Sistemas seguros de acceso y transmisión de datos.

IFCT0109 – Seguridad informática

MF0489_3 (60 horas)

Criptografía

- Introducción
- Perspectiva histórica y objetivos de la criptografía
- Teoría de la información
- Propiedades de la seguridad que se pueden controlar mediante la aplicación de la criptografía: confidencialidad, integridad, autenticidad, no repudio, imputabilidad y sellado de tiempos
- Elementos fundamentales de la criptografía de clave privada y de clave pública
- Características y atributos de los certificados digitales
- Identificación y descripción del funcionamiento de los protocolos de intercambio de claves usados más frecuentemente
- Algoritmos criptográficos más frecuentemente utilizados
- Elementos de los certificados digitales, los formatos comúnmente aceptados y su utilización
- Elementos fundamentales de las funciones resumen y los criterios para su utilización
- Requerimientos legales incluidos en la ley 59/2003, de 19 de diciembre, de firma electrónica (Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza)
- Elementos fundamentales de la firma digital, los distintos tipos de firma y los criterios para su utilización
- Criterios para la utilización de técnicas de cifrado de flujo y de bloque
- Protocolos de intercambio de claves
- Uso de herramientas de cifrado
- Resumen

Análisis forense informático

Introducción

La criptografía, el arte de escribir con clave secreta o de un modo enigmático, ha acompañado a la humanidad desde la Antigüedad. Su objetivo: proteger la información confidencial.

A lo largo de la historia, los métodos criptográficos han evolucionado al ritmo de la tecnología. Desde los sencillos sistemas de sustitución hasta los complejos algoritmos informáticos actuales, la criptografía ha jugado un papel fundamental en la seguridad de las comunicaciones.

En este capítulo, exploraremos la fascinante historia de la criptografía, desde sus inicios hasta la actualidad. Abordaremos los conceptos básicos de esta disciplina, las técnicas más comunes y su papel en la sociedad actual.

Perspectiva histórica y objetivos de la criptografía

Introducción

La criptografía, una rama de la criptología, se encarga de proteger la información mediante técnicas que la vuelven incomprensible para terceros no autorizados. A lo largo de la historia, ha experimentado una notable evolución, desde métodos rudimentarios hasta sofisticados sistemas computacionales.

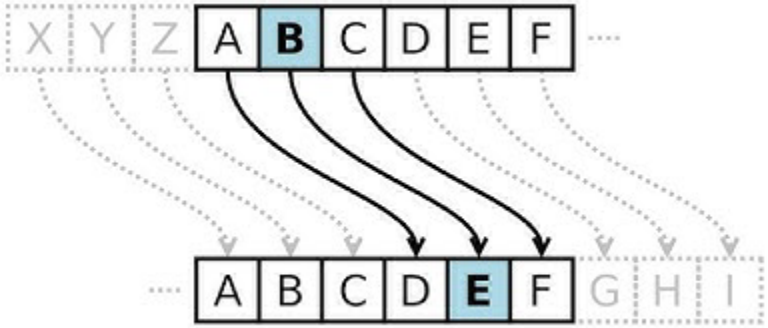
Evolución histórica de la criptografía:

Antigüedad:

- Escítala (siglo IV a.C.): Un bastón de madera para transposición de caracteres. Cambiar el orden en el que los caracteres aparecen en un texto.

- Cifrado de César (siglo I a.C.): Sustitución monoalfabética simple.

  Cada una de las letras del mensaje se sustituye por la situada X posiciones más adelante en el alfabeto. Inconveniente: la frecuencia del patrón de letras en el texto cifrado proporciona una gran pista para descifrar el mensaje completo. Por ejemplo, si la letra “E” aparece con frecuencia en el texto cifrado, es probable que corresponda a la letra “A” en el texto original. Vídeo



Perspectiva histórica y objetivos de la criptografía

Introducción

Evolución histórica de la criptografía:

Edad Media y Renacimiento:

Cifrado de Vigenère (siglo XVI): Sustitución polialfabética con clave. Utiliza múltiples alfabetos y una clave para dificultar el análisis de frecuencias de aparición de las letras. Vídeo.

Siglo XX:

Máquina Enigma (1918): Sistema complejo de rotores para cifrado. Elimina la repetición y crea aleatoriedad evitando patrones predecibles.

Era digital:

- Criptografía de clave pública (1976): RSA, Diffie-Hellman, etc. (utiliza dos claves una pública y una privada). La pública es conocida, encripta los datos y sólo se puede desencriptar con la clave privada. La privada desencripta los datos cifrados con la clave pública.
- Criptografía de curvas elípticas: Mayor rapidez y eficiencia.
- Criptografía cuántica: En desarrollo, basada en fotones.

Perspectiva histórica y objetivos de la criptografía

Introducción

Objetivos de la criptografía:

- Confidencialidad: Asegurar que solo los destinatarios autorizados puedan leer el mensaje.
- Integridad: Garantizar que el mensaje no ha sido modificado desde su origen.
- Autenticación: Verificar la identidad de las entidades participantes.
- No repudio: Impedir que una entidad niegue haber enviado o recibido un mensaje.

Esteganografía: A diferencia de la criptografía, la esteganografía oculta el mensaje para que pase desapercibido. Se utilizan técnicas como:

- Tinta invisible: Mensajes ocultos que solo se revelan con calor o químicos.
- Modificación de imágenes: Alteración imperceptible de tonos para ocultar información.

Ventajas e inconvenientes de la esteganografía:

Ventajas: El mensaje pasa desapercibido para el atacante y mayor seguridad si el mensaje oculto está cifrado.

Inconvenientes: Menor eficiencia en comparación con la criptografía y vulnerabilidad si se descubre el sistema utilizado.

Perspectiva histórica y objetivos de la criptografía

Fundamentos del criptoanálisis

El criptoanálisis, según la RAE, es el "arte de descifrar criptogramas". Aunque originalmente se centraba en el cifrado, hoy en día abarca el estudio y la explotación de vulnerabilidades en cualquier mecanismo criptográfico.

Objetivo: El criptoanalista busca comprender el funcionamiento de un sistema criptográfico para predecir su salida para cualquier mensaje. Para ello, se suele analizar como una "caja negra" que transforma una entrada (texto claro) en una salida (texto cifrado).

Tipos de criptoanálisis:

- Solo texto cifrado: El criptoanalista solo tiene acceso al texto cifrado. Es la situación más desafiante.
- Texto en claro conocido: Se dispone de una parte del texto en claro y su correspondiente texto cifrado.
- Texto en claro escogido: El criptoanalista puede elegir el texto en claro que se desea cifrar y obtener el texto cifrado.
- Texto cifrado escogido: Se elige un texto cifrado y se busca el texto en claro original (poco común).

Importancia: El criptoanálisis juega un papel fundamental en la seguridad de la información. Al identificar las debilidades de los sistemas criptográficos, se pueden desarrollar soluciones más seguras y confiables.

Ejemplo: El criptoanálisis fue crucial para descifrar el código Enigma utilizado por la Alemania nazi durante la Segunda Guerra Mundial.

Perspectiva histórica y objetivos de la criptografía

Fundamentos del criptoanálisis

Enfoque. El criptoanálisis se basa en diferentes técnicas para atacar los sistemas criptográficos:

- Análisis estadístico: Se buscan patrones en el texto cifrado para deducir información sobre la clave o el algoritmo utilizado.
- Ataques por fuerza bruta: Se prueban todas las claves posibles hasta encontrar la correcta.
- Ataques de canal lateral: Se explotan las características físicas del sistema para obtener información sobre la clave o el algoritmo.
- Criptoanálisis diferencial: Se analizan las diferencias entre pares de textos cifrados para deducir información sobre la clave.
- Criptoanálisis lineal: Se utilizan técnicas matemáticas para encontrar relaciones lineales entre el texto claro y el texto cifrado.

Teoría de la información

Introducción

La Teoría de la Información, desarrollada por Claude Shannon en 1948, establece límites fundamentales en la transmisión y compresión de datos. Su impacto en la criptografía es crucial, ya que permite evaluar la robustez y seguridad de los algoritmos criptográficos.

Definición de Algoritmo: Un conjunto finito y ordenado de pasos u operaciones que permiten resolver un problema.

Capacidad del Canal: En un canal de comunicación (como Internet), la cantidad de información que se puede transmitir sin errores está limitada por su capacidad. Shannon demostró que existe una capacidad máxima efectiva de transmisión de información para cada canal.

Entropía: La entropía mide la cantidad de información contenida en un mensaje, es decir, su grado de incertidumbre o aleatoriedad. Cuanto mayor sea la incertidumbre, mayor será la entropía.

Ejemplo:

En un coro de 10 personas, la selección de 4 miembros puede tener diferentes niveles de entropía:

> Máxima entropía: Si hay 5 chicos y 5 chicas, la probabilidad de elegir un chico o una chica es la misma. La entropía es máxima porque hay mayor incertidumbre.
>
> Mínima entropía: Si hay 9 chicos y 1 chica, la probabilidad de elegir un chico es mucho mayor. La entropía es mínima porque hay poca incertidumbre.

Entropía y seguridad

Entropía y seguridad:

La entropía no solo mide la incertidumbre de un evento, sino también la incertidumbre que el conocimiento de un evento aporta sobre otro. En criptografía, esto es crucial para la seguridad del sistema.

En criptografía, la seguridad se relaciona con la información que se deduce sobre la entrada a partir de la salida de una función criptográfica.

Sistema incondicionalmente seguro:

Un sistema es incondicionalmente seguro si conocer la salida de la función criptográfica no proporciona información sobre la entrada. El cifrador de Vernam es el único que cumple esta condición, pero es poco práctico. Ya lo veremos posteriormente

Teoría de la información

Redundancia y compresión de datos:

Redundancia:

- La redundancia es la repetición de información en un mensaje.
- Es deseable eliminarla para mejorar la eficiencia de la transmisión.
- Sin embargo, se necesita cierta redundancia para proteger contra errores en el canal de transmisión.

La frase "La casa es grande y espaciosa" contiene redundancia porque la información “espaciosa" ya está implícita en la palabra “grande".

Códigos de redundancia cíclica (CRC):

- Los CRC son códigos que se añaden a un mensaje, a un archivo, para detectar errores en la transmisión.
- Se calcula utilizando un algoritmo y un polinomio CRC. No pueden detectar manipulaciones del mensaje.

Compresión de datos:

- La entropía se puede utilizar para medir la compresibilidad de un mensaje.
- Un mensaje con alta entropía es difícil de comprimir.
- Un mensaje con baja entropía es fácil de comprimir.

Teoría de la información

Redundancia y compresión de datos:

Ejemplo de compresión de datos en teoría de la información:

Imagina que tienes un archivo de texto que contiene la siguiente frase: "La casa es grande y espaciosa."

Esta frase tiene 27 caracteres.

Si queremos comprimir el archivo, podemos utilizar un algoritmo de compresión sin pérdida, que puede comprimir un archivo sin perder ninguna información. En este caso, vamos a usar un algoritmo de compresión que se basa en la redundancia (repetición innecesaria de información)

En la frase "La casa es grande y espaciosa", hay redundancia porque la palabra "grande" ya implica que la casa es espaciosa. El algoritmo de compresión puede eliminar la redundancia de la frase para reducir su tamaño.

El resultado de la compresión es la siguiente frase: "La casa es grande."

Esta frase comprimida tiene 21 caracteres, lo que representa una reducción del 22% en el tamaño del archivo.

Cuando el usuario necesite leer la frase original, el algoritmo de descompresión puede recuperar la información original a partir de la frase comprimida.

Propiedades de la seguridad que se pueden controlar mediante la aplicación de la criptografía: confidencialidad, integridad, autenticidad, no repudio, imputabilidad y sellado de tiempos

La seguridad de la información busca controlar, mitigar o prevenir problemas de seguridad, tales como el acceso no autorizado a datos o la manipulación maliciosa de estos. Es crucial comprender las propiedades clave que la criptografía pretende salvaguardar, las amenazas que estas enfrentan y los mecanismos diseñados para contrarrestar tales amenazas.

Confidencialidad

Esencial en la era digital, la confidencialidad asegura que la información solo sea accesible para destinatarios autorizados. El cifrado desempeña un rol crítico aquí, permitiendo que solo quienes posean la clave adecuada accedan a los datos. Amenazas como el malware o la ingeniería social subrayan la necesidad de robustas medidas de seguridad.

Integridad

Asegura que la información no se altere, garantizando su exactitud y completitud. La aplicación de técnicas criptográficas, especialmente funciones resumen, es vital para prevenir alteraciones, como las provocadas por ataques de intermediarios.

Autenticidad

Verifica que un mensaje o entidad sea genuino. La criptografía permite asegurar la autenticidad de mensajes mediante cifrados y códigos de autenticación, y la de entidades a través de firmas digitales. Las técnicas de autenticación varían desde contraseñas hasta métodos biométricos, ofreciendo diferentes niveles de seguridad.

Propiedades de la seguridad que se pueden controlar mediante la aplicación de la criptografía: confidencialidad, integridad, autenticidad, no repudio, imputabilidad y sellado de tiempos

No Repudio

Impide que las entidades nieguen haber realizado ciertas acciones. La firma digital es un mecanismo común para asegurar el no repudio, aunque su eficacia puede verse comprometida por el robo de claves. Protocolos específicos pueden reforzar esta propiedad.

Imputabilidad

Relacionada con el no repudio, la imputabilidad permite rastrear las acciones de los usuarios, asegurando la responsabilidad por sus actos. Las firmas electrónicas, complementadas con ficheros de auditoría, son herramientas clave para lograrlo.

Sellado de Tiempo

Confirma que la información existió en un momento determinado y no ha sido alterada desde entonces. La fiabilidad del sellado de tiempo depende de la autoridad de sellado y de fuentes de tiempo confiables, como el Real Instituto y Observatorio de la Armada.

Propiedades de la seguridad que se pueden controlar mediante la aplicación de la criptografía: confidencialidad, integridad, autenticidad, no repudio, imputabilidad y sellado de tiempos

Aplicación Práctica

En el contexto de un portal web de servicios, es crucial definir los servicios de seguridad adecuados para cada funcionalidad.

La integridad y la confidencialidad son fundamentales en todas las áreas, mientras que la autenticación asegura la identidad de los interlocutores.

El no repudio y el sellado de tiempo son especialmente relevantes en funciones como la consulta de facturas y el buzón de reclamaciones, respectivamente, para garantizar la validez y el origen de la información y las acciones realizadas.

Elementos fundamentales de la criptografía de clave privada y de clave pública

La criptografía es esencial en la protección de la información digital, empleando algoritmos matemáticos complejos para cifrar y descifrar datos. Su utilidad abarca desde la confidencialidad y la integridad de los datos hasta la autenticación y el no repudio. Existen dos principales sistemas criptográficos: la criptografía de clave privada (o simétrica) y la criptografía de clave pública (o asimétrica), cada una con sus características y aplicaciones específicas.

Criptografía de Clave Privada

En la criptografía de clave privada, tanto el cifrado como el descifrado se realizan con la misma clave. Esto requiere que la clave se comparta de forma segura entre el emisor y el receptor antes de la comunicación, lo cual presenta un desafío logístico en la distribución segura de claves.

Ventajas:

Mayor velocidad de cifrado y descifrado en comparación con los sistemas de clave pública.

Eficiencia en la gestión para grupos pequeños de usuarios.

Desafíos:

La distribución segura de claves entre partes.

La escalabilidad es problemática en redes grandes debido al número de claves necesarias.

Elementos fundamentales de la criptografía de clave privada y de clave pública

Criptografía de Clave Privada

En la criptografía de clave privada se utilizan principalmente dos familias de sistemas: los cifradores de bloque y los cifradores de flujo. Cada familia tiene sus propias características y aplicaciones, adaptándose a diferentes necesidades de seguridad.

Los cifradores de flujo son un tipo de cifrado simétrico donde la información de la comunicación se cifra bit a bit (o byte a byte), utilizando una clave secreta (serie cifrante) compartida previamente entre emisor y receptor.

Este método permite una comunicación segura: El emisor utiliza esta clave para cifrar el mensaje, transformándolo en un texto cifrado que solo puede ser descifrado por alguien que posea la misma clave. Después, el receptor utiliza la misma clave para descifrar el mensaje y leer el contenido original.

Este tipo de cifrado se utiliza principalmente para proteger la transmisión de datos en entornos donde es posible establecer y compartir una clave secreta de manera segura. Son especialmente útiles para cifrar la transmisión de datos en tiempo real o en situaciones donde el tamaño del mensaje no es predecible.

Los hay de dos tipos: los cifradores síncronos y los autosíncronos.

Elementos fundamentales de la criptografía de clave privada y de clave pública

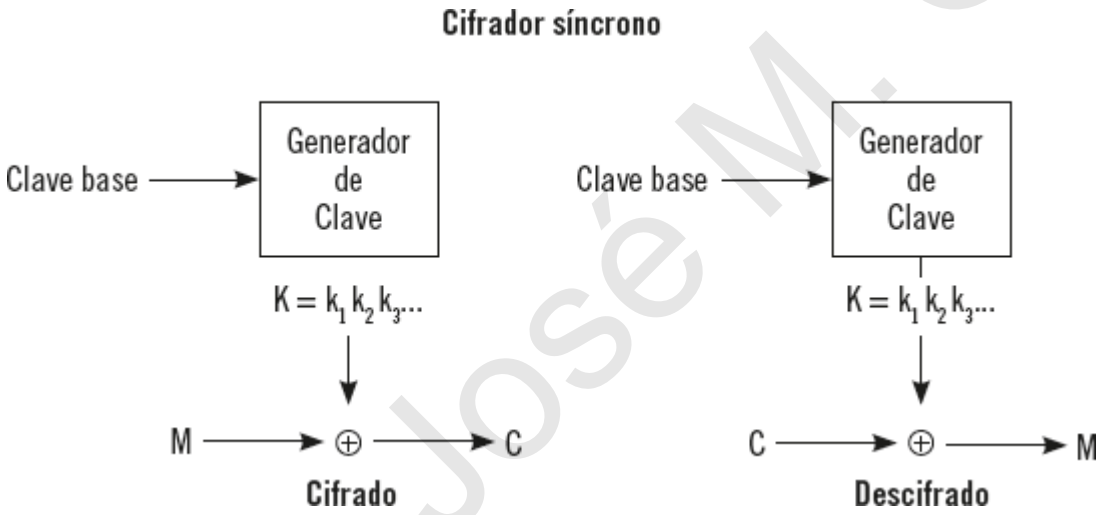
Criptografía de Clave Privada

Cifradores de flujo

Los cifradores de flujo síncronos:

Son un tipo de cifrado de flujo donde se crea una secuencia de cifrado o clave (K) de manera independiente al mensaje original (M) y al mensaje cifrado (C), es decir, la clave no cambia basándose en el mensaje que está siendo cifrado o el mensaje ya cifrado. Imagínalo como una corriente constante de números o letras que solo tiene sentido si conoces la clave secreta para descifrarla.

Un criptograma es simplemente el resultado del cifrado; es decir, es la información cifrada que se ha vuelto incomprensible a menos que tengas la clave para descifrarla y revertirla a su forma original.



Un ejemplo de uso de los cifradores de flujo síncronos es el protocolo RC4 en sistemas de seguridad inalámbrica, como WEP (Wired Equivalent Privacy) y en menor medida WPA (Wi-Fi Protected Access).

Elementos fundamentales de la criptografía de clave privada y de clave pública

Criptografía de Clave Privada

Cifradores de flujo

Los cifradores de flujo síncronos (Propiedades)

- Sincronización: Es crucial que tanto el emisor como el receptor estén perfectamente alineados en términos de la secuencia de cifrado. Si se pierde esta sincronización, la información descifrada no tendrá sentido, por lo que es necesario implementar métodos para resincronizar, como reiniciar el proceso de cifrado o insertar puntos de sincronización en el flujo de datos.

- No Propagación de Errores: Si ocurre un error durante la transmisión (por ejemplo, un bit cambia de valor), solo afecta a ese bit específico en el mensaje descifrado, sin alterar el resto de la información.

- Resistencia a Ataques Activos: Los cifradores síncronos pueden identificar ciertos tipos de ataques, como la eliminación o inserción de bits, que desincronizan la clave. Un ataque de modificación hará que solo parte del mensaje sea incomprensible, lo cual puede servir como una alerta de que la comunicación ha sido comprometida.

En resumen, en los cifradores síncronos la clave de cifrado se genera de manera independiente del texto que se cifra, asegurando que la comunicación sea privada y segura, siempre y cuando tanto el emisor como el receptor mantengan sus operaciones perfectamente sincronizadas y el secreto de la clave.

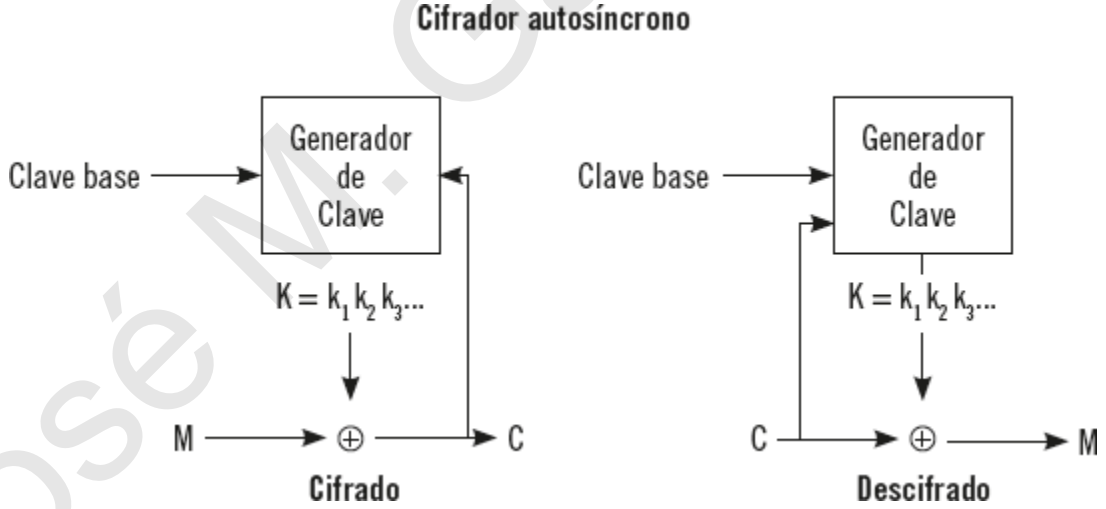
Elementos fundamentales de la criptografía de clave privada y de clave pública

Criptografía de Clave Privada

Cifradores de flujo

Los cifradores de flujo autosíncronos

Los cifradores autosíncronos, o asíncronos, son una forma de cifrado de flujo donde la secuencia de cifrado (K) no se genera de forma aislada, sino que depende tanto de una clave base como de partes del mensaje que ya han sido cifradas anteriormente. Esto quiere decir que para cifrar o descifrar un mensaje, se utiliza información de los fragmentos previos del propio mensaje cifrado.



Elementos fundamentales de la criptografía de clave privada y de clave pública

Criptografía de Clave Privada

Cifradores de flujo

Los cifradores de flujo autosíncronos (Propiedades)

- Sincronización Automática: permiten que emisor y receptor se mantengan sincronizados de forma natural, ya que el proceso de descifrado necesita solo de un segmento previo del criptograma. Si se pierde sincronización por alguna razón, se puede recuperar rápidamente tras procesar un número específico de caracteres previos.
- Errores de Propagación Limitados: Si ocurre un error o modificación en un bit o carácter del criptograma, este error afectará solo a una parte limitada del mensaje. Esto significa que el error no se propaga más allá de un número determinado de caracteres afectados.
- Detección de Ataques Activos: Modificaciones, eliminaciones, o inserciones en el mensaje cifrado son más fáciles de detectar con este tipo de cifradores, ya que alteran la secuencia esperada de caracteres. Aunque identificar un ataque puede ser más complejo en comparación con los cifradores síncronos, la naturaleza autosincrónica ayuda a notar cuando algo no va bien.
- Mejor Resistencia contra Análisis Estadístico: Cada parte del mensaje cifrado influye en la siguiente, lo que dispersa las propiedades estadísticas del texto en claro a lo largo del criptograma. Esto hace que los cifradores autosíncronos sean más resistentes a ataques que explotan patrones y redundancias en el texto original.

En resumen, los cifradores autosíncronos ofrecen una manera robusta y flexible de cifrar la información, facilitando la sincronización y la recuperación tras errores, a la vez que mejoran la seguridad frente a ataques que intentan descifrar o alterar los mensajes.

Elementos fundamentales de la criptografía de clave privada y de clave pública

Criptografía de Clave Privada

Cifradores de flujo síncronos vs asíncronos

Característica	Cifradores de flujo síncronos	Cifradores de flujo asíncronos
Generación de clave	Independiente del texto claro y cifrado.	Depende del texto cifrado anterior.
Sincronización	Necesaria entre emisor y receptor. Una pérdida de sincronización requiere resincronización.	Se autorecupera usando el propio criptograma, facilitando la resincronización.
Propagación de errores	Un error afecta solo al bit específico, sin propagación a bits siguientes.	Un error puede afectar a los siguientes bits hasta que el cifrador se resincronice.
Detección de ataques	Más susceptible a ataques de inserción o borrado que desincronizan.	La estructura autosincronizante puede detectar alteraciones más fácilmente.
Ventajas	Simpleza de implementación Eficiencia en el procesamiento Precomputación del flujo de clave.	Recuperación automática de la sincronización Resistencia mejorada a la pérdida de datos Adecuado para transmisiones ruidosas o inestables.
Inconvenientes	Requiere mecanismos externos para mantener la sincronización Vulnerable a errores de transmisión.	Mayor complejidad en el diseño Potencialmente más lento debido a la dependencia de datos previos.

Elementos fundamentales de la criptografía de clave privada y de clave pública

Criptografía de Clave Privada

Los cifradores de bloque

Los cifradores de bloque son como cajas fuertes digitales que protegen tus datos dividiéndolos primero en piezas de tamaño igual, como si estuvieras cortando un pastel en pedazos iguales antes de guardarlo en diferentes cajas fuertes. Cada pedazo del pastel (o bloque de datos) se cierra con la misma llave, pero de manera que cada uno queda asegurado por separado.

Uno de los trucos más ingeniosos para cerrar estas cajas fuertes es el método de Feistel, usado en famosos candados digitales como DES. Imagina que cada vez que cierras una de estas cajas, divides el pastel en dos, transformas una mitad con un poco de magia (la subclave) y luego mezclas esa mitad transformada con la otra mitad usando un poco de lógica matemática (XOR). Repites este truco varias veces, y justo antes de terminar, intercambias las mitades del pastel. Lo especial de este truco es que para abrir la caja y recuperar el pastel intacto, solo necesitas hacer todo al revés.

Cuando estos cifradores trabajan, pueden hacerlo de diferentes maneras, llamadas modos de operación, como si tuvieras distintos métodos para guardar y asegurar tus pasteles en las cajas fuertes:

- ECB (Electronic Code Book): Cada pedazo se guarda sin depender de los otros.
- CBC (Cipher Block Chaining): Cada pedazo se mezcla con el pedazo anterior antes de ser guardado.
- CFB (Cipher Feedback) y OFB (Output Feedback): Transforman el cifrado de bloque en un flujo continuo, como un río que fluye, asegurando los datos poco a poco.
- CTR (Counter): Usa un contador para asegurar cada pedazo de manera única, como si numeraras cada pieza del pastel antes de cerrarla en su caja.

Elementos fundamentales de la criptografía de clave privada y de clave pública

Criptografía de Clave Privada

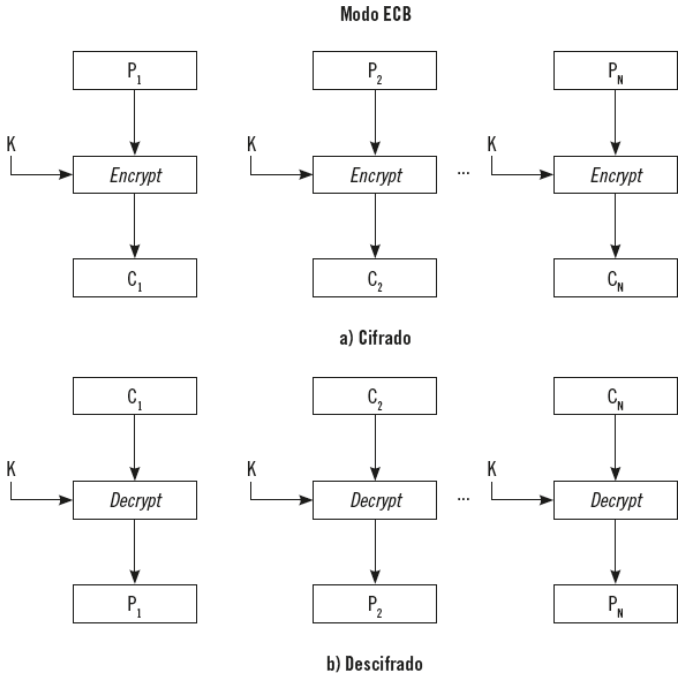
Los cifradores de bloque - ECB (Electronic Code Book)

El modo de cifrado Electronic Code Book (ECB) es como tener una máquina mágica para cerrar cajas. Imagina que tienes un montón de cajas (bloques de datos) y una llave mágica especial (la clave de cifrado). Con ECB, usas esta llave mágica para cerrar cada caja individualmente. Si alguna vez necesitas abrir una caja para ver qué hay dentro, usas la misma llave para desbloquearla.

Cada vez que cierras una caja con un contenido específico, siempre se verá igual por fuera. Esto significa que si tienes dos cajas con el mismo contenido y usas tu llave mágica, ambas cajas cerradas se verán idénticas. Esto es simple y directo, pero tiene un par de desventajas:

- No Propaga Errores: Si en el camino se pierde o cambia una caja, solo esa caja se ve afectada. Esto suena bien, pero significa que si alguien malintencionado quita o cambia una caja, es posible que no te des cuenta de inmediato.
- Patrones Visibles: Debido a que el contenido idéntico siempre se ve igual una vez que se cierra la caja, alguien que esté observando podría empezar a notar patrones.

Se suelen utilizar para cifrar claves de licencia o tokens de autenticación.



Elementos fundamentales de la criptografía de clave privada y de clave pública

Criptografía de Clave Privada

Los cifradores de bloque - Cipher Block Chaining (CBC)

El Cipher Block Chaining (CBC) es una forma de cifrado que se puede imaginar como un tren de bloques de datos, donde cada vagón (bloque de datos) se modifica antes de ser enviado al siguiente. Paso a paso de manera sencilla:

- Inicio: Tienes una fila de bloques de datos que necesitas cifrar. Para empezar el proceso, necesitas un vector de inicialización (VI), que es como un empujón inicial para el primer bloque. Algo conocido entre emisor y receptor, pero que no es la clave secreta.
- Cifrado de Cada Bloque: Antes de cifrar un bloque con tu llave secreta, tomas el bloque anterior ya cifrado y mezclas su contenido con tu bloque actual usando una operación llamada XOR. Esto hace que cada bloque cifrado dependa del anterior. El primer bloque se mezcla con el VI en lugar de otro bloque cifrado, porque es el primero de la fila.
- Descifrado: Cuando descifras, haces lo contrario. Primero descifras un bloque con tu llave, y luego mezclas el resultado con el bloque cifrado anterior para obtener el texto original. Para el primer bloque, usas nuevamente el VI en la mezcla.

La operación XOR es una forma de comparar dos cosas para ver si son diferentes. Es como responder a la pregunta: ¿Es uno de estos diferente al otro? Si la respuesta es "sí", entonces el resultado es "sí" (1). Si ambos son iguales, entonces la respuesta es "no" (0).

En criptografía, XOR es útil porque es reversible; si aplicas la misma operación XOR dos veces con el mismo valor, vuelves al valor inicial. Esto hace que sea una operación fundamental en muchos algoritmos de cifrado, donde puedes "mezclar" los datos con una clave y luego "desmezclarlos" con la misma clave para recuperar los datos originales.

Elementos fundamentales de la criptografía de clave privada y de clave pública

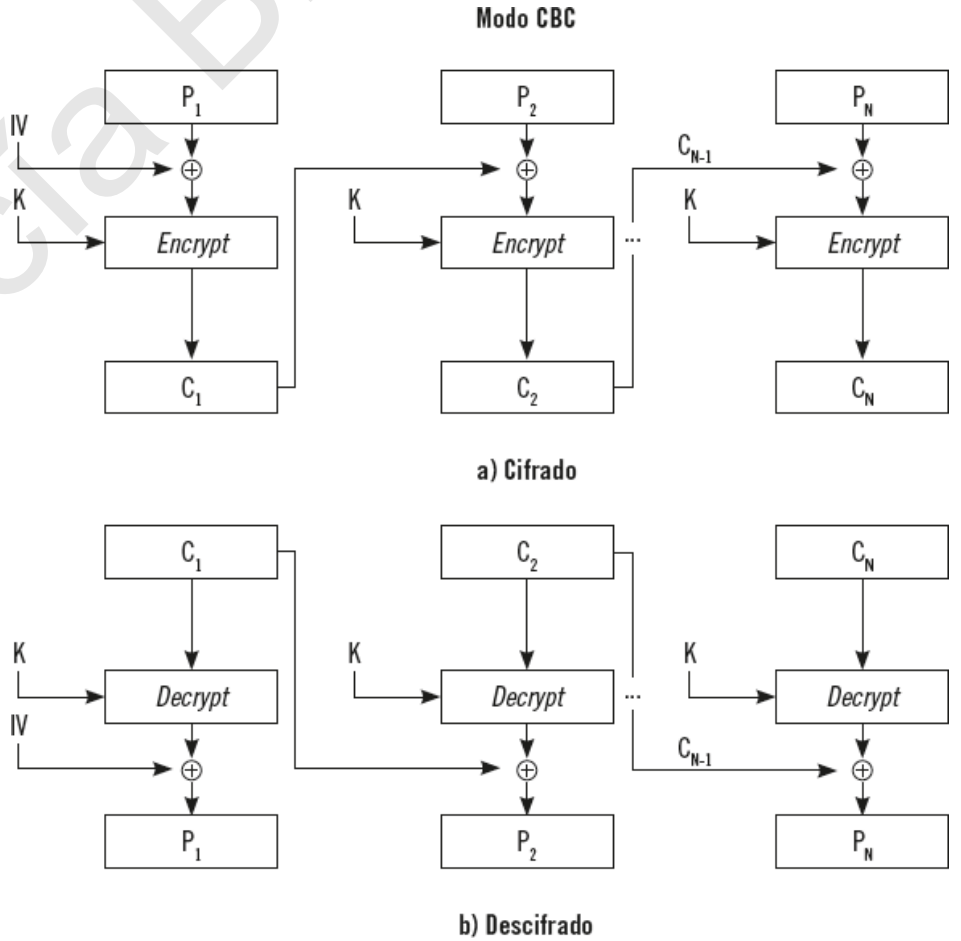
Criptografía de Clave Privada

Los cifradores de bloque - Cipher Block Chaining (CBC)

Al mezclar cada bloque con el anterior cifrado, haces que el cifrado de un bloque dependa de todos los bloques anteriores. Esto evita que patrones repetidos en tu mensaje original se muestren como patrones repetidos en el mensaje cifrado, haciendo más difícil para alguien malintencionado adivinar qué contienen tus datos basándose en el aspecto del cifrado.

Sin embargo, si hay un error en la transmisión de un bloque cifrado, afectará no solo a ese bloque cuando lo descifres, sino también al siguiente, ya que cada bloque depende del resultado del anterior.

El modo de cifrado CBC (Cipher Block Chaining) se utiliza frecuentemente en el cifrado de archivos y discos duros. Por ejemplo, programas como TrueCrypt o sistemas operativos como algunos Linux para el cifrado de discos completos emplean CBC. Además, en el ámbito de las comunicaciones seguras por Internet, protocolos como TLS (Transport Layer Security), que es utilizado para proteger la transmisión de datos en páginas web seguras (HTTPS), pueden utilizar CBC para cifrar datos que se envían a través de la red.



Elementos fundamentales de la criptografía de clave privada y de clave pública

Criptografía de Clave Privada

Los cifradores de bloque - Cipher Feedback (CFB)

El modo Cipher Feedback (CFB) es como una cadena de secretos que se van pasando de uno a otro, donde el mensaje se transforma paso a paso. Imagínate que tienes una fila de personas (cada una representa un bloque de datos) y un mensaje secreto que quieres pasar a lo largo de la fila, pero de manera cifrada. Paso a paso:

- Inicio: Comienzas con un Vector de inicialización (VI)
- Cifrado de los Datos: Toma el VI o el resultado del cifrado anterior (un secreto ya compartido) y lo metes en una "máquina de cifrado" junto con una clave secreta. Luego, sacas un código cifrado de esa máquina y lo mezclas (usando XOR) con el mensaje actual que quieres cifrar. El resultado de esta mezcla es el mensaje cifrado que pasas al siguiente en la fila (el próximo bloque).
- Descifrado de los Datos: Para descifrar, tomas el mismo bloque cifrado que enviaste y lo metes en la máquina de cifrado (la misma clave, el mismo VI o bloque cifrado anterior). El resultado de la máquina se mezcla con el bloque cifrado que recibiste para descifrar el mensaje original.

Elementos fundamentales de la criptografía de clave privada y de clave pública

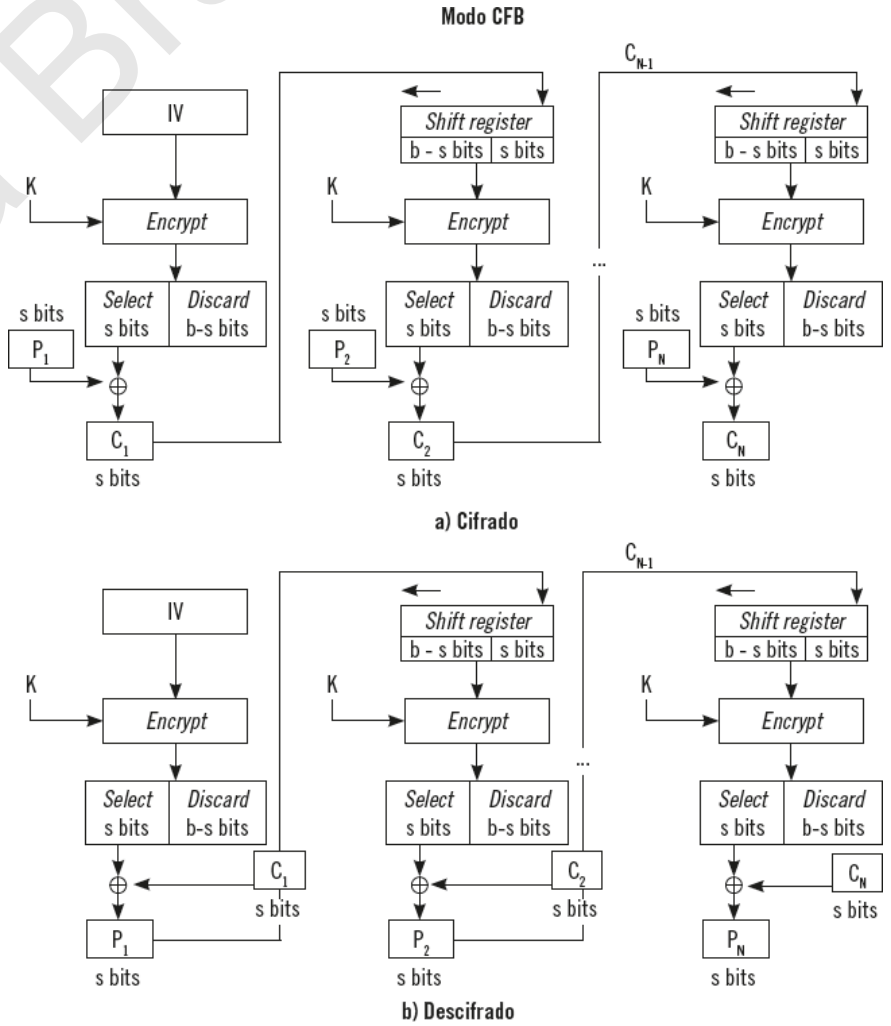
Criptografía de Clave Privada

Los cifradores de bloque - Cipher Feedback (CFB)

Si algo sale mal en la transmisión de uno de estos mensajes cifrados (como si alguien tropezara al pasar el secreto), el error no solo afectará a ese bloque, sino también al siguiente. Esto es porque cada bloque depende del cifrado del anterior.

Cada pieza de información cifrada depende de la anterior, creando una cadena segura de mensajes que se van transformando uno tras otro. Esto lo hace diferente del modo ECB, donde cada bloque se cifra de forma independiente, y similar a CBC, pero con la flexibilidad de trabajar con tamaños de bloque menores.

Una aplicación práctica es en la transmisión de datos en tiempo real o en situaciones donde la cantidad de datos no se ajusta a los tamaños de bloque estándar. CFB permite cifrar datos en unidades más pequeñas que un bloque completo, lo que lo hace adecuado para aplicaciones como la transmisión de voz sobre IP (VoIP) o el envío de mensajes en una aplicación de chat, donde los datos llegan de manera continua y no se pueden predecir de antemano sus tamaños exactos. Esto es útil porque no tienes que esperar a tener un bloque completo de datos para comenzar a cifrar, lo que significa que puedes comenzar a enviar o recibir datos cifrados inmediatamente, sin retrasos.



Elementos fundamentales de la criptografía de clave privada y de clave pública

Criptografía de Clave Privada

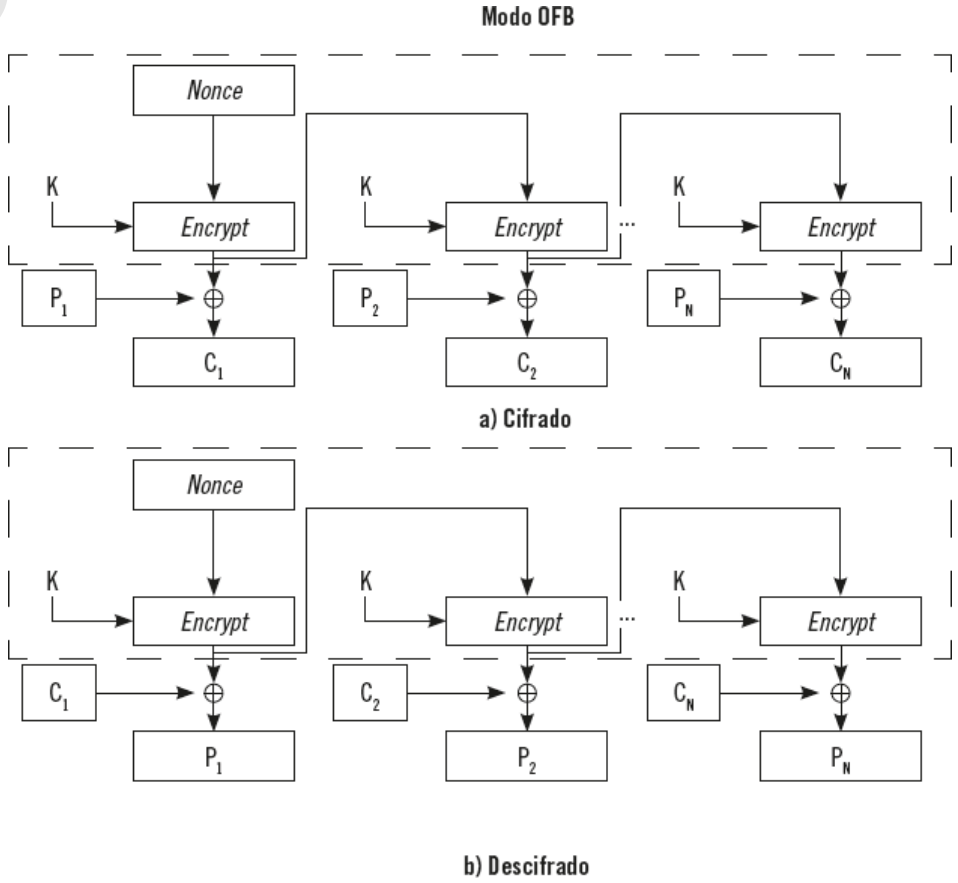
Los cifradores de bloque - Output Feedback (OFB)

El modo Output Feedback (OFB) es una manera de cifrar datos en donde el cifrado de un bloque de datos no depende directamente del bloque de texto plano ni del bloque de texto cifrado anterior, como en otros modos. En su lugar, OFB usa una secuencia de bits pseudoaleatorios que se genera a partir de una clave y de un vector de inicialización (IV), que es un número aleatorio único para cada sesión de cifrado (Nonce).

Cifrado y descifrado es similar a CFB. La diferencia radica en que tanto en cifrado como en descifrado la entrada a la función que realiza el cifrado/descifrado se corresponde con la salida de la función anterior.

La ventaja de OFB es que los errores no se propagan, un problema en un bloque de datos cifrados no afecta a los bloques que siguen. Porque el cifrado de un bloque posterior no depende del bloque anterior sino de la función de cifrado del bloque anterior.

Esto lo hace útil para la transmisión de datos en tiempo real como el video o la voz, donde un pequeño error no debe arruinar todo el flujo de datos. Además, al ser cada IV único y usar una secuencia de bits que no está atada al texto plano o cifrado, OFB proporciona una buena seguridad manteniendo el mismo nivel de complejidad en el cifrado y descifrado.



Elementos fundamentales de la criptografía de clave privada y de clave pública

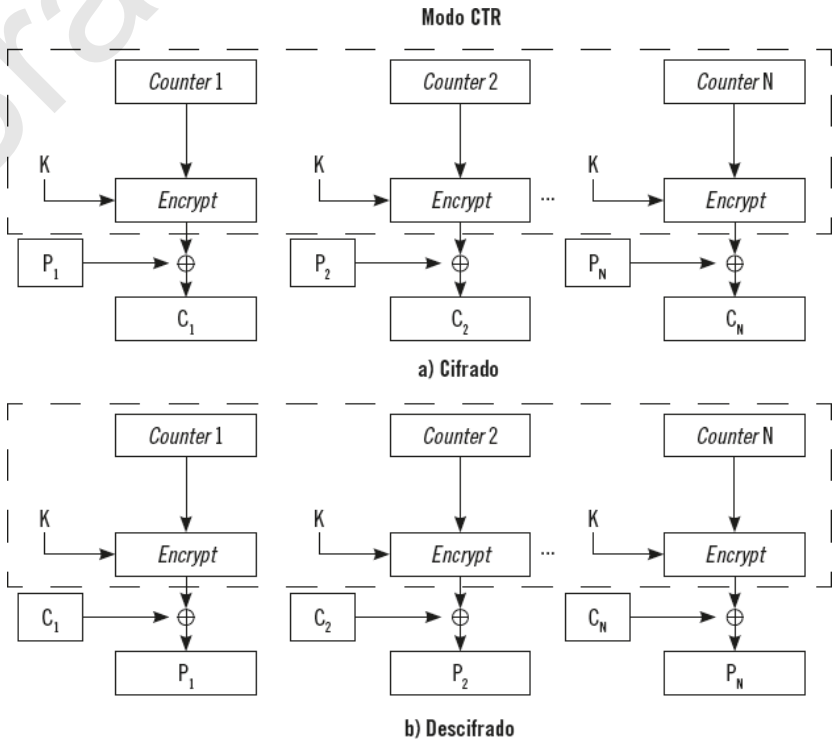
Criptografía de Clave Privada

Los cifradores de bloque - Counter Mode (CTR)

El modo de operación de cifrado de bloques conocido como Counter Mode (CTR) es relativamente simple y efectivo. En CTR, no se cifra directamente el texto claro (o sea, la información original que deseas proteger). En lugar de ello, se crea una secuencia de números únicos llamados nonces (o contadores), que son como números de serie. Cada uno de estos nonces es único para cada bloque de texto durante una sesión de cifrado.

Estos nonces se cifran con una clave de cifrado (que solo conocen el emisor y el receptor) usando un algoritmo de cifrado de bloques estándar, como AES. El resultado de cifrar el nonce es un bloque de "texto cifrado", pero este texto cifrado no es el resultado final. En lugar de eso, se combina (usando la operación XOR) con el texto claro para producir el texto cifrado final. Para descifrar, se realiza el mismo proceso: se cifra el nonce, se realiza la operación XOR con el texto cifrado, y el resultado es el texto claro original.

Este método tiene la ventaja de que se puede realizar el cifrado y el descifrado en paralelo y también permite el acceso aleatorio a los datos cifrados. Además, si un solo bit del texto cifrado se altera durante la transmisión, solo ese bit afectará al texto claro cuando se descifre. Esto lo hace muy adecuado para entornos donde se necesita una alta eficiencia y la integridad de los datos es crítica, como en la transmisión de video en tiempo real o en la comunicación de grandes bases de datos distribuidas.



Un ejemplo real de aplicación de CTR es el cifrado de datos en discos duros. CTR se usa en algoritmos como BitLocker de Microsoft. Otro ejemplo podría ser el protocolo de seguridad de la capa de transporte (TLS) que a menudo utiliza AES en modo CTR para cifrar la comunicación en Internet, como los datos que pasan a través de una conexión HTTPS.

Elementos fundamentales de la criptografía de clave privada y de clave pública

Criptografía de Clave Privada

Los cifradores de bloque - Counter Mode (CTR) vs Output Feedback (OFB)

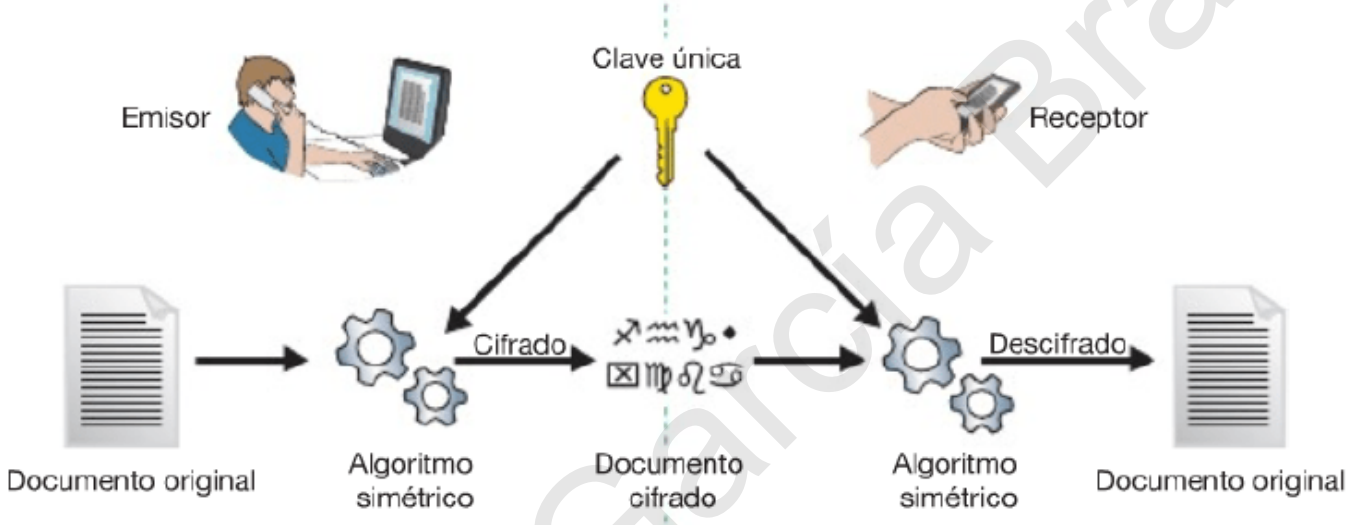
La principal diferencia entre OFB y CTR es cómo generan la secuencia de claves (keystream) que se utiliza para cifrar los datos.

En OFB, el bloque de cifrado inicial se cifra y luego se usa el resultado para cifrar el primer bloque de datos. Este resultado también se vuelve a cifrar para producir el siguiente segmento del keystream, y así sucesivamente. La secuencia de cifrado es dependiente; cada bloque depende del anterior. Esto significa que cualquier error en un bloque puede afectar todos los bloques siguientes.

CTR, por otro lado, no depende de bloques de cifrado anteriores. En lugar de eso, utiliza un contador que se incrementa para cada bloque de datos. El contador se cifra con la clave y el resultado es el keystream para ese bloque. Esto hace que CTR sea más eficiente y adecuado para operaciones paralelas, ya que cada bloque se puede calcular de forma independiente. También significa que los errores en un bloque no se propagan a otros bloques.

Elementos fundamentales de la criptografía de clave privada y de clave pública

Criptografía de Clave Privada



El algoritmo de clave simétrica para ser seguro, debe cumplir:

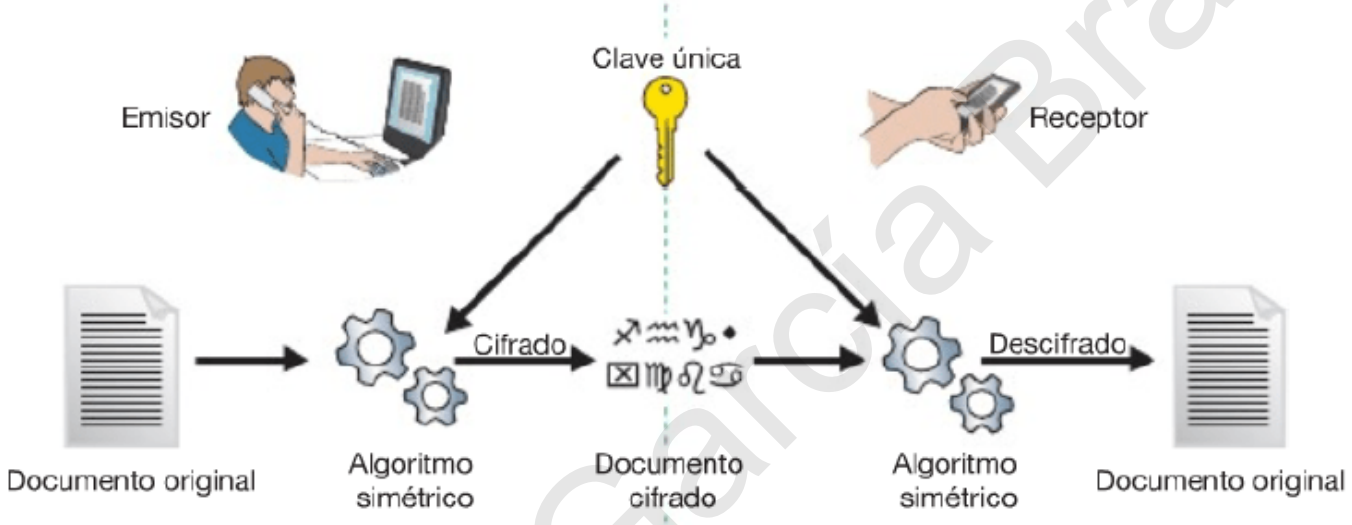
- Una vez cifrado el mensaje no se podrá obtener la clave de cifrado ni tampoco el mensaje en claro (por ningún método)
- Conocido el mensaje el claro y el cifrado, se debe gastar más tiempo y dinero para obtener la clave para acceder al mensaje en claro que el posible valor que pueda tener la información a la que se quiere acceder.

El gran enemigo de los algoritmos de criptografía simétrica son los ataques de fuerza fruta, teniendo en cuenta que los algoritmos son públicos.

La fuerza del algoritmo recae sobre su funcionamiento interno y la longitud de la clave.

Elementos fundamentales de la criptografía de clave privada y de clave pública

Criptografía de Clave Privada



Lo más importante es proteger la clave privada o contraseña.

Problema: la distribución de la contraseña.

Ventaja: los algoritmos de este tipo de criptografía son muy rápidos, pero depende del hardware del equipo en el que se generen.

Esta criptografía se está incorporando en los últimos años en las CPUs, Servidores, Routers y dispositivos de aceleración de cifrado por hardware (que nos permite enviar datos vía VPN de forma rápida).

La velocidad de generación del cifrado depende del algoritmo utilizado.

Entre los algoritmos más rápidos y seguros tenemos AES y ChaCha20.

Elementos fundamentales de la criptografía de clave privada y de clave pública

Criptografía de Clave Pública

La criptografía de clave pública utiliza pares de claves únicos para cada usuario: una clave pública, que puede ser compartida abiertamente, y una clave privada, que se mantiene en secreto. El usuario genera la clave privada y deriva la clave pública a través de una relación matemática, garantizando que el par de claves sea exclusivo. Este método se utiliza tanto para cifrar y descifrar mensajes como para autenticar firmas digitales.

Dentro de la criptografía de clave pública, encontramos dos tipos de algoritmos:

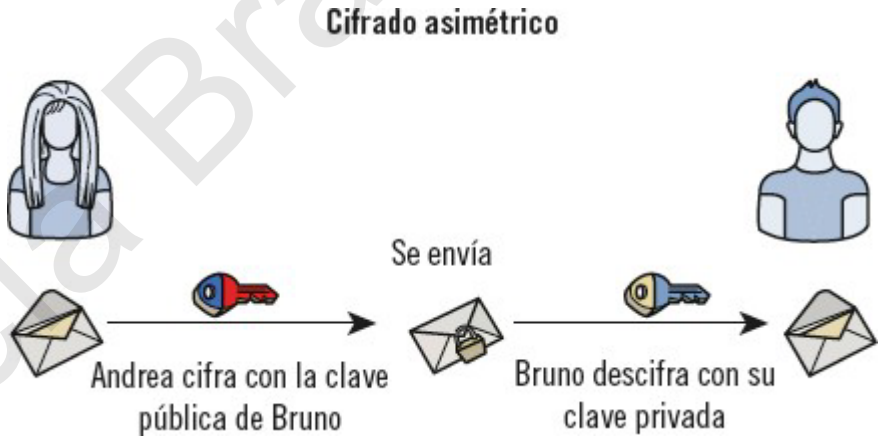
- Reversibles: permiten cifrar y descifrar mensajes, siendo posible recuperar el mensaje original a partir del cifrado. RSA es el algoritmo reversible más conocido.
- Irreversibles: se usan principalmente para verificación de firmas digitales, asegurando que la firma hecha con la clave privada corresponda a la clave pública asociada, sin posibilidad de descifrar mensajes. El Gamal es un ejemplo de algoritmo irreversible.

Elementos fundamentales de la criptografía de clave privada y de clave pública

Criptografía de Clave Pública

Las parejas de claves deben:

- Cifrar la información
- Asegurar la integridad de la información transmitida
- Garantizar la autenticidad del emisor.



La estructura matemática del funcionamiento del cifrado asimétrico sería:

- Mensaje + clave pública = Mensaje cifrado
- Mensaje cifrado + clave privada = Mensaje descifrado
- Mensaje + clave privada = Mensaje firmado
- Mensaje firmado + clave pública = Mensaje autenticado

Elementos fundamentales de la criptografía de clave privada y de clave pública

Criptografía de Clave Pública

En la criptografía simétrica el cifrado aporta confidencialidad.

La criptografía asimétrica aporta además: autenticidad, integridad y no repudio.

Para que un algoritmo sea considerado seguro debe cumplir:

- Si se conoce el texto cifrado, debe resultar muy difícil o prácticamente imposible extraer el texto en claro y la clave privada por cualquier método.
- Si se conoce el texto en claro y el cifrado, debe resultar más costoso obtener la clave privada que el texto en claro.
- Si los datos han sido cifrados con la clave pública, sólo debe existir una clave privada capaz de descifrarlo, y viceversa.

Inconveniente en la criptografía de clave pública: lentitud en el proceso de cifrado.

Solución: combinación de ambos sistemas (IPSec o OpenVPN para VPN, HTTPS para conexiones web seguras o conexiones SFTP)

¿Cómo se combinan los cifrados?

- Se crea la clave secreta con un algoritmo simétrico y se cifra con la clave pública del receptor.
- Se envían estos datos cifrados por el canal inseguro.
- El receptor descifra los datos mediante su clave privada, creada a partir de su clave pública.
- Ahora la clave simétrica está en los dos puntos y se puede empezar la comunicación simétrica.
- Más rápido que usar la criptografía asimétrica.

Elementos fundamentales de la criptografía de clave privada y de clave pública

Criptografía de Clave Pública

Desafío-respuesta (Método para comprobar la seguridad)

El receptor envía un texto al emisor, utilizando su clave pública.

El emisor lo cifra con su clave privada (lo estaría firmando)

El emisor nos envía el texto cifrado (firmado), utilizando nuestra clave pública.

El receptor lo descifra con la clave (con lo que estamos comprobando la firma). Tenemos la clave pública del emisor para proceder al descifrado.

El receptor comprueba que el mensaje recibido es el mismo que el enviado al emisor en primera instancia.

Si alguien intercepta el mensaje haciéndose pasar por el emisor real, no tendría la clave privada, porque está asociada en el cifrado a las claves públicas.

Elementos fundamentales de la criptografía de clave privada y de clave pública

Criptografía de Clave Pública

Firma electrónica

- Permite al receptor conocer que el origen es auténtico y que el mensaje no ha sido modificado.
- Falsificar la firma es posible conociendo la clave del que firma.

Fases de una firma electrónica:

- Proceso: emisor cifra los datos con clave privada y los envía al receptor
- Verificación: el receptor descifra los datos usando la clave pública del emisor y comprueba que la información coincide con los datos originales enviados, mediante el uso de funciones Hash (SHA2-256 y SHA2-512)

Funciones HASH

Usadas para obtener una huella digital, ya que el cifrado asimétrico es lento.

- El emisor de una comunicación al cifrar aplica una función HASH (algoritmo) al mensaje original para obtener una huella digital.
- La huella digital se cifra con la clave privada y se envía al receptor para que la descifre.
- El receptor aplica la función HASH a la comunicación cifrada recibida.
- Se comparan ambos HASH, el recibido y el obtenido.
- Si los HASH son iguales la información no ha sido alterada y la comunicación se llevará a cabo sin problemas.

Elementos fundamentales de la criptografía de clave privada y de clave pública

Criptografía de Clave Pública

Funciones HASH

Con la aplicación de las funciones HASH habremos cumplido:

- Autenticidad, el emisor es quien dice ser. La firma en origen y destino es la misma.
- Integridad, el mensaje no ha sido modificado. Lo obtenido y lo recibido es igual.
- No repudio, el emisor no puede negar haber enviado el mensaje al receptor. La Firma electrónica no varía.

Para incluir la confidencialidad en la comunicación, el emisor debe cifrar el mensaje original con la clave pública del receptor.

Propiedades:

- Independientemente del tamaño del mensaje original, al aplicarle la función hash, la huella resultante siempre tendrá el mismo tamaño.
- Si el hash es cambiado quiere decir que, con tan solo cambiar un bit del mensaje original, salta la alarma.
- Resistencia a la segunda preimagen: dado un mensaje x, no es posible encontrar otro mensaje x que produzca el mismo valor hash, salvo que sean el mismo mensaje. El atacante de ese mensaje no puede encontrar un mensaje x que produzca el mismo valor hash.
- Resistencia a colisiones: no es posible encontrar dos entradas que den lugar al mismo valor hash, salvo que las entradas sean las mismas.

Elementos fundamentales de la criptografía de clave privada y de clave pública

Criptografía de Clave Pública

Funciones HASH

Aplicaciones:

- Protección de contraseñas.
- Se utilizan como parte de algunos de los pasos de los algoritmos de cifrado simétrico y asimétrico citados anteriormente.
- Es una parte fundamental del mecanismo de Firma electrónica.
- Se emplea para garantizar la integridad de un flujo de datos, como el software que nos descargamos

Elementos fundamentales de la criptografía de clave privada y de clave pública

Criptografía de Clave Pública

Las claves públicas no requieren un canal seguro para su intercambio, dado que están destinadas a ser conocidas por todos. Sin embargo, la generación de claves y los procesos de cifrado y descifrado pueden ser computacionalmente intensivos y no son prácticos para datos muy grandes.

Los algoritmos de clave pública suelen requerir claves más largas para proporcionar la misma seguridad que la criptografía de clave privada.

En un escenario con seis personas que necesitan comunicarse de forma segura, un sistema de clave privada requeriría 15 claves diferentes, una para cada par de usuarios. Con la criptografía de clave pública, cada usuario necesita solo un par de claves, reduciendo la necesidad a 12 claves en total. A diferencia de los algoritmos simétricos, no es necesario intercambiar todas las claves, solo compartir las claves públicas.

La seguridad de la criptografía de clave pública se basa en problemas matemáticos difíciles de resolver computacionalmente, como los problemas NP y NP-completos. Los algoritmos RSA y El Gamal son ejemplos, basados respectivamente en la dificultad de la factorización de enteros y del logaritmo discreto.

Problema NP y NP-Completo

Un problema se considera de clase NP si puede ser resuelto en tiempo polinomial no determinista, donde no determinista significa que cada paso a realizar tiene muchas posibles opciones y la complejidad se calcula suponiendo que, en cada paso, se escoge la peor opción. Por otro lado, los problemas NP-Completos son los más complejos dentro de NP.

Tiempo polinomial es cuánto tiempo necesita un algoritmo en resolver un problema dependiendo del tamaño de ese problema. El tiempo crece de forma razonable a medida que el tamaño del problema aumenta.

Elementos fundamentales de la criptografía de clave privada y de clave pública

Criptografía de Clave Pública

Problema de la factorización

La factorización de un número consiste en descomponerlo en un conjunto de números primos que, multiplicados, dan como resultado el número original. Los números primos son aquellos que solo tienen dos divisores: 1 y ellos mismos.

El proceso de factorización se basa en encontrar estos números primos. Una vez identificados, el número original se puede expresar como el producto de estos primos, a veces elevados a ciertas potencias si se repiten.

Un ejemplo: $3630 = 2 \times 3 \times 5 \times 11^2$

Descomponemos 3630 en sus factores primos:

- Primero, 3630 se divide por el menor número primo posible, 2, resultando en 1815.
- Luego, 1815 se divide por el menor primo que lo divide exactamente, 3, dando 605.
- 605 se divide por 5, resultando en 121.
- Finalmente, 121 es 11 al cuadrado (11^2).

Así, 3630 se descompone en el producto de 2, 3, 5, y 11^2. Cada número en esta descomposición es un número primo, y multiplicados todos juntos te dan el número original, 3630. Este proceso ayuda en diversas áreas de las matemáticas y la informática, especialmente en criptografía, donde la dificultad de factorizar grandes números primos es fundamental para la seguridad de muchos sistemas de encriptación.

Elementos fundamentales de la criptografía de clave privada y de clave pública

Criptografía de Clave Pública

Problema del logaritmo discreto

El problema del logaritmo discreto es un desafío matemático importante especialmente en el campo de la criptografía, debido a su dificultad de resolución en conjuntos de números finitos. A diferencia de los logaritmos comunes que trabajan con números reales y pueden tener cualquier valor, el logaritmo discreto opera dentro de un conjunto finito de números enteros bajo la operación de aritmética modular.

Imagina que tienes un conjunto finito de números que va del 0 hasta un número "n-1". Cuando realizas operaciones con estos números (como sumarlos), si el resultado excede el valor "n-1", simplemente divides este resultado por "n" y tomas el residuo; esto es lo que se conoce como operar "módulo n". Este proceso asegura que el resultado siempre sea un número dentro de nuestro conjunto original.

Aplicado a los logaritmos, el problema del logaritmo discreto busca encontrar un número "**x**" (el exponente) tal que, al elevar la base "**a**" a "**x**" y operar módulo un número "**p**", se obtenga un número "**b**" específico. En otras palabras, si conoces "**a**" y "**b**" y operas en un sistema módulo "**p**", ¿cuál es el valor de "**x**" que hace que $\mathbf{a^x \equiv b \pmod p}$?

En la fórmula $2^5 \equiv 10 \pmod{11}$, el signo ≡ significa "congruente con" en el contexto de la aritmética modular. Esto indica que dos números son equivalentes bajo una cierta operación de módulo. En este caso, decir que $32 \equiv 10 \pmod{11}$ significa que 2^5 (32) y 10 dejan el mismo resto cuando son divididos por 11.

Este problema es especialmente difícil de resolver cuando los números involucrados son grandes, lo cual lo hace útil en la criptografía para asegurar la comunicación en internet. La seguridad de muchos sistemas criptográficos, como el intercambio de claves Diffie-Hellman y el algoritmo de firma digital DSA, se basa en la dificultad de resolver el logaritmo discreto en grupos grandes y especialmente elegidos de números.

Elementos fundamentales de la criptografía de clave privada y de clave pública

Criptografía de Clave Pública – Curvas elípticas

La criptografía con curvas elípticas es un avance crucial en la seguridad digital, nacido para superar las debilidades de los métodos tradicionales de criptografía de clave pública. Estos sistemas anteriores enfrentaban problemas como la susceptibilidad al criptoanálisis y la necesidad de utilizar claves más grandes para asegurar la información adecuadamente.

La susceptibilidad al criptoanálisis se refiere a la vulnerabilidad o propensión de un sistema criptográfico (como un algoritmo de cifrado) a ser analizado y eventualmente roto o descifrado sin autorización. Este análisis busca encontrar debilidades o patrones que puedan ser explotados para revelar la información cifrada sin necesidad de la clave de cifrado.

El criptoanálisis emplea una variedad de técnicas y métodos matemáticos y estadísticos para intentar romper los criptosistemas. Estos métodos pueden incluir, entre otros, el análisis de frecuencias, ataques de texto claro conocido, texto cifrado conocido y ataques de texto elegido.

La solución que aportan las curvas elípticas radica en su compleja estructura matemática y la dificultad para resolver ciertos problemas matemáticos asociados, como el del logaritmo discreto. Esto permite usar claves más cortas sin sacrificar seguridad, optimizando así el uso de recursos computacionales, reduciendo la memoria necesaria y haciendo más eficientes tanto el procesamiento como la transferencia de datos.

Hoy en día, esta tecnología se emplea en diversos campos como la protección de datos en dispositivos móviles, seguridad en transacciones financieras y mantenimiento de la integridad en redes de sensores. La adopción generalizada de la criptografía de curvas elípticas se debe a su capacidad para ofrecer alta seguridad sin demandar grandes cantidades de recursos, convirtiéndola en la elección preferente para salvaguardar la información en nuestro entorno digital.

Características y atributos de los certificados digitales

Los certificados digitales actúan como una forma de identificación electrónica para individuos, servidores, y diversas entidades, facilitando tanto la firma digital como el cifrado de datos.

Estos documentos son cruciales para asegurar la autenticidad y la seguridad en el entorno digital, ligando pares de claves criptográficas a las entidades certificadas.

La gestión segura de la clave privada, parte esencial del par, es fundamental para evitar accesos no autorizados y garantizar la integridad de las comunicaciones.

Existen diversas Autoridades de Certificación responsables de emitir estos certificados tras verificar la identidad de los solicitantes.

Estos certificados encuentran aplicación en una variedad de escenarios digitales, desde la firma de correos electrónicos hasta la realización de trámites oficiales en línea, como los que se exigen en España para interactuar con la administración pública.

La clasificación de los certificados digitales se basa en el ámbito de aplicación y el nivel de validación requerido. Por ejemplo, existen certificados específicos para usuarios individuales, organizaciones, servidores, y para el intercambio seguro entre empresas.

Se distinguen principalmente tres tipos de certificados según el nivel de validación: de validación de dominio (DV), de validación de organización (OV), y de validación extendida (EV), ofreciendo todos un grado de seguridad equivalente, aunque ciertas operaciones pueden requerir niveles específicos de validación para asegurar una mayor confianza.

La correcta selección y uso de estos certificados digitales es esencial para la protección de la identidad digital y la seguridad de las transacciones electrónicas, siendo también vital en el ámbito empresarial para asegurar la autenticidad y la confianza en las operaciones comerciales y financieras en línea.

Características y atributos de los certificados digitales

En base a los tipos de certificados, dependiendo del nivel de validación requerido, se pueden encontrar las siguientes clases:

- Clase 1: para los usuarios, especialmente para el correo.
- Clase 2: para las organizaciones, de modo que se pueda probar su identidad.
- Clase 3: para los servidores y las firmas de los programas.
- Clase 4: para trámites online entre empresas.
- Clase 5: para empresas privadas y de seguridad gubernamentales.

Identificación y descripción del funcionamiento de los protocolos de intercambio de claves usados más frecuentemente

Introducción

Los protocolos de intercambio de claves facilitan la creación de una clave secreta compartida entre dos entidades a través de un medio no seguro. Su propósito es asegurar que la comunicación cifrada sea accesible solo para las partes involucradas, protegiendo así la transferencia de datos contra interceptaciones. Los aspectos críticos a considerar en su diseño y análisis incluyen:

- Autenticación: Verificación de la identidad de las entidades y de la clave compartida. Es fundamental decidir si se requiere autenticación unilateral o mutua y si es necesario confirmar la recepción de la clave.
- Frescura de la clave: Importancia de garantizar que la clave permanezca válida y protegida contra ataques, manteniendo su confidencialidad a lo largo del tiempo.
- Gestión de la clave: Algunos protocolos permiten que una entidad seleccione la clave y la envíe a la otra, mientras que otros facilitan una colaboración para generar una clave a partir de contribuciones mutuas.
- Eficiencia: Evaluación del número de mensajes intercambiados, el consumo de ancho de banda y la complejidad computacional implicada.
- Participación de terceros: Determinación de la necesidad y el papel de una tercera entidad, considerando si su intervención es en tiempo real o no.
- Uso de certificados: Si se incluyen terceras partes, evaluar la distribución y gestión de certificados digitales.

Entre los protocolos destacados se encuentra el Diffie-Hellman, pionero en el establecimiento de una clave segura entre partes sin necesidad de un canal seguro previo. Este método es fundamental en numerosos sistemas de cifrado, ofreciendo una base para la seguridad en la transmisión de datos.

Identificación y descripción del funcionamiento de los protocolos de intercambio de claves usados más frecuentemente

Protocolo Diffie-Hellman (1976)

Está basado en las propiedades de los logaritmos discretos y no proporciona ningún tipo de autenticación, permitiendo la existencia de un ataque de hombre en el medio. Lo explicaremos de una manera sencilla:

Ana y Bea quieren tener una conversación privada a través de un medio inseguro (como internet).

Ana y Bea eligen dos números: **p** y **g**

- El número **(p)** debe ser un número enorme, difícil de adivinar (por ejemplo, un número con 300 dígitos)
- El número **(g)** es un número que cumple que al hacer ciertas operaciones matemáticas con él (dividir sus sucesivas potencias con el número **p** se obtienen todos los restos entre 1 y **p**-1) nos genera un conjunto muy variado de números.

Ana escoge un número secreto **(a)** y lo usa para transformar el numero **(g)** en otro número (M_A) y se lo envía a Bea.

$M_A=g^a mod(p)$ *mod* es la operación de módulo que encuentra el resto cuando g^a se divide por **p** M_A sería la clave pública de Ana

Bea escoge un número secreto **(b)** y lo usa para transformar el numero **(g)** en otro número (M_B) y se lo envía a Ana.

$M_B=g^b mod(p)$ *mod* es la operación de módulo que encuentra el resto cuando g^b se divide por **p** M_B sería la clave pública de Bea

Tanto Ana como Bea utilizando cada una de ellas su propio número secreto **(a** y **b)** en combinación con el número que recibieron respectivamente (**M_A** y **M_B**) llegarán al mismo código secreto (**K_s)** compartido para la conversación.

Ana: $\mathbf{K_s} = (M_B)^a mod(p)$ Bea: $\mathbf{K_s} = (M_A)^b mod(p)$

Este proceso es especial porque, aunque otras personas sepan los números públicos (**p, g**) y hayan visto los números transformados (**MA, MB**), sin conocer los números secretos de Ana y Bea, no pueden descifrar el "código secreto" que comparten.

Algoritmos criptográficos más frecuentemente utilizados

Introducción

En el campo de la criptografía, hay dos tipos principales de algoritmos: los de clave privada, como DES, Triple DES, AES, IDEA y Blowfish, entre otros, y los de clave pública, destacando RSA y El Gamal. Ambos tipos tienen sus ventajas y limitaciones.

Por ello, los algoritmos híbridos, que combinan métodos de clave privada y pública, son comúnmente empleados para mejorar la seguridad.

Además de estos algoritmos de cifrado, existen otros diseñados para funciones como la creación de resúmenes criptográficos o firmas electrónicas, los cuales serán explicados posteriormente.

Algoritmos criptográficos más frecuentemente utilizados

Algoritmos de criptografía de clave privada

Data Encryption Standard (DES)

El Data Encryption Standard (DES) es un algoritmo de cifrado por bloques que fue estandarizado por el NIST en 1977. Pese a su uso extendido, la capacidad para romper su cifrado en menos de tres días demostró su vulnerabilidad, lo que condujo al desarrollo y adopción del Advanced Encryption Standard (AES) en 2001.

DES usa una clave de 64 bits para cifrar la información en bloques de igual tamaño, aunque efectivamente solo 56 de estos bits son utilizados para la seguridad; el resto es para la verificación de la integridad de la clave. El proceso de cifrado incluye 16 rondas de operaciones (red de Feistel) complejas sobre el bloque de datos, que se pueden resumir en estos pasos:

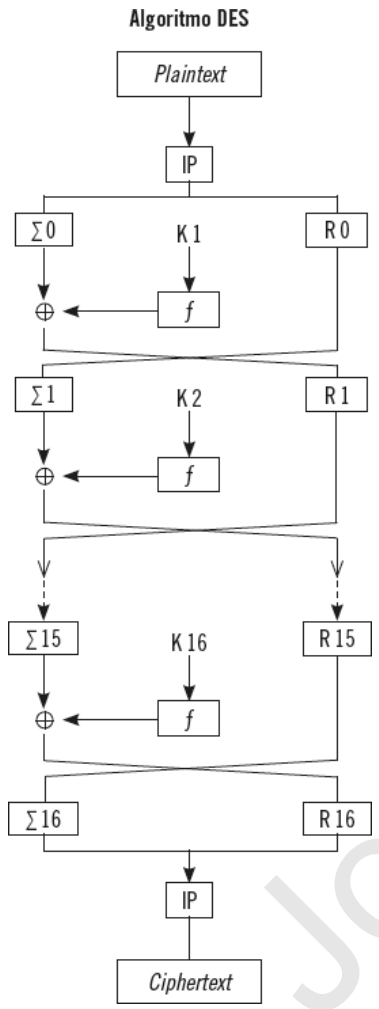
- División del mensaje en bloques de 64 bits.
- Selección y descomposición de un bloque en sus bits constituyentes.
- Aplicación de una permutación inicial (IP) que reordena los bits según reglas predeterminadas.
- Ejecución de 16 rondas de transformaciones (red de Feistel) que incluyen:
  - Dividir el bloque en dos mitades de 32 bits.
  - Expandir y permutar la mitad derecha (R0) a 48 bits usando la Caja E (Expansión), para aumentar la longitud.
  - Combinar la salida de la Caja E con una clave de ronda de 48 bits mediante XOR.
  - Pasar este resultado a través de las Cajas S (Sustitución) , que reducen de 48 a 32 bits.
  - Permutar el resultado final de las Cajas S.
  - Realizar XOR del resultado con la mitad izquierda del bloque (L0), dando como resultado R1, que será la mitad derecha en la siguiente ronda, mientras que R0 se convierte en la nueva mitad izquierda (L1).

La secuencia de operaciones en DES está diseñada para ser suficientemente compleja como para prevenir ataques, pero las vulnerabilidades encontradas con el tiempo llevaron a la necesidad de reemplazarlo con sistemas más seguros como el AES.

Algoritmos criptográficos más frecuentemente utilizados

Algoritmos de criptografía de clave privada

Data Encryption Standard (DES)



Triple DES, implementado en 1999, es una evolución del DES original que aumenta la seguridad mediante la aplicación del algoritmo DES tres veces con dos claves distintas.

Funciona cifrando primero con una clave, descifrando con la segunda clave y volviendo a cifrar con la primera clave.

Este método de encriptación mejorado surgió porque el Doble DES no ofrecía una mejora de seguridad sustancial, mientras que Triple DES sí lo hacía, a pesar de requerir la administración de dos claves en lugar de una.

Algoritmos criptográficos más frecuentemente utilizados

Algoritmos de criptografía de clave privada

International Data Encryption Algorithm (IDEA)

- Es un algoritmo de cifrado diseñado en 1991 para ser un sucesor más seguro del Data Encryption Standard (DES).
- IDEA trabaja con bloques de 64 bits y utiliza claves de 128 bits a lo largo de 8 rondas de cifrado complejo, y fue incorporado en versiones iniciales de Pretty Good Privacy (PGP), una herramienta de encriptación de uso extendido.
- IDEA se distingue por combinar operaciones de distintos grupos algebraicos (XOR, suma y multiplicación) para transformar tanto el texto plano como las subclaves durante su proceso de cifrado.

Blowfish

- Desarrollado en 1993, es otro algoritmo de cifrado simétrico que también fue propuesto como reemplazo de DES y IDEA.
- Blowfish cifra bloques de datos de 64 bits y puede utilizar claves de longitud variable, desde 32 hasta 448 bits.
- Su arquitectura es una red de Feistel de 16 rondas que utiliza S-boxes (cajas de sustitución) al igual que DES.
- Aunque Blowfish es conocido por su velocidad y eficiencia, y es de dominio público, no se estandarizó de manera global como lo hizo el Advanced Encryption Standard (AES).

Algoritmos criptográficos más frecuentemente utilizados

Algoritmos de criptografía de clave privada

Advanced Encryption Standard (AES)

El Advanced Encryption Standard (AES) es una mejora sobre DES y Triple DES y se basa en el algoritmo Rijndael. Seleccionado por el NIST en 2001, AES se convirtió en el estándar para una variedad de usos gubernamentales y privados debido a su robustez y confiabilidad.

AES es un cifrador de bloque que trabaja con bloques de 128 bits y permite el uso de claves de 128, 192 o 256 bits. Destaca por su eficiencia en distintas plataformas, desde hardware hasta software, y por su implementación que no requiere grandes cantidades de memoria.

Los pasos del algoritmo AES son:

- División del mensaje en bloques de 128 bits.
- Inicialización de la matriz de Estado con un XOR entre el bloque de entrada y la clave inicial.
- Aplicación de las siguientes funciones en N rondas (10, 12 o 14 rondas dependiendo de la longitud de la clave):

  a. SubBytes: sustitución no lineal usando una tabla de sustitución predefinida (S-box).

  b. ShiftRows: desplazamiento de filas; cada fila de la matriz de Estado se desplaza un número determinado de bytes.

  c. MixColumns: combinación de columnas utilizando una operación de multiplicación de polinomios.

  d. AddRoundKey: suma de la clave de ronda con la matriz de Estado utilizando XOR.

AES y DES comparten la estructura general de ser cifradores de bloque, pero AES tiene más rondas, utiliza un esquema de clave más complejo y su matriz de Estado agrega un nivel adicional de confusión y difusión a través de sus funciones específicas.

Algoritmos criptográficos más frecuentemente utilizados

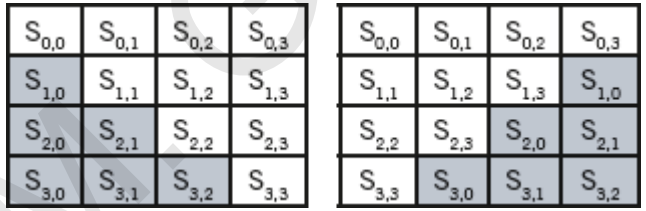
Algoritmos de criptografía de clave privada

Advanced Encryption Standard (AES)

¿Qué es la matriz de estado?

Es una matriz de 4×4 bytes (16bytes * 8bits/byte= 128bits) sobre la que se realizan todas las operaciones de cifrado y descifrado. En AES, el texto plano se divide en bloques de 128 bits, y cada bloque se asigna a esta matriz de estado para su procesamiento.

Durante las distintas fases de AES —como SubBytes, ShiftRows, MixColumns y AddRoundKey—, la matriz de estado se modifica y mezcla sistemáticamente para producir el texto cifrado



Algoritmos criptográficos más frecuentemente utilizados

Algoritmos de criptografía de clave pública

RSA

El algoritmo RSA, creado en 1978 por Rivest, Shamir y Adleman, fue pionero en la criptografía de clave pública, ofreciendo métodos efectivos tanto para cifrado de mensajes como para la firma electrónica. Este algoritmo ha resistido la prueba del tiempo, a diferencia de muchos de sus predecesores.

En RSA, se utiliza una clave pública para cifrar mensajes o verificar firmas, y una clave privada para descifrar mensajes o generar firmas. Los conceptos matemáticos que sustentan RSA son la operación módulo y el indicador de Euler, ϕ**(n),** que es la cantidad de enteros menores o iguales a **(n)** que son coprimos con **(n).**

Un coprimo, también conocido como primo relativo o primo entre sí, se refiere a dos números enteros **a** y **b** que no tienen ningún factor primo en común excepto 1.

Es decir, el máximo común divisor (m.c.d.) de ambos números es exactamente 1. Esto significa que no existe ningún número mayor que 1 que pueda dividir a ambos números sin dejar residuo.

Por ejemplo, los números 8 y 15 son coprimos porque los únicos divisores de 8 son 1, 2, 4, y 8, mientras que los divisores de 15 son 1, 3, 5, y 15; el único divisor común es el 1.

Por ejemplo, para (n = 9), los números coprimos con 9 son 1, 2, 4, 5, 7 y 8, lo que significa que (ϕ(9) = 6).

Algoritmos criptográficos más frecuentemente utilizados

Algoritmos de criptografía de clave pública

RSA

Suponiendo que A quiere mandar un mensaje cifrado a B, el proceso de ejecución de RSA es el siguiente:

- El remitente A escoge dos números primos muy grandes y no públicos, **p** y **q**, de modo que obtiene **$n=p \cdot q$**
- A escoge un número entero **e** que sea primo relativo con **$\phi(n)$**.
- A escoge un número **d** tal que **$e \cdot d=1 \bmod(\phi(n))$.**
- La clave pública de A es (e, n), mientras que la clave privada es (d, n). A distribuye su clave pública utilizando cualquiera de los mecanismos de distribución de claves públicas.
- B envía un mensaje cifrado (que llamaremos M) a A, **$C = M^e \bmod(n)$**

  Recuérdaque esta operación se realiza, primero, multiplicando el mensaje por sí mismo tantas veces como indique "e" y, posteriormente, se obtiene el resto de dividir el resultado por el número "n". Es importante resaltar que el mensaje M tiene que ser numérico, por lo que si fuese un texto será necesario representarlo como número.
- A descifra el mensaje haciendo uso de la clave privada, **$M = C^d \bmod(n)$**

Algoritmos criptográficos más frecuentemente utilizados

Algoritmos de criptografía de clave pública

GAMAL

El algoritmo de ElGamal, desarrollado por Taher ElGamal en 1984, es un método de criptografía asimétrica que extiende el concepto del protocolo de intercambio de claves Diffie-Hellman. Este algoritmo se emplea tanto en la encriptación de datos como en la creación de firmas digitales, siendo cada variante específica para su propósito. Se destaca en aplicaciones como el Pretty Good Privacy (PGP) para asegurar la privacidad y autenticidad de la comunicación.

ElGamal se fundamenta en la dificultad de resolver el problema del logaritmo discreto en matemáticas, lo que le confiere robustez frente a intentos de descifrado sin autorización. A diferencia de RSA, que genera un resultado único de cifrado para un mensaje dado y una clave, ElGamal produce resultados diferentes cada vez que se cifra el mismo mensaje con la misma clave pública, mejorando la seguridad al hacer más difícil el análisis criptográfico por parte de atacantes.

Esta variabilidad se logra mediante el uso de un valor aleatorio en el proceso de cifrado, que, aunque complica el análisis criptográfico, implica también una gestión cuidadosa de estos valores para mantener la seguridad del sistema. La firma digital de ElGamal, por otro lado, garantiza la integridad y autenticidad de los mensajes, permitiendo al receptor verificar que el mensaje no ha sido alterado y que proviene del remitente esperado.

A pesar de su seguridad y eficacia, la implementación de ElGamal puede resultar más compleja y generar mensajes cifrados más largos en comparación con RSA, lo que puede influir en la elección del algoritmo dependiendo del contexto de uso específico.

Algoritmos criptográficos más frecuentemente utilizados

Robustez y eficiencia práctica de los algoritmos

Los algoritmos criptográficos son fundamentales para la seguridad de la información digital, pero su robustez y eficiencia práctica están significativamente influenciadas por la calidad de su implementación.

El cifrador de Vernam, también conocido como el cifrado de un solo uso, es el único método considerado absolutamente seguro según la teoría de la información de Claude Shannon, siempre que la clave sea verdaderamente aleatoria, tan larga como el mensaje y utilizada una sola vez.

Vulnerabilidades del Software

La calidad de la programación de los algoritmos criptográficos es crítica. Un error de programación o configuración puede hacer que el algoritmo sea vulnerable a ataques, reduciendo su seguridad efectiva. Para gestionar y mitigar estas vulnerabilidades, se utilizan bases de datos como la Common Vulnerability Exposure (CVE), que ofrece un sistema uniforme para identificar y corregir errores.

Gestión de Claves

La forma en que se manejan las claves en la criptografía simétrica es otro punto crítico. Algunos sistemas aplican una función resumen (Hash) a la clave proporcionada por el usuario para generar la clave de cifrado, buscando hacerla menos predecible. Sin embargo, si el proceso es previsible o si la clave se incrusta en el software, puede ser extraída por atacantes avanzados.

Algoritmos criptográficos más frecuentemente utilizados

Robustez y eficiencia práctica de los algoritmos

Relevancia de la Auditoría y Certificación

Las auditorías y las certificaciones son esenciales para confirmar que los sistemas criptográficos funcionan según lo previsto. Organismos como el National Institute of Standards and Technology (NIST) en EE. UU. y el Centro Criptológico Nacional en España ofrecen certificaciones que validan el cumplimiento de normas específicas como FIPS 140-1 o evaluaciones EAL4+, respectivamente.

Eficiencia Práctica

Para ser viables en aplicaciones reales, los algoritmos deben ser computacionalmente eficientes, minimizando el uso de recursos como memoria y procesador, y consumiendo una cantidad moderada de energía en dispositivos portátiles. La eficiencia se puede mejorar mediante hardware dedicado, como circuitos lógicos específicos o coprocesadores criptográficos, que aceleran las operaciones criptográficas sin estar ligados a un algoritmo específico.

La implementación y gestión adecuadas de los algoritmos criptográficos, junto con una vigilancia continua de las vulnerabilidades y una gestión cuidadosa de las claves, son fundamentales para mantener la integridad, confidencialidad y disponibilidad de la información en el mundo digital.

Elementos de los certificados digitales, los formatos comúnmente aceptados y su utilización

Introducción

Los certificados digitales son esenciales para la seguridad en internet, proporcionando la identificación de entidades digitales y facilitando transacciones seguras.

Entre los formatos más reconocidos están los certificados X.509 y PGP (Pretty Good Privacy), cada uno con aplicaciones y características específicas, aunque comparten componentes clave en su estructura:

- Número de Serie: Un identificador único asignado al certificado por la autoridad de certificación (CA) que lo emite.
- Nombre de la Entidad Emisora: La identidad de la autoridad de certificación que emite y firma el certificado.
- Periodo de Validez: Las fechas de inicio y finalización de la validez del certificado, fuera de las cuales el certificado no debe ser considerado confiable.
- Nombre del Sujeto Propietario del Certificado: Identificación del individuo, servidor, dispositivo o entidad que posee el certificado.
- Clave Pública del Sujeto Propietario del Certificado: La clave pública asociada con el sujeto, utilizada para cifrar mensajes o verificar firmas digitales que solo la correspondiente clave privada del sujeto puede descifrar o firmar.

Elementos de los certificados digitales, los formatos comúnmente aceptados y su utilización

Certificados X.509

Los certificados X.509 son una parte fundamental de las infraestructuras de clave pública (PKI), permitiendo la verificación de identidades digitales y facilitando comunicaciones seguras en internet. Estos certificados han evolucionado a través de tres versiones principales:

- X.509v1 (1988): La versión original, introducida para establecer una Infraestructura de Clave Pública (PKI), marcó el inicio del estándar X.509.
- X.509v2 (1993): Introdujo campos adicionales para identificar de manera unívoca tanto al emisor (Autoridad de Certificación, AC) como al titular del certificado, mejorando la estructura para una identificación más precisa.
- X.509v3 (2008): Esta versión surgió como respuesta a la necesidad de una mayor flexibilidad y capacidad de extensión, incorporando un conjunto amplio de campos adicionales que pueden ser definidos en estándares o registrados por comunidades u organizaciones específicas.

Usos de los certificados X.509 son extensos, incluyendo la autenticación en administración electrónica, la transmisión segura de datos entre servidores mediante SSL/TLS, y otros escenarios donde se requiere confiabilidad y seguridad en la identificación y comunicación digital

Elementos de los certificados digitales, los formatos comúnmente aceptados y su utilización

Certificados X.509

Contenidos clave de los certificados X.509v3 incluyen:

- Versión: Indica la versión del certificado (1, 2, o 3).
- Número de Serie: Un identificador único asignado por la Autoridad de Certificación (AC) emisora.
- Identificador del Algoritmo de Firma: Especifica el algoritmo de firma utilizado para el certificado.
- Nombre del Emisor: El nombre de la Autoridad de Certificación que emite el certificado.
- Periodo de Validez: Define la fecha de inicio y fin de la validez del certificado.
- Nombre del Sujeto: Identifica al usuario o entidad a la que se le otorga el certificado.
- Información de la Clave Pública del Sujeto: Contiene la clave pública, parámetros asociados y el identificador del algoritmo para su uso.
- Firma Digital del Emisor: La firma de la Autoridad de Certificación (AC) que valida el certificado.
- Extensiones (Opcional): Proporcionan información adicional dividida en tres categorías: información de la clave y la política, atributos del sujeto y de la AC, y limitaciones del camino de los certificados.

Elementos de los certificados digitales, los formatos comúnmente aceptados y su utilización

Certificados PGP

Los Certificados PGP (Pretty Good Privacy) son fundamentales en la criptografía de clave pública, diseñados por Phil Zimmermann en 1991. Estos certificados, a diferencia de los X.509 emitidos por Autoridades de Certificación (AC), son generados por los propios usuarios, que crean un par de claves, pública y privada, asociando la pública a un certificado PGP.

La peculiaridad de los certificados PGP radica en el modelo de confianza descentralizado que emplean. Dado que no existe una entidad central que verifique la propiedad de las claves, la confianza en un certificado PGP depende de las firmas de otros usuarios sobre dicho certificado, introduciendo el concepto de "anillo de confianza".

Este enfoque posibilita que los usuarios establezcan niveles de confianza en las claves a través de un esquema de voto, siendo la confianza depositada en las claves directamente proporcional a la cantidad y calidad de las firmas que estas posean.

A diferencia de los certificados X.509, que dependen de una infraestructura de clave pública centralizada, los certificados PGP ofrecen una alternativa basada en la confianza entre pares. Esto los hace particularmente útiles en contextos donde la creación de certificados por parte de usuarios es práctica y deseada, como el intercambio seguro de correos electrónicos, entre otros usos.

Elementos de los certificados digitales, los formatos comúnmente aceptados y su utilización

Certificados PGP

El contenido típico de un certificado PGP incluye:

- Número de versión: Especifica la versión de PGP usada.
- Clave pública: La clave pública del propietario.
- Algoritmo de creación de claves: El algoritmo usado para generar el par de claves.
- Información del sujeto: Datos personales del titular del certificado.
- Firma digital del sujeto: También conocida como autofirma, asegura que el certificado ha sido generado por el propietario de la clave privada correspondiente.
- Periodo de validez: La duración de la validez del certificado.
- Algoritmo simétrico preferido: La preferencia del propietario por un algoritmo de cifrado específico.

Elementos de los certificados digitales, los formatos comúnmente aceptados y su utilización

Diferencias Clave X509 vs PGP

Diferencias Clave

- Modelo de Confianza: X.509 utiliza un modelo jerárquico con ACs, mientras que PGP emplea una red de confianza entre pares.
- Emisión de Certificados: En X.509, los certificados son emitidos por ACs. En PGP, los usuarios crean y firman sus propios certificados, con la opción de recibir firmas de otros usuarios.
- Uso: X.509 es predominante en aplicaciones de seguridad en la web y en sistemas de correo electrónico seguro como S/MIME. PGP es ampliamente usado para cifrado de correo electrónico y archivos a través de OpenPGP.
- Estructura: X.509 tiene una estructura más rígida y estandarizada, mientras que PGP permite mayor flexibilidad.

Ambos sistemas tienen sus ventajas y se utilizan en diferentes contextos según las necesidades específicas de seguridad, confianza y administración de claves .

Elementos fundamentales de las funciones resumen y los criterios para su utilización

Introducción

Las funciones resumen en criptografía son procedimientos esenciales para asegurar la integridad de la información y autenticar datos. Al aplicar estas funciones a cualquier mensaje, se obtiene un "resumen" o "huella digital" de longitud fija, independientemente del tamaño original del mensaje. Esta característica fundamental permite identificar de manera única los datos, facilitando su verificación sin necesidad de manejar el contenido completo.

Propiedades Clave

- Difusión (Efecto Avalancha): Un cambio mínimo en el mensaje de entrada (por ejemplo, modificar un solo bit) resulta en un cambio significativo en la salida, haciendo que esta parezca completamente distinta. Este efecto asegura que no se puedan predecir cambios en la salida basados en cambios en la entrada.
- Determinismo: Para un conjunto dado de datos de entrada, la función resumen siempre producirá el mismo resultado, lo que es crucial para verificar la integridad de los datos.
- Eficiencia: Las funciones resumen son diseñadas para ser rápidas de calcular, permitiendo su uso en sistemas en tiempo real y en dispositivos con limitaciones de recursos.

Elementos fundamentales de las funciones resumen y los criterios para su utilización

Introducción

Resistencias Necesarias

- Resistencia a la Primera Preimagen:

  Hace computacionalmente inviable deducir el mensaje original a partir de su resumen.

- Resistencia a la Segunda Preimagen:

  Impide encontrar otro mensaje que genere el mismo resumen que un mensaje dado.

- Resistencia a Colisiones:

  Evita encontrar dos mensajes distintos que resulten en el mismo resumen.

Estructura de Merkle-Damgard

Uno de los enfoques para construir funciones resumen es mediante la estructura de Merkle-Damgard, que asegura la resistencia a colisiones a través de iteraciones encadenadas de una función de compresión. Este diseño es la base de algoritmos conocidos como MD5, SHA-1, SHA-2 y SHA-3.

Actualidad y Seguridad

Con el avance de la tecnología computacional, algunas funciones como MD5 y SHA-1 han sido comprometidas, evidenciando la importancia de la evolución continua en el desarrollo de estas funciones. SHA-3 es el resultado de una competición organizada por el NIST, reflejando un diseño robusto que supera a sus predecesores en términos de seguridad.

Elementos fundamentales de las funciones resumen y los criterios para su utilización

Funciones resumen con clave

Las funciones resumen con clave, conocidas como HMAC (Hash-based Message Authentication Code), son una especialización de las funciones de hash que incluyen un elemento adicional de seguridad mediante el uso de una clave secreta. Esto les permite no solo generar un resumen del mensaje (como lo hacen las funciones hash convencionales) sino también autenticar el origen del mismo.

El proceso de HMAC implica combinar el mensaje de entrada con una clave secreta antes de aplicar la función hash. Esto significa que el resumen resultante no solo depende del contenido del mensaje sino también de la clave secreta utilizada. Por lo tanto, cualquier cambio en el mensaje o en la clave producirá un resumen completamente diferente.

El uso de HMAC es especialmente útil en entornos donde la autenticación del mensaje es crítica. Por ejemplo, en un contexto bancario, el uso de HMAC permite al banco verificar no solo que el mensaje no ha sido alterado durante la transmisión (integridad) sino también que fue efectivamente creado por un emisor autorizado (autenticidad). Esto se debe a que solo el emisor legítimo y el receptor deberían conocer la clave secreta compartida.

La efectividad de HMAC radica en la dificultad de encontrar dos mensajes diferentes que, al aplicarles la misma función HMAC (usando la misma clave), produzcan el mismo resumen. Además, es computacionalmente inviable derivar la clave secreta a partir del resumen generado, lo que añade una capa de seguridad adicional a la comunicación.

HMAC proporciona una herramienta robusta para la autenticación de mensajes en la criptografía, siendo aplicable en una amplia gama de situaciones donde la verificación de la integridad y la autenticidad del mensaje es fundamental. Su implementación se basa en el principio de que el conocimiento de una clave compartida secreta se utiliza como mecanismo de autenticación, añadiendo así un nivel de seguridad que va más allá de las funciones hash tradicionales .

Elementos fundamentales de la firma digital, los distintos tipos de firma y los criterios para su utilización

Esquema básico

La Ley 6/2020, promulgada el 11 de noviembre de 2020, introduce regulaciones actualizadas para los servicios electrónicos de confianza en España, derogando la anterior Ley 59/2003 de firma electrónica.

Esta actualización responde a la necesidad de alinear la legislación nacional con el Reglamento Europeo eIDAS de 2014, el cual establece un marco único europeo para estos servicios.

La autenticación, esencial en la firma electrónica, asegura la identidad de una entidad o individuo.

La Ley 6/2020 establece cambios significativos, especialmente en lo que respecta a la identificación electrónica y la firma electrónica. Destaca que solo las personas físicas pueden generar firmas electrónicas, excluyendo a las personas jurídicas de esta capacidad. Sin embargo, estas últimas pueden representarse a través de certificados de firma de personas físicas autorizadas. Además, se equipara legalmente la firma electrónica cualificada con la manuscrita, asegurando su equivalencia jurídica.

Los servicios electrónicos de confianza ampliados incluyen:

- Sello electrónico: Permite a las personas jurídicas firmar electrónicamente y autenticarse en línea.
- Validación de firmas y sellos cualificados: Verifica la vigencia y validez de firmas o sellos.
- Sellado de tiempo electrónico: Confirma la existencia e inmutabilidad de datos en un momento específico.
- Entrega electrónica certificada: Prueba la entrega de mensajes o documentos electrónicos.
- Certificados de autenticación web: Aseguran comunicaciones seguras con sedes electrónicas.

Elementos fundamentales de la firma digital, los distintos tipos de firma y los criterios para su utilización

Tipos de firmas

La Unión Europea, a través del Reglamento eIDAS, establece tres niveles de firma electrónica: simple, avanzada y cualificada. Cada uno ofrece distintos niveles de seguridad y autenticación.

Firma Electrónica Simple: Este es el nivel más básico de firma electrónica. No requiere de certificado digital específico y puede ser tan simple como un nombre escrito al final de un correo electrónico. Aunque la firma electrónica simple puede no garantizar la identidad del firmante, es útil para documentos de bajo riesgo donde la autenticidad no es crítica.

Firma Electrónica Avanzada (AdES): Proporciona un mayor nivel de seguridad que la firma simple. La firma avanzada está vinculada de forma única al firmante y es capaz de identificar al firmante. Se crea utilizando datos de creación de firma que el firmante puede usar bajo su control exclusivo. A diferencia de la firma simple, la firma avanzada garantiza la integridad del documento, ya que cualquier cambio posterior a la firma es detectable.

P.e. Soluciones empresariales o implementaciones de software que garantizan la identidad de los firmantes.

Firma Electrónica Cualificada (QES): Es el nivel más seguro y ofrece la mayor garantía legal, equiparable a la firma manuscrita en muchos contextos legales dentro de la UE. Se basa en un certificado digital cualificado y debe ser creada utilizando un dispositivo seguro de creación de firma. Este tipo de firma requiere la verificación de la identidad del firmante por una Autoridad de Certificación antes de emitir el certificado digital.

Elementos fundamentales de la firma digital, los distintos tipos de firma y los criterios para su utilización

Tipos de firmas

- Los certificados cualificados pueden terminar por caducidad o revocación. La Ley 6/2020 detalla las causas de revocación, incluyendo solicitud del titular o descubrimiento de falsedades en los datos proporcionados.
- Los certificados tienen una validez máxima de 5 años, y los prestadores de servicios deben mantener la información relevante por 15 años tras finalizar el servicio.
- El Ministerio de Asuntos Económicos y Transformación Digital supervisa a los prestadores de servicios de confianza, desarrollando inspecciones y manteniendo una lista actualizada de prestadores cualificados.
- La ley también impone a todos los prestadores de servicios de confianza la obligación de adoptar medidas organizativas y técnicas para manejar riesgos de seguridad y notificar cualquier incidente de seguridad.
- Finalmente, se actualiza la regulación sobre el Documento Nacional de Identidad electrónico, definiéndolo como medio para acreditar electrónicamente la identidad del titular y garantizar la integridad de los documentos firmados electrónicamente.

Criterios para la utilización de técnicas de cifrado de flujo y de bloque

Los criterios para la elección entre técnicas de cifrado de flujo y de bloque dependen de la naturaleza de los datos a proteger y del contexto de su uso.

Los cifradores de flujo, caracterizados por su rapidez y simplicidad, cifran los datos bit a bit o byte a byte, lo que les hace ideales para entornos donde los datos se generan o transmiten de forma continua, como en la transmisión de audio o video en tiempo real.

Su principal ventaja reside en la capacidad de iniciar el proceso de descifrado con tan solo una pequeña porción de los datos, lo que reduce la latencia en la comunicación. Sin embargo, su seguridad depende críticamente de la no reutilización de la clave de cifrado y de la generación de una secuencia cifrante impredecible.

Por otro lado, los cifradores de bloque trabajan con bloques de datos de tamaño fijo, aplicando una transformación compleja en cada bloque. Esto proporciona una alta difusión, lo que significa que pequeños cambios en el texto plano resultan en cambios significativos en el texto cifrado, dificultando el análisis criptográfico.

Son especialmente útiles para el cifrado de datos almacenados, como archivos o bases de datos, donde el tamaño total de los datos es conocido de antemano. No obstante, requieren mecanismos de relleno para ajustar el último bloque de datos al tamaño fijo, y son susceptibles a ciertos tipos de ataques si no se implementan modos de operación seguros.

La elección entre un cifrador de flujo y uno de bloque se basa en el tipo de datos a cifrar y en los requisitos específicos del sistema en el que se implementan. Los cifradores de flujo son preferidos para datos en tiempo real o streaming, mientras que los cifradores de bloque son la opción para el cifrado de datos estáticos o almacenados.

Protocolos de intercambio de claves

Introducción

Los protocolos de intercambio de claves son esenciales en la criptografía para asegurar una comunicación segura entre dos partes. Se dividen principalmente en base al uso de claves secretas o públicas, y su implementación puede ser a través de métodos de criptografía simétrica o asimétrica.

Intercambio de claves secretas mediante criptografía simétrica

Este método implica que ambas partes compartan una clave secreta que se usa tanto para cifrar como para descifrar los mensajes. Los métodos para distribuir estas claves secretas incluyen:

- Entrega Física Directa: Una parte genera la clave y la entrega físicamente a la otra.
- Tercera Parte: Un intermediario selecciona la clave y la distribuye físicamente a ambas partes.
- Uso de Claves Anteriores: Si las partes han compartido claves anteriormente, pueden usar una clave previa para cifrar y enviar la nueva clave.
- Centro de Distribución de Claves (CDC): Un CDC puede generar la clave y enviarla a ambas partes de manera segura, utilizando claves maestras compartidas con cada entidad para cifrar las claves de sesión.

Cada método tiene sus ventajas y limitaciones. La entrega directa y a través de un intermediario son seguras pero poco prácticas a gran escala. El uso de claves anteriores puede ser vulnerable si la clave se compromete. El CDC ofrece una solución más escalable y segura, utilizando una jerarquía de claves para facilitar la distribución.

La criptografía simétrica es efectiva para el intercambio punto a punto, pero en redes más grandes, la gestión de claves y la necesidad de intercambio dinámico hacen que sea desafiante. Además, si se compromete la clave compartida, todos los mensajes cifrados anteriores y futuros están en riesgo.

Protocolos de intercambio de claves

Intercambio de claves secretas mediante criptografía simétrica

Control de Uso de Claves

La gestión eficaz de las claves incluye no solo la distribución sino también el control sobre cómo se utilizan las claves. Las técnicas incluyen:

- Etiquetas de Clave: Identificadores cifrados que especifican el uso permitido de una clave.
- Vectores de Control: Campos que detallan el uso y restricciones de la clave, ofreciendo una solución más flexible que las etiquetas de clave debido a su capacidad para incluir información detallada y su distribución en claro.

Estos métodos ayudan a asegurar que las claves se utilicen de manera apropiada y dentro de los límites definidos, mitigando el riesgo de uso indebido.

Protocolos de intercambio de claves

Intercambio de claves secretas mediante criptografía asimétrica

La criptografía asimétrica es un pilar fundamental para la seguridad digital, especialmente en el intercambio de claves secretas entre dos partes sin necesidad de un canal seguro previamente establecido. Este enfoque aborda la principal debilidad de la criptografía asimétrica, su alta demanda computacional, concentrándose en su utilidad primordial: el intercambio seguro de claves.

En un escenario con dos entidades, A y B, deseando compartir una clave secreta común, la implementación de un protocolo basado en criptografía asimétrica procede de la siguiente manera:

- Generación y Envío de Clave Pública: A crea un par de claves, una pública y otra privada, y envía su clave pública junto con su identificador a B.
- Cifrado y Envío de la Clave Secreta: B genera una clave secreta (Ks), la cifra usando la clave pública de A y la envía a A.
- Descifrado de la Clave Secreta: A utiliza su clave privada para descifrar el mensaje recibido y así obtener Ks.

Protocolos de intercambio de claves

Intercambio de claves secretas mediante criptografía asimétrica

Aunque este protocolo facilita el intercambio seguro de claves, es vulnerable a ataques de intermediario, donde un atacante podría interponerse entre A y B, interceptando y posiblemente alterando las claves compartidas.

Para mitigar este riesgo y garantizar tanto la confidencialidad como la autenticidad de los mensajes, se puede emplear un esquema mejorado que incorpora pares de claves público-privadas para ambas entidades (A y B) y utiliza nonces (valores numéricos que se usan solo una vez) en el intercambio de mensajes:

- Identificación y Envío de Datos: A cifra y envía a B un nonce (N1) junto con su identificador (IDA), usando la clave pública de B.
- Confirmación y Envío de Nonce: B descifra estos datos y responde enviando a A un nuevo nonce (N2) junto con N1, cifrado con la clave pública de A, lo que confirma su identidad a A.
- Envío de la Clave de Sesión: A confirma su identidad a B enviando N2 y una clave de sesión (Ks) firmada, lo que garantiza que solo A podría haber enviado el mensaje y que solo B puede descifrarlo.

Este protocolo avanzado no solo asegura la confidencialidad y la autenticidad de la comunicación, sino que también protege contra ataques de intermediarios, haciendo que la criptografía asimétrica sea una herramienta valiosa en la protección de la información digital y el intercambio seguro de claves en entornos donde la interceptación es una preocupación viable.

Los protocolos de intercambio de claves secretas mediante criptografía asimétrica, especialmente aquellos que integran medidas de seguridad adicionales como el uso de nonces y la firma de claves de sesión, representan un avance significativo en la seguridad cibernética, permitiendo intercambios seguros y autenticados incluso en ausencia de un canal seguro preexistente.

Protocolos de intercambio de claves

Intercambio de claves secretas mediante sistemas híbridos

Los criptosistemas híbridos combinan la eficiencia de la criptografía simétrica con la seguridad de la criptografía asimétrica para el intercambio de claves, lo que resulta en un método de distribución de claves altamente eficaz y seguro.

Esta metodología aprovecha lo mejor de ambos mundos: la criptografía asimétrica se utiliza para distribuir de manera segura las claves maestras entre los usuarios, y la criptografía simétrica, que es más eficiente desde el punto de vista computacional, se emplea para el intercambio posterior de claves de sesión.

En este esquema, el Centro de Distribución de Claves (CDC) juega un papel crucial. Primero, el CDC asigna a cada usuario una clave maestra única, la cual se distribuye utilizando criptografía de clave pública. Esto asegura que solo el destinatario previsto pueda descifrar y obtener su clave maestra, gracias al uso de su clave privada única.

Luego, para la comunicación específica entre usuarios, el CDC genera claves de sesión y las cifra con las claves maestras de los usuarios implicados, recurriendo esta vez a la criptografía simétrica. De esta manera, se garantiza que solo los usuarios con las claves maestras correspondientes puedan descifrar y utilizar las claves de sesión para comunicarse de manera segura.

Este procedimiento permite una distribución eficaz y segura de claves de sesión a un amplio conjunto de usuarios, facilitando así la comunicación cifrada sin comprometer la seguridad. Al emplear criptosistemas híbridos, se equilibra la necesidad de seguridad en el intercambio de claves con la eficiencia requerida para su implementación práctica en redes de gran escala.

Protocolos de intercambio de claves

Intercambio de claves públicas

La distribución de claves públicas es un componente crítico de los sistemas de criptografía asimétrica, proporcionando la base para asegurar comunicaciones y transacciones en un entorno digital. Este proceso se puede gestionar mediante diversos métodos, cada uno con sus propias ventajas y limitaciones. A continuación, se exploran los cuatro protocolos principales para la distribución de claves públicas: anuncio público, directorio público, autoridad de clave pública y certificados de clave pública.

Anuncio Público

El anuncio público permite a cualquier entidad difundir su clave pública libremente. Aunque es un método simple y directo, sufre del riesgo de suplantación de identidad, ya que cualquier atacante puede presentarse como otra entidad emitiendo una clave pública diferente.

Directorio Público

Un directorio público mejora la seguridad agrupando todas las claves públicas en un repositorio gestionado por una autoridad. Este enfoque centraliza la validación de las claves públicas pero mantiene el riesgo de que un atacante pueda comprometer o manipular el directorio.

Autoridad de Clave Pública

Este método introduce una autoridad que gestiona activamente la distribución de claves públicas, manteniendo un directorio y asegurando la correspondencia entre las claves públicas y privadas. Aunque este proceso refuerza la confianza en la autenticidad de las claves públicas, puede generar cuellos de botella y sigue siendo susceptible a la alteración del directorio.

Protocolos de intercambio de claves

Intercambio de claves públicas

Certificados de Clave Pública

> Los certificados de clave pública representan la evolución natural de los métodos anteriores, vinculando firmemente las claves públicas a las identidades de las entidades mediante un documento certificado. Este método elimina la necesidad de una autoridad central activa para cada intercambio de claves, proporcionando una forma segura y autónoma de verificar la propiedad de una clave pública.

Cada uno de estos métodos tiene su propio conjunto de desafíos y consideraciones de seguridad. La elección entre ellos depende de las necesidades específicas de seguridad, escalabilidad y eficiencia de la red o sistema en cuestión. Los certificados de clave pública, en particular, ofrecen un equilibrio entre seguridad y autonomía, permitiendo a las entidades verificar las claves públicas de manera segura sin la intervención constante de una autoridad central.

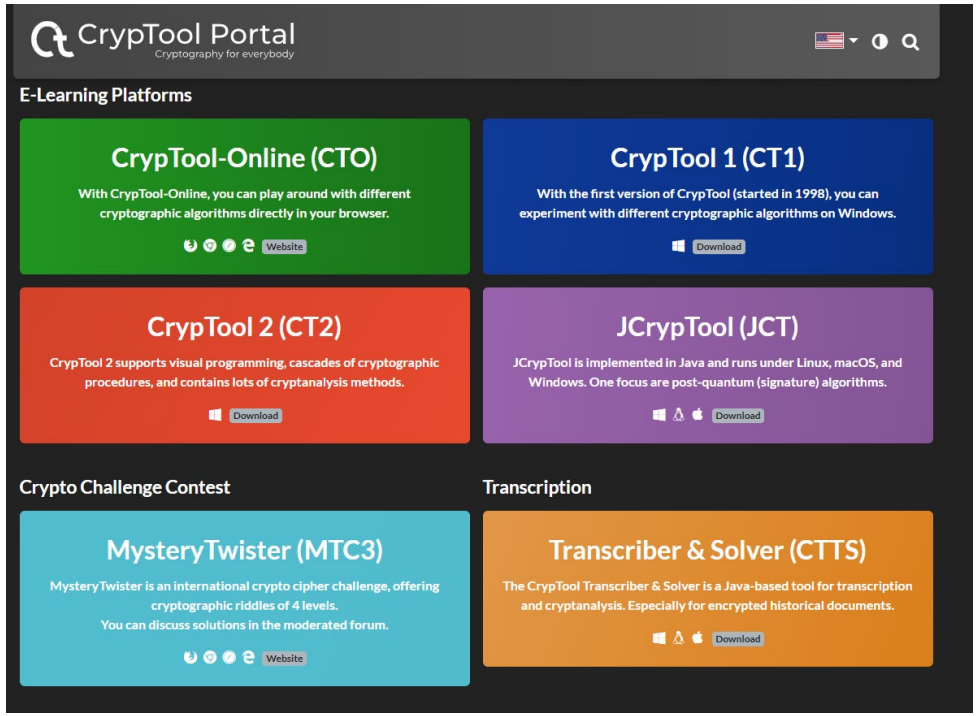
Uso de herramientas de cifrado tipo PGP, GPG o Cryptool

Cryptool

CrypTool es un software libre diseñado para ilustrar conceptos criptográficos y facilitar el aprendizaje en esta área. Se ha convertido en el programa de aprendizaje electrónico más utilizado en el mundo para enseñar y comprender la criptografía, abarcando tanto el cifrado de archivos y datos de manera gráfica, como el estudio de algoritmos criptográficos y el criptoanálisis de mensajes cifrados.

Originalmente, CrypTool fue desarrollado como una aplicación empresarial interna para la formación en seguridad de la información, evolucionando con el tiempo para convertirse en una herramienta educativa importante en el ámbito de la criptografía .

Enlace descarga.



Uso de herramientas de cifrado tipo PGP, GPG o CryptoLoop

GPG4Win

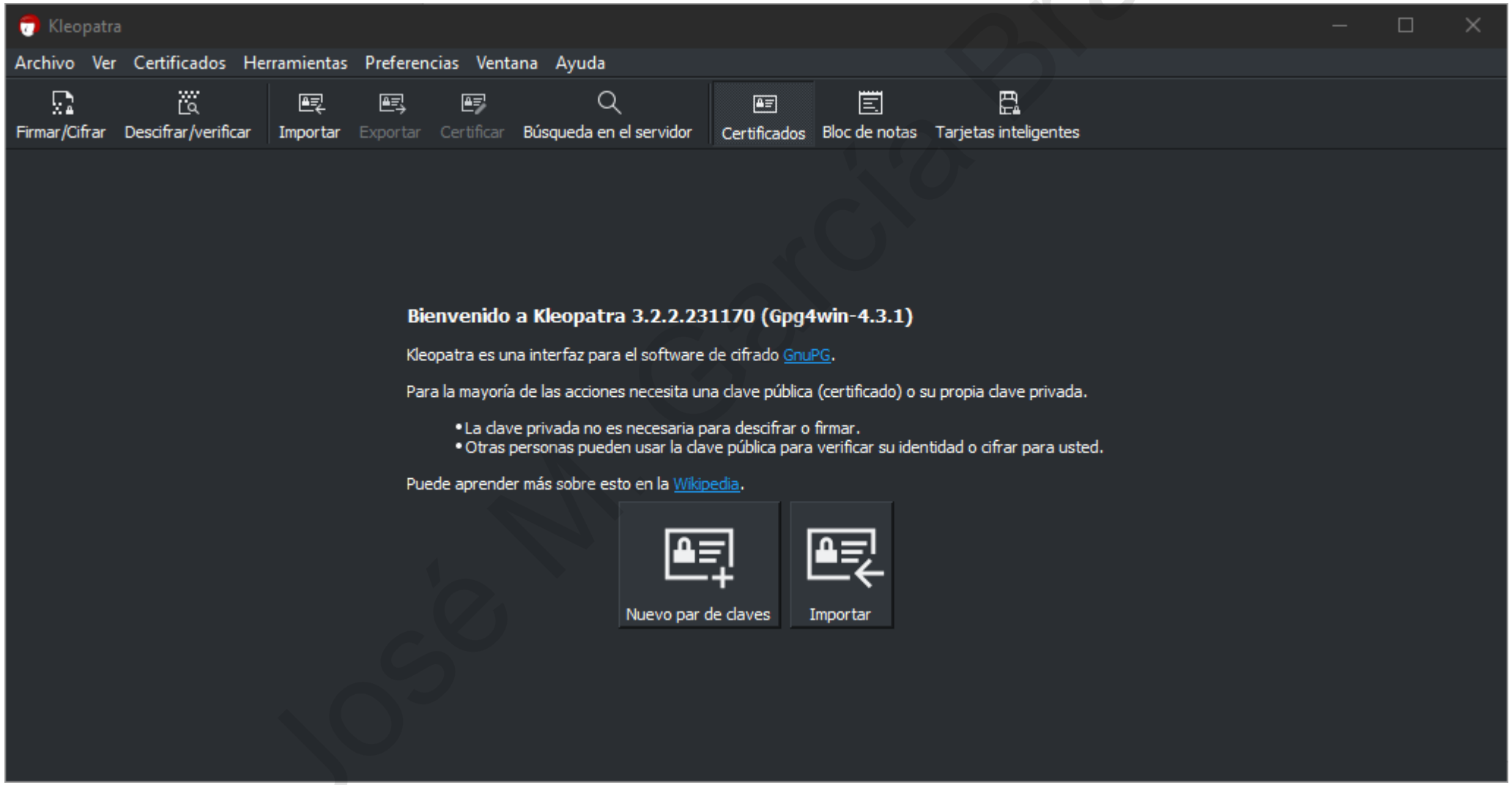
Gpg4win (GNU Privacy Guard for Windows) es un software de encriptación destinado a la firma y cifrado de archivos y correos electrónicos en sistemas operativos Windows. Este paquete incluye herramientas y aplicaciones que utilizan el marco de trabajo de GnuPG, proporcionando estándares criptográficos de alta seguridad recomendados por la GNU Privacy Guard. Es una distribución oficial de GnuPG para Windows, compatible con la mayoría de versiones de este sistema operativo y con Microsoft Outlook, facilitando así la encriptación de correo electrónico y archivos para los usuarios de Windows.

La principal función de Gpg4win es asegurar que la comunicación por correo electrónico y el intercambio de archivos sean privados y seguros, protegiéndolos contra accesos no autorizados. Permite a los usuarios generar un par de claves (una pública y una privada) para el cifrado y descifrado de información, asegurando que solo los destinatarios previstos puedan leer los mensajes. Además, la posibilidad de firmar digitalmente los correos electrónicos y archivos garantiza la autenticidad e integridad de los datos enviados, proporcionando una capa adicional de seguridad y confianza en las comunicaciones digitales .

Enlace descarga.

Uso de herramientas de cifrado tipo PGP, GPG o Cryptool

GPG4Win



Uso de herramientas de cifrado tipo PGP, GPG o Cryptool

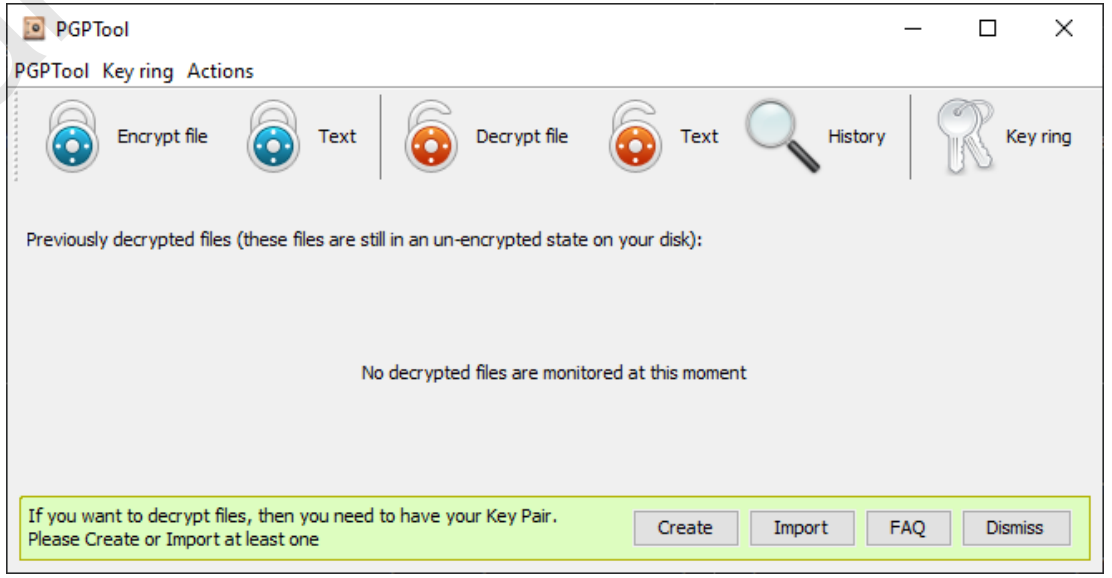
PGPTool

PGPTool es una herramienta diseñada para facilitar el cifrado y descifrado de información mediante el uso de la tecnología PGP (Pretty Good Privacy).

PGP es un programa desarrollado por Phil Zimmermann que tiene como objetivo principal proteger la información distribuida a través de la red, asegurando la privacidad y autenticación de los datos enviados. Utiliza una combinación de cifrado de clave pública y cifrado convencional para ofrecer servicios de seguridad robustos para la comunicación electrónica.

Las utilidades de PGP incluyen, entre otras, la capacidad de adjuntar firmas digitales a documentos o archivos, proporcionando así veracidad y permitiendo al receptor verificar la autenticidad del remitente.

PGPTool, en este contexto, facilita la generación de claves PGP, así como el cifrado y descifrado de archivos, haciendo el proceso más accesible y manejable para los usuarios que buscan mejorar la seguridad de sus comunicaciones en línea .



[Enlace descarga.]

Resumen

La criptología emerge como una ciencia esencialmente vinculada a la salvaguardia de datos.

Los esquemas criptográficos tradicionales se categorizan en monocriptográficos, ejemplificados por el cifrado de César, y polialfabéticos, ilustrados por el cifrado de Vigenère. Un denominador común entre estos era que la llave utilizada para cifrar era idéntica a la empleada para descifrar, razón por la cual se les denominaba sistemas de llave secreta o simétrica.

En el año de 1976, nació la criptografía de llave pública o asimétrica, introduciendo el uso de un dúo de llaves: una pública y otra privada.

Según los requerimientos, la criptografía faculta la garantía de diversas propiedades de seguridad. La selección se fundamenta en los participantes de la comunicación para asegurar la autenticidad, la prevención del acceso indebido para garantizar la confidencialidad, la obstrucción de alteraciones en el mensaje para preservar la integridad, la eliminación de envíos no consentidos para el no repudio, el rastreo de acciones ejecutadas para la imputabilidad y la certificación de la temporalidad de la comunicación mediante el sellado de tiempo.

No obstante, la realización de estas propiedades de seguridad se apoya en la implementación de un abanico de mecanismos, como el cifrado, la firma digital o la generación de sumarios.

Tanto la criptografía simétrica como la asimétrica proveen las herramientas esenciales para la aplicación de estos mecanismos, siendo vital la elección adecuada en cada instancia.

Resumen

Por un lado, la criptografía simétrica se distingue por su eficacia en velocidad, mientras que la asimétrica tiene la ventaja de obviar la necesidad de un canal seguro para el intercambio de llaves de cifrado.

Adicionalmente, dado el requerimiento de intercambio de llaves en ambos estilos criptográficos, es imprescindible considerar el protocolo a emplear, evaluando si el intercambio se efectúa entre emisor y receptor directamente o si se requiere de una entidad mediadora.

Un aspecto crítico de los sistemas de llave pública es la verificación de la identidad de su titular, para lo cual surgen los certificados de llave pública.