GESTIÓN Y SOPORTE DE SEGURIDAD EN HARDWARE Y SOFTWARE

Fundamentos criptográficos

Unidad 2

ESCUELA DE CONSTRUCCIÓN E INGENIERÍA

Director: Marcelo Lucero Yañez

ELABORACIÓN

Experto disciplinar: Felipe Reyes Cáceres

Diseñador instruccional: Antonio Colmenares Prieto

Editora instruccional: María José Fonseca Palacios

VALIDACIÓN

Experto disciplinar:

Jefa de Diseño Instruccional: Alejandra San Juan Reyes

EQUIPO DE DESARROLLO

Didactic

AÑO

2022

Tabla de contenidos

Aprendizaje esperado

Identifican conceptos de criptografía en llaves públicas y llaves privadas, considerando sistemas vigentes internacionales.

Configuran cifrado, encriptación y firmas digitales de forma básica, considerando diversos algoritmos.

Introducción

El cifrado es una forma de codificar datos para que solo las partes autorizadas puedan entender la información. En términos técnicos, es el proceso de convertir texto sin formato legible por humanos en texto incomprensible, también conocido como texto cifrado. Si usamos términos más simples, el cifrado toma datos legibles y los cambia para que aparezcan aleatoriamente.

El cifrado requiere el uso de una clave de cifrado, un conjunto de valores matemáticos que acuerdan tanto el remitente como el receptor de un mensaje cifrado.

En esta ocasión, estudiaremos lo relacionado a la encriptación en llaves públicas y privadas, complementando lo estudiado y practicado en la semana anterior.

1. Las llaves públicas y privadas

El cifrado es una parte esencial de la seguridad de nuestros datos. Hay muchas herramientas que pueden encriptar archivos en nuestras computadoras de forma gratuita, o pueden ser herramientas pagas que nos permiten encriptar y firmar correos electrónicos con GPG.

Diferentes programas usan cifrado simétrico, que usa la misma clave para cifrar y descifrar información, o infraestructura de clave pública, un sistema compuesto por una clave pública y una clave privada. Una

infraestructura de clave pública popular es la jerga relacionada con la criptografía para la criptografía asimétrica o de clave pública.

El cifrado de datos es importante si necesita mantener la información privada o si necesita mantener una conversación confidencial. También es útil si necesita almacenar cualquier dato en su computadora o dispositivo que deba mantenerse en secreto. Al utilizar el cifrado de datos, podemos asegurarnos de que nadie pueda acceder a la información contenida en nuestros mensajes; en su lugar, solo verán galimatías. Pero cualquiera que no pueda descifrar nuestros mensajes no podrá entender lo que significan. Con el cifrado de datos, tenemos una comunicación segura que mantiene nuestras conversaciones privadas.

La criptografía utiliza dos tipos diferentes de cifrado de datos según el tipo de comunicación que se utilice.

En la criptografía simétrica, se utiliza la misma clave tanto para el cifrado como para el descifrado de datos. La criptografía asimétrica utiliza dos claves separadas; una clave pública que se puede compartir con otras personas y una clave privada que solo puede usar el propietario. Los datos se cifran con la clave pública y luego se descifran con la clave privada. La criptografía simétrica es rápida y sencilla, lo que proporciona un punto fuerte en su rendimiento general. Esto se debe a que los procesos de cifrado y descifrado son rápidos y fáciles. Como resultado, la criptografía simétrica se usa a menudo para cifrar volúmenes de

datos, particiones o incluso discos duros completos. Las personas pueden incluso crear contenedores encriptados con este tipo de criptografía.

Protege la información con encriptación de grado militar.

La criptografía de clave pública se utiliza para cifrar correos electrónicos. Este proceso pasa por el cifrado asimétrico, que es mucho más lento que el cifrado simétrico. El cifrado asimétrico se usa a menudo para proteger la clave privada de un sistema de cifrado simétrico, de modo que la comunicación posterior se pueda realizar a través del cifrado simétrico. De manera similar, PGP usa criptografía de clave pública para cifrar mensajes. Este método pasa por alto la clave pública y va directamente al cifrado simétrico, por lo que se usa en HTTPS y otras VPN.

Cuando un cliente se conecta a un servidor a través de una VPN, el cifrado de datos ayuda a que el proceso de conexión funcione sin problemas. El cifrado también protege el canal de control, la conexión inicial entre el cliente y el servidor que establece la confianza, cuando se utilizan protocolos como OpenVPN o IPsec. Cuando comienzan las transferencias de datos, los clientes usan algoritmos de encriptación simétrica, como AES, para velocidades de carga y descarga más rápidas. Esto se debe a que los servidores y clientes con aceleración de hardware para AES-NI vienen preinstalados con potencia de

procesamiento acelerado. Esto les ayuda a obtener el cien por cien de sus ciclos de CPU sin exceder los límites de las CPU ordinarias.

Las VPN utilizan ambos métodos de encriptación para brindar la mejor seguridad y rendimiento. También tienen como objetivo eliminar los cuellos de botella causados por el tráfico de la red. Ambos métodos de encriptación trabajan juntos para brindar la mejor seguridad y rendimiento posibles.

Agregar una capa de seguridad TLS al protocolo FTP crea el protocolo FTPES. El protocolo FTPES agrega una capa de seguridad TLS al protocolo FTP original. También añade una versión segura del protocolo FTP que utiliza algoritmos de cifrado simétrico como AES-128-GCM o AES-256-GCM. Esta capa adicional de cifrado aumenta la seguridad de la transmisión de datos entre clientes y servidores. También agrega autenticación mediante contraseñas e intercambio seguro de mensajes.

La criptografía de clave pública asimétrica utiliza un par de claves pública y privada para codificar la información. La gente usa los términos "clave pública" y "clave privada" indistintamente. Ambas claves están relacionadas con el cifrado, pero tienen propósitos diferentes. Una clave privada se usa solo para el cifrado; nunca se revela a nadie más. Una clave pública está asociada con una identidad, que cualquiera puede ver.

Las claves utilizadas para el cifrado simétrico deben ser las mismas para cifrar y descifrar datos. Sin la contraseña correcta, solo alguien con la clave privada puede cifrar o descifrar datos.

Los pares de claves realizan una variedad de funciones importantes en un sistema de criptografía de clave pública. Usan constantemente las mitades pública y privada de sus claves de diferentes maneras. Además de eso, los pares de claves son extremadamente importantes para la seguridad de estos sistemas.

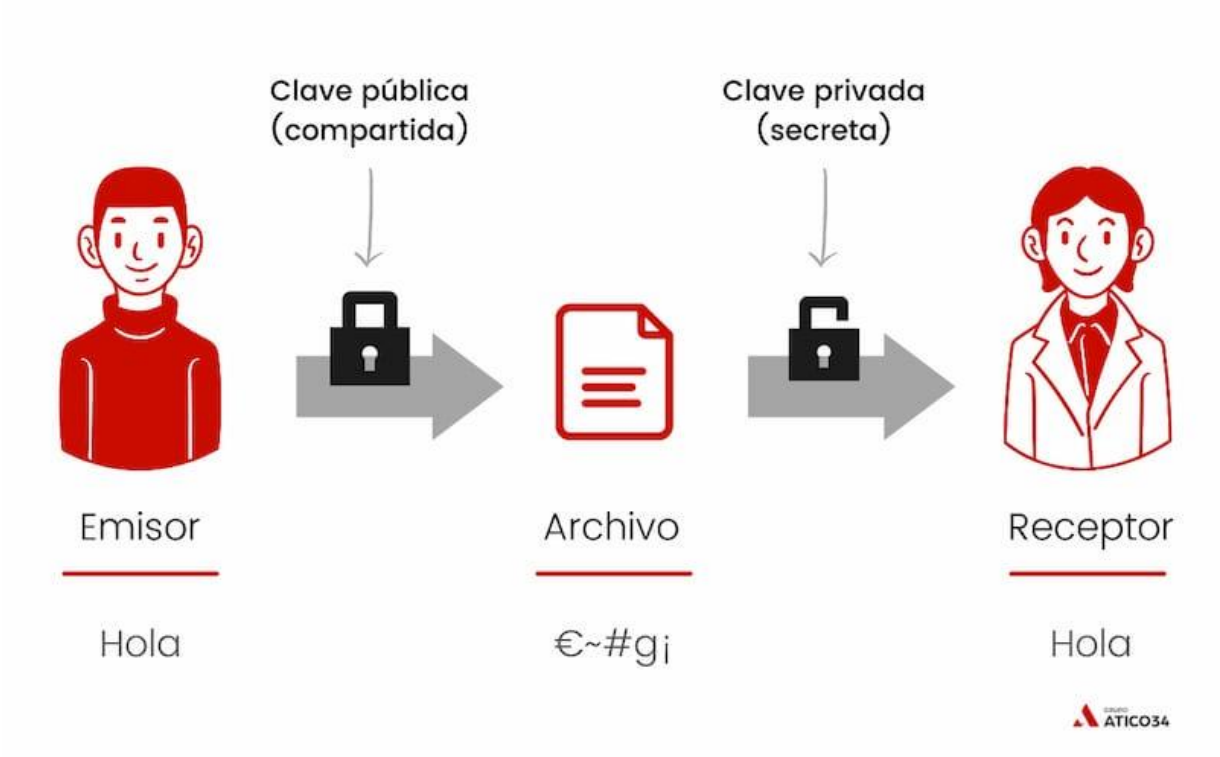

Figura 1. Llaves públicas y privadas.
Fuente: protecciondatos-lopd.com (2020)

2. Estándares de llaves privadas

Al verificar documentos electrónicos, entra en juego la necesidad de firmas digitales y certificados relacionados. Estos estándares deben implementarse con cuidado, ya que dependen de protocolos y estándares internacionales.

El directorio: Marcos para certificados de clave pública y atributos proporcionados por tecnología de la información – Interconexión de sistemas abiertos – La Recomendación ITU-T X.509 es un estándar internacional que facilita la verificación de firmas y certificados digitales. También asegura la interoperabilidad de las aplicaciones y entre Certificadores Licenciados nacionales. Esto garantiza la seguridad jurídica y técnica de las transacciones electrónicas porque permite procesos de verificación efectivos. Un estándar internacional que define los marcos para los certificados de clave pública y los certificados de atributo.

Además, describe las especificaciones de los atributos utilizados para representar certificados, así como una lista de atributos revocados. Detalla los componentes esenciales de un sistema PKI completo, aunque no crea uno completamente. La extensión del estándar X.509 abre más posibilidades para las organizaciones.

La tercera versión de X.509 describe la adición de datos específicos de la organización y Listas de revocación de certificados, o CRL, que se conoce con el acrónimo en inglés "CRL". También explica cómo

mantener listas de claves públicas en un directorio y cómo comparar los valores actuales con los almacenados. El directorio y sus anexos, incluyendo A y B, funcionan como servicios de autenticación para la Base de Información del Directorio (DIB), lo que se conoce por sus siglas en inglés. El DIB se utiliza generalmente para facilitar la comunicación entre directorios como listas de distribución, aplicaciones, terminales y personas.

Cada uno de estos objetos tiene un propósito específico en el mundo. Por ejemplo, los DIB se utilizan para comunicarse entre personas o terminales, que realizan tareas específicas, como programar reuniones o llevar registros. Todas las definiciones incluidas en el Anexo A están relacionadas con el marco del certificado. El acrónimo en inglés de los Identificadores de objetos enumerados en el Anexo F es OID. El OID enumera los nombres en inglés de los algoritmos de encriptación y autenticación que operan fuera de un registro. RFC 6960 – X.509 Infraestructura de clave pública de Internet es un documento que coincide con el Anexo F. Además, incluye el Protocolo de estado de certificado en línea u OCSP.

Este protocolo mantiene el estado de un certificado digital sin requerir su lista de revocación o CRL. Las especificaciones técnicas actuales no proporcionan mecanismos adicionales que aborden las consideraciones operativas. El Protocolo de estado de certificado en línea proporciona una aplicación con información sobre el estado de un certificado, incluida la revocación. Las CRL no brindan esta información tan rápido como OCSP y no pueden brindar información adicional sobre el estado

de los certificados. Al verificar el estado de un certificado, una aplicación necesita solicitar un servidor OCSP para proporcionar la información de estado. Este protocolo detalla los datos necesarios entre aplicaciones y servidores que realizan esta tarea.

3. Modo de operación de instituciones certificadores de tipo pago

El comercio electrónico puede resultar en la creación de una nueva legislación para respaldarlo. Esto se debe al mayor uso de nuevas herramientas tecnológicas que provocan cambios significativos en el comercio global. Esto incluye documentos electrónicos y firmas electrónicas avanzadas. Además, el comercio puede ser respaldado por cosas como firmas automáticas, almacenamiento económico e impresión de contratos, y contratos que se firman de forma remota para que alguien no tenga que aparecer físicamente.

El gobierno nacional ya ha comenzado a abordar esto a través de ciertas leyes y reglamentos. Por ejemplo, las empresas públicas pueden celebrar reuniones de directorio sin asistencia física. También pueden realizar pagos mensuales y pagos anuales de manera oportuna. Y, por último, las declaraciones de impuestos se pueden realizar de manera vinculante y oportuna con poco o ningún costo adicional. La Ley de Chile sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación se denomina simplemente "La Ley". Se aprobó para ayudar

a facilitar el uso de nuevas tecnologías para facilitar mejor la firma de contratos. La aprobación de la Ley implicó la aplicación de principios de neutralidad tecnológica y equivalencia funcional, que se describen en la ley como el principio de equivalencia del soporte electrónico al soporte en papel. El propósito de estas leyes era ayudar mejor a los ciudadanos en su vida cotidiana.

4. Modo de operación de instituciones certificadores de tipo opensource

La encuesta anual de la Fundación Linux, "Las habilidades críticas y las tendencias en la contratación y el empleo de código abierto", revela muchos datos interesantes. Estos incluyen el hecho de que el mayor uso de código abierto empuja a las empresas a transformar los sistemas antiguos en sistemas digitales; el impulso de la transformación digital presiona a las empresas para aumentar la seguridad; y la demanda reprimida de más soluciones de código abierto, lo que genera dificultades de contratación. Además, esto conduce a problemas de retención; Los profesionales con certificación tienen una gran demanda. En conjunto, estos factores presentan serios desafíos para las empresas que buscan contratar personal certificado en código abierto.

Los profesionales de la ciberseguridad requieren de los profesionales más certificados y capacitados. Necesitan especialistas en Linux, DevOps/GitOps/DevSecOps y Cloud. Además, la demanda de

desarrollo web está disminuyendo a medida que se capacita a más personas en estas áreas.

Según un análisis de MarketandMarket, se prevé que el tamaño del mercado mundial de servicios de código abierto aumente de 21 700 millones de dólares a 50 000 millones de dólares en 2026.

Una encuesta encontró que aproximadamente el 73% de los profesionales encuestados pensaban que sería fácil encontrar un nuevo trabajo con una certificación de código abierto. Sin embargo, el 93 % de los gerentes de contratación reportaron dificultades para encontrar candidatos certificados o calificados de código abierto. Además, casi el 70 % de los profesionales certificados en código abierto no habían cambiado de trabajo durante el último año.

Los empleadores afirman que están dispuestos a pagar para que el 90 % de sus empleados obtengan la certificación. Además, el 81% de los profesionales planea certificarse. El 69% de los empleadores dicen que contratarán a un profesional certificado en código abierto. El 46 % de los empleadores planea aumentar la contratación de profesionales certificados en código abierto en los próximos seis meses. Muchas empresas afirman que necesitan contratar personal certificado debido al aumento en el uso de software de código abierto. El 77% de las empresas mencionaron trabajar con tecnologías de nube y contenedores, mientras que el 76% de los encuestados ha trabajado en un proyecto relacionado con Linux. Alrededor del 40% de los empleadores informan que tener personal certificado en ciberseguridad

tiene el mayor efecto en sus decisiones de contratación. Le siguen DevOps, Linux y la computación en la nube. Muchos profesionales optan por formar a sus empleados en ciberseguridad.

Aumentar la confianza como propietario de un negocio nivela de forma beneficiosa la productividad y hace que los empleados sean más eficientes. El aumento de la empleabilidad y las oportunidades de creación de redes resultan de ofrecer este producto a los clientes. Una red mundial de profesionales de Linux comprende un grupo de profesionales que tienen la misma credencial. Esa credencial es una experiencia en la administración del sistema operativo Linux.

5. La encriptación en sistemas webs

La gente debate agregar una S al final de HTTP para hacer que los sitios web sean más seguros. Sin embargo, no sabes cómo implementar HTTPS en un sitio web si trabajas en una empresa.

El uso de Secure Sockets Layer, o SSL, ayuda a proteger las comunicaciones entre los sitios web y sus clientes con datos cifrados.

Proporcionar expectativas adecuadas es crucial cuando se asegura un sitio web con un certificado de seguridad. Cualquier beneficio adicional son solo dos, y son menores. para el logro de objetivos específicos. Esto se logra a través de la capacidad de los certificados para lograr propósitos específicos.

Dar garantías a los clientes sobre con quién se está comunicando es fundamental a la hora de mantener comunicaciones privadas. Esta es la razón por la que el software debe proporcionar cifrado entre un cliente y un servidor. Además, debería bloquear los ataques de suplantación de identidad y el phishing falso.

El cifrado es una herramienta poderosa para proteger los sitios web de diversas amenazas. Estas amenazas incluyen ataques DoS, inyección SQL, aplicaciones web con codificación deficiente y secuencias de comandos entre sitios. HTTPS no brinda ninguna protección adicional contra estas amenazas; es solo otra forma de asegurar las comunicaciones. Sin embargo, las personas preocupadas por su seguridad deben saber que el cifrado previene estas amenazas. Ya comprende el Protocolo de transferencia de hipertexto, o HTTP, que es el protocolo de la Web. Cualquier entidad entre usted y el servidor puede ver los datos que ha transferido a través de HTTP. Esto incluye a cualquier persona en la red del servidor o en cualquier segmento de su propia red que se conecte al servidor.

Este además, debe proteger los intercambios de información personal, las transacciones financieras confidenciales y otras funciones privadas mediante el protocolo HTTPS. Esto se debe a que alguien puede espiar estas actividades simplemente mirando los datos intercambiados. Al agregar Secure Sockets Layer (SSL) al protocolo HTTP básico, agrega cifrado a HTTPS. Esto hace que sea imposible que alguien espíe cualquiera de estos textos sin romper el cifrado.

Para conectarse a un servidor web a través de SSL, su navegador web primero abre una página web protegida con el prefijo https:// en su URL. Luego solicita acceso al puerto HTTPS, también conocido como puerto TCP 443, desde el servidor web. Después de recibir una copia del certificado SSL del servidor web, su navegador se conecta de forma segura. Para verificar la identidad de un servidor web remoto, su navegador web utiliza el certificado. Luego extrae la clave pública del certificado de identidad del servidor. A continuación, su navegador cifra una clave de sesión con la clave pública.

Posteriormente, envía la clave cifrada al servidor, que utiliza su clave privada para descifrarla. Para una comunicación segura, los clientes y los servidores utilizan la clave de sesión para cifrar las comunicaciones posteriores. Es fácil proteger su sitio web con un certificado SSL, que permite a los usuarios conectarse a través de una conexión HTTPS encriptada. Una autoridad de certificación debe revisar y aprobar su solicitud de un certificado SSL antes de que pueda pagarlo. Esto puede costar entre $ 150 y $ 400 por año para un certificado básico.

Es crucial seleccionar una CA de buena reputación al comprar certificados. Antes de que se venda el certificado, esta autoridad verificará su identidad. Antes de emitir un certificado, la CA debe asegurarse de que se haya realizado una investigación exhaustiva. Idealmente, se deben elegir los certificados emitidos por las CA incluidas en la lista raíz de autoridades confiables de Windows. Si una CA no está incluida en esta lista, los visitantes que utilicen sistemas Windows recibirán un mensaje de advertencia.

6. Algoritmos de encriptación

La NSA utiliza el cifrado público AES (Advanced Encryption Standard) para proteger los documentos con la clasificación de "alto secreto". Este es uno de los métodos de cifrado más utilizados y seguros actualmente disponibles; es de acceso público. El NIST, o Instituto Nacional de Estándares y Tecnología, comenzó a buscar un reemplazo para el estándar de cifrado DES en 1997. El algoritmo actual es "Rijndael", inventado por dos criptógrafos belgas llamados Daemen y Rijmen. Ofrecía una seguridad y flexibilidad superiores al mismo tiempo que proporcionaba un rendimiento excelente.

El nombre blockcipher proviene del hecho de que un algoritmo se basa en bloques de 16 bytes. Utiliza varias transformaciones, permutaciones y sustituciones lineales para ocultar datos. Este algoritmo se anunció como el nuevo estándar de encriptación AES en 2001 después de superar a otros competidores. El cifrado AES utiliza una clave circular que se calcula a partir de la clave de cifrado.

Cada ronda de cifrado AES tiene una clave circular única porque el círculo se calcula a partir de la clave de cifrado cada vez que se calcula. AES-128, AES-192 y AES-256 son estructuras de bloques diferentes con 128, 192 o 256 bloques respectivamente. Esto es significativo porque el cifrado DES de 56 bloques tiene una longitud de clave significativamente más corta que AES. Usando una supercomputadora de primera línea, descifrar una clave AES de 256 bits llevaría más tiempo que el universo

mismo. Boxcryptor utiliza claves de 128 bits. La facilidad de cifrado que proporciona Advanced Encryption Standard lo convierte en el estándar para sistemas de alta seguridad como bancos y gobiernos de todo el mundo. No existe una forma factible de atacar AES, por lo que sigue siendo el estándar.

En 1973, la agencia de inteligencia británica GCHQ descubrió el sistema de cifrado RSA. Fue uno de los sistemas de cifrado asimétrico más exitosos que se utilizan en la actualidad, y la NSA mantuvo su clasificación de "alto secreto". En la década de 1970, el público redescubrió una oscura forma de arte gracias a tres matemáticos: Adleman, Rivest y Shamir. Resolvieron un dilema criptográfico cuando accidentalmente encontraron otra solución.

Al usar RSA, los datos se cifran y descifran con dos claves diferentes. Una clave es pública y una clave es privada. La clave privada no se puede calcular a partir de la clave pública, por lo que solo la clave pública está disponible para el público. Al realizar un cifrado o descifrado, las personas usan una clave para cifrar datos y otra para descifrar datos.

Las firmas digitales RSA utilizan una huella dactilar cifrada incrustada para probar la autenticidad de un documento y su remitente. Esto se hace cifrando la clave pública RSA de uno con la huella digital del destinatario y luego firmando la clave pública con su clave privada. Esto se hace por motivos de privacidad y seguridad, porque demuestra que ambas partes son quienes dicen ser. También utiliza problemas matemáticos como la factorización de enteros como base para su

seguridad. Cualquier mensaje a cifrar se considera equivalente a un gran número. Antes de cifrar el mensaje, se multiplica por dos números primos que son casi iguales en tamaño. Luego, se cifra con la clave principal y se reparte entre el resto. Si lo hace, descifrará repetidamente el texto en su forma original. La criptografía moderna se basa en claves de al menos 3072 bits para la seguridad. Esto se debe a que actualmente es imposible calcular los factores necesarios para descifrar cifrados mediante divisiones con más de 768 bits de datos. Sin embargo, actualmente se están realizando investigaciones que pueden permitir descifrar claves de cifrado más grandes.

7. Encriptación simétrica y asimétrica

La seguridad de los datos es esencial en el mundo actual debido al predominio de las redes de comunicación modernas. Esto se debe al hecho de que la seguridad de los datos aparentemente se basa en métodos obsoletos que los piratas informáticos pueden explotar. Este artículo analiza dos esquemas de encriptación populares, encriptación simétrica y asimétrica, que se pueden usar para fortalecer la seguridad de las comunicaciones.

La criptografía simétrica es muy eficiente porque no lleva mucho tiempo cifrar o descifrar la información. También ofrece cierto grado de verificación gracias al hecho de que las claves simétricas no pueden descifrar información cifrada con otra clave. Esto significa que ambas partes involucradas en una comunicación cifrada pueden estar seguras

de que se están comunicando entre sí siempre que mantengan su clave en secreto.

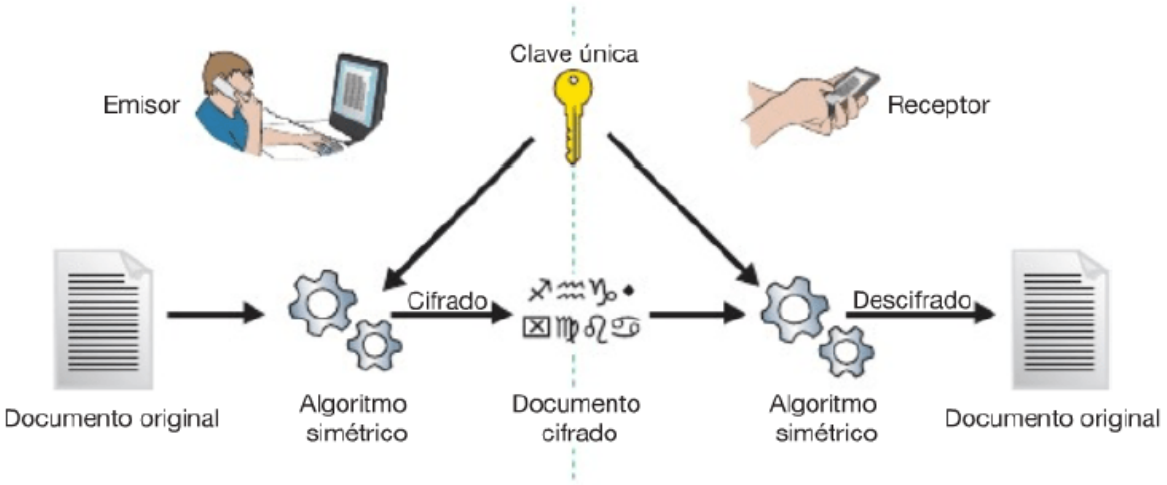

Figura 2. Criptografía simétrica

Fuente: jesusfernandeztoledo.com (2020)

Se requiere una clave especial para intercambiar mensajes cifrados con otra persona. Sin embargo, debido a que estos mensajes se intercambian entre dos personas que tienen cada una una clave privada, las claves son secretas. Por lo tanto, los sistemas de clave simétrica se denominan cifrados de clave secreta. Cada participante debe proteger su clave individual de la divulgación para garantizar la seguridad del cifrado. Una persona con una clave simétrica no autorizada puede descifrar mensajes cifrados con esa clave y cifrar mensajes nuevos. Alguien más que encuentre la clave puede comprometer tanto la confidencialidad como la autenticación.

La criptografía de clave pública utiliza una clave pública y una clave privada para cifrar y descifrar datos. Utiliza el hecho de que las claves

públicas y privadas están relacionadas pero no relacionadas. Este sistema impide que cualquier persona acceda o utilice un mensaje si no tiene la clave privada.

Una clave que cualquier persona puede usar para cifrar datos se denomina clave pública. Solo alguien con la clave privada puede descifrar los mensajes cifrados con su clave pública.

Los directorios públicos proporcionan a los destinatarios una clave pública que se puede utilizar para cifrar los mensajes antes de transmitirlos. Esta clave se puede usar para descifrar cualquier mensaje que se haya cifrado con la clave privada del remitente.

Dado que el destinatario solo necesita la clave pública del remitente para leer el mensaje, el remitente solo puede autenticarse si lo encripta con su clave privada. Este proceso automático no requiere que el remitente bloquee y desbloquee físicamente su mensaje.

El cifrado asimétrico ofrece una mayor seguridad de los datos en comparación con su contraparte simétrica. Esto se debe a que nunca se requiere la distribución de claves cuando se usa este método; esto hace que sea más difícil para los ciberdelincuentes interceptar cualquier información que transmita un usuario.

El cifrado asimétrico es más nuevo que el cifrado simétrico. Utiliza dos claves: una clave pública compartida con todos y una clave privada que solo conserva el remitente. Un mensaje cifrado con estas claves solo puede ser descifrado por el remitente o por alguien que tenga la clave

privada. El cifrado simétrico utiliza una única clave que debe ser compartida tanto por el remitente como por el receptor. Los pares de claves públicas y privadas son necesarios para los sistemas de cifrado simétrico. Como resultado, el cifrado simétrico tiene inherentemente un problema de uso compartido de claves. El cifrado asimétrico supera este problema al proporcionar la capacidad de crear claves privadas y públicas. Debido a esto, se puede decir que el cifrado asimétrico requiere más tiempo que el cifrado simétrico. Cuando se trata de cifrar información, los esquemas más nuevos generalmente se consideran la mejor opción. Constantemente se desarrollan nuevos algoritmos de cifrado para mantenerse al día con los nuevos desarrollos en técnicas de espionaje. Esto se debe a que los expertos en criptografía necesitan desarrollar nuevos algoritmos para adelantarse a los espías y proteger la información confidencial. Espere grandes avances de la comunidad criptográfica en el futuro debido al hecho de que los piratas informáticos siempre encuentran nuevas formas de meterse con ellos.

8. Configuración básica de firmas digitales

Muchas personas firman documentos con la misma firma en varios escritos. Esto se conoce como una firma básica.

Cree una imagen con forma de firma con la herramienta Scribble, luego firme un documento sin usar ninguna herramienta de dibujo.

Alternativamente, dibuje un objeto y firme ese documento. Los certificados digitales agregan una capa adicional de seguridad al firmar documentos. Esta opción se elige con frecuencia debido a las muchas formas en que se puede aplicar.

Algunos organismos legales y gubernamentales requieren el uso de una firma digital. Consulte la sección sobre el uso de una firma digital a continuación. Cree una firma única usando la herramienta Scribble para dibujar su firma. Al agregar elementos adicionales a su firma, puede crear una obra de arte original.

Puede agregar fácilmente cualquier firma escaneada a un PDF como cualquier otra imagen. Para que el fondo de la firma sea transparente, utilice el método que prefiera.

Para agregar una imagen, haga clic en la herramienta Cuentagotas en la esquina inferior derecha de la ventana de su firma y seleccione el color de fondo de su firma. Alternativamente, puede arrastrar y soltar un archivo de imagen como PNG o TIFF en su firma.

Luego puede combinarlo con otras piezas de texto usando Agregar imágenes. Para recortar el tamaño de su firma, seleccione Editar > Hacer que la imagen sea transparente. Luego seleccione Selección de cultivos para ajustar sus dimensiones. El control deslizante Tolerancia ajusta la nitidez del borde de la transparencia. Haga clic en Hacer transparente cuando esto ocurra para que la transparencia sea visible. Agrega una firma a tus publicaciones seleccionando Editar > Deshacer.

Seleccione el tamaño de su firma usando los controladores en la esquina inferior derecha del área de edición. A continuación, seleccione Editar > Rehacer para reducir el grosor de su firma. Luego puede usar los controles de cambio de tamaño con la tecla Mayús presionada para ajustar la proporción de su firma para que encaje correctamente dentro del marco de texto.

Puede agregar una firma a un documento PDF una vez que lo haya escaneado en la aplicación. Si su imagen escaneada es demasiado grande, puede recortarla antes de agregar su firma. Después de esto, puede guardar el documento en la biblioteca para uso futuro.

9. Las instituciones certificadoras

Una Entidad de Certificación es una organización privada cuyo propósito es evaluar el cumplimiento y luego certificar el cumplimiento de un estándar. Esto podría ser un estándar de referencia para un producto, un servicio o el sistema de gestión de una organización. Debe ser independiente del organismo fiscalizador, y no haber realizado ningún otro trabajo para éste. En concreto, la Entidad de Certificación deberá realizar una auditoría a las organizaciones que soliciten la certificación de su sistema de gestión de calidad ISO 9001:2015, su sistema de gestión ambiental ISO 14001:2015, etc.

Estas organizaciones crean los estándares que están certificados para su cumplimiento. Por ejemplo, la siguiente tabla muestra muchos organismos de estandarización que crean estándares internacionales.

Los organismos de normalización siguen un conjunto estándar de procedimientos para garantizar la uniformidad. Estos procedimientos se implementan a través de los Comités Técnicos de cada organismo, que representan diversos temas e intereses.

Luego de ser evaluada por la Entidad Nacional de Acreditación, la Entidad de Certificación es reconocida como entidad evaluadora conforme. Cada país tiene un organismo de normalización y una entidad de acreditación. La Entidad de Acreditación es responsable de evaluar la conformidad y emitir informes sobre los organismos de evaluación de la conformidad: entidades de certificación, calibración e inspección. De esta forma, cada país cuenta con una infraestructura de calidad con una entidad nacional de acreditación y un organismo de normalización. Para facilitar la validez internacional de los certificados emitidos por la entidad certificadora que acredita, cada país mantiene entre ellos una organización mayor denominada IAF - International Accreditation Forum. Esta organización funciona como un lugar de encuentro para las entidades de acreditación de diferentes países para discutir el reconocimiento de sus certificados emitidos por la entidad certificadora que acreditan.

Cierre

Después de estudiado lo correspondiente a la semana, se puede destacar lo siguiente:

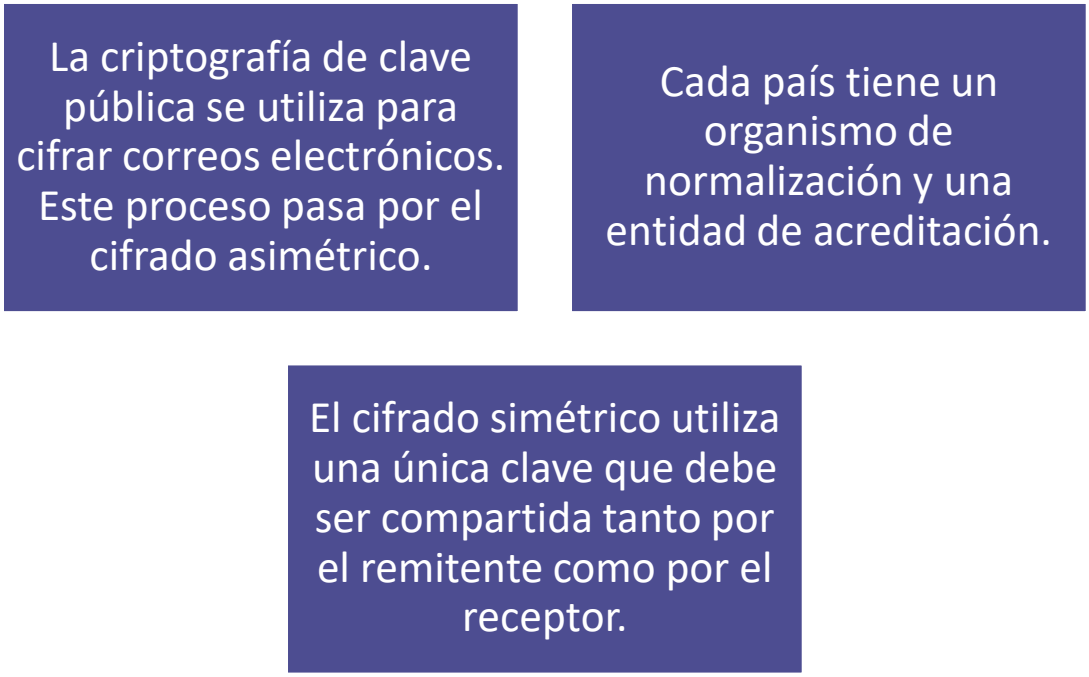

Figura 3. Ideas Claves, semana 5

Fuente: Reyes, F. (2022)

Referencias bibliográficas

CCNA Security 210-260 Official Cert Guide (Santos, Stuppi 2016)

Ramírez, H. (2020, mayo 12). Qué es la criptografía asimétrica y cómo funciona. Grupo Atico34; Ático34 Protección de datos para empresas y autónomos. https://protecciondatos-lopd.com/empresas/criptografia-asimetrica/

Toledo, J. F. (2020, noviembre 4). Criptografía Simétrica. Jesusfernandeztoledo.com; Jesús Fernández Toledo. https://jesusfernandeztoledo.com/criptografia-simetrica/