SESION 5 1ER PARCIAL

Criptografía moderna

Objetivo: al finalizar la sesión el alumno identificara algunos algoritmos criptográficos modernos para el tratamiento de información segura

Las técnicas, estrategias, mecanismos que permiten ocultar de forma digital la información y datos se realizan mediante la criptografía modernos se dividen en:

a) Cifrado en flujo

El emisor usa un algoritmo moderno secreto (generar pseudoaleatorio) para generar secuencias binarias, hexadecimales con permutación y factorización. Realizando una misma operación para un descifrado, utiliza una clave.

Ejemplo algoritmo DES estándar de datos encriptado 3DES, Algoritmo 4RC

b) Cifrado en bloque. La información y datos se dividen por secciones y en cada sección se aplicará un algoritmo criptográfico y puede ser en distintos componentes o elementos de envió de la información. Utiliza una clave para cifrar y descifrar IDEA (algoritmo de encriptación de datos internacional), algoritmo Rijndael

Algortimi por hash toma una cadena y regresa un valor de longitud MD% de 128 bits y SHA1, SHA2, SHA3, de 256 bits

c) Cifrado en llave

d) Cifrado por certificados

Desarrollo. Descargue la herramienta Stools para encriptar mensaje en texto (Frase célebre de ciberseguridad) y con el proceso blinder (juntar archivos) en una imagen tipo bmp adjuntar las imágenes y el texto seleccione el algoritmo IDEA

Desarrollo 2. En una imagen BMP guarde las definiciones de algunos autores de administración de seguridad informática

Suba ejercicios a tablón con sus datos precisos

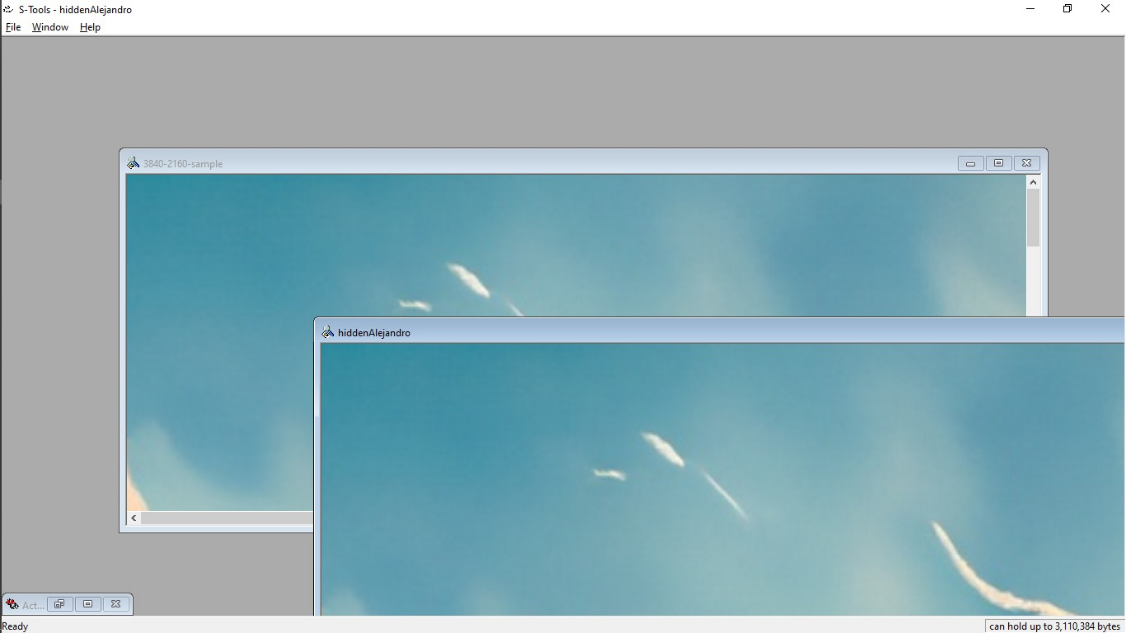
Clave w4S\_=k86U6q=R|h

Password

cfd6f6c95313dd5e91e31b7180fcf69a

esteganografía el arte ocultar.

Aplicar el mismo procedimiento de ocultar la información en un texto clave



Ejemplo

La noche se presenta un cantante famoso donde su éxito mayor es huida y despedida con desesperación no olides nada.

Mensaje principal: esparase a a la medianoche en la plaza es punto de encuentro

Un archivo de texto guardarlo como esteganografiaAlejandro

Conclusión

S-Tools es una herramienta útil para ocultar información dentro de archivos multimedia, proporcionando una forma discreta de compartir datos. Es importante utilizarla de manera responsable y comprender sus limitaciones