Escuela de Educación Técnica Nº 3139 Gral. Martin Miguel de Güemes

TECNICATURA EN INFORMATICA PROFESIONAL Y PERSONAL

MATERIA: CONEXIÓN A REDES EXTENDIDAS

TEMA: CRIPTOGRAFIA

Prof. SEBASTIAN JAVIER GARCIA

Criptografía

Introducción

La criptografía es un método de protección de la información y las comunicaciones mediante el uso de **códigos**, de modo que solo aquellos a quienes está destinada la información puedan leerla y procesarla.

En informática, la criptografía se refiere a técnicas seguras de información y comunicación derivadas de conceptos matemáticos y un conjunto de cálculos basados en reglas llamados **algoritmos**, para transformar mensajes de manera que sean difíciles de **descifrar**. Estos algoritmos deterministas se utilizan para la generación de **claves criptográficas**, la **firma digital**, la **verificación** para proteger la privacidad de los datos, la navegación web en Internet y las comunicaciones confidenciales, como transacciones con tarjetas de crédito y correo electrónico.

TLS es un **protocolo criptográfico** que proporciona seguridad de extremo a extremo de los datos enviados entre aplicaciones a través de Internet. En su mayoría, es familiar para los usuarios a través de su uso en la navegación web segura y, en particular, **el ícono de candado** que aparece en los navegadores web cuando se establece una sesión segura. Sin embargo, también puede y debe utilizarse para otras aplicaciones como correo electrónico, transferencias de archivos, videoconferencias/audioconferencias, mensajería instantánea y voz sobre IP, así como servicios de Internet como DNS y NTP.

En esta clase estudiaremos los fundamentos de la criptografía, las principales técnicas y el funcionamiento del protocolo TLS.

Objetivos

Los estudiantes que completen esta clase deberán poder:

- Comprender los conceptos de confidencialidad, integridad, autenticación y no repudio.
- Describir las claves simétricas y asimétricas.
- Identificar las ventajas, desventajas y usos de una clave simétrica y una clave asimétrica.
- Comprender el mecanismo Diffie-Hellman y Diffie-Hellman de curva elíptica para el intercambio seguro de claves.
- Comprender el funcionamiento del protocolo TLS.
- Analizar certificados digitales.
- Implementar certificados de seguridad digitales.

Actividades

- Leer atentamente y completar el trabajo practico.

Conceptos generales

La criptografía está estrechamente relacionada con las disciplinas de la **criptología** (o el estudio de los sistemas, claves y lenguajes ocultos o secretos) y el **criptoanálisis** (rama de criptografía que estudia cómo romper códigos y criptosistemas). Incluye técnicas como micropuntos, fusionar palabras con imágenes y otras formas de ocultar información almacenada o en tránsito. Sin embargo, en el mundo centrado en la computadora de hoy, la criptografía se asocia con mayor frecuencia con la **codificación de texto sin formato** (texto ordinario, a veces denominado **texto sin cifrar**) en **texto cifrado** (un proceso llamado **cifrado**) y luego de vuelta (conocido como **descifrado**). Las personas que practican este campo se conocen como criptógrafos.

La criptografía moderna se ocupa de los siguientes cuatro objetivos:

1- **Confidencialidad:** La información no puede ser entendida por nadie para quien no estaba destinada.
2- **Integridad:** La información no se puede alterar durante el almacenamiento o el tránsito entre el remitente y el receptor previsto sin que se detecte la alteración.
3- **Autenticación:** El remitente y el receptor pueden confirmar la identidad del otro y el origen/destino de la información.
4- **No repudio:** El creador/remitente de la información no puede negar en una etapa posterior sus intenciones en la creación o transmisión de la información.

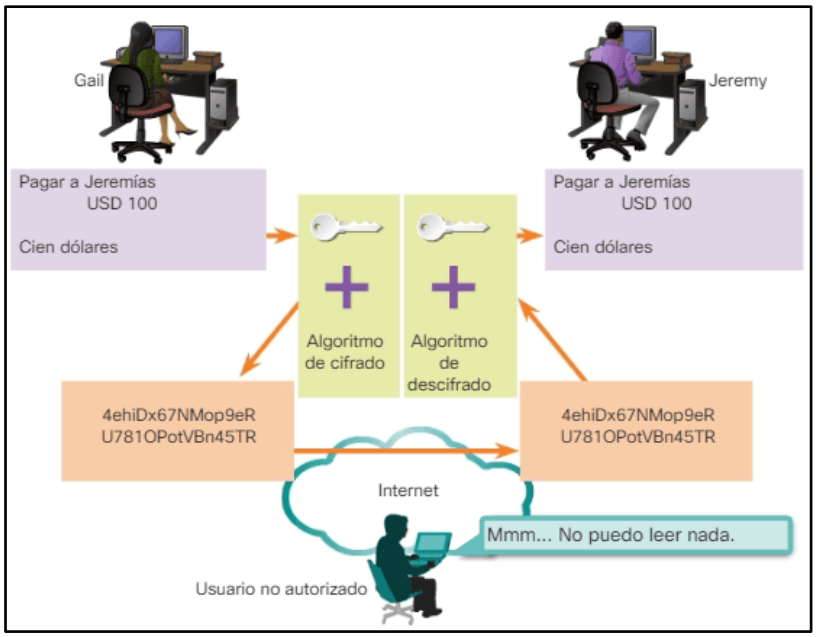
.

<u>Confidencialidad con cifrado</u>

El tráfico en redes inseguras se mantiene confidencial con el cifrado. Los datos de texto no cifrado que se transportan a través de Internet pueden interceptarse y leerse. El **cifrado digital** de los datos hace que estos sean ilegibles hasta que el receptor autorizado los descifre.

Para que la comunicación cifrada funcione, el emisor y el receptor deben conocer las reglas que se utilizan para transformar el mensaje original a su forma cifrada. Las reglas se basan en **algoritmos y claves asociadas**.

En el contexto del cifrado, ***un algoritmo es una secuencia matemática de pasos que combina un mensaje***, texto, dígitos o las tres cosas ***con una cadena de dígitos denominada "clave"***. El resultado es una ***cadena de cifrado ilegible***. El algoritmo de cifrado también ***especifica cómo se descifra un mensaje*** cifrado. El descifrado es extremadamente difícil o imposible sin la **clave correcta**.



En la ilustración, Gail desea enviar una transferencia electrónica de fondos (EFT) a Jeremías a través de Internet:

- En el extremo local, el documento se combina con una clave y se procesa con un algoritmo de cifrado.
- El resultado es un texto cifrado.
- El texto cifrado se envía a través de Internet.
- En el extremo remoto, el mensaje se vuelve a combinar con una clave y se devuelve a través del algoritmo de cifrado.
- El resultado es el documento financiero original.

La confidencialidad se logra con el cifrado del tráfico mientras viaja por una red insegura. El grado de seguridad depende de la **longitud de la clave del algoritmo** de cifrado y la **sofisticación del algoritmo**.

> **Dato**: Una computadora relativamente sofisticada puede tardar aproximadamente un año para descifrar una clave de 64 bits.

1- Algoritmos de cifrado

El grado de seguridad depende de la longitud de la clave del algoritmo de cifrado. Cuanto más larga es la clave, se torna más difícil descifrarla. Sin embargo, ***una clave más larga requiere más recursos*** de procesador para cifrar y descifrar datos.

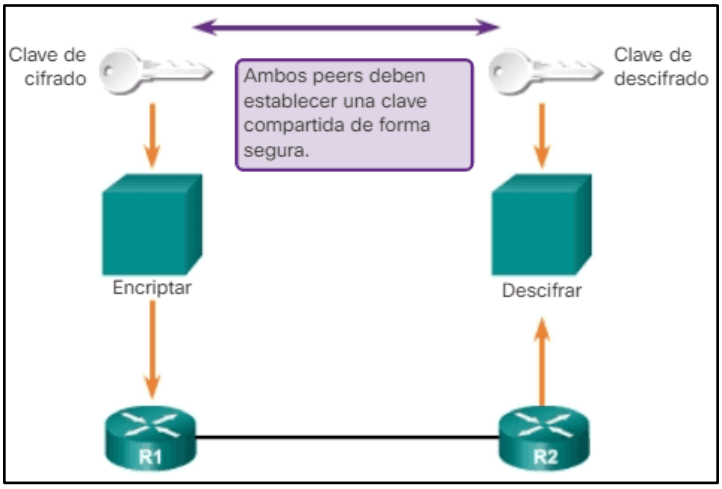
DES y **3DES** ya no se consideran seguros; por lo tanto, se recomienda utilizar **AES**. La mejor seguridad para el cifrado entre dispositivos la proporciona la opción de **256 bits** de AES.

Además, dado que se descifraron claves de **Rivest, Shamir y Adleman** (**RSA**) de **512 bits** y **768 bits**, se recomienda utilizar claves de **2048 bits** con en caso de utilizar cifrado con **RSA**.

Los generadores **pseudoaleatorios** desempeñan un papel principal en la construcción de los esquemas de encriptado. En concreto, **permiten generar claves de encriptado privadas**. Los **algoritmos deterministas** permiten extender una secuencia de **números aleatorios** “semilla”, para obtener una secuencia de bits más larga y **que parece aleatoria, aunque no lo es**.

2- Intercambio de claves de Diffie-Hellman

Diffie-Hellman (**DH**) no es un mecanismo de cifrado y no se suele utilizar para cifrar datos. En cambio, ***es un método para intercambiar con seguridad las claves que cifran datos***. Los algoritmos (DH) permiten que dos partes ***establezcan la clave secreta compartida*** que usan el **cifrado** y los **algoritmos de hash**.



Los algoritmos de cifrado, como **DES**, **3DES** y **AES**, así como los algoritmos de hash **MD5** y **SHA-1**, requieren una clave secreta compartida simétrica para realizar el cifrado y el descifrado.

¿Cómo obtienen la clave secreta compartida los dispositivos de cifrado y descifrado? El método más sencillo de intercambio de claves es un método de intercambio de clave pública entre dispositivos de cifrado y descifrado.

El algoritmo DH ***especifica un método de intercambio de clave pública que proporciona una manera para que dos peers establezcan una clave secreta compartida*** que solo ellos conozcan, aunque se comuniquen a través de un **canal inseguro**. Como todos los algoritmos criptográficos, el intercambio de claves DH se basa en una secuencia matemática de pasos.

Integridad con los algoritmos de hash

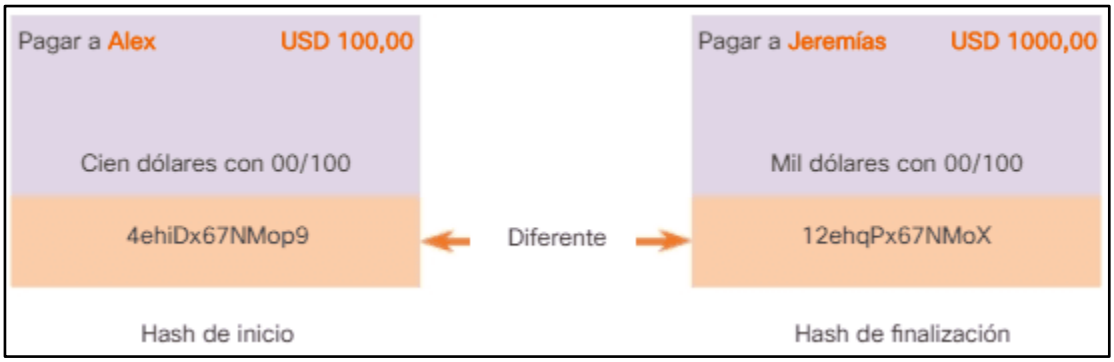
Los algoritmos de hash manejan la integridad y la autenticación del tráfico por redes inseguras. Los hashes proporcionan integridad y autenticación de datos ***al asegurar que las personas no autorizadas no alteren los mensajes transmitidos***.

Un hash, también denominado "**síntesis del mensaje** ", es un número que se genera a partir de una cadena de texto. El hash es más corto que el texto en sí. Se genera mediante el uso de una fórmula, de tal manera que es muy poco probable que otro texto produzca el mismo valor de hash.

- El emisor original genera un hash del mensaje y lo envía con el mensaje propiamente dicho.
- El destinatario analiza el mensaje y el hash, produce otro hash a partir del mensaje recibido y compara ambos hashes.
- Si son iguales, el destinatario puede estar lo suficientemente seguro de la integridad del mensaje original.

1- Ejemplo del algoritmo de hash

En la ilustración, Gail le envió a Alex un EFT de USD 100. Jeremías interceptó y alteró este EFT para mostrarse como el destinatario y que la cantidad sea USD 1000. En este caso, si se utilizara un algoritmo de integridad de datos, los hashes no coincidirían, y la transacción no sería válida.



Como se muestra, existe la posibilidad de que se intercepten y se modifiquen estos datos. Para protegerlos contra esta amenaza, ***los hosts pueden agregar un hash al mensaje***.

2- HMAC

El código de autenticación de mensajes basado en hash (HMAC) es un mecanismo para la autenticación de mensajes mediante funciones de hash.

Un HMAC con clave es un algoritmo de integridad de datos que garantiza la integridad de un mensaje.

Un HMAC tiene dos parámetros: una entrada de mensaje y una clave secreta que solo conocen el autor del mensaje y los destinatarios previstos.

- El emisor del mensaje utiliza una función HMAC para producir un valor (el código de autenticación de mensajes) que se forma mediante la compresión de la clave secreta y la entrada de mensaje.
- El código de autenticación de mensajes se envía junto con el mensaje.
- El receptor calcula el código de autenticación de mensajes en el mensaje recibido con la misma clave y la misma función HMAC que utilizó el emisor.
- A continuación, el receptor compara el resultado que se calculó con el código de autenticación de mensajes que se recibió.

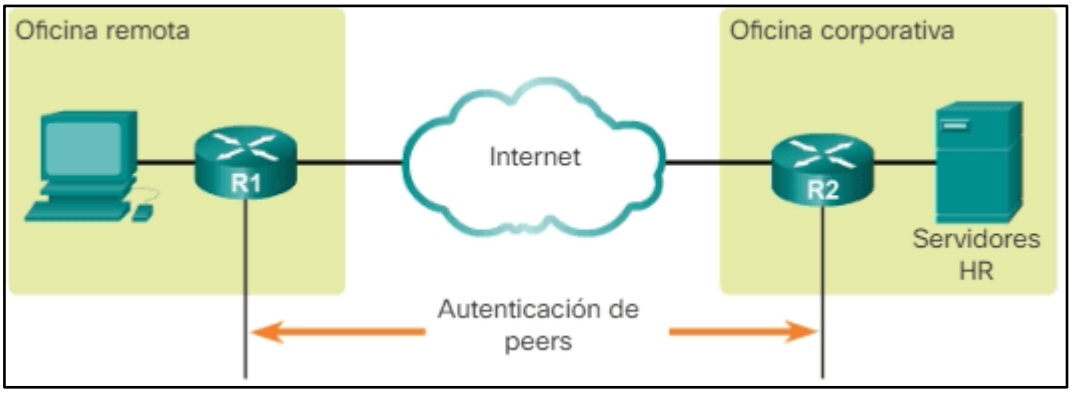
Hay dos algoritmos HMAC comunes:

- **MD5**: utiliza una clave secreta compartida de **128 bits**. El mensaje de longitud variable y la clave secreta compartida se combinan y se procesan con el algoritmo de hash HMAC-MD5. El resultado es un hash. ***El hash se adjunta al mensaje original y se envía al extremo remoto***.

- **SHA**: El mensaje de longitud variable y la clave secreta compartida se combinan y se procesan con el algoritmo de hash HMAC-SHA1/256/512. El resultado es un hash. El hash se adjunta al mensaje original y se envía al extremo remoto.

Autenticación

Al realizar comunicaciones a larga distancia, es necesario saber quién está del otro lado del teléfono o del correo electrónico. Lo mismo sucede con las redes extendidas.



El dispositivo en el otro extremo se debe autenticar para que la ruta de comunicación se considere segura, como se indica en la ilustración. Existen dos métodos de autenticación de **peers**:

- **PSK:** es una clave secreta que se comparte entre las dos partes que utilizan un canal seguro antes de que se necesite utilizarla. Las **claves previamente compartidas** (PSK) utilizan algoritmos criptográficos de clave simétrica. Se introduce una PSK en cada peer de forma manual y se la utiliza para autenticar el peer. En cada extremo, la PSK se combina con otra información para formar la clave de autenticación.

- **Firmas RSA:** se intercambian **certificados digitales** para autenticar los peers. El dispositivo local deriva un hash y lo cifra con su clave privada. El hash cifrado, o la firma digital, se vincula al mensaje y se reenvía hacia el extremo remoto. En el extremo remoto, se descifra el hash cifrado con la clave pública del extremo local. Si el hash descifrado coincide con el hash recalculado, la firma es genuina.

No Repudio

El no repudio en seguridad de la información es la **capacidad de demostrar o probar la participación de las partes** (origen y destino, emisor y receptor, remitente y destinatario), mediante su identificación, en una comunicación o en la realización de una determinada acción.

Para garantizar el no repudio en seguridad informática se necesitan establecer los siguientes mecanismos:

- **Identificación:** mecanismo o proceso que provee la capacidad de identificar a un usuario de un sistema.

- **Autenticación:** permite verificar la identidad o asegurar que un usuario es quien dice ser.

1- Tipos de no repudio

- **En origen:** consiste en garantizar que una persona envió un determinado mensaje. El remitente no puede negar que lo mandó, ya que el destinatario dispone de pruebas del envío.

- **En destino:** avala que alguien recibió un determinado mensaje. En este caso, el destinatario no podrá rebatir que no lo recibió porque el remitente cuenta con pruebas de la recepción.

2- La firma electrónica

En ciberseguridad uno de los mecanismos más importante de no repudio es la firma electrónica. ***Esta es el conjunto de datos asociados a un documento electrónico que identifican al firmante y dotan de validez legal al documento que se firma***.

Para garantizar el no repudio, esta firma debe estar vinculada exclusivamente a la persona que firma e identificarla unívocamente. Además, la rúbrica debe realizarse a través de un medio electrónico o digital que el firmante tiene bajo su único control y vincularse a los datos que se firman de tal manera que no se puedan modificar sin ser detectados los cambios.

Las firmas deben cumplir los siguientes requisitos técnicos para que garanticen el no repudio:

- La clave de firma está asignada a una persona u organización identificable.
- La clave privada está únicamente bajo el control de la persona u organización que firma.

3- Tipos de firma electrónica

Los distintos tipos de firma electrónica son:

- **Simple:** Se trata de aceptar o rechazar el contenido de un documento, son típicas en las condiciones generales de uso, políticas de seguridad o privacidad…

- **Avanzada OTP:** La persona firmante recibe un código a través de un canal de comunicaciones distinto al de la operativa de firma (p. ej. móvil o correo electrónico) al momento de firmar. Es típica su utilización en compras electrónicas u operaciones de banca electrónica.

- **Biométrica:** La persona firma físicamente en una tablet o dispositivo electrónico. Se utiliza, por ejemplo, en el servicio de correo o transporte de paquetería, en las sucursales bancarias…

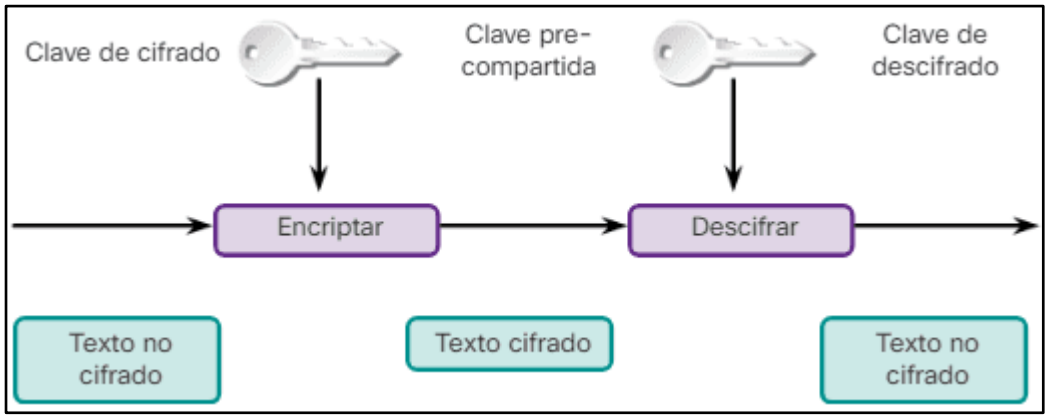
- **Certificado digital:** Se firma mediante un certificado que se apoya en un par de claves, una privada y una pública. El certificado digital es un documento que nos identifica en internet para poder realizar trámites online y que permite la firma electrónica.

CLAVES SIMETRICAS Y ASIMETRICAS

Cifrado simétrico

Los algoritmos de cifrado, como AES, requieren una **clave secreta compartida** para el cifrado y el descifrado. Cada uno de los dos dispositivos de red debe conocer la clave para decodificar la información. Con el **cifrado de clave simétrica**, también denominado “cifrado de la clave secreta”, cada dispositivo cifra la información antes de enviarla a través de la red al otro dispositivo.

El cifrado de clave simétrica ***requiere saber qué dispositivos se comunican*** entre sí para poder configurar la misma clave en cada dispositivo.



- Por ejemplo, un emisor crea un mensaje cifrado en el que cada letra se reemplaza por otra letra que está dos lugares más adelante en el abecedario: A se convierte en C, B se convierte en D y así sucesivamente. En este caso, la palabra SECRET se convierte en UGETGV.
- El emisor ya le dijo al destinatario que la clave secreta se corre dos letras.
- Cuando el destinatario recibe el mensaje UGETGV, la computadora del destinatario decodifica el mensaje corriendo dos letras hacia atrás y calcula la palabra SECRET.
- Cualquier persona que ve el mensaje solo ve el mensaje cifrado, que parece no tener sentido, a menos que la persona conozca la clave secreta.

A continuación, se muestra una sinopsis para los algoritmos simétricos:

- Utilizan criptografía de clave simétrica.
- El cifrado y el descifrado **utilizan la misma clave**.
- Por lo general, se utilizan para **cifrar el contenido del mensaje**.
- El cifrado de clave privada necesita una clave por cada par de usuarios que necesite comunicarse. La cantidad de claves necesarias aumentan a medida que se incrementa el número de participantes que requieren comunicación privada.
- Las claves deben ser compartidas por cada par de emisor y receptor que haya, por lo que las claves se deberán distribuir a los usuarios que hayan participado. Cuando se empiezan a transmitir las claves secretas, se incrementan las posibilidades de robo, a través de la interceptación en el proceso de transmisión o comunicación de la clave.
- Los mensajes cifrados no se pueden enviar de modo espontáneo, sino que los participantes necesitan comunicarse acordándolo previamente.
- Ambos usuarios deben establecer acuerdos para comunicarse compartiendo las claves correspondientes.
- El cifrado se destaca por su sencilla implementación y utilización.
- El cifrado de clave simétrico también es denominado “de clave privada”.

- Algoritmos: **DES (data encryption standard)**, **3DES (triple data encryption standard)**, **AES (advanced encryption standard)** y **RC4 (rivest cipher4)**.

Adicionalmente, existen **2 modelos** de operación de cifrado. ***El cifrado en bloques y el cifrado de flujo***.

- **Cifrado en bloques:** la información que se va a cifrar está dividida en **bloques de longitud fija (64 o 128 bits**), y, para aplicar el algoritmo de cifrado a cada uno de los bloques, se utiliza la clave. Además, se emplean combinaciones basadas en sustituciones y cambios de posición que se rigen por la clave de cifrado. Ejemplos de este cifrado pueden ser **DES**, **3DES** y **AES**.

- **Cifrado de flujo:** son algoritmos capaces de realizar **cifrados incrementales, bit a bit**. Los algoritmos de cifrado de bloque cifran bloques enteros de varios bytes a la vez. Este tipo descifrado de flujo es muy utilizado en telecomunicaciones. Ejemplo de este tipo de cifrado es el **RC4**, uno de los más usados para proteger el tráfico de Internet.
-

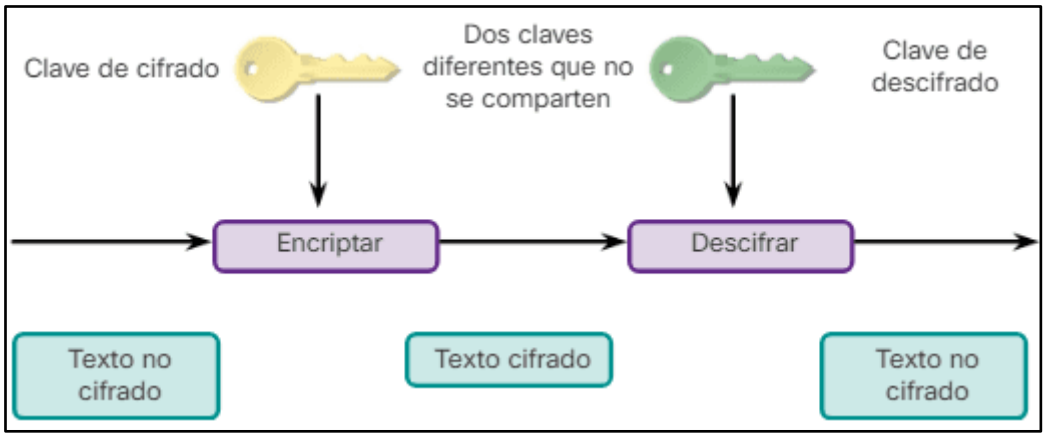
Normalmente, los algoritmos de cifrado de bloque necesitan más recursos para funcionar debido a que trabajan con bloques de datos mayores que los de flujo.

¿Cómo es que los dispositivos de cifrado y descifrado tienen una clave secreta compartida? Para ***enviar*** las claves secretas compartidas a los administradores de los dispositivos, se podría utilizar el correo electrónico, el servicio de mensajería común o de entrega urgente. **Otro método más seguro es el cifrado asimétrico**.

Cifrado asimétrico

Existe otro sistema de cifrado, llamado **"criptografía de clave pública"** o **"sistemas de cifrado de clave pública"**, también conocido como **"cifrado asimétrico"**.

El cifrado asimétrico utiliza claves diferentes para el cifrado y el descifrado. Aunque conozca una de las claves, un pirata informático no puede deducir la segunda clave y decodificar la información. Una clave cifra el mensaje, mientras que una segunda clave descifra el mensaje. **No es posible cifrar y descifrar con la misma clave**.



Whitfield Diffie y **Martin Hellman** fueron los primeros en introducir el concepto de **"criptografía asimétrica"** a mediados de la década de 1970. ***El algoritmo criptográfico de D-H se desarrolló específicamente para manejar los problemas de distribución segura de claves de***

cifrado simétrico. El algoritmo de D-H se basa en las matemáticas de logaritmos discretos y, aunque no es tan popular como la criptografía asimétrica de **RSA**, es muy utilizado.

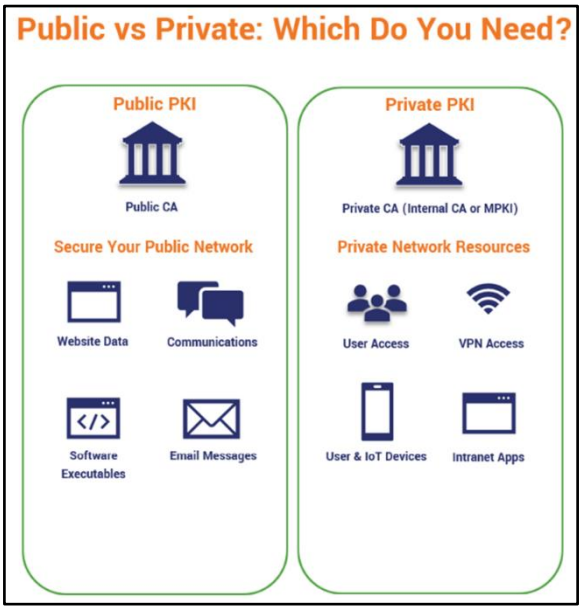
El algoritmo de RSA fue el algoritmo asimétrico más exitoso y es el más estudiado. Superó muchos ataques a través de su larga vida, y la patente fundamental del algoritmo expiró en septiembre del año 2000. El **algoritmo de RSA** fue desarrollado en el **MIT** por **Rivest**, **Shamir** y **Adleman** (de ahí el nombre).

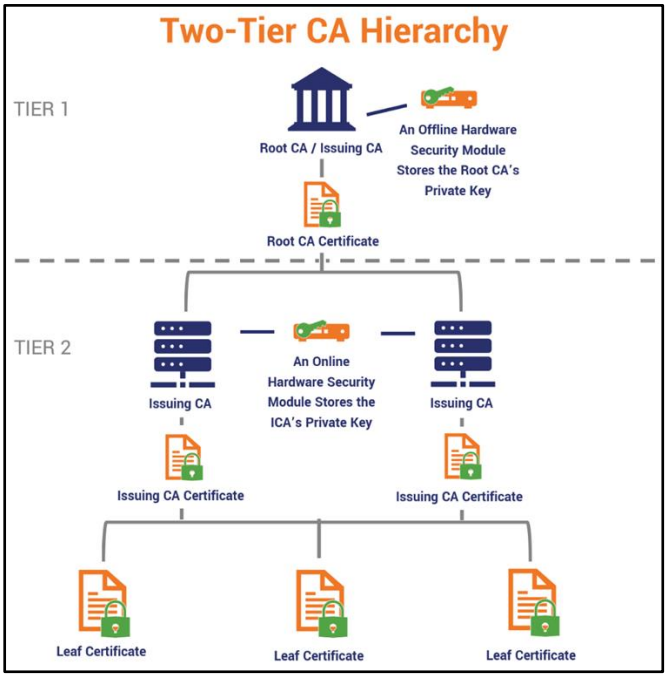
1- PKI - Infraestructura de Clave Pública

Para poder continuar desarrollando los conceptos de "clave privada" y "clave pública", es importante tener claro el concepto de **"public key infrastructure" (PKI)** o **"infraestructura de clave pública"**.

La PKI es un sistema de claves públicas encargado de la gestión de certificados digitales y aplicaciones de firma digital. El objeto de la PKI es garantizar la integridad de un sistema informático y confirmar la identidad de los usuarios.

La PKI está basada en un sistema de confianza en el que ambas partes de la comunicación (emisor y receptor) confían en la entidad emisora para verificar y confirmar la identidad de ambas partes.





Dentro de los componentes de una PKI, tenemos a la **Autoridad Certificante** o **Certificate Authority (CA)**, que es la entidad que asegura la identidad de todos los usuarios que utilizan los certificados digitales. ***Esta CA consta de una clave pública y una privada, y firma digitalmente los certificados que emite con su clave***.

Las principales aplicaciones para la criptografía de clave pública son las firmas digitales y el cifrado. A diferencia del cifrado simétrico, en este sistema se utilizan dos claves. La clave pública puede ser enviada a cualquier persona, pero la clave privada, como su nombre lo indica, debe ser guardada y se debe restringir el acceso a ella, de modo que solamente sea conocida por su propietario. **Es decir, se utiliza una clave para cifrar, la pública, y otra para descifrar, la privada**.

- El cifrado de clave pública es una variante del cifrado asimétrico que ***utiliza una combinación de una clave privada y una pública***.
- El destinatario brinda una clave pública a cualquier emisor con el que desee comunicarse.

- El emisor utiliza una clave privada que se combina con la clave pública del destinatario para cifrar el mensaje. Además, el emisor debe compartir su clave pública con el destinatario.
- Para descifrar un mensaje, el destinatario utiliza la clave pública del emisor con su propia clave privada.

2- Certificados con DV, OV y EV

Tres niveles de autenticación, confianza y protección de la marca: con **Validación de Dominio (DV)**, con **Validación de Empresa (OV)** y con **Validación Extendida (EV)**.

Los certificados **TLS/SSL** cumplen **dos funciones**. En primer lugar, proporcionan una ***conexión segura a un sitio web cifrando los datos que se transmiten entre los usuarios y el dominio***. En segundo lugar, los certificados ***verifican la propiedad y la identidad de la empresa o persona propietaria de la URL***. Al igual que un certificado físico, un certificado digital certifica esencialmente el derecho a representar a una empresa u organización en Internet.

a) Validación de dominio (DV)

Los certificados con **validación de dominio (DV)** son los certificados SSL **con menor validación de identidad y se pueden obtener con facilidad y rapidez**, incluso utilizando para ello un bot malicioso. Son certificados de bajo costo; ***la validación solo consiste en verificar que una empresa o persona tenga el control del dominio web para el que desea obtener el certificado***.

Para obtener un certificado con DV, el propietario del sitio web recibe un correo electrónico de confirmación de la CA emisora a la dirección de correo electrónico que figura en el registro WHOIS del dominio. ***Los certificados con DV se suelen utilizar para sitios web que no realizan transacciones comerciales ni con tarjetas de crédito***.

Tipos de sitios web que utilizan certificados con DV:

- Blogs.
- Sitios web personales.
- Cualquier sitio web que no realice transacciones ni recopile información personal.

b) Validación de empresa (OV)

Los certificados con **validación de empresa (OV)** se autentican con **nueve comprobaciones de validación y se consideran un certificado empresarial de nivel medio**. Con los certificados con OV, las CA autentican la propiedad del dominio de forma similar a los certificados con DV.

La diferencia entre la validación de empresa (VO) y la validación de dominio (VD) radica en los pasos que siguen las CA ***para autenticar que la organización empresarial (es decir, Inc., Corp., LLC, Ltd., Pty. Ltd., etc.) afiliada al certificado sea válida y que todo esté en regla***.

Se utilizan sobre todo en estos sitios y páginas web:

- Pantallas de inicio de sesión.
- Sitios web comerciales.

c) Validación extendida (EV)

Los certificados con **validación extendida (EV)** se autentican con **18 comprobaciones de validación** que requieren el máximo nivel de verificación por parte de las CA. ***Los certificados con EV protegen la identidad de la marca debido a la rigurosidad del proceso necesario para obtenerlos***.

Además de todos los pasos de autenticación que siguen las CA para los certificados con DV y OV, los certificados con EV ***comprueban la existencia operativa de la empresa y la dirección postal, además de realizar una llamada telefónica para verificar la situación laboral del solicitante***.

Se utilizan sobre todo en estos sitios y páginas web:

- Bancos y empresas de servicios financieros internacionales.
- Comercio electrónico.
- Grandes empresas.

Desafortunadamente, la mayoría de los sitios tienen un candado y un certificado DV. Por eso es importante mirar más allá del candado en la barra de URL. Si ve el nombre de la organización, ahora puede tomar una mejor decisión sobre en quién confía.

A continuación, se muestra una sinopsis para los algoritmos asimétricos:

- Utilizan criptografía de clave pública.
- El cifrado y el descifrado utilizan **claves diferentes**.
- Por lo general, se usan en la **certificación digital** y la **administración de claves**.
- El emisor quiere enviarle un documento al receptor, así que procede a conseguir su clave pública.
- Una vez que obtiene la clave pública y el documento, procede a aplicar el algoritmo simétrico. Una vez que el documento haya sido cifrado, se puede enviar al receptor.
- El mensaje llega al receptor, quien se encarga de desencriptar el documento a través de la aplicación del algoritmo asimétrico con el uso de su clave privada.
- Si el receptor quisiera enviar una respuesta cifrada, deberá conocer la clave pública del emisor y seguir los mismos pasos.
- Se destaca que cualquiera puede cifrar un mensaje con la clave pública, pero solo el propietario lo puede descifrar con su clave privada.
- Algoritmos: **RSA** y **curvas elípticas**.

Debido a este procedimiento, ya no son necesarios los canales seguros para enviar la clave. La clave que se distribuye es la pública, lo que simplifica y aumenta la seguridad del proceso y, además, hace la distribución de las claves más sencilla y segura. Además, a su vez, deja la clave privada para uso exclusivo de su propietario.

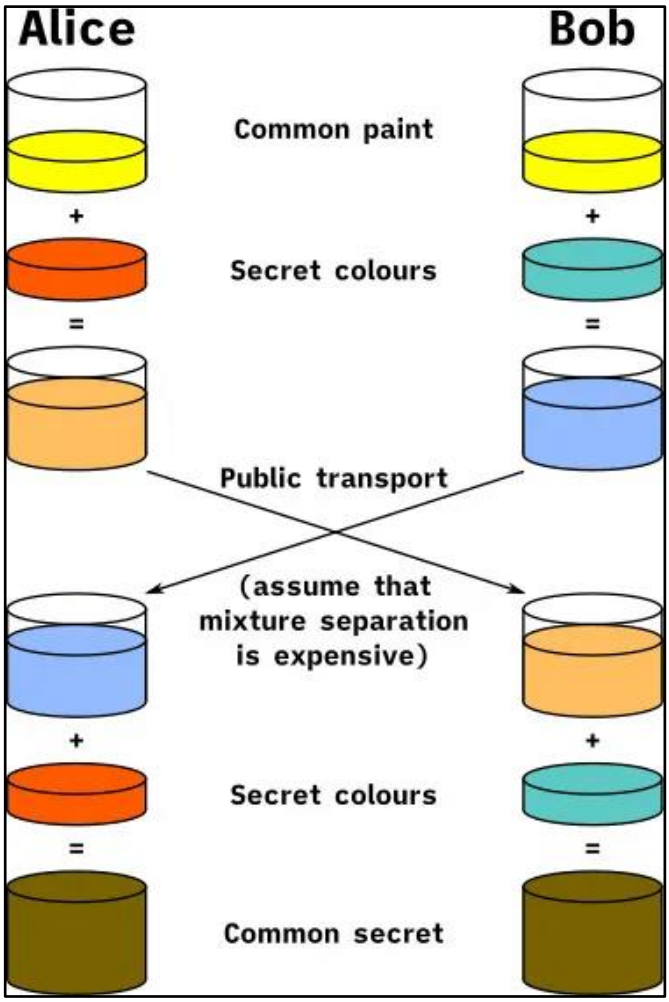
<u>Características de clave simétrica y asimétrica</u>

Atributo	Clave simétrica	Clave asimétrica
Uso principal	Cifrado de grandes volúmenes de datos	intercambio de claves, firma digital
Estándar actual	DES, Triple DES, AES	RSA, Curvas elipticas
Velocidad	Rápida	Lenta
Claves	Compartidas entre emisor y receptor	Privada: Solo conocida por una persona. Pública: Conocida por todos
Intercambio de claves	Difícil de intercambiar por un canal seguro	La clave pública se comparte por cualquier canal. La privada nunca se comparte
Longitud de claves	56 bits (vulnerable) 256 bits (seguro)	1024 - 2048 (RSA); 172 (curvas elípticas)
Servicios de seguridad	Confidencialidad, integridad y autenticación	Confidencialidad, integridad, autenticación y no repudio

Diffie-Hellman

Diffie-Hellman permite que las **dos partes intercambien su secreto sin necesidad de un canal seguro**. De hecho, esto se puede usar en cualquier canal no seguro. ***El secreto generado por el intercambio se puede usar para encriptar comunicaciones posteriores utilizando encriptación simétrica con el secreto generado***.

Una analogía ilustra el concepto de intercambio de clave pública mediante el uso de colores en lugar de números muy grandes que en realidad se utilizan durante el proceso.



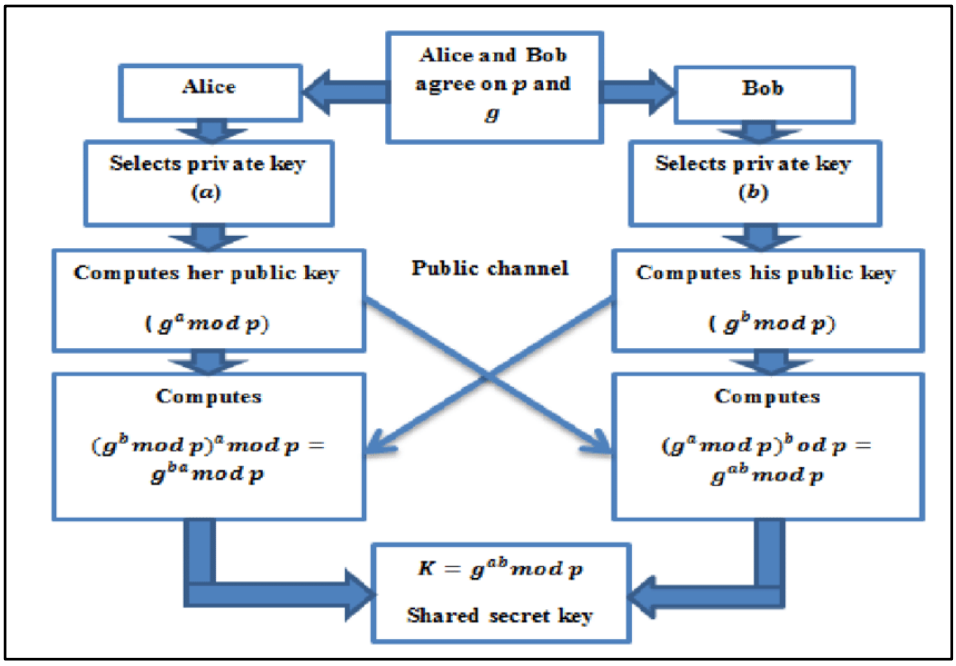
Supongamos que un tercero fuera a inspeccionar el intercambio en la comunicación no segura. Solo verían el color común (amarillo en este caso) y el primer conjunto de colores mixtos (naranja claro y azul claro). Sería extremadamente difícil para la tercera parte calcular el color final. En lugar de colores, se utilizan números extremadamente grandes; esta determinación es computacionalmente costosa. Es inviable intentar calcular el color final, incluso para las supercomputadoras modernas.

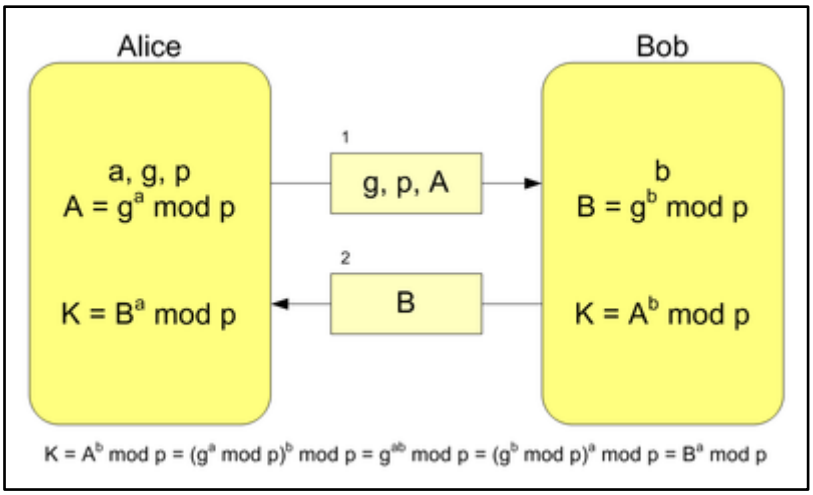
1- Descomposición

1- Genero un número primo (llamado p) y un número (llamado g) que es coprimo de p. Luego te digo ambos números.
2- Eliges un secreto (llamado a). Luego calcula (g^a mód p) (llamado A) y me lo envía de vuelta.
3- Hago lo mismo y elijo un secreto (llamado b). (g^b mod p) (llamado B) y te lo mando.
4- Usa el número que te envié para hacer la misma operación. (B^a mod p)

5- Hago la misma operación con A (A^b mod p) Los números que obtenemos en 4 y 5 son los mismos.

Si obtenemos los mismos números en los pasos 4 y 5, podemos usar ese valor como nuestro secreto para el cifrado simétrico. Las matemáticas anteriores realmente se reducen a las propiedades de los exponentes de módulo.





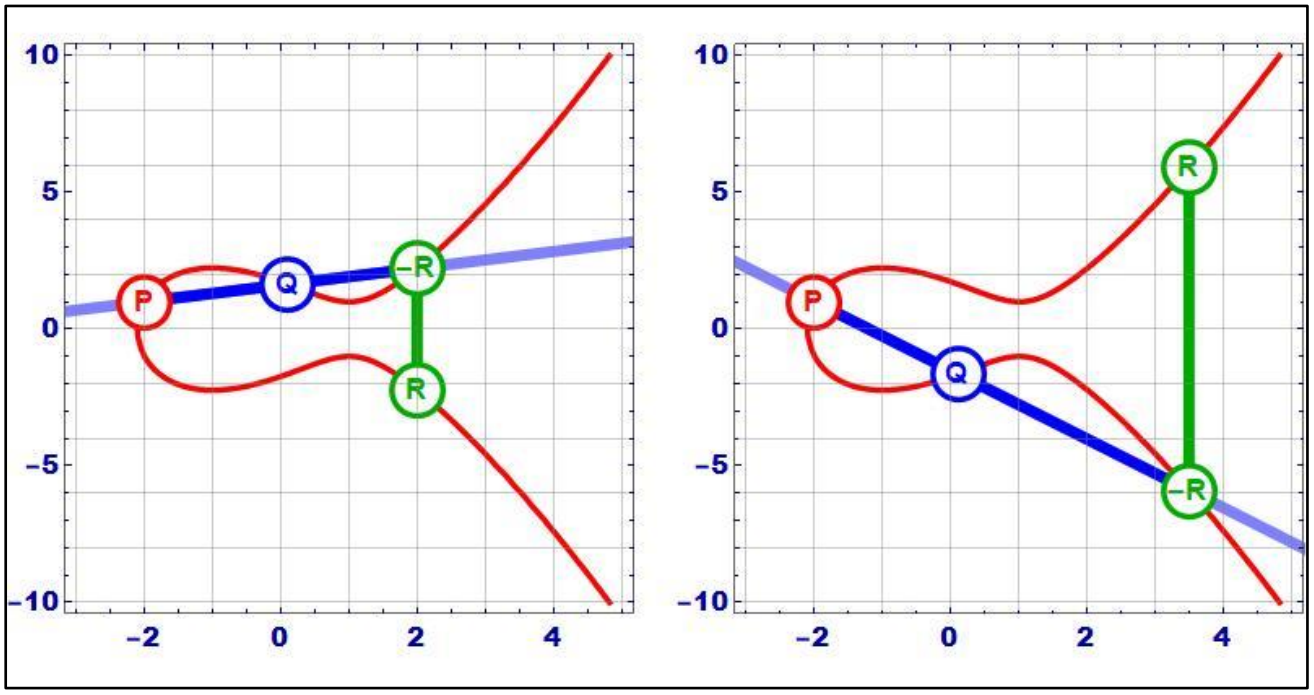
<u>Diffie-Hellman de curva elíptica</u>

Entonces, ahora que sabemos cómo funciona el intercambio normal de claves Diffie-Hellman, podemos entrar en **Diffie-Hellman de curva elíptica (ECDH)**. ***El concepto es más o menos el mismo. Se realiza el mismo proceso, pero, además utiliza curvas algebraicas para generar claves a ser utilizadas por las partes***. Además, ambas partes deben ponerse de acuerdo sobre una curva elíptica de antemano. ***Usar curvas elípticas también es mucho más rápido que usar los grandes números requeridos en DH normal***. El problema del logaritmo discreto de la curva elíptica también es más difícil de resolver que el problema del logaritmo discreto normal. Lo que significa que podemos salirnos con la nuestra con claves más pequeñas que con DH.

1- ¿Qué es una curva elíptica?

En matemáticas, una curva elíptica es una curva algebraica suave, proyectiva, de género uno, en la que hay un punto específico O. Cada curva elíptica sobre un campo de característica diferente de 2 y 3 puede describirse como una curva algebraica plana. por una ecuación de la forma: **$y^2 = x^3 + ax + b$**

Así es como se ve una curva elíptica real:



2- ¿Cómo funciona ECDH?

Entonces, primero decidió qué **curva elíptica usarán las dos partes**. Una vez que se haya decidido, se habrán seleccionado los **parámetros del dominio**. Algunas curvas son más seguras que otras. Esto es lo mismo que elegir buenos números primos en Diffie-Hellman normal.

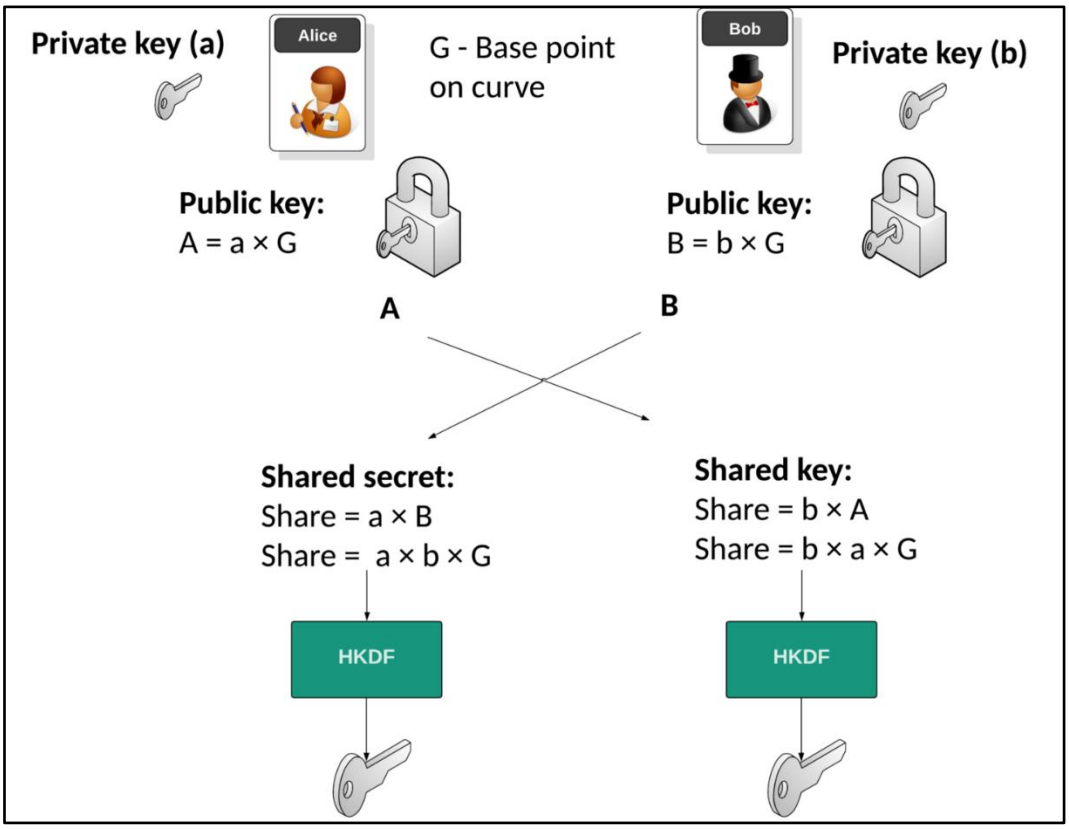
Los siguientes son los parámetros de dominio especificados:

- **E**: la propia curva elíptica
- **G**: un punto en **E** que se establece como el punto base

3- Descomposición

1 - Genero un entero (pseudo) aleatorio como mi clave privada.
2 - Genero mi clave pública A computando aG.
3 - Generas un entero (pseudo) aleatorio b como tu clave privada.
4 - Generas tu clave pública B calculando bG.
5 - Intercambiamos claves públicas.
6 - Calculo K como aB.
7 - Calculas K como bA.

Si obtenemos los mismos números en los pasos 6 y 7, podemos usar ese valor como nuestro secreto para el cifrado simétrico. Este intercambio de clave de curva elíptica es difícil de romper porque alguien necesitaría resolver el problema del logaritmo discreto.



4- Entonces, ¿por qué curvas elípticas?

Como se puede ver, la diferencia entre ECDH y DH no es muy diferente y no es demasiado complicada de implementar. Se debe recordar que para grandes cantidades de cómputo que se llevan a cabo (como un sitio web con mucho tráfico), el tiempo ahorrado al usar curvas elípticas en lugar de grandes números primos se sumará. Es posible que uno no vea la diferencia en un sitio web pequeño, pero cuanto más tráfico, más evidente es el aumento del rendimiento.

TLS

El **protocolo de seguridad de la capa de transporte** es uno de los protocolos de seguridad que están diseñados para facilitar la privacidad y la seguridad de los datos para las comunicaciones a través de Internet. ***El uso principal de TLS es cifrar la comunicación entre las aplicaciones web y los servidores, como los navegadores web que cargan un sitio web***.

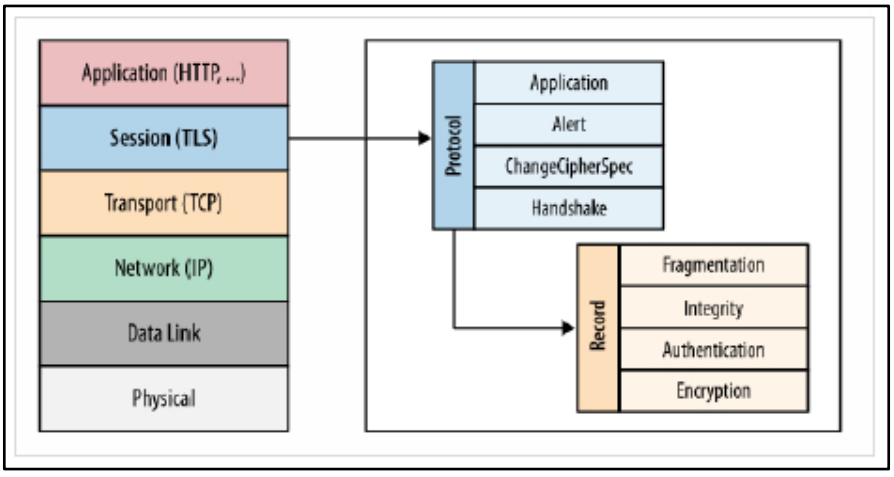
TLS se utiliza para cifrar otras comunicaciones como correo electrónico, mensajería y voz sobre IP (VoIP). TLS fue propuesto por el Grupo de trabajo de ingeniería de Internet (IETF), que es una organización internacional de estándares.

Componentes

Los tres componentes principales que logra TLS son los siguientes:

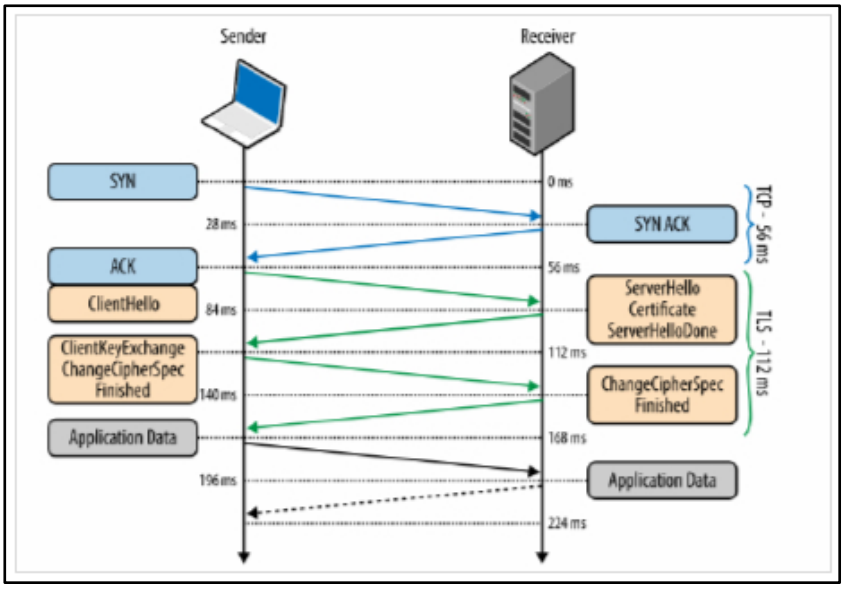
- **Cifrado:** se utiliza para ocultar los datos que se transfieren a terceros.
- **Autenticación:** siempre garantiza que las partes que intercambian información son quienes dicen ser.
- **Integridad:** la integridad verifica que los datos no hayan sido manipulados.

A continuación, se muestra la representación pictórica del protocolo de seguridad de la capa de transporte (TLS):



Protocolo de enlace TLS

Las condiciones de trabajo del **Handshake** (proceso de establecer conexión segura) del protocolo TLS se muestran a continuación:



Características

TLS evolucionó a partir de **Secure Socket Layers (SSL)**, que fue desarrollado originalmente por Netscape Communications Corporation en 1994 para proteger las sesiones web. SSL 1.0 nunca se lanzó públicamente, mientras que SSL 2.0 fue reemplazado rápidamente por SSL 3.0 en el que se basa TLS.

Cabe señalar que TLS no protege los datos en los sistemas finales. Simplemente asegura la entrega segura de datos a través de Internet, evitando posibles escuchas y/o alteración del contenido.

TLS normalmente se implementa sobre **TCP** para **cifrar los protocolos de la capa de aplicación**, como HTTP, FTP, SMTP e IMAP, aunque también se puede implementar en **UDP**, **DCCP** y **SCTP** (por ejemplo, para usos de aplicaciones basadas en **VPN** y **SIP**). Esto se conoce como **Seguridad de la capa de transporte de datagramas (DTLS)**.

Las versiones recientes de todos los principales navegadores web actualmente son compatibles con TLS, y es cada vez más común que los servidores web admitan TLS de forma predeterminada.

TLS utiliza una combinación de **criptografía simétrica y asimétrica**, ya que proporciona un buen compromiso entre el rendimiento y la seguridad cuando se transmiten datos de forma segura.

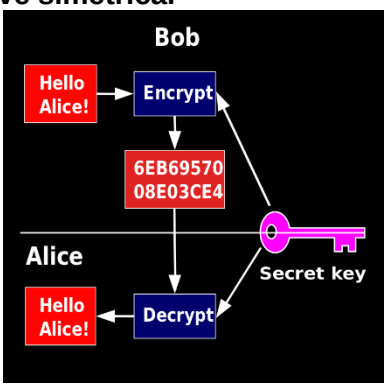
Por este motivo, TLS utiliza **criptografía asimétrica para generar e intercambiar de forma segura una clave de sesión**. Luego, **la clave de sesión se usa para cifrar los datos transmitidos** por una parte y para descifrar los datos recibidos en el otro extremo. ***Una vez finalizada la sesión, la clave de sesión se descarta***.

Con TLS también es deseable que un cliente que se conecta a un servidor pueda validar la propiedad de la clave pública del servidor. Esto normalmente se lleva a cabo utilizando un **certificado digital X.509** emitido por un tercero de confianza conocido como **Autoridad de Certificación (CA)** que afirma la autenticidad de la clave pública. ***En algunos casos, un servidor puede usar un certificado autofirmado en el que el cliente debe confiar explícitamente (los navegadores deben mostrar una advertencia cuando se encuentra un certificado que no es de confianza)***, pero esto puede ser aceptable en redes privadas y/o donde el certificado seguro la distribución es posible. Sin embargo, se recomienda encarecidamente utilizar certificados emitidos por CA de confianza pública.

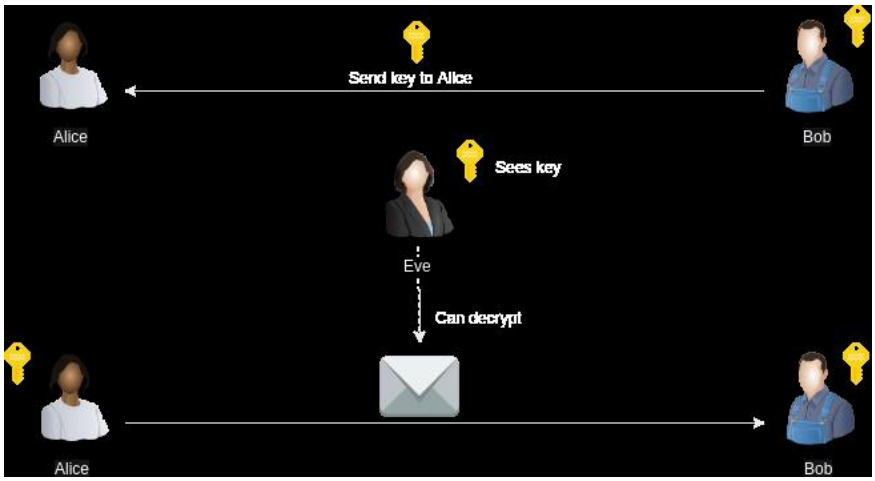
TLS paso a paso

Veamos a continuación concretamente cómo funciona TLS:

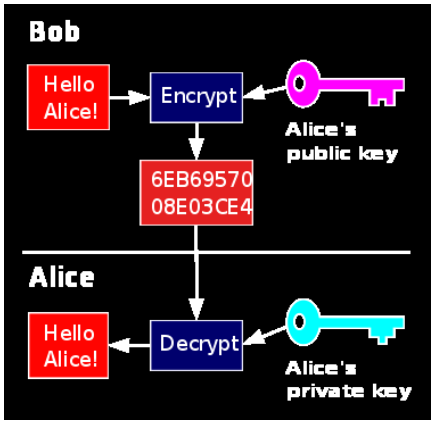
1- **Queremos asegurar la comunicación entre dos personas en Internet.**
2- **Criptografía de clave simétrica.**



3- Se ve bien, hagámoslo, pero espera, ¿cómo intercambias la llave en primer lugar? No se puede hacer eso en Internet, está lleno de espías.



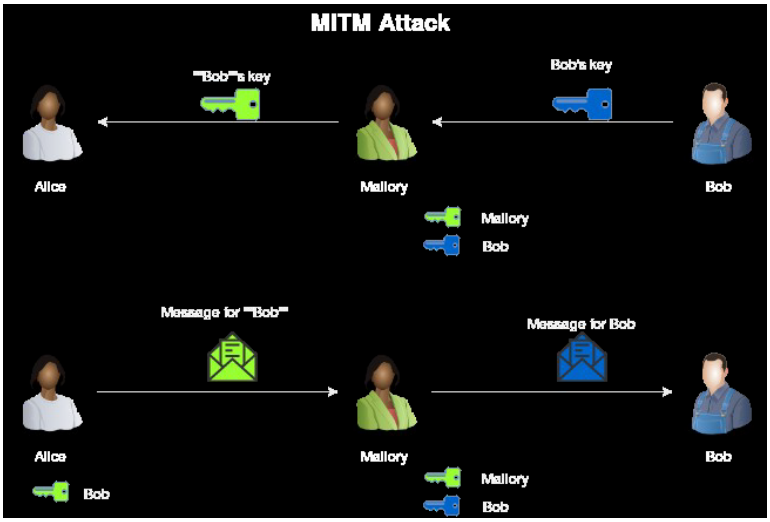
4- Encriptación de clave pública.



5- ¿Y en qué nos ayuda esto?

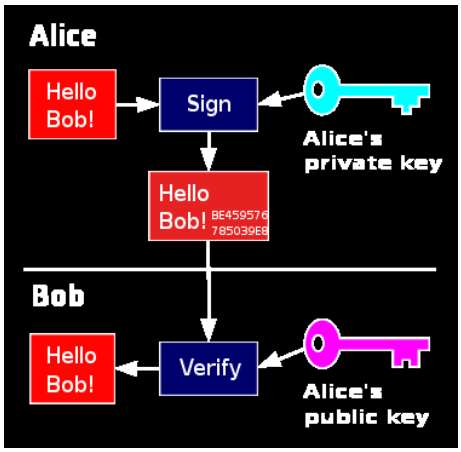
- Si Bob nos envía su clave pública, podemos enviarle un mensaje que solo él puede descifrar
- Pero espera….

6- El ataque (wo) man in the middle (MITM).



7- De nuevo. ¿Cómo podemos asegurarnos de que la clave pública de Bob pertenece a Bob?

8- Firma.



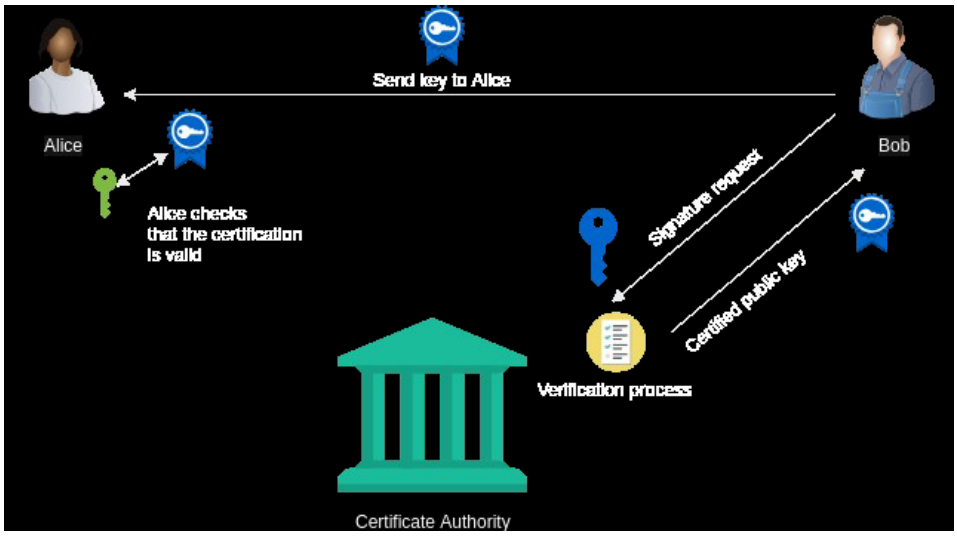
9- Entonces…

- Nuestro objetivo original era la confidencialidad.
- La firma es una propiedad de seguridad diferente: demuestra autenticidad.
- A menudo combinado con una función hash para la integridad

10- ¿Cómo nos ayuda la firma?

- Bob no puede firmar la clave de Bob porque no se confía en su clave todavía.
- Necesitamos un tercero de confianza

11- Tercero de confianza



12- Autoridades de certificación

- Organizaciones que entregan certificados
  – Un documento que contenga una clave pública y una identidad, y algunos metadatos
  – Una firma de la clave privada de la CA los une.
- La seguridad del todo es tan buena como la seguridad del proceso de verificación
  – ¡Mallory puede intentar que su clave pública sea certificada como la de Bob!

13- ¿Nos ayuda?

- Sí, si todo el mundo confía en la autoridad de certificación, entonces todo lo que necesitamos es la clave pública de la CA, ¡y podemos comunicarnos con cualquiera!

14- Infraestructura de Clave Pública

- Un sistema basado en Autoridades de Certificación es uno, pero hay muchas formas posibles de distribuir claves públicas.
- Dichos sistemas se denominan infraestructuras de clave pública
  – Hay otros tipos (de confianza web, blockchain...).

15- En resumen…

16- Finalmente, un sistema seguro

- La CA todopoderosa en el centro de todo
- Cada vez que cualquiera de los participantes quiera enviar algo, necesita cifrarlo con la clave pública del otro participante.
- ¿Qué puede salir mal?

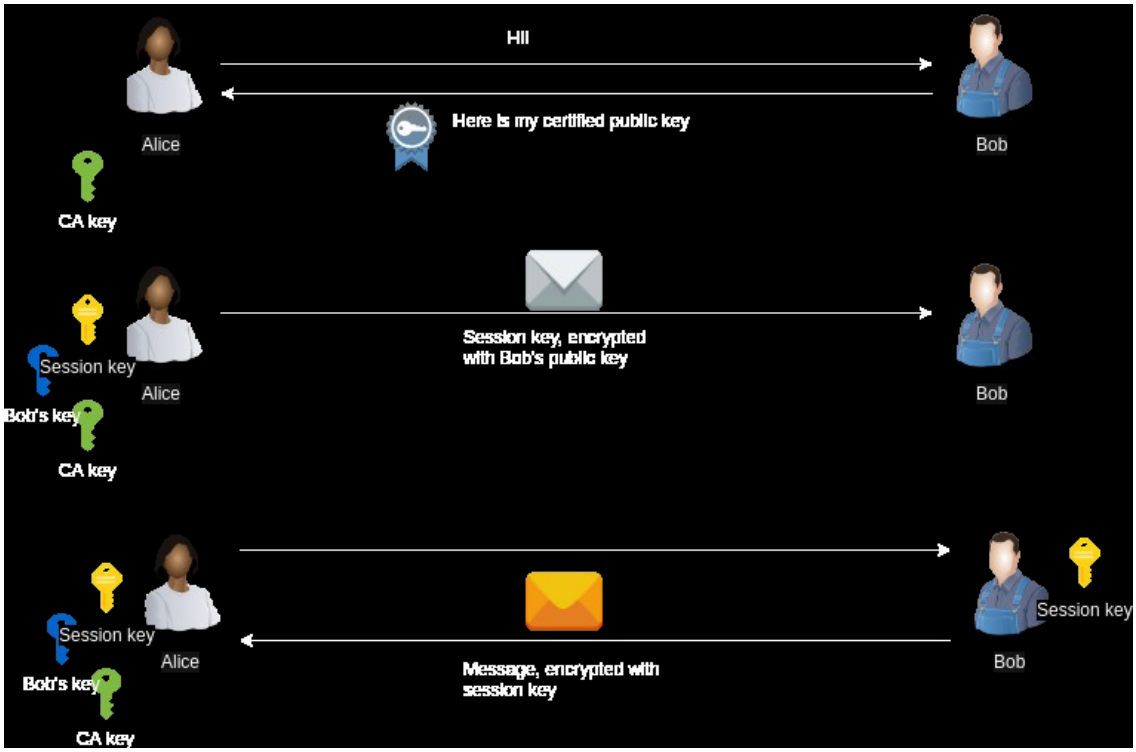
17- ¡Demasiado lento!

- La criptografía de clave pública es demasiado lenta
- ¿Pero sabes lo que no lo es?
  – Criptografía simétrica
  – ¡Pero es inseguro!
- A MENOS QUE…

18- Lo mejor de ambos mundos

- Las claves son solo mensajes
- Podemos generar una clave simétrica
- Envíelo de forma segura mediante criptografía de clave pública y luego, comience a usarlo inmediatamente
- De esa manera, la baja de desempeño solo se usa en el comienzo de la conexión

19- Nuestro esquema actual



20- Felicidades

- ¡Acabamos de inventar TLS!

21- TLS, a grandes rasgos

- **Fase 1**: Autenticación y cambio de clave
  – El servidor se autentica ante el cliente
  – A veces, el cliente también se autentica en el servidor
  – Se produce el intercambio de claves
- **Fase 2**: Intercambio de datos
  – Utiliza encriptación simétrica

Resumen general

1- Validación de certificados

- Al recibir un certificado, debemos asegurarnos de que
  – Pertenece a la persona con la que queríamos hablar
- Para sitios web, significa que se envió al dominio correcto.
  – No es demasiado viejo o demasiado joven
  – Fue firmado por una autoridad de confianza
  – La firma es válida
- El software TLS hace esto por defecto
  – No lo deshabilites
  -- Un certificado vincula una clave pública a una identidad.
- La CA tiene que hacer su propia verificación
  – Por lo general, solo necesita demostrar la propiedad del dominio mencionado en el certificado
- Cualquiera puede obtener un certificado para https://esto.es.google.lo.ju.ro/
  – Los certificados EV cubren la entidad legal detrás de la solicitud

2- La realidad es compleja

- En realidad, no SOLO usamos un cifrado simétrico
  – La integridad está garantizada a través de HMAC o AEAD
- Hay muchas versiones de TLS
  – SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3
- Use TLS 1.2 y comience a planificar para TLS 1.3
- El intercambio de claves Diffie-Hellman garantiza un reenvío perfecto secreto
- Hay muchos algoritmos y parámetros
  – Por lo general, se negocia automáticamente, pero...

3- Seguridad del canal

- A las CA les gusta ser ambiguos sobre esto
- La fuerza del cifrado simétrico no tiene NADA que hacer contra certificados.
  – Excepto obsoletos.
- Pero si el certificado es demasiado débil, corre el riesgo de MITM.
  – Puede tener un canal seguro súper fuerte para un hacker.

4- ¿TLS hará que mi sitio web sea más lento?

- Respuesta corta: no
- Respuesta larga:
  – Hace que la conexión sea más lenta
- Vale la pena
- Usa keepalive
  – Si utiliza CPU modernas, la sobrecarga del cifrado simétrico es insignificante

5- ¿Qué son las curvas elípticas?

- Una herramienta matemática utilizada en criptografía (ECC)
- Se utiliza en el cifrado de clave pública, por lo que solo durante la fase de certificado
- Utilizan claves son más pequeñas que el esquema RSA
  – Tiempo de conexión más rápido
  – Menor consumo de CPU