SESION 4 1ER PARCIAL

Capa de usuarios para la seguridad informática.

Objetivo: al finalizar la sesión el alumno identificara diversas técnicas, estrategias tecnológicas para la capa de usuarios aplicando CRIPTOGRAFIA, manejo de contraseñas seguras.

Consideraciones teóricas:

La administración de la seguridad informática en la capa de usuarios estable los principios de integridad, disponibilidad, protección y salvaguarda de datos, utilizado diversos mecanismos como:

a) criptografía

Es la disciplina computacional en el área de ciberseguridad que se encarga del estudio de los principios, métodos y medio de transformar los datos para ocultar su significado Estudio principios, métodos para ocultar, transformar, garantizar la integridad, autoridad y prevenir repudio.

Se base en criptosistemas modernos y clásicos

Sus elementos base son:

Criptograma. Mensaje encriptado

Cifrador. Ente o elemento aplicador del método

Canal. Medio en que se envía

Generación de claves. Datos de seguridad encriptados o simples

Descifrador. Proceso inverso para generar la información inicial

criptoanálisis. aplicación de algoritmos, técnicas, estrategias criptográficas su función es recuperar claves e información cifrada

tipos de algoritmos criptográficos

a) clásicos. fundamento principal abecedario y sus permutaciones combinaciones

algoritmo inverso

algoritmo cesar

algoritmo de transposición

b) Modernos

Llaves secretas (simetría)

Llave publica (asimetría)

Algoritmo DES o 3DES estándar en encriptación de datos

Funciones Hash

Firmas digitales

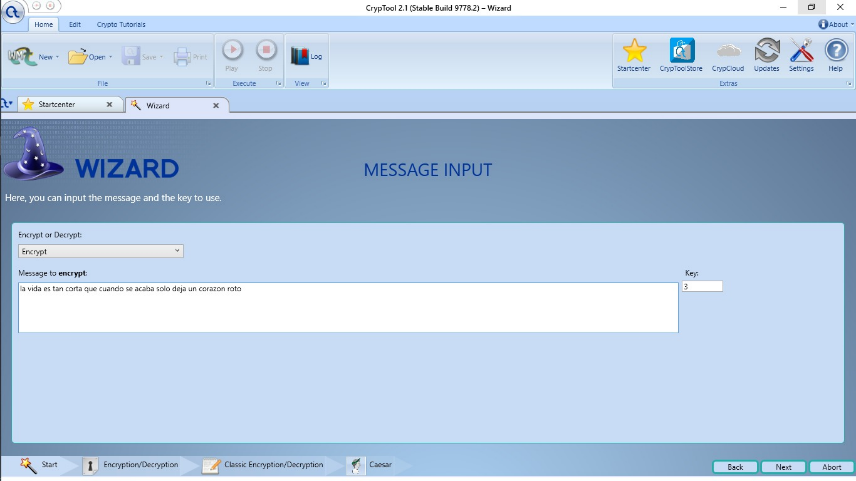
Desarrollo 1. Aplique algoritmo cesar a una frase de tipo ciberseguridad en clave 1 (posición 1 del alfabeto) NIVEL 1 de aplicación de ciberseguridad o protección de datos

“divide y venceras”

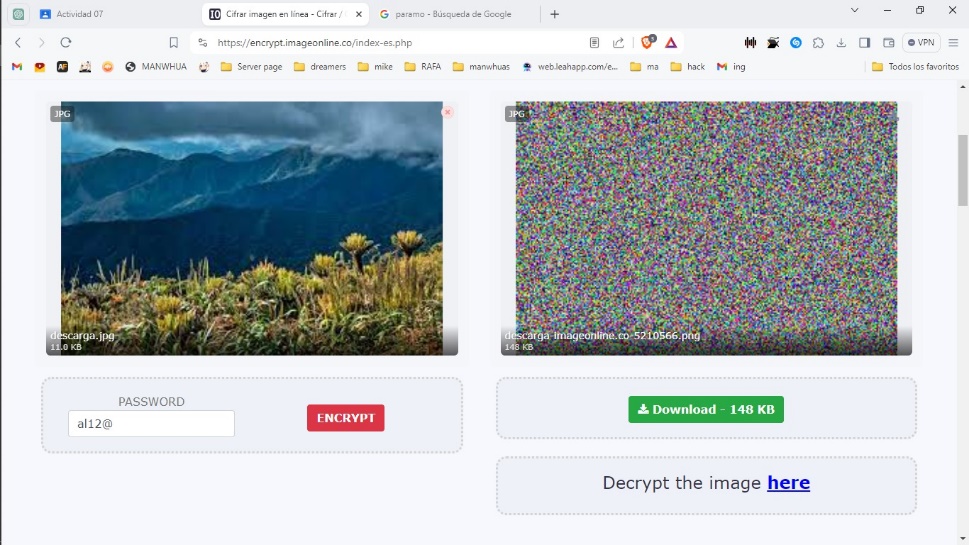
ejwjef z wfñdfsbt

desarrollo 2

descargue e instale la herramienta criptográfica CryptoTool (mensaje 500 algoritmos criptográficos tanto clásicos como modernos) y confirme el descifrado del ejercicio anterior

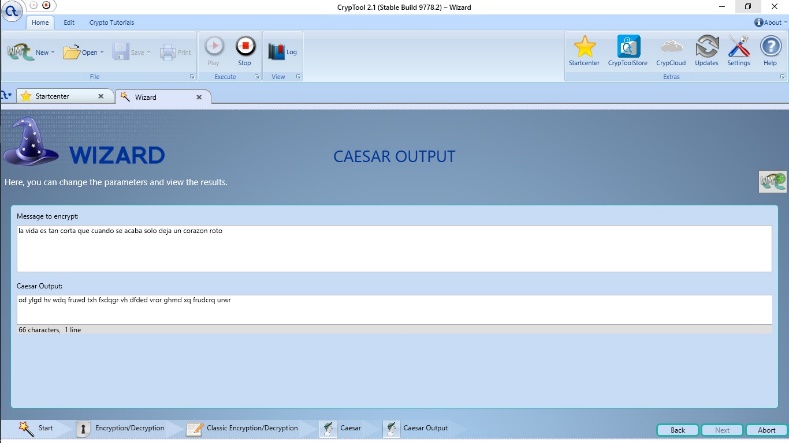


desarrollo 3. Encripte una imagen llamada imagen1crypto\_Alejandro con password algoritmo clásico cesar, guardar y enviar a compañero de trabajo para que le desencripte



DESARROLLO 4

Realice un cripto análisis del sig. Texto cifrado en algoritmo clásico e indique el numero de clave



En conclusión, las herramientas criptográficas son fundamentales para asegurar la confidencialidad e integridad de los datos en el entorno digital. Su correcta implementación y gestión son clave para garantizar una protección efectiva contra las amenazas cibernéticas.