El futuro digital es de todos

MinTIC

UNIVERSIDAD DEL NORTE

Vigilada Mineducación

CICLO III:

Desarrollo de software

MisionTIC2022

El futuro digital es de todos

MinTIC

UNIVERSIDAD DEL NORTE

Vigilada Mineducación

Sesión 15:

Desarrollo Software

Establecimiento de un canal seguro entre el cliente y servidor.

MisiónTIC2022

Objetivos de la sesión

Al finalizar esta sesión estarás en capacidad de:

1. Explicar y aplicar los conceptos básicos de criptografía simétrica y asimétrica
2. Explicar y aplicar el funcionamiento básico de TLS y HTTPS.
3. Explicar y aplicar el concepto básico de certificados digitales

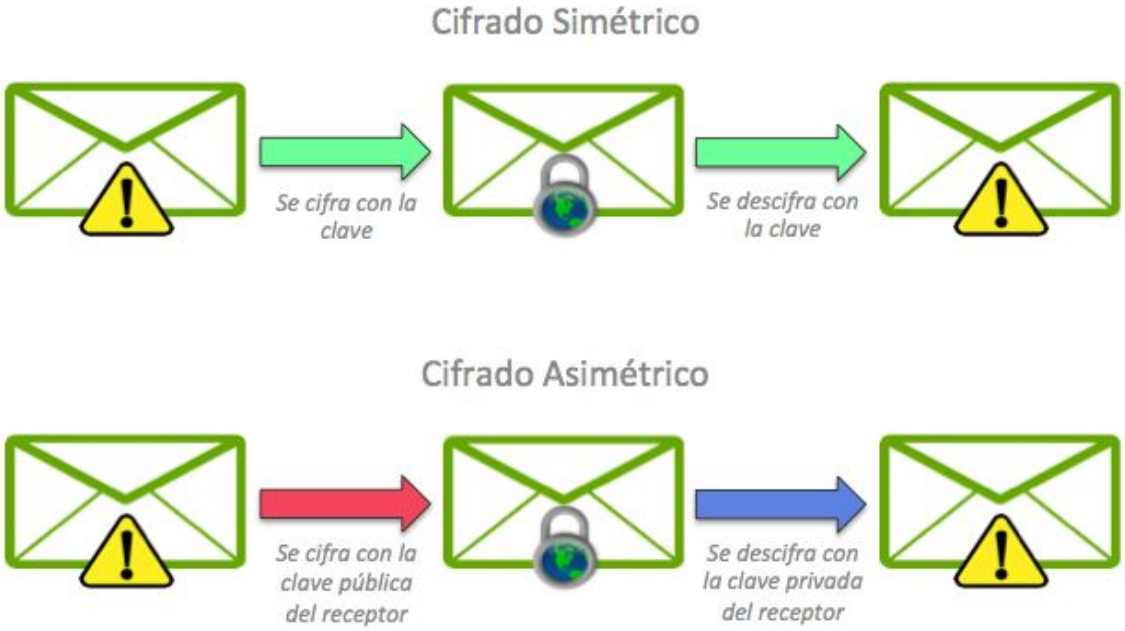
Tipos de sistemas criptográficos

Según el tipo de llave (o clave), existen dos métodos:

- **Criptosistemas de llave única o métodos simétricos**: son aquellos donde los procesos de cifrado y descifrado se realizan con base en una única llave.

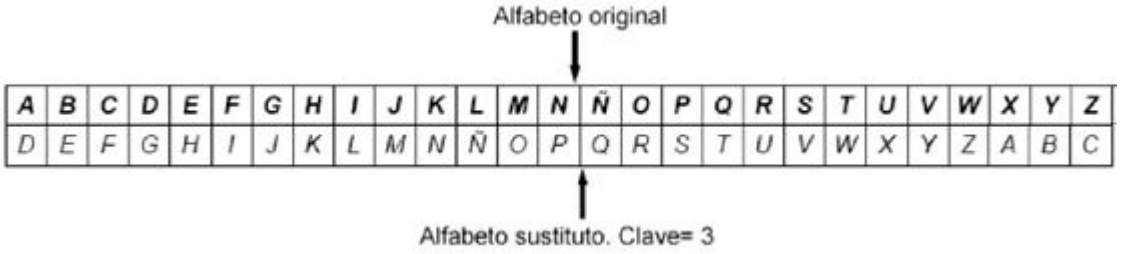
- **Criptosistemas de llave pública o asimétrica**: son aquellos donde los procesos de cifrado y descifrado se realizan con dos llaves distintas y complementarias.

Tipos de sistemas criptográficos



Algoritmos de cifrado simétricos históricos

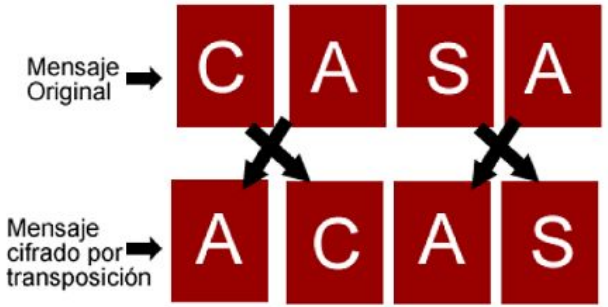
- **Cifrado por sustitución**: Consiste en establecer una correspondencia entre las letras del alfabeto en el que está escrito el mensaje original y los elementos de otro alfabeto (puede ser el mismo u otro). Logrando que cada letra del texto original sea sustituida por un símbolo correspondiente en la elaboración del criptograma. El receptor por su parte, conoce la correspondencia establecida, y sustituye cada símbolo del criptograma por el símbolo correspondiente del alfabeto original, y de esta forma recupera el mensaje enviado originalmente.



La frase: CASA
Pasaría a ser: FDVD

Algoritmos de cifrado simétricos históricos

- **Cifrado por transposición:** Consiste en reorganizar los símbolos del mensaje original colocándolos en un orden distinto, de tal manera que el criptograma contengan los mismos elementos del mensaje original, pero en diferentes posiciones de tal forma que resultan inentendibles. El receptor, como ya conoce la transposición, organiza los símbolos desordenados del criptograma en su posición original.



El futuro digital es de todos MinTIC

UNIVERSIDAD DEL NORTE
Vigilada Mineducación

Tipos de sistemas criptográficos
Cifrado simétrico

En estos criptosistemas se utiliza una llave secreta, llamada secreto compartido, y es conocida únicamente por el emisor y receptor.

- El emisor usa el algoritmo de cifrado, junto con la llave secreta, para cifrar los datos.
- El receptor sa el algoritmo de descifrado, junto con la llave secreta, para cifrar los datos.

Existen dos métodos de cifrado:

- **Cifrado por bloque**: Es aquel en el que se cifra el mensaje original por bloques de tamaño fijo, por ejemplo 64 bits.
- **Cifrado por flujo**: Es aquel en el que se cifra el mensaje original bit a bit o byte a byte.

Los sistemas de cifrado simétrico tienen dos grandes desventajas:

- La distribución de las llaves en un medio público.
- La dificultad de almacenar y proteger muchas llaves diferentes (una para cada receptor).

Mision TIC 2022

Cifradores de bloque modernos

- **DES** (Data Encryption Standard): Es un algoritmo de cifrado por bloques de 64 bits. Fue ideado por IBM y aceptado por US National Institute of Standards and Technology (NIST). Aunque el tamaño de la llave, en bits, es 64 bits, sólo 56 bits son usados para la llave, pues los 8 bits restantes son de paridad y se usan para corrección de errores. Por tanto, este criptosistema es vulnerable a ataques de fuerza bruta.

- **Triple-DES** (Triple - Data Encryption Standard): Dada la capacidad de cómputo actual y la relativa facilidad que supone romper el algoritmo DES, se desarrolló DES TRIPLE, el cual consiste en aplicar tres veces el algoritmo DES en un orden específico. Primero se cifra el dato con una llave el resultado de esto es descifrado con otra llave y por último el resultado del descifrado es cifrado nuevamente. La llave que se emplea en este último paso puede ser la primera clave utilizada o puede ser una nueva llave.

Cifradores de bloque modernos

AES (Advanced Encryption Algorithm):

AES es el cifrador simétrico más usado hoy en día. El algoritmo para AES fue escogido por NIST en un proceso de selección de varios años.

Los requerimientos para todos los candidatos a AES fueron:

- Cifrador de bloque con tamaño de bloque de 128 bits.
- Tres longitudes de claves: 128, 192 y 256 bits
- Seguridad relativa a otros algoritmos candidatos.
- Eficiencia en software y Hardware.

El algoritmo ganador es conocido como Rijndael.

Cifradores de flujos modernos

eSTREAM (the ECRYPT Stream Cipher Project). Fue un proyecto activo por 4 años, desde 2004 a 2008, para promover el diseño de cifradores de flujos eficientes y compactos para uso masivo. En 2008, se seleccionaron siete cifradores de flujos categorizados en dos perfiles:

- Cifradores de flujo para aplicaciones en software:
  - HC-128
  - Rabbit
  - Salsa 20/12
  - SOSEMANUK
- Cifradores de flujo para aplicaciones en hardware con recursos limitados:
  - Grain V1
  - Mickey 2.0
  - Trivium

Tipos de sistemas criptográficos
Cifrado asimétrico

En este tipo de cifrado se utilizan dos llaves: una llave secreta (o privada) y una llave pública.

- El mensaje se cifra con la llave pública del destinatario.
- Este mensaje se puede descifrar con la correspondiente llave privada.
- La ventaja de este sistema es que el usuario no necesita la llave privada de otro para poder enviar un mensaje en forma segura. Se usa la llave pública, la cual no necesita mantenerse segura. Al utilizar la llave pública del destinatario, se asegura que sólo esa el propietario de la llave privada puede descifrarlo utilizando la llave privada.
- Este sistema presenta algunas desventajas: para una misma longitud de llave y mensaje se necesita mayor tiempo de proceso, las llaves deben ser de mayor tamaño que las simétricas y el mensaje cifrado ocupa más espacio que el original.

Tipos de sistemas criptográficos
Cifrado asimétrico - Algoritmos

Protocolo de acuerdo de llaves Diffie - Hellman:

- Es un protocolo que permite intercambiar y establecer una llave secreta compartida entre dos partes. Es decir, si dos partes (cliente y servidor) siguen el protocolo, terminan acordando un clave secreta, conocida únicamente a las dos partes involucradas.

- Su seguridad se basa en la dificultad de resolver una instancia del logaritmo discreto (y del problema de **Diffie - Hellman**) dentro de una estructura matemática (grupo), en donde estos problemas son considerados computacionalmente costosos. Ejemplos: grupo de curvas elípticas y grupos modulares.

Tipos de sistemas criptográficos
Cifrado asimétrico - Algoritmos

RSA (Rivest - Shamir - Adleman): La seguridad de este algoritmo se centra en la dificultad para factorizar grandes números enteros. Los mensajes enviados se representan mediante números y el funcionamiento se basa en el producto de dos números primos grandes elegidos al azar y mantenidos en secreto. Como en todo sistema de clave pública, cada usuario tiene dos claves de cifrado: una pública y otra privada. Cuando se quiere enviar un mensaje, el emisor busca la clave pública del receptor, cifra su mensaje con esa clave, y una vez que el mensaje cifrado llega al receptor, éste lo descifra usando su clave privada.

Ventajas:

- Resuelve el problema de la distribución de las llaves simétricas (cifrado simétrico).
- Se puede emplear para ser utilizado en firmas digitales.

Desventajas:

- La seguridad depende de la eficiencia de los ordenadores.
- Es más lento que los algoritmos de clave simétrica.
- La clave privada debe ser cifrada por algún algoritmo simétrico.

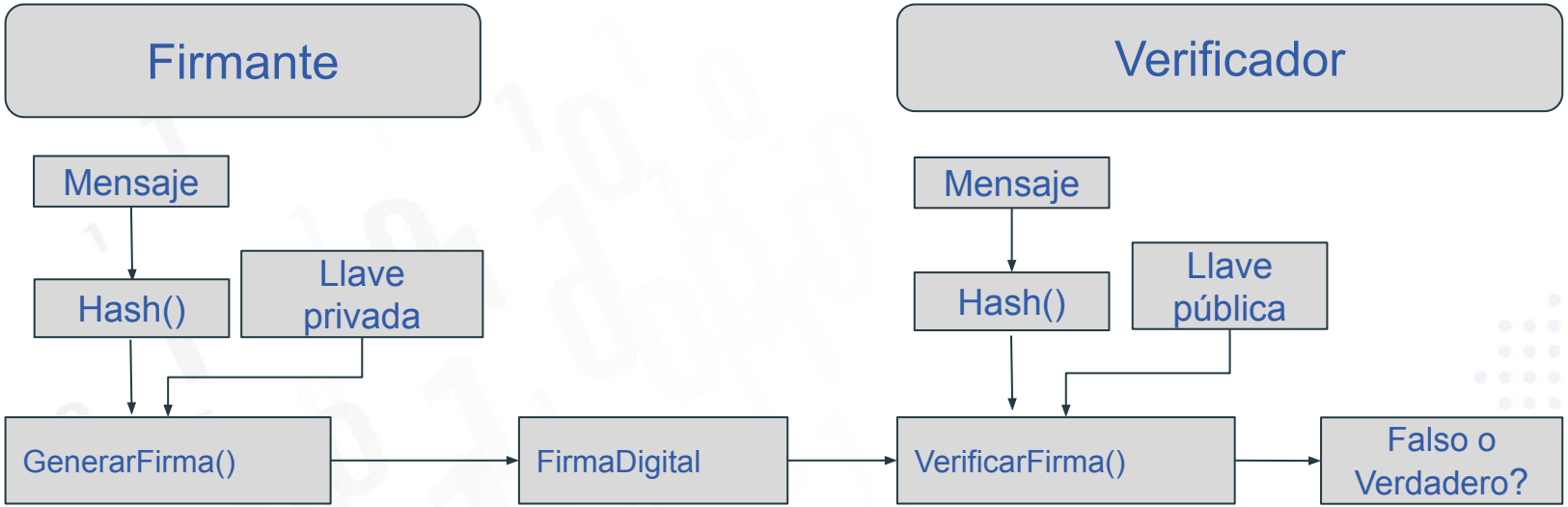
Tipos de sistemas criptográficos
Cifrado asimétrico - Algoritmos

Protocolo de acuerdo de llaves Diffie - Hellman:

- Este protocolo, sin embargo, tiene un problema, que es su falta de autenticación. Es decir, no puede validar la identidad de las partes, por lo que si un tercera parte se pone en medio de la «conversación», también podría establecer claves secretas tanto con el emisor como con el receptor, suplantando a ambos.

- Este protocolo es usado como componente fundamental para construir otros protocolos más robustos y seguros, y además esquemas de cifrado asimétricos. Por ejemplo, el esquema de llave pública ElGamal se construye a partir del protocolo Diffie-Hellman.

Esquemas de firma digital



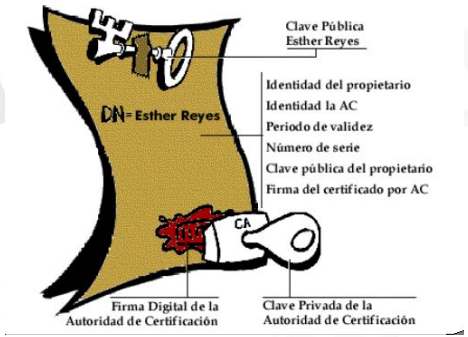
Esquemas de firma digital

Algunos ejemplos de esquemas de firma digital usados actualmente.

- DSA es similar al criptosistema de llave pública RSA usado como esquema de firma digital.

- EdDSA es un esquema de firma digital cuya seguridad se fundamenta en la dificultad de resolver una instancia del problema del logaritmo discreto sobre una curva elíptica. Por ejemplo Ed25519 es un esquema de firma EdDSA que usa la función hash SHA-512 y la curva Curve25519.

Sistemas criptográficos
Certificados digitales



Estándar X.509

- Un certificado digital es un documento electrónico que asocia una clave pública con la identidad de su propietario.
- Contiene los datos de identificación de una persona o entidad (empresa, servidor Web, etc.), otros atributos (ámbito de uso de la clave pública, fechas de validez, etc.) y una firma digital de una autoridad certificadora.
- Las principales autoridades certificadoras actuales que existen son: VeriSign, SecureSign, GlobalSign, Thawte y CertiSign.
- El formato de los certificados digitales es estándar, siendo X.509 v3 el recomendado por la Unión Internacional de Comunicaciones (ITU) y usado por la mayoría de navegadores.

Certificados digitales - Ejemplo

Asuma que usted desea obtener un certificado para su dominio su-dominio.com.

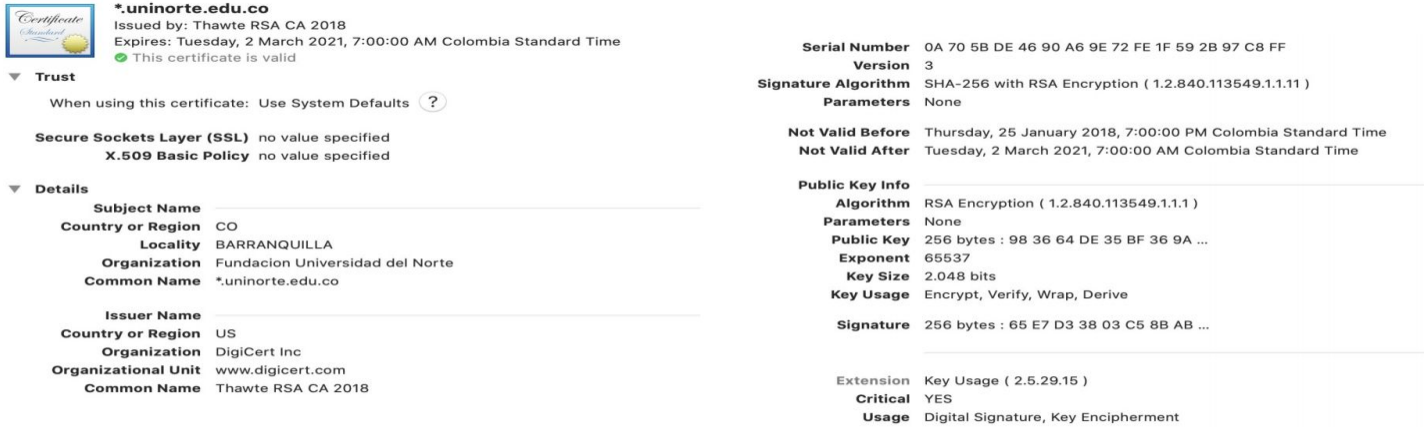
1. Debe enviar una petición de generación de certificado a la entidad certificadora, que contenga su identidad, dirección de correo, y la llave pública que desea corresponder con su dominio.

2. Una vez que la entidad certificadora recibe la petición, chequea que usted es quien dice ser, por medio de los soportes enviados. Si todas las verificaciones son exitosas, la entidad certificadora incluye toda los datos relevantes dentro de la estructura del certificado, y lo firma usando un esquema de firma digital y su llave privada.

3. La firma per se está incluida en el certificado, el cual corresponde la llave pública encontrada en la petición con su identidad.

4. Este certificado firmado puede ser enviado a cualquiera que necesita comunicarse de forma segura con usted. En tal caso, ese ente usando la llave pública de la entidad certificadora puede verificar el certificado y estar seguro que la llave incluida en él corresponde a usted.

Sistemas criptográficos
Certificados digitales - Ejemplo



***.uninorte.edu.co**
Issued by: Thawte RSA CA 2018
Expires: Tuesday, 2 March 2021, 7:00:00 AM Colombia Standard Time
This certificate is valid

Trust

When using this certificate: Use System Defaults ?

Secure Sockets Layer (SSL) no value specified
X.509 Basic Policy no value specified

Details

Subject Name
Country or Region CO
Locality BARRANQUILLA
Organization Fundacion Universidad del Norte
Common Name *.uninorte.edu.co

Issuer Name
Country or Region US
Organization DigiCert Inc
Organizational Unit www.digicert.com
Common Name Thawte RSA CA 2018

Serial Number 0A 70 5B DE 46 90 A6 9E 72 FE 1F 59 2B 97 C8 FF
Version 3
Signature Algorithm SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters None

Not Valid Before Thursday, 25 January 2018, 7:00:00 PM Colombia Standard Time
Not Valid After Tuesday, 2 March 2021, 7:00:00 AM Colombia Standard Time

Public Key Info
Algorithm RSA Encryption (1.2.840.113549.1.1.1)
Parameters None
Public Key 256 bytes : 98 36 64 DE 35 BF 36 9A ...
Exponent 65537
Key Size 2.048 bits
Key Usage Encrypt, Verify, Wrap, Derive

Signature 256 bytes : 65 E7 D3 38 03 C5 8B AB ...

Extension Key Usage (2.5.29.15)
Critical YES
Usage Digital Signature, Key Encipherment

El futuro digital es de todos | MinTIC

UNIVERSIDAD DEL NORTE
Vigilada Mineducación

Sistemas criptográficos
Certificados digitales

Validación de certificados digitales

Los certificados no son documentos permanentes.

- Al estar basados en el uso de claves, no es recomendable que sean válidos por largos períodos de tiempo, ya que entre más duración tenga, será más fácil que se conozca la clave. También es cierto, que cada vez los computadores vienen con más recursos para realizar operaciones o cálculos, lo cual facilita el trabajo de los criptoanalistas. Por esta razón los certificados digitales tienen especificado un período de validez, que generalmente es de un año.

MisiónTIC2022

Sistemas criptográficos
Certificados digitales

Proceso general para verificar certificados.

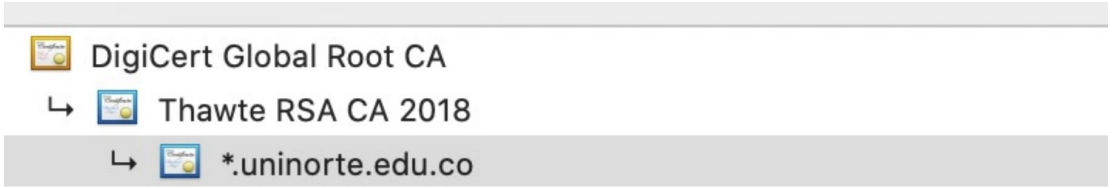
- Hay muchas entidades certificadoras que generan certificados. Así que hay un reto relacionado a la distribución de las llaves públicas de las entidad certificadoras a los usuarios finales.
- La solución, llamada cadena de certificados, es permitir que una entidad certificadora certifique la llave pública de otra entidad certificadora.
- Este proceso se puede repetir recursivamente, resultando en una cadena de certificados donde cada certificado en la cadena certifica la llave pública de la próxima entidad certificadora en la cadena.

Sistemas criptográficos
Certificados digitales

Para verificar esta cadena de certificados de longitud tres, se procede así:

1. El verificador (el navegador, normalmente) usa una copia local confiable de la llave pública de la entidad certificadora raiz (DigiCert) para verificar la validez del certificado generado para la entidad certificadora intermedia (Thawte RSA). SI es válido, el verificador asume que la entidad certificadora intermedia se confiable.

2. El verificador ahora verifica la validez del certificado generado para uninorte.edu.co por parte de la entidad certificadora intermedia. Si es válido, entonces el verificador asume que obtiene la llave pública correcta para uninorte.edu.co.



Protocolos criptográficos TLS/HTTPS

Protocolo TLS Transport Layer Security (seguridad de la capa de transporte)

- TLS es la evolución del protocolo SSL(Secure Sockets Layer). Como su nombre lo indica, este protocolo funciona en la cuarta capa del modelo OSI. El objetivo de TLS es ofrecer mayor seguridad y privacidad a las conexiones, evitar que los datos puedan ser interceptados y también ofrecer mayor velocidad y rendimiento que el SSL. Es considerado un protocolo seguro (desde TLS 1.2 en adelante).
- Este protocolo no solo se usa para comunicaciones entre páginas web por medio de HTTPS. Sino que también es implementado en servidores VPN (Virtual Private Network) de tipo SSL/TLS. Su éxito radica en la interoperabilidad entre el cliente y el servidor al encriptar la información.

Sistemas criptográficos TLS/HTTPS

- El objetivo de seguridad de este protocolo es proveer confidencialidad e integridad de los datos transmitidos por dos computadoras que se comunican sobre una red de datos.
- El protocolo TLS posee dos componentes:

1. El componente de intercambio (TLS handshake) permite que dos partes (comúnmente el navegador y el servidor) se autentiquen entre ellas (usando certificados por ejemplo), negocien un conjunto de cifradores y otros parámetros, además establezcan una secreto compartido entre las dos partes y luego lo usen para proteger la confidencialidad y la integridad de los datos transmitidos por la red.

2. El componente TLS record lo usan las partes para transmitir datos entre los dos, usando la llave secreta compartida, los cifradores y otros parámetros negociados anteriormente.

Sistemas criptográficos TLS/HTTPS

Protocolo HTTPS

- El protocolo HTTP representaba un riesgo por lo que se hizo necesario la actualización hacia un nuevo protocolo.
- Su sucesor es HTTPS (Hyper Text Transfer Protocol Secure) o protocolo de transferencia de hipertexto. Se puede definir de igual forma que el HTTP, solo que más seguro.
- HTTPS funciona en la capa de aplicación del modelo OSI y utiliza algoritmos de cifrado simétrico y asimétrico; y de intercambio de claves. Se utiliza para intercambio de información sensible como datos bancarios y contraseñas.
- HTTPS se ha convertido en el protocolo más conocido y usado debido a que se puede visualizar sus siglas en las direcciones de las páginas web. Es más, es el indicador de que una página es segura.

El futuro digital es de todos | MinTIC

UNIVERSIDAD DEL NORTE
Vigilada Mineducación

Sistemas criptográficos TLS/HTTPS

Protocolo HTTPS

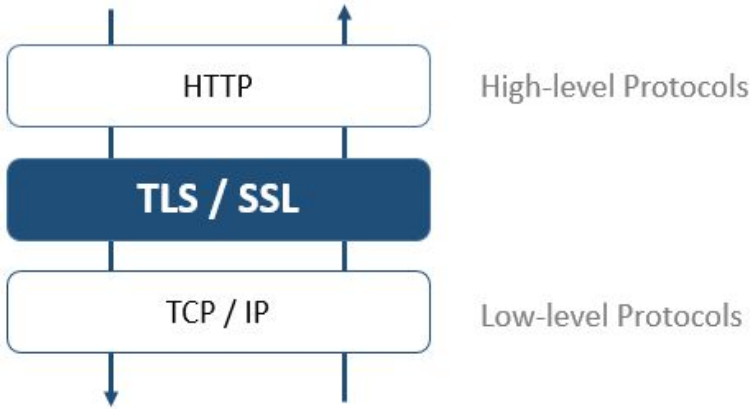
- HTTPS es una combinación del protocolo HTTP (usado en cada transacción web) con el protocolo SSL/TLS usada para establecer comunicaciones cifradas en sitios web.

- Si un sitio web hace uso del protocolo HTTPS, esto significa entonces que usa SSL/TLS para establecer un canal seguro entre las partes. Una vez este canal seguro haya sido establecido, entonces el cliente envía paquetes HTTP a través del canal seguro.

MisionTIC2022

Sistemas criptográficos TLS/HTTPS

Estos protocolos están diseñados para mejorar la seguridad de los navegantes. Son importantes en los sitios webs actuales y que pretenden adaptarse a las exigencias del día a día, ya que en temas de SEO (Search Engine Optimization), es muy importante que una web cuente con estos protocolos.



HTTPS es una implementación del cifrado TLS sobre el protocolo HTTP, que utilizan todos los sitios web, así como algunos otros servicios web. Por lo tanto, cualquier sitio web que utilice HTTPS utiliza cifrado TLS.

El futuro digital es de todos

MinTIC

UNIVERSIDAD DEL NORTE

Vigilada Mineducación

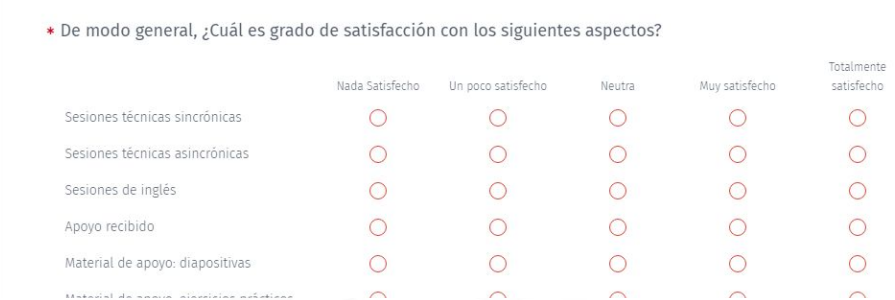
Ejercicios de práctica

Mision TIC 2022

El futuro digital es de todos | MinTIC

UNIVERSIDAD DEL NORTE
Vigilada Mineducación

Seguimiento Habilidades Digitales en Programación



* De modo general, ¿Cuál es grado de satisfacción con los siguientes aspectos?

	Nada Satisfecho	Un poco satisfecho	Neutra	Muy satisfecho	Totalmente satisfecho
Sesiones técnicas sincrónicas	○	○	○	○	○
Sesiones técnicas asincrónicas	○	○	○	○	○
Sesiones de inglés	○	○	○	○	○
Apoyo recibido	○	○	○	○	○
Material de apoyo: diapositivas	○	○	○	○	○

Completa la siguiente encuesta para darnos retroalimentación sobre esta semana ▼▼▼

https://www.questionpro.com/t/ALw8TZlxOJ

MisionTIC2022

El futuro digital es de todos

MinTIC

UNIVERSIDAD DEL NORTE

Vigilada Mineducación

¡GRACIAS

POR SER PARTE DE ESTA EXPERIENCIA DE APRENDIZAJE!

Mision TIC 2022