Actividad:

Claves simétricas

Este método emplea una única clave para cifrar y descifrar datos. Este método de cifrado requiere menos procesamiento que el cifrado asimétrico sin embargo es menos seguro.

Para entender el problema que pueden llegar a tener los sistemas de clave simétrica respecto a la seguridad y la eficiencia computacional, se desarrollará la siguiente actividad. correos electrónicos o de mensajes instantáneos para emular el comportamiento de los paquetes de datos que viajan por internet siendo visibles para todos.

Utilizaremos la librería Cryptography para no tener que desarrollar desde ceros los algoritmos de cifrado y enfocar la actividad en la técnica de seguridad.

El algoritmo de encriptado sé que utilizará es el AES, el cual, genera una clave con la que es posible encriptar y desencriptar la información.

Como información para trabajar, utilizaremos mensajes de texto e imágenes. Pida a los estudiantes que se agreguen a la lista de correos o al grupo de mensajería instantánea (puede servir un grupo de Whats'app o de Telegram).

Continúe con la actividad siguiendo las instrucciones del cuaderno adjunto llamado: *ejercicio01: clave_simetrica.ipynb* (También disponible en el repositorio de GitHub del curso).

https://github.com/oscaraen/cursociberseguridad_talento_tech