

Actividad de clase - Crear códigos

Objetivos

En esta práctica de laboratorio crearán y cifrarán mensajes con herramientas en línea.

Parte 1: Buscar una herramienta de codificación y decodificación en línea.

Parte 2: Cifrar un mensaje y enviarlo por correo electrónico a su compañero.

Parte 3: Descifrar el texto cifrado

Aspectos Basicos / Escenario

Los códigos secretos se han empleado por miles de años. En la antigua Grecia y Esparta se utilizaba una escitala para codificar mensajes. Los romanos utilizaban un cifrado conocido como César para cifrar mensajes. Hace aproximadamente 100 años, los franceses utilizaban la clave Vigenère para codificar mensajes. Actualmente se pueden codificar mensajes de muchas maneras.

Se pueden utilizar varios algoritmos de cifrado para cifrar y descifrar mensajes. Comúnmente, se utilizan Redes Privadas Virtuales (VPN, Virtual Private Network) para automatizar el proceso de cifrado y descifrado.

En esta práctica de laboratorio, trabajarán con un compañero y utilizarán una herramienta en línea para cifrar y descifrar mensajes.

Recursos Necesarios

- Computadora con acceso a Internet

Instrucciones

Parte 1: Buscar una herramienta de codificación y decodificación en línea.

En las redes modernas se utilizan muchos tipos diferentes de algoritmos de cifrado. Uno de los más seguros es el algoritmo de cifrado simétrico llamado Estándar de Cifrado Avanzado (Advanced Encryption Standard, AES). En nuestra demostración utilizaremos este algoritmo.

- a. Busquen “**cifrar y descifrar AES en línea**” en un navegador web. En los resultados de la búsqueda aparecerá una lista con varias herramientas.
- b. Examinar los diferentes enlaces y elijan una herramienta. En nuestro ejemplo, usamos la herramienta disponible de:

<http://aesencryption.net/>

Parte 2: Cifrar un mensaje y enviarlo por correo electrónico a su compañero

En este paso, cada compañero cifrará un mensaje y enviará el texto cifrado al otro.

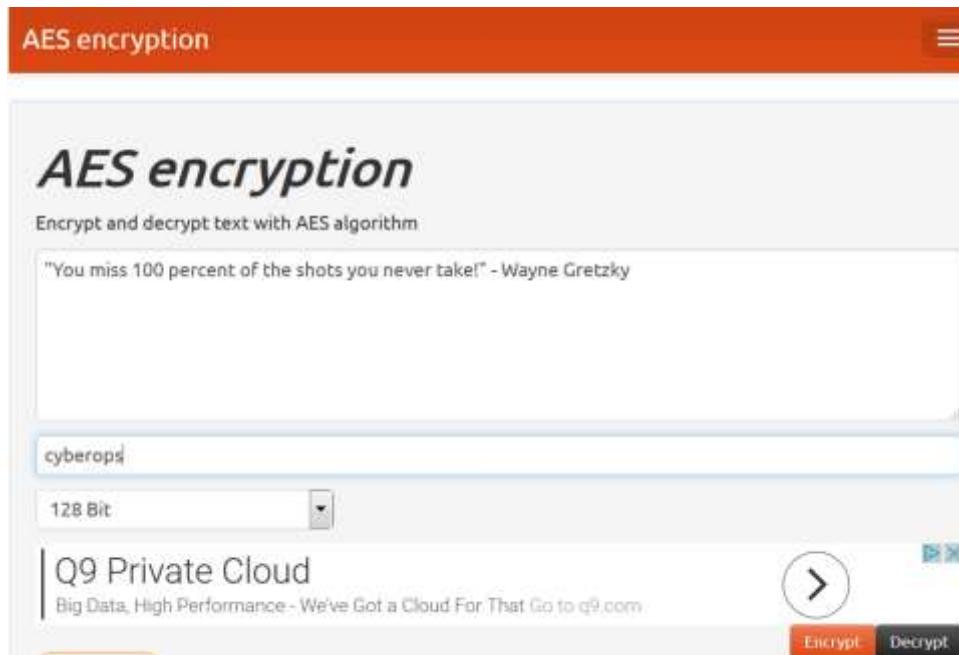
Nota: Los mensajes no cifrados se conocen como texto plano, mientras que a los cifrados se los conoce como texto cifrado.

- a. Escribir un mensaje en texto plano de su elección en el cuadro de texto. El mensaje puede ser muy breve o extenso. Deben asegurarse de que su compañero no vea el mensaje en texto plano.

Usualmente se necesita una clave secreta (es decir, una contraseña) para cifrar un mensaje. La clave secreta se utiliza junto con el algoritmo de cifrado para cifrar el mensaje. Solamente quien conozca la clave secreta podrá descifrar el mensaje.

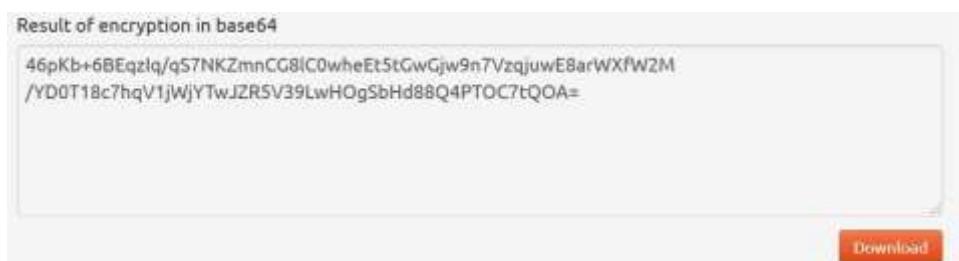
Actividad de clase - Crear códigos

- b. Introducir una clave secreta. Es posible que algunas herramientas les pidan que confirmen la contraseña. En nuestro ejemplo utilizamos **cyberops** como clave secreta.



- c. A continuación, hacer clic en **Encrypt** (Cifrar).

En la ventana “Result of encryption in base64” (“Resultado del cifrado en base64”) verán texto aleatorio. Se trata del mensaje cifrado.



- d. Ahora deben Copiar o Descargar el mensaje resultante.

- e. Enviar el mensaje cifrado a su compañero.

Parte 3: Descifrar el texto cifrado

AES es un algoritmo de cifrado simétrico. Esto quiere decir que las dos partes que se están intercambiando mensajes cifrados deben conocer la clave secreta con antelación.

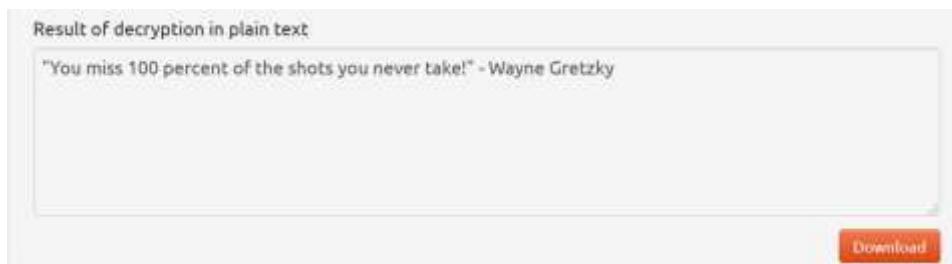
- Abrir el correo electrónico de su compañero.
- Copiar el texto cifrado y péguenlo en el cuadro de texto.

Actividad de clase - Crear códigos

- c. Introducir la clave secreta previamente compartida.



- d. Hacer clic en **Decrypt** (Descifrar) debería aparecer el mensaje en texto plano original.



¿Qué sucede si utilizan una clave secreta incorrecta?