****ESCUELA DE EDUCACIÓN TÉCNICA Nº 3139**

**“GRAL. MARTIN M. DE GÜEMES”**

Dirección: CASEROS N° 1615 – Telf.: (0387) 4320294

SALTA – CAPITAL

**TRABAJO PRACTICO CRIPTOGRAFIA**

FECHA:

NOMBRE:

CURSO: TURNO:

1. Describa brevemente los siguientes conceptos indicando sus respectivas tecnologías: confidencialidad, integridad, autenticación, no repudio.
2. Indicar la respuesta correcta:
3. En un cifrado simétrico se utiliza la misma clave para cifrar y descifrar.

Verdadero.

Falso.

1. En un cifrado asimétrico se utiliza la clave publica para descifrar y la clave privada para cifrar.

Verdadero.

Falso.

1. Un cifrado simétrico se utiliza para:

Intercambiar claves.

Cifrar contenido.

Firmar digitalmente.

1. Un cifrado asimétrico se utiliza para:

Intercambiar claves.

Cifrar contenido.

Firmar digitalmente.

1. Indique tipos de cifrado simétrico

PKI.

Por bloque.

Por flujo.

Curvas elípticas.

1. PKI se utiliza solo en ámbitos públicos.

Si, porque requiere de CA.

No, hay situaciones que la única entidad de confianza es la propia organización.

1. El tamaño de un bloque en un cifrado por bloque es de:

64 bits.

256 bits.

32 bits.

128 bits.

1. El máximo nivel de seguridad de un certificado que emite un CA es:

Validación de dominio (DV).

Validación extendida (EV).

Validación de empresa (OV).

1. Un certificado con la validación de empresa se utiliza para:

Sitios web personales.

Sitios web comerciales.

Bancos y empresas de servicios financieros internacionales.

Comercio electrónico.

Pantallas de inicio de sesión.

Cualquier sitio web que no realice transacciones ni recopile información personal.

1. Un certificado con la validación extendida se utiliza para:

Sitios web personales.

Sitios web comerciales.

Bancos y empresas de servicios financieros internacionales.

Comercio electrónico.

Pantallas de inicio de sesión.

Cualquier sitio web que no realice transacciones ni recopile información personal.

1. Un certificado con la validación de dominio se utiliza para:

Sitios web personales.

Sitios web comerciales.

Bancos y empresas de servicios financieros internacionales.

Comercio electrónico.

Pantallas de inicio de sesión.

Cualquier sitio web que no realice transacciones ni recopile información personal.

1. Diffie Hellman es:

Un protocolo de cifrado asimétrico.

Un método de intercambio seguro de claves.

1. Diffier Hellman de curva elíptica se diferencia de Diffie Hellman tradicional por:

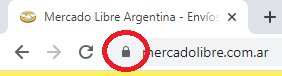
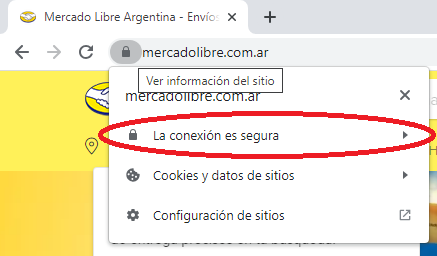
Utiliza cifrado asimétrico.

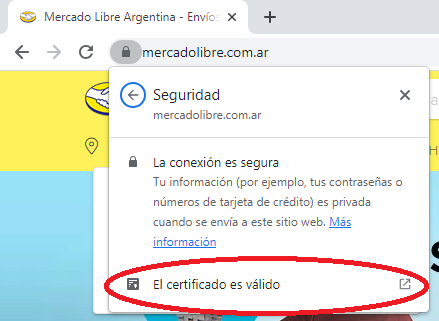
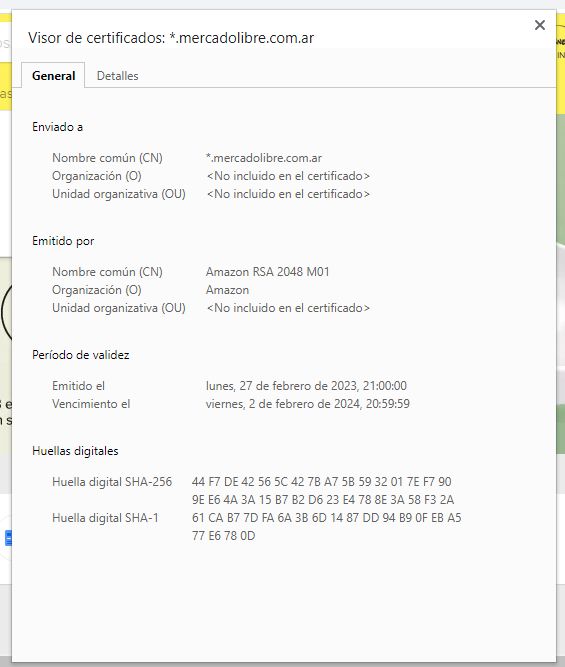
Utiliza curvas algebraicas para generar claves.

Es más liviano.

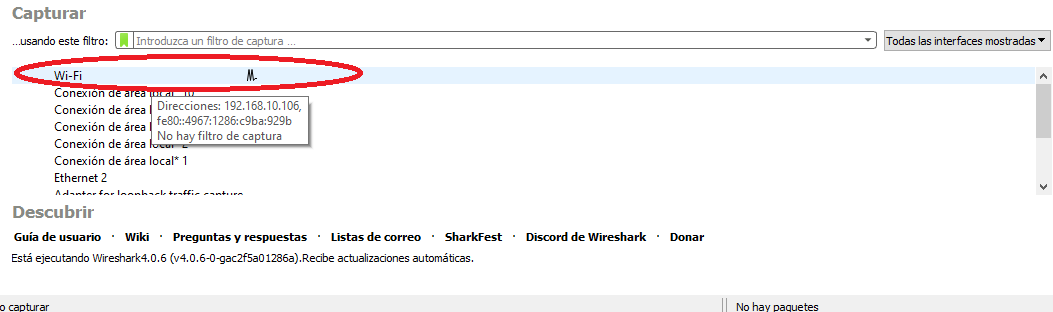
El procedimiento es diferente.

1. Con el navegador Chrome abrir cualquier sitio con navegación segura (https) y completar la siguiente actividad:
2. Hacer click en el candado de seguridad -> La conexión es segura -> El certificado es válido:

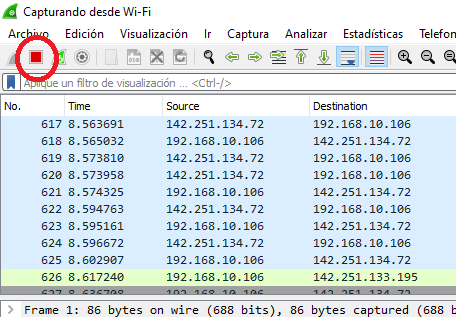




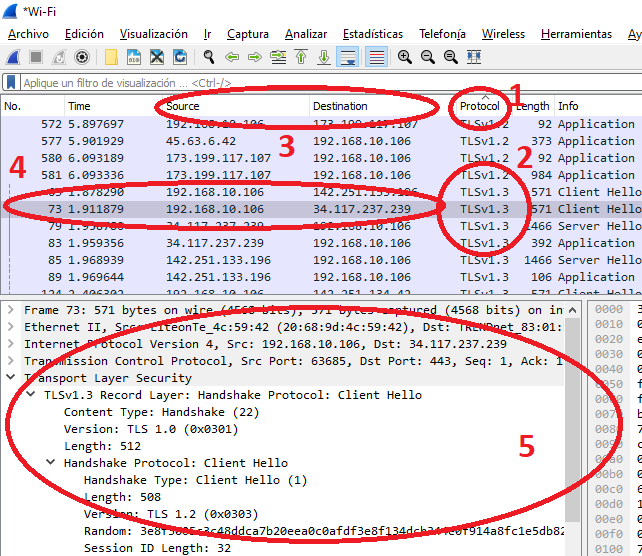
1. En el cuadro resultante indicar la información (con captura de pantalla) correspondiente a confidencialidad, integridad, autenticación y PKI de TLS.
2. Realizar un diagrama del handshake TLS con información real, siguiendo los siguientes pasos:
3. Instalar el software open source analizador de protocolos Wireshark (<https://www.wireshark.org/download.html>). Utilizar como referencia el sitio elegido en el punto 3.
4. Cerrar todo navegador y soft que utilice la red, abrir Wireshark y seleccionar la interfaz de red conectada a internet.



1. Abrir el navegador, e ingresar al sitio con conexión https del punto anterior, volver a Wireshark y observar que se haya generado información, detener la captura.



1. Ordenar la información por protocolo (columna **Protocol**), ubicar TLS y completar el diagrama. Tener en cuenta las columnas **Source** y **Destination** para completar cada “vuelo”, elegir cada línea involucrada en el proceso y extraer la información necesaria.



1. Investigar sobre el proyecto Let’s Encript e indicar como obtener un certificado de seguridad con el mismo.
2. Investigar e indicar como generar un certificado de seguridad autofirmado con OpenSSL.
3. Realizar una conclusión final sobre la diferencia entre los certificados generados en los puntos 5 y 6.