Certificado de Profesionalidad en Seguridad Informática

IronHack - SOC

Módulo 4

Criptografía

Práctica 1

Alumno: Julián Gordon

Indice

Enunciado

Criptografía - Actividad 1

La universidad politécnica de Madrid ofrece recursos muy interesantes para aprender criptografía. En concreto dos colecciones:

- **Intypedia, disponible en Youtube**
- **Píldoras formativas Thoth**

Os aviso que la calidad, que sí el contenido, de los vídeos no es de lo mejor que se ha hecho.

Ambos son muy interesantes y recomendables para que los vayas viendo a tu elección. El segundo profundiza mucho en el tratamiento matemático de la criptografía y el criptoanálisis.

- **Intypedia:**
    - **o** Lección 2, sistemas de clave simétrica. https://www.youtube.com/watch?v=46Pwz2V-t8Q&list=PL8bSwVy8_IcMOdOouph8-mFagDEcrXe1w&index=6&t=2s
    - o Lección 3, sistemas de clave pública, https://www.youtube.com/watch?v=46Pwz2V-t8Q&list=PL8bSwVy8_IcMOdOouph8-mFagDEcrXe1w&index=6&t=2s
    - o Lección 9, introducción al protocolo SSL (hoy TLS), https://www.youtube.com/watch?v=pOeWmStBOYY&list=PL8bSwVy8_IcMOdOouph8-mFagcrXe1w&in

- Proyecto Thoth
    - Píldora 27, Simétrica VS Asimétrica, https://www.youtube.com/watch?v=0qfOVm-dtcQ&list=PL8bSwVy8_IcNNS5QDLjV7gUg8dIeMFSER&index=27
    - Píldora 36, Codificación BASE 64, https://www.youtube.com/watch?v=TvIHDA0J7QM&list=PL8bSwVy8_IcNNS5QDLjV7gUg8dIeMFSER&index=36&t=307s
    - Píldora 43, funciones hash, https://www.youtube.com/watch?v=FRBIc0udwv0&list=PL8bSwVy8_IcNNS5QDLjV7gUg8dIeMFSER&index=43

Contesta a las siguientes preguntas?

- ¿Qué tipo de criptografía usarías para cifrar un pendrive?
- ¿Y para enviar un correo?
- ¿Qué utilidad real ves a los hashes?
- ¿Es lo mismo codificación que encriptación? Averigua y cita algún sistema de codificación.
- Un texto codificado en BASE 64, ¿puede tener espacios? Quiere decirse, un texto claro codificado en Base64, cuando se obtiene la codificación y se manipula esa codificación, añadiendo espacios intermedios, ¿afecta esta operación al mensaje en claro inicial?
- Si fuera un mensaje encriptado, ocurriría lo mismo. Comprueba y documenta ambas cosas.
- ¿Podemos saber la clave pública de un servidor SSL (TLS)? Gráficamente y por comando, si es posible, en sistemas operativos.

Introducción

En el mundo actual, la seguridad de la información es fundamental. Con el aumento del intercambio de datos digitales, es muy importante comprender y aplicar correctamente diversas técnicas criptográficas y métodos de codificación. Este trabajo práctico aborda una serie de preguntas relacionadas con la criptografía y la codificación, proporcionando una visión detallada de su aplicación práctica en diferentes escenarios. Desde la elección del tipo de criptografía adecuada para cifrar un pendrive y enviar correos electrónicos, hasta la utilidad de las funciones hash y la diferenciación entre codificación y encriptación, este trabajo pretende esclarecer conceptos cruciales y su implementación. También se examina el impacto de la manipulación de datos codificados y encriptados, así como la obtención de claves públicas de servidores SSL/TLS, tanto gráficamente como por línea de comandos.

¿Qué tipo de criptografía usarías para cifrar un pendrive?

Para cifrar un pendrive, la criptografía más adecuada es la simétrica. El mismo usuario o alguien autorizado, necesitará cifrar y descifrar los datos, y la criptografía simétrica es más rápida para este tipo de operaciones. Un ejemplo es BitLocker, una herramienta de cifrado desarrollada por Microsoft que suele venir preinstalada en versiones de Windows. BitLocker utiliza cifrado simétrico para proteger los datos de almacenamiento, asegurando el acceso solo mediante una contraseña o clave de recuperación. Cabe destacar que cifrar todo el espacio del pendrive puede llevar un tiempo considerable.

¿Y para enviar un correo?

Para cifrar un correo electrónico, se recomienda usar criptografía de clave pública (PKI). Por ejemplo, el remitente Pepe necesita la clave pública del destinatario Juan para cifrar el correo. Solo el destinatario puede descifrar el mensaje, ya que posee la clave privada correspondiente. Esto garantiza que solo la persona autorizada pueda leer el correo.

¿Qué utilidad real ves a los hashes?

Las funciones hash son algoritmos que convierten datos de entrada en una cadena de longitud fija, determinística para un mismo conjunto de datos. Se utilizan ampliamente en criptografía, protección de contraseñas, verificación de integridad de datos, detección de malware, indexación en bases de datos y mapeo de caché.

Algunas aplicaciones específicas incluyen:

- **Protección de contraseñas:** Los hashes criptográficos almacenan contraseñas de forma segura. Al ingresar una contraseña, se compara el hash de la entrada con el hash almacenado.
- **Integridad de datos:** Los hashes verifican que un archivo descargado no ha sido alterado comparando su hash con el original.
- **Detección de malware:** Se comparan los hashes de archivos sospechosos con hashes conocidos de malware.
- **Indexación en bases de datos y mapeo de caché:** Permiten búsquedas rápidas y acceso eficiente a datos almacenados.

¿Es lo mismo codificación que encriptación? Averigua y cita algún sistema de codificación.

No, la codificación y la encriptación son conceptos distintos:

- **Codificación:** Transforma datos de un formato a otro sin seguridad en mente, no usa claves secretas y su objetivo principal es la representación de datos. Un ejemplo es Base64, que convierte datos binarios en texto ASCII.
- **Encriptación:** Hace que los datos sean ilegibles sin una clave específica, utilizando algoritmos complejos para garantizar la confidencialidad. Solo las partes autorizadas pueden acceder a la información encriptada.

Ejemplo de sistema de codificación: Base64 utiliza un alfabeto de 64 caracteres para representar datos binarios en formato ASCII, facilitando la transmisión y manipulación de datos binarios en contextos de texto.

Un texto codificado en BASE64, ¿puede tener espacios?

Sí, un texto codificado en Base64 puede tener espacios añadidos, y estos no afectan al mensaje original al decodificarlo. Por ejemplo, si "Hola, mundo" se codifica como "SG9sYSwgbXVuZG8=", agregar espacios ("SG9sYSwg bXVuZG8=") no cambiará el mensaje original al decodificarlo.

Si fuera un mensaje encriptado, ocurriría lo mismo? Comprueba y documenta ambas cosas.

No, si un mensaje encriptado se manipula añadiendo espacios, el mensaje original se altera y su integridad se compromete. Por ejemplo, encriptar "HolaMundo" y luego manipular el texto desencriptado añadiendo espacios cambia su significado y estructura. Cualquier alteración en el texto desencriptado puede resultar en datos incorrectos o inservibles.

Encriptación y desencriptación: Al encriptar un mensaje original (texto claro) utilizando una clave simétrica, se genera un texto cifrado. Al desencriptar este texto cifrado, se recupera el mensaje original en su forma clara.

Manipulación del texto claro: Al agregar espacios dentro del texto claro desencriptado, se altera el contenido del mensaje. Por ejemplo, el texto original "HolaMundo" puede convertirse en "Hola Mundo" o "H o l a M u n d o", dependiendo de la ubicación y cantidad de espacios añadidos.

Impacto en el mensaje original:

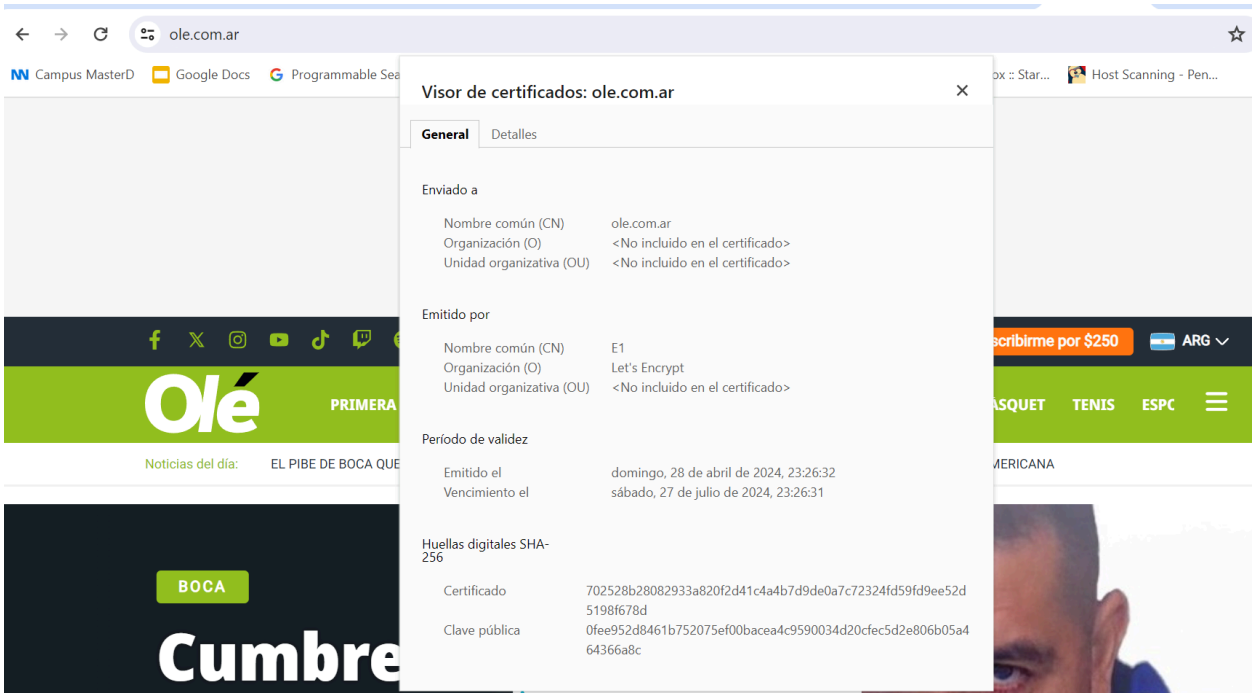
- **Significado:** En muchos casos, agregar espacios puede cambiar el significado del mensaje. Por ejemplo, "buendia" y "buen dia" tienen significados distintos.
- **Integridad del mensaje:** Si el mensaje es estructuralmente sensible, como en el caso de códigos, contraseñas o datos organizados, cualquier modificación puede resultar en un mensaje incorrecto o inutilizable.
- **Reconstrucción:** Si alguien intenta usar el mensaje modificado, es probable que no obtenga los resultados deseados, ya que no coincidirá con el original.

¿Podemos saber la clave pública de un servidor SSL (TLS)? Gráficamente y por comando, si es posible, en sistemas operativos.

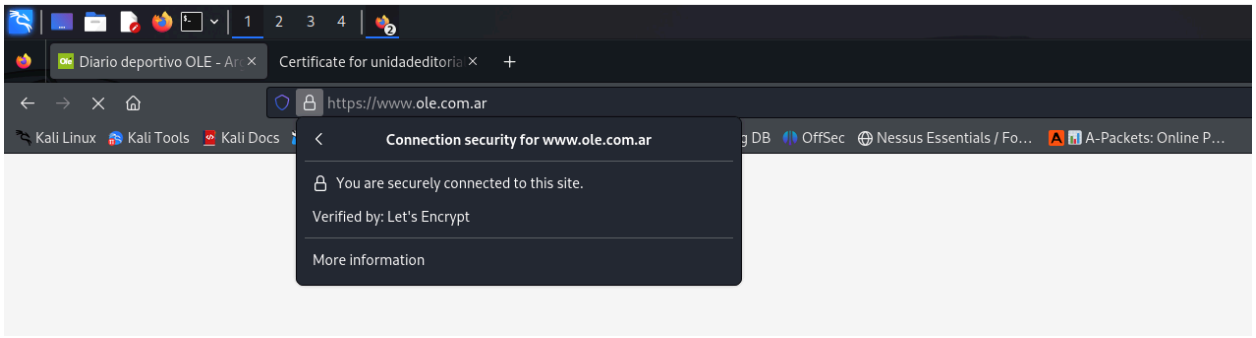
Sí, se puede obtener la clave pública de un servidor SSL (TLS).

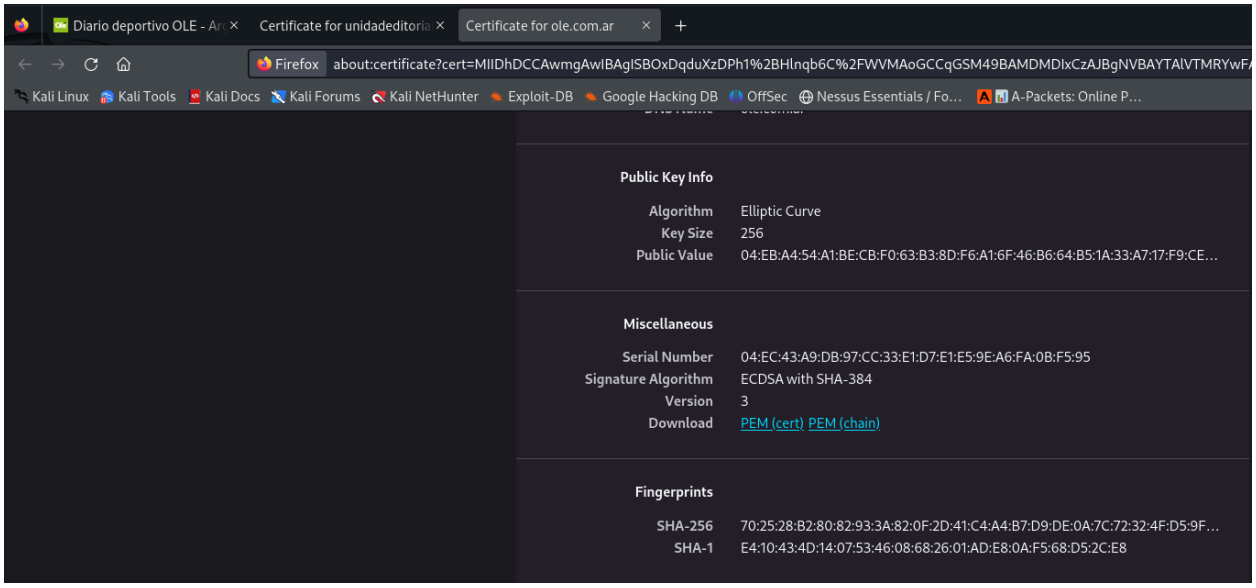
Interfaz gráfica

Google Chrome: Abrir el sitio web, hacer clic en el candado en la barra de direcciones, seleccionar "Certificado (Válido)" y ver los detalles del certificado.



Mozilla Firefox: Abrir el sitio web, hacer clic en el candado, seleccionar la flecha junto al mensaje de conexión segura, hacer clic en "Más información" y luego en "Ver certificado".





Por comando:

Linux: Usar OpenSSL con el comando:

openssl s_client -connect www.ole.com.ar:443 -servername www.ole.com.ar </dev/null | openssl x509 -pubkey -noout

Windows: Usar OpenSSL en Git Bash o PowerShell con el comando:

openssl s_client -connect www.ole.com.ar:443 -servername www.ole.com.ar <NUL | openss

Conclusiones

A través de este análisis, se ha demostrado la importancia de seleccionar y aplicar correctamente las técnicas criptográficas y de codificación según el contexto. Para el cifrado de pendrives, la criptografía simétrica se destaca por su eficiencia y facilidad de uso, mientras que la criptografía de clave pública es esencial para la seguridad de los correos electrónicos. Las funciones hash, por su parte, juegan un papel determinante en la protección de contraseñas, la verificación de la integridad de datos y la detección de malware. Además, se ha clarificado la diferencia entre codificación y encriptación, destacando el uso de sistemas como Base64 para la codificación. Se ha demostrado que la manipulación de datos codificados en Base64 no afecta al mensaje original, en contraste con la manipulación de datos desencriptados, que altera significativamente su integridad y significado. Finalmente, se ha ilustrado cómo obtener la clave pública de un servidor SSL/TLS tanto gráficamente como mediante comandos en distintos sistemas operativos, subrayando la accesibilidad y transparencia de la seguridad en línea. Este trabajo resalta la necesidad de un conocimiento profundo y aplicado de estas técnicas para asegurar la protección de la información en diversos entornos digitales.