TECNICO EN CONTROL DE LA SEGURIDAD DIGITAL

CRIPTOGRAFIA

INTRODUCCION

La criptografía es el estudio y la técnica que se utiliza para proteger la confidencialidad, integridad, autenticidad y no repudio de la información. En un mundo cada vez más digitalizado, donde la transmisión de datos es constante, la criptografía se ha vuelto esencial para garantizar la seguridad de la información y protegerla de posibles ataques o accesos no autorizados

Tipos de Criptografía

Existen varios tipos de criptografía, cada uno con sus propias características y aplicaciones. A continuación, presentaremos los dos tipos principales:

1. Criptografía Simétrica

La criptografía simétrica, también conocida como criptografía de clave secreta, es un sistema en el cual tanto el emisor como el receptor utilizan la misma clave para cifrar y descifrar la información. La ventaja de este enfoque es su rapidez y eficiencia en el procesamiento de grandes volúmenes de datos. Sin embargo, la principal desventaja es la necesidad de compartir la clave de forma segura entre el emisor y el receptor.

2. Criptografía Asimétrica

La criptografía asimétrica, también llamada criptografía de clave pública, utiliza un par de claves: una clave pública, que se comparte abiertamente, y una clave privada, que se mantiene en secreto. El emisor cifra los datos utilizando la clave pública del receptor, mientras que el receptor utiliza su clave privada para descifrarlos. Este enfoque proporciona una mayor seguridad y soluciona el problema de compartir claves de forma segura. Sin embargo, la criptografía asimétrica es más lenta y requiere más recursos computacionales que la criptografía simétrica

Funciones Criptográficas

Las funciones criptográficas son algoritmos matemáticos utilizados para cifrar y descifrar información. Algunas de las funciones criptográficas más comunes son:

- Función de resumen criptográfico: esta función toma una entrada de cualquier tamaño y produce una cadena de salida de tamaño fijo. Las funciones de resumen criptográfico se utilizan para garantizar la integridad de los datos, ya que cualquier cambio en los datos resultará en un valor de resumen completamente diferente.

- Algoritmo de cifrado: estos algoritmos toman los datos en texto claro y los transforman en texto cifrado utilizando una clave. Solo las personas que poseen la clave adecuada pueden descifrar los datos y volverlos legibles.
- Función hash: las funciones hash son similares a las funciones de resumen criptográfico, pero no se utilizan para cifrar o descifrar datos. En cambio, se utilizan para verificar la integridad de los datos, ya que cualquier alteración en los datos resultará en un valor hash completamente diferente.

CONCLUSION

En conclusión, los fundamentos de la criptografía son esenciales para comprender cómo se asegura la confidencialidad, integridad y autenticidad de la información en sistemas de comunicación seguros. A través del estudio de los principios criptográficos, hemos aprendido sobre la importancia de utilizar algoritmos sólidos y claves adecuadas para proteger la información sensible.

Funcionamiento del cifrado simétrico

El funcionamiento del cifrado simétrico se basa en una operación matemática que se aplica a los datos que se desean cifrar. Esta operación se realiza utilizando una clave secreta, que es la que permite transformar los datos originales en información ilegible. La clave utilizada en el cifrado simétrico debe ser secreta y compartida únicamente entre las partes que desean comunicarse de manera segura. El hecho de que se utilice la misma clave tanto para cifrar como para descifrar la información implica que se requiere un alto grado de confianza en la forma en que se maneja y comparte esta clave.

Ventajas del cifrado simétrico

El cifrado simétrico ofrece varias ventajas. En primer lugar, es un método rápido y eficiente, ya que el procesamiento de los datos es bastante simple y directo. Esto hace que el cifrado y el descifrado de la información sean rápidos y no añadan una gran carga computacional.

Además, el cifrado simétrico es adecuado para la transmisión de grandes volúmenes de datos, ya que el tamaño de la clave utilizada no está vinculado al tamaño de los datos a cifrar. Esto significa que, en teoría, se puede utilizar una clave de cualquier tamaño para cifrar cualquier cantidad de datos

Desventajas del cifrado simétrico

A pesar de sus ventajas, el cifrado simétrico también presenta algunas desventajas. Una de ellas es la necesidad de compartir y gestionar la clave secreta entre las partes que desean comunicarse de manera segura. Si esta clave cae en manos equivocadas, la confidencialidad de la información se verá comprometida. Además, el cifrado simétrico no es adecuado para entornos en los que se requiere

una comunicación segura entre más de dos partes. Si se desea asegurar la comunicación entre múltiples participantes, se deberá utilizar un enfoque de cifrado asimétrico, que es capaz de manejar esta situación.

Ejemplos de algoritmos de cifrado simétrico

Existen varios algoritmos de cifrado simétrico ampliamente utilizados en la actualidad. Algunos ejemplos famosos son:

Data Encryption Standard (DES): fue uno de los primeros algoritmos de cifrado simétrico desarrollados en la década de 1970. Sin embargo, debido a su longitud de clave corta, ha sido sustituido por algoritmos más seguros en la mayoría de las aplicaciones.

Advanced Encryption Standard (AES): es uno de los algoritmos más ampliamente utilizados hoy en día. Es considerado seguro y eficiente, y se utiliza en muchas aplicaciones y protocolos de seguridad.

CONSLUSION

En resumen, el cifrado simétrico es un método eficiente y rápido para cifrar y descifrar información utilizando una clave compartida. Hemos explorado el algoritmo AES como una de las opciones más populares para el cifrado simétrico debido a su seguridad y rendimiento. Con los conocimientos adquiridos en este módulo, estamos preparados para aplicar el cifrado simétrico en diversas situaciones que requieran protección de datos.

CIFRADO ASIMETRICO

El cifrado asimétrico, también conocido como criptografía de clave pública, es un método de cifrado utilizado en criptografía moderna. A diferencia del cifrado simétrico, que utiliza una única clave para el proceso de cifrado y descifrado, el cifrado asimétrico utiliza un par de claves diferentes: una clave pública y una clave privada.

¿Cómo funciona?

En el cifrado asimétrico, cualquier persona puede tener acceso a la clave pública, ya que no se considera confidencial. Por otro lado, la clave privada debe mantenerse en secreto. Ambas claves están matemáticamente relacionadas, de manera que la información cifrada con una clave solo puede ser descifrada por la otra clave del par. Para realizar el cifrado, se utiliza la clave pública del destinatario para transformar el mensaje original en un texto cifrado. Este mensaje cifrado solo puede ser descifrado por la clave privada correspondiente, que solo el destinatario posee. Esto proporciona un nivel adicional de seguridad, ya que incluso si alguien intercepta el mensaje cifrado, no podrá descifrarlo sin la clave privada.

Ventajas y desafíos

Una de las principales ventajas del cifrado asimétrico es que no requiere un intercambio previo de claves entre el emisor y el destinatario. Esto es especialmente útil en entornos en los que las partes involucradas no se conocen previamente o no pueden confiar entre sí. Además, el cifrado asimétrico permite la creación de firmas digitales, que son utilizadas para verificar la autenticidad e integridad de un mensaje. Mediante el uso de la clave privada para firmar digitalmente un mensaje, el receptor puede utilizar la clave pública correspondiente para verificar la firma y asegurarse de que el mensaje no ha sido modificado y proviene del emisor legítimo. No obstante, este tipo de cifrado también presenta algunos desafíos. El cifrado asimétrico es computacionalmente más costoso que el cifrado simétrico, lo que puede afectar su rendimiento en aplicaciones donde se requiere un procesamiento rápido de grandes volúmenes de datos. Además, debido a la complejidad matemática involucrada, puede ser más susceptible a ataques criptográficos avanzados si no se implementa correctamente.

Aplicaciones

El cifrado asimétrico se utiliza en diversas aplicaciones que requieren seguridad en la transmisión de datos. Algunos ejemplos comunes incluyen:

Seguridad de correo electrónico: el cifrado asimétrico se utiliza para cifrar los correos electrónicos y proteger la confidencialidad de su contenido.

Transacciones en línea: se utiliza para proteger las transacciones en línea, como compras en comercio electrónico y transacciones bancarias.

Autenticación y firma digital: se utiliza para verificar la identidad de una persona o entidad y garantizar la integridad de los documentos digitales.

En resumen, el cifrado asimétrico es una técnica de cifrado clave pública que proporciona seguridad en la transmisión de datos al usar un par de claves diferentes: una clave pública y una clave privada. Aunque presenta desafíos y es computacionalmente más costoso que el cifrado simétrico, su capacidad para garantizar la confidencialidad y autenticidad de los datos lo convierte en una herramienta esencial en el campo de la criptografía moderna

En síntesis, el cifrado asimétrico ofrece un enfoque innovador para garantizar la seguridad de la comunicación y el intercambio de información. Mediante el uso de claves públicas y privadas, hemos descubierto cómo cifrar y descifrar mensajes sin la necesidad de compartir una clave secreta previamente acordada. El algoritmo RSA ha demostrado ser ampliamente utilizado y confiable en el cifrado asimétrico. Ahora tenemos los conocimientos necesarios para implementar soluciones de cifrado asimétrico en entornos donde la confianza y el intercambio seguro de información son fundamentales.

- Mensaje + clave pública = Mensaje cifrado
- Mensaje encriptado + clave privada = Mensaje descifrado
- Mensaje + clave privada = Mensaje firmado
- Mensaje firmado + clave pública = Autenticación

ACTIVIDADES

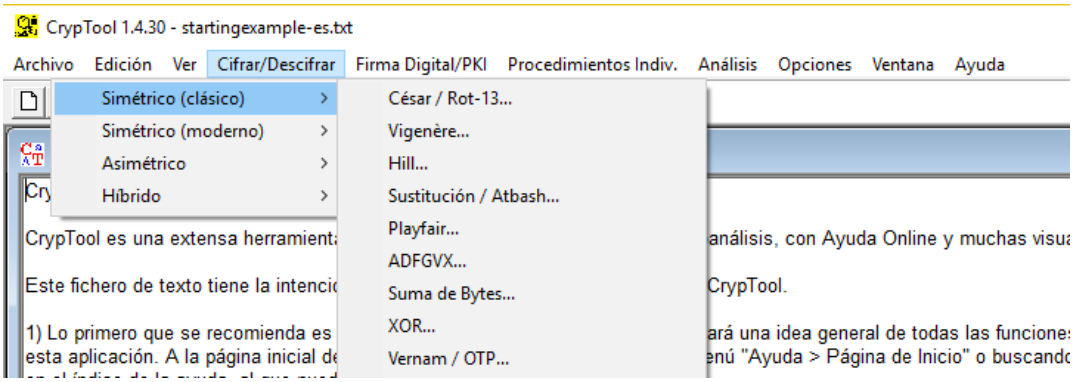
1. Explorar los diferentes tipos de ataques criptográficos, como el ataque por fuerza bruta, el criptoanálisis y el ataque de hombre en el medio. Describir cómo funcionan y qué medidas de seguridad pueden mitigar estos ataques

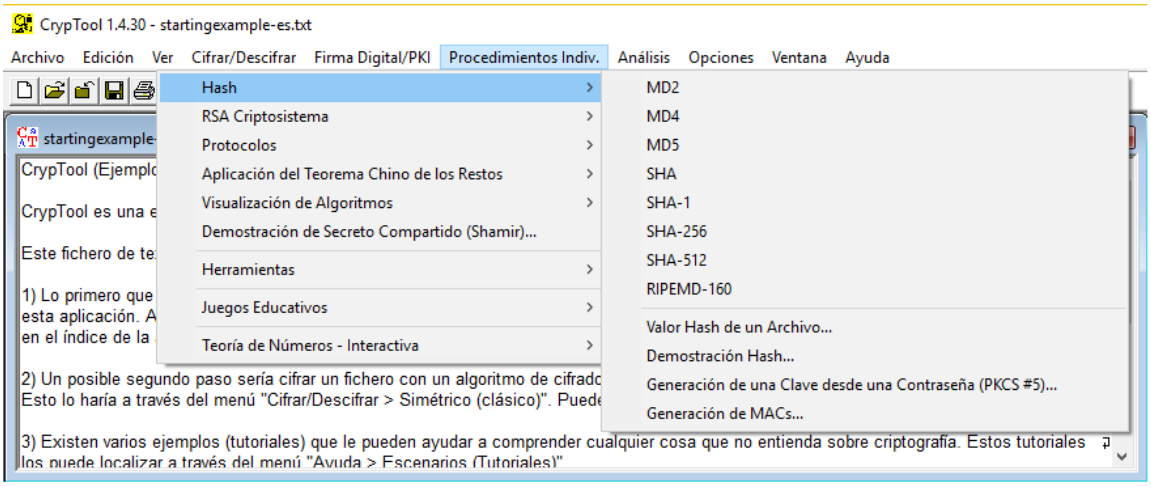
Ejercicios de Encriptación con Cryptool

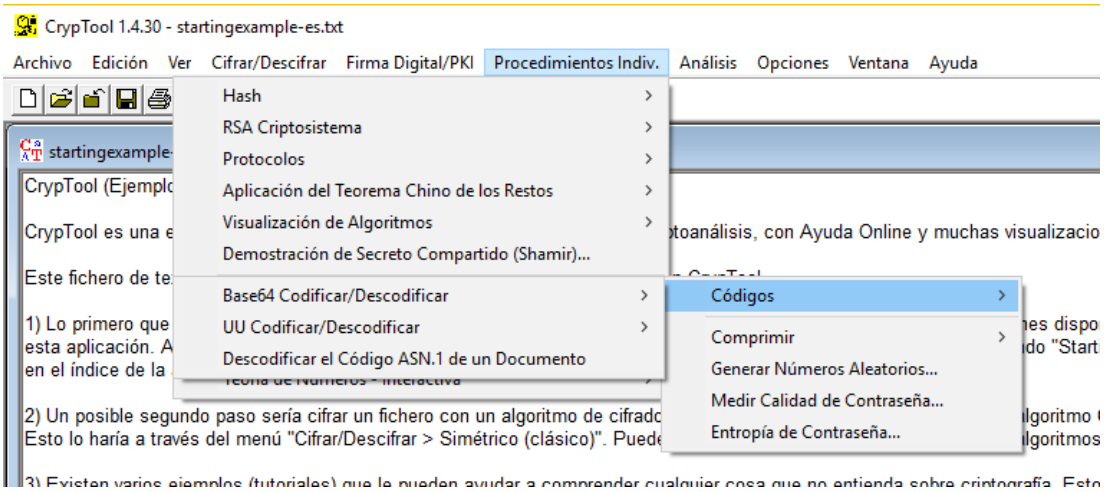
Ejercicio 1:

Descarga e instala la aplicación **Cryptool**. Navega por los menús de la aplicación y localiza los siguientes algoritmos criptográficos: Vigenère, Rijndael, MD5, SHA-256, RIPEMD-160. Localiza también la conversión a/de base64.

Evidencia a entregar (captura o pantallazo señalando los algoritmos)

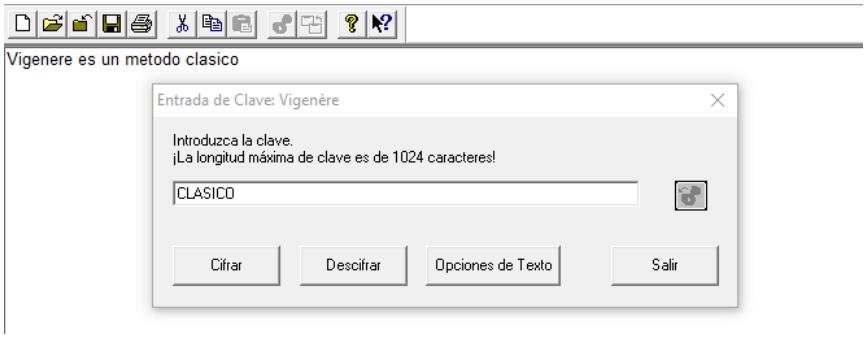


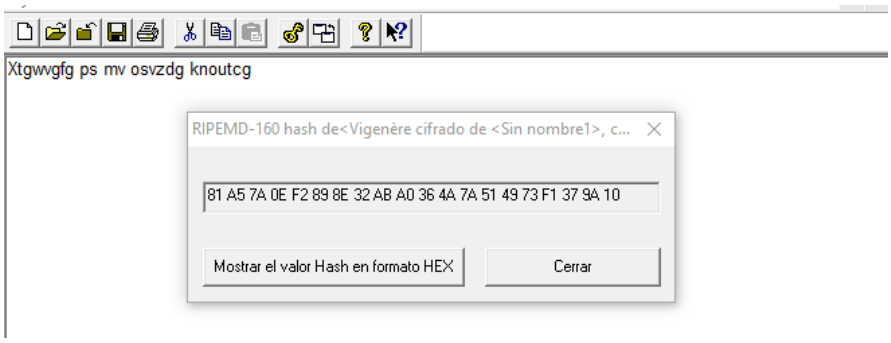




Ejercicio 2:

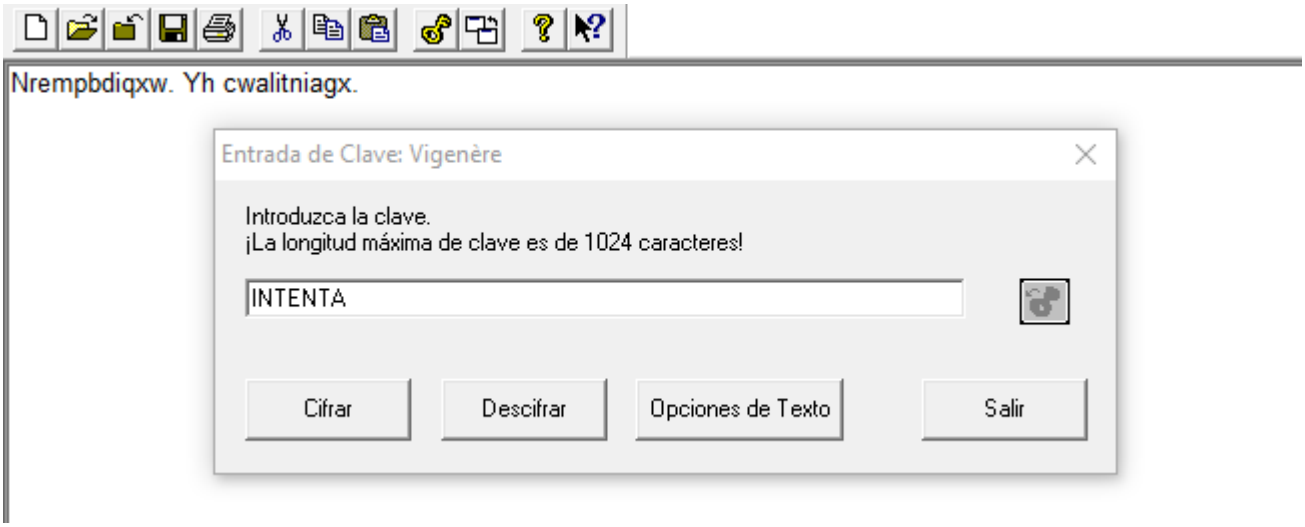
Encripta con el algoritmo de Vigenère el texto "**NOTAS DEL COLEGIO MARISCAL SUCRE 2023**"1 usando la clave "CLASICO". Y verifica que el hash RIPEMD-160 del resultado es "81 A5 7A 0E F2 89 8E 32 AB A0 36 4A 7A 51 49 73 F1 37 9A 10".





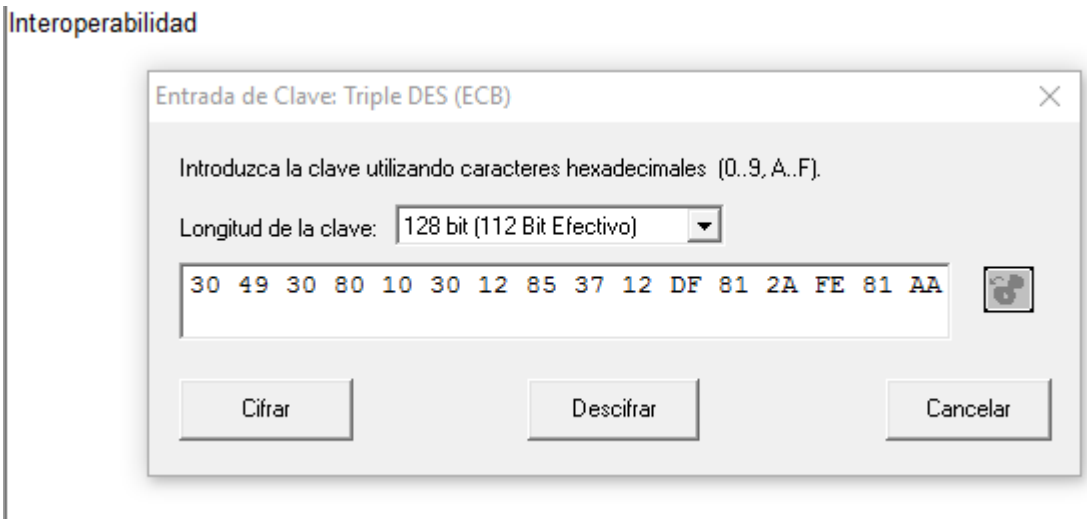
Ejercicio 3:

Desencripta el texto "Nrempbdiqxw. Yh cwalitniagx." mediante el algoritmo de Vigenère usando la clave "INTENTA". Si lo haces bien al desencriptar podrás ver la frase "Felicidades. Lo conseguiste."



Ejercicio 4:

Encripta con Cryptool el texto "Interoperabilidad" usando el algoritmo Triple-DES en modo Electronic Codebook (ECB) con la clave hexadecimal "304930801030128537 12DF812AFE81AA"



Verifica con Cryptool que el hash RIPEMD-160 del resultado es "DD00D19DD412EC76A165951D0152530D6776828A".

EJERCICIO 5.

PRIMER ATAQUE QUE VAMOS A REALIZAR APLICANDO INGENIERIA SOCIAL

Creando el cifrado de flujo RC4

Elige una frase que quieras encriptar y elige una clave de cifrado. En este ejemplo, usaremos: 00 00 00 como clave de cifrado.

- Abre CrypTool.
- Reemplaza el texto por la frase que quieras.
- Haz clic en el menú Cifrar / Descifrar.
- Selecciona Simétrico (moderno) y luego selecciona RC4.
- En la siguiente ventana. Selecciona 24 Bits y como clave de cifrado: Agrega el valor 00 00 00 (o tu frase elegida).
- Pulsa sobre Cifrar.
- Obtendrás el cifrado de flujo.

Atacando el cifrado de flujo

- Haz clic en el menú de Análisis.
- Apunta a Symmetric Encryption (moderno) y luego selecciona RC4.
- En la siguiente ventana. Selecciona 24 Bits e introduce: ** ** ** (sustituye cada carácter de tu frase cifrada por un comodín, dejando los mismos espacios en blanco).
- Haz clic en el botón de Inicio.
- Cuando se complete el análisis, obtendrás resultados, entre los que debería estar tu frase descifrada.

Resumen

- La criptografía es la ciencia de cifrar y descifrar mensajes.

- Un cifrado es un mensaje que se ha transformado en un formato no legible por humanos.
- Descifrar es invertir un cifrado en el texto original.
- El criptoanálisis es el arte de descifrar cifrados sin el conocimiento de la clave utilizada para cifrarlos.
- La criptología combina las técnicas tanto de la criptografía como del criptoanalista.

EJERCICIO 7.

GENERACION DE FIRMA DIGITAL

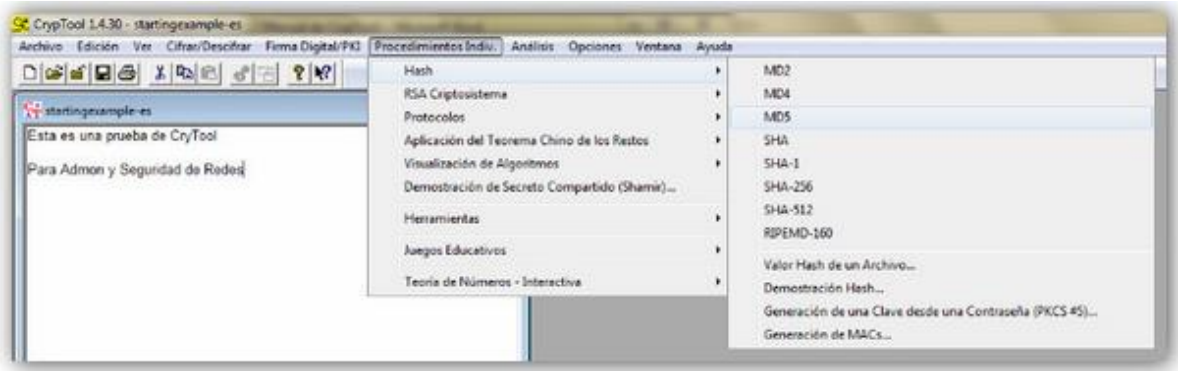
Apreciado Técnico dentro de las técnicas de seguridad a la firma digital en los documentos es importante el reto está en seguir el manual Firma Digital- ADOBE.pdf y realizar su firma digital

NOTA: LOS CINCO PRIMEROS APRENDICES QUE LO REALICEN GANARAN BONIFICACION)

EJERCICIO 8.

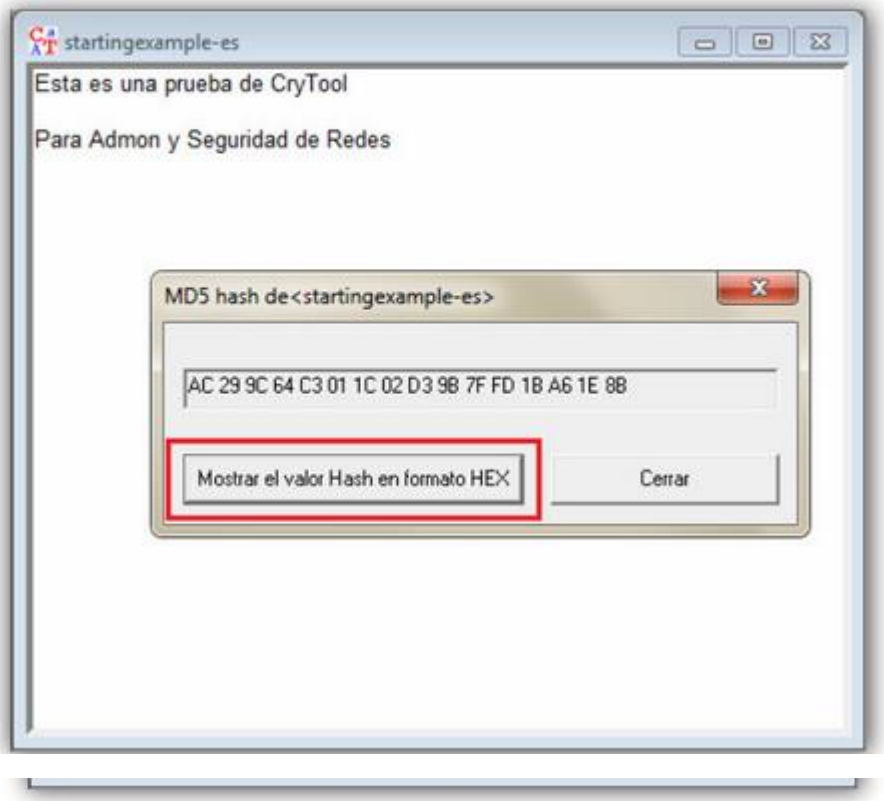
Algoritmo HASH

Genera un archivo plano con el bloc de notas, guardarlo y genere el MD5, anotarlo o tomar pantallazo.



Tome el mismo archivo anterior y modifique el texto agregando la línea, un intruso entro al archivo, y genere nuevamente el HASH con MD5, compárelo e indique si cambio o quedo igual.

Damos click en el botón "**Mostrar el valor Hash en formato HEX**".



Este es el resultado del valor Hash

