una estructura confiable para la seguridad en línea.

Los certificados se utilizan de diversas formas: para asegurar conexiones web mediante TLS/SSL, para firmar digitalmente software con certificados de código, para cifrar y autenticar correos electrónicos con S/MIME y para autenticar usuarios en servidores y aplicaciones con certificados de autenticación de clientes. Cada certificado digital contiene información como nombres de dominio, direcciones de correo y clave pública, esenciales para establecer comunicaciones seguras y confiables.

La confianza en los certificados emitidos por una CA se establece mediante cadenas de certificados que vinculan certificados de entidad final con certificados raíz de CA confiables. Esto asegura que los certificados puedan ser verificados por sistemas con certificados raíz preinstalados, proporcionando un entorno seguro en línea.

La gestión adecuada de las claves privadas es fundamental para mantener la seguridad y la validez de los certificados emitidos. Las CA juegan un papel crucial en la infraestructura de seguridad de Internet al facilitar comunicaciones seguras y confiables entre entidades en la red global.

Mecanismo de firma

El usuario que va a emitir el mensaje realiza un hash del mismo, y cifra ese hash con su clave privada (Generando así la firma). Luego se encarga de enviar el mensaje y el hash cifrado al receptor. El receptor recibe tanto el mensaje como el hash cifrado y para comprobar tanto la integridad del mensaje como la identidad de la persona, toma el certificado digital asociado al usuario emisor del mensaje, descifra el hash con la clave pública asociada al mismo y luego realiza

ISSN: 2525-1333. Vol.: 9 - Nro. 1 (JULIO-2024)

la función de hash sobre el mensaje con el mismo algoritmo que el emisor. Si ambos hashes coinciden, el receptor puede estar seguro de que el mensaje no fue violentado y que el usuario emisor es el asociado al certificado utilizado.

VI. IMPLEMENTACIÓN

Realizamos la implementación de la Autoridad Certificante Raíz a través de openssl. Generamos la clave privada para la CA y creamos el certificado de la CA.

Luego, emitimos el certificado para un usuario. Generamos la clave privada del usuario, y como usuario solicitamos un certificado a la CA. Como CA autorizamos la solicitud de certificado del usuario. Generamos el archivo .pfx del usuario, el mismo contiene tanto el certificado como la clave privada del usuario.

Pasamos a la firma digital del archivo. Sacamos la clave pública del certificado y firmamos el archivo correspondiente con la clave privada.

Verificamos la firma del archivo con la clave pública, respuesta esperada “Verified OK”.

Luego, modificamos el archivo.txt y volvemos a verificar la firma, donde obtenemos como respuesta “Verification failure”.

Realizamos la implementación para emitir un certificado para el dominio “criptografía-unlam.com”. Creamos una clave privada para el dominio y creamos una solicitud de firma de certificado (CSR). Luego, generamos el archivo “criptografía-unlam.ext” de configuración (extensiones) para el certificado. Firmamos el CSR con la CA para obtener el certificado. Por último, configuramos el XAMPP para levantar nuestro servidor local y demostrar la implementación realizada.

VII. CONCLUSIÓN

En la era digital, donde las comunicaciones se realizan predominantemente a través de internet, garantizar la autenticidad y confidencialidad de los mensajes es esencial. El artículo ha explorado cómo estos objetivos se logran mediante el uso de firmas digitales y criptografía asimétrica.

Inicialmente, la principal preocupación en las comunicaciones digitales era la confidencialidad, abordada eficazmente con sistemas de cifrado simétrico y asimétrico. Sin embargo, con la proliferación de fuentes desconocidas en internet, la autenticidad del emisor se convirtió en un problema crítico. La firma digital surgió como una solución robusta, permitiendo autenticar la identidad del remitente y asegurar que el mensaje no haya sido alterado durante la transmisión.

Se analizó el algoritmo RSA, uno de los más populares en criptografía asimétrica, que utiliza un par de claves (pública y privada) para cifrar y descifrar mensajes, garantizando tanto la autenticidad como la confidencialidad. Aunque los

algoritmos asimétricos son más seguros debido a la mayor longitud de sus claves, su velocidad de cifrado es inferior a la de los simétricos.

Las funciones de hash, que generan un resumen fijo de los datos de entrada, son cruciales para la firma digital, permitiendo autenticar mensajes sin necesidad de cifrar todo el contenido, lo cual mejora la eficiencia. Estas funciones son fundamentales para diversas aplicaciones, incluyendo contraseñas, firmas digitales y blockchain.

La Infraestructura de Clave Pública (PKI) y los certificados digitales son esenciales para verificar la autenticidad de las claves públicas. Las Autoridades Certificantes (AC) emiten y verifican estos certificados, creando una cadena de confianza que asegura la autenticidad de las comunicaciones. La PKI, con sus componentes clave como las ACs y las políticas de certificación, facilita la autenticación, confidencialidad e integridad en las comunicaciones digitales.

A pesar de la robustez de estos sistemas, existen vulnerabilidades y desafíos, como la necesidad de una gestión adecuada de las claves privadas y la confianza en las Autoridades Certificantes. La seguridad de los sistemas criptográficos depende tanto de la fortaleza de los algoritmos utilizados como de la fiabilidad de las ACs.

En resumen, la combinación de criptografía asimétrica, funciones de hash y una infraestructura sólida de clave pública proporciona un marco seguro para proteger las comunicaciones en internet, garantizando tanto la autenticidad como la privacidad de los mensajes. Estos mecanismos son fundamentales para mantener la confianza y la seguridad en la era digital.

VIII. REFERENCIAS Y BIBLIOGRAFÍA

[1] Lucena Lopez, Manuel jose (1999). Criptografia y seguridad en computadores (Segunda edición). Universidad de Jaén

[2] Gomez Urgellés, Joan (2010). Matemáticos,espías y piratas informáticos codificación y criptografía. Editec

[3] Equipo de soporte SSL (5 de enero 2024). *¿Qué es una Autoridad de Certificación (CA)?*. SSL. https://www.ssl.com/es/art%C3%ADculo/%C2%BFQu%C3%A9-es-una-autoridad-certificadora-ca%3F/

[4] Profe Sang (29 de enero 2023). Firmas, Certificados Digitales y PKI (Parte del Curso de Criptografía). https://www.youtube.com/watch?v=IunNxCN3YgY&ab_channel=ProfeSang

[5] Edge Seguridad Informática y SysAdmin (4 de mayo 2021). Practica Firmar un documento PDF con certificado digital auto firmado y CA Privada con Openssl. https://www.youtube.com/watch?v=XcoLb04KleM&t=1732s&ab_channel=EdgeSeguridadInform%C3%A1ticaySysAdmin

[6] La cueva del ultimo dragon Last Dragon (4 de julio 2021). Certificados auto firmados con tu propia CA, Let's Encrypt e instalación en de CA en Windows. https://www.youtube.com/watch?v=iokyGm2UDIU&ab_channel=LacuevadelultimodragonLastDragon

ISSN: 2525-1333. Vol.: 9 - Nro. 1 (JULIO-2024)

[7] Diego Córdoba (2 de enero 2023). OpenSSL y certificados digitales – Práctica. https://juncotic.com/openssl-y-certificados-digitales-practica/

[8] Stallings, William. (2017). Cryptography and Network Security: Principles and Practice. Pearson.

[9] Schneier, Bruce (2015). Applied Cryptography: Protocols, Algorithms, and Source Code in C. Wiley.

Recibido: 2024-04-24
Aprobado: 2024-06-05
Hipervínculo Permanente: https://doi.org/10.54789/reddi.9.1.5
Datos de edición: Vol. 9-Nro. 1-SA. 2
Fecha de edición: 2024-07-31