Actividades propuestas del libro

Aarón Cañamero Mochales

Las Naves Salesianos

1. Averigua qué es una escítala y explica en qué consistía. Consigue una imagen y referencias web.

Es un sistema de criptografía utilizado por los éforos espartanos para el envío de mensajes secretos.

Está esta formada por varas de grosor variable y una tira de cuero o papiro.



https://es.wikipedia.org/wiki/Esc%C3%ADtala

<https://joseluistabaracarbajo.gitbooks.io/criptografia->clasica/content/Cripto03.html

1. Investiga los orígenes del cifrado Cesar. En qué consiste y qué vulnerabilidades presenta. Crea un mensaje cifrado utilizando este método y entrégaselo a un compañero para que lo descifre.

Se usó con un desplazamiento de tres espacios para proteger sus mensajes importantes del contenido militar.

Consiste en un cifrado por desplazamiento, esto quiere decir que se desplazaba un determinado numero de veces a la izquierda o la derecha.

Hay muchos tipos de cifrado Cesar, se va sumando dependiendo de cual es desde ROT0 a ROT26, esto quiere decir cuanto desplazamiento tiene que hacer a la izquierda o la derecha.

Lo malo esque es demasiado sencillo, y tiene un patrón muy claro, entonces es muy facil de descifrar. Se puede averiguar por fuerza bruta.

Vamos a coger el ROT10.

Mi mensaje es: Aarón es un crak.

Cifrado sería así: **Kkbów ñc ew mbkt.**

1. Cifra el mensaje “Bienvenidos a la criptología” mediante la técnica de sustitución, usando la siguiente tabla de equivalentes.

El mensaje sería este: **KQNVEVQMXB J TJ LAQYCXTOQJ**.

1. Si tenemos seis usuarios que quieren comunicarse por medio de cifrado simétrico, ¿cuántas claves serán necesarias? ¿Cuántas se necesitarían si se aumentara en un usuario más?

Se necesitarían 25 claves. Si se añadiese un usuario más serian 5 claves más, en un total de 30 claves para 7 usuarios.

1. Investiga qué otros algoritmos de clave simétrica existen además de los expuestos en este apartado y explica brevemente en qué consisten.

**3DES**: Este aplica un algoritmo DES, tres veces, puede tener una longitud de clave de 168 bits.

**BLOWFISH:**  Variables seguras, la longitud de la clave es variable y puede ser hasta de 448 bits, lo que permite negociar entre trabajar a alta velocidad.

**Gost**: La clave de 256 bits es fragmentada en ocho subclaves de 32 bits, cada una de las cuales es utilizada cuatro veces en el algoritmo; de las rondas 1 a 24 las subclaves se introducen al algoritmo una por una en orden ascendente; en las rondas 25 a 32 las subclaves se introducen de manera inversa.

1. ¿En qué consiste el cifrado de clave asimétrica? Cita algunos ejemplos, además de los indicados en el texto, de algoritmos de cifrado de este tipo.

Esta emplea dos llaves diferentes en cada uno de los extremos de comunicación. Cada usuario tiene una clave privada y otro pública.

La privada tiene que ser protegida y guardada por el usuario, esta es secreta y no la deberá conocer nadie.

La publica es accesible a todos los usuarios del sistema de comunicación.

Diffie-Hellman.

Criptografía de curva elíptica.

Criptosistema de Merkle-Hellman.

1. Busca en internet una web que permita cifrar online un texto usando el algoritmo MD5 (por ejemplo, la siguiente: ). Cifra el siguiente texto: “Buenos días, soy un alumno”. ¿Cuál es el resultado de cifrar la cadena anterior?

Es el siguiente: **ae9f6c12f8e53493a6d7dee91c6ad49.**

1. Realiza un breve resumen con las características más significativas de los algoritmos hash que se citan en el texto.

**SHA**: Es una familia de funciones Hash, en verdad la primera fue el SHA-0.

**SHA-1**: Esta función hash toma una entrada y produce un valor de 160 bits como resumen del mensaje, se suele representar como un numero hexadecimal de 40 dígitos.

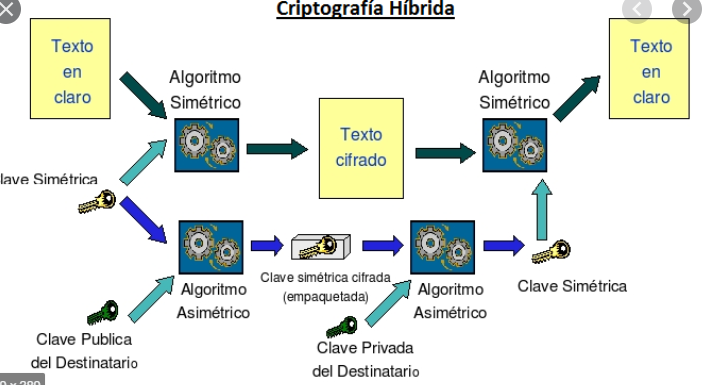
**MD**5: Reduce de 128 bits. Se utiliza para comprobar que algun archivo no haya sido anteriormente modificado.

**RIPE-MD**: Es un algoritmo hash de 128, 256 y 320 bits. Basado en MD4, es similar al SHA-1, este disminuye la posibilidad de colisiones hash accidentales.

1. ¿En qué se basan los criptosistemas híbridos?

Este método usa tanto el cifrado simétrico como el asimétrico. Este utiliza la clave pública para compartir una clave para el cifrado simétrico. Ya que el echo de compartir una clave simétrica no es muy seguro, por ello esa es diferente para cada sesión.

Aquí tenemos un esquema que lo representa muy bien.



1. Indica algunas aplicaciones de los sistemas híbridos nombrados en el texto.

**PGP**: Permite el cifrado de datos, archivos y mensajes mediante la utilización de codificación asimétrica junto la simétrica. Cifrado de ficheros, documentos y discos. Firma digital y cifrado de correos electrónicos.

**OpenPGP**: Sirve para crear mensajes encriptados, firmas, certificados e intercambio de claves privadas. Es el estándar en encriptación de correos electrónicos.

**GnuPG**: Es utilizada para el cifrado y firmas digitales. Es mejor respecto al PGP.

Se utiliza en algunos sistemas operativos, como Linux, MAC o Windows.

Se utiliza en algunos gestores de información personal y de correo electrónico.