



CRIPTOGRAFIA

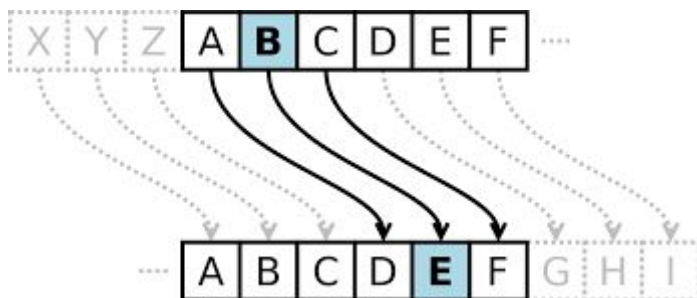
HISTORIA

El primer método sistemático de cifrado lo encontramos en esparta en el siglo V a.c. con el nombre de escítala
ejemplo:

*escítala lacedemonia → método espartano entre generales y responsables del gobierno



*Metodo Cesar: consistió en sustituir cada letra por aquella situada 3 posiciones en el alfabeto



OBJETIVOS

La tarea específica de la criptografía es brindar a la información:

- *confidencialidad
- *seguridad

un sistema criptográfico es seguro respecto a una tarea si un adversario con capacidades especiales no puede romper esa seguridad

TIPOS DE CRIPTOGRAFÍAS

- *criptografía simétrica(privada): se apoya en una sola clave secreta es decir sólo utiliza una clave para cifrar y descifrar
- *asimétrica(pública): se apoya en una pareja de claves que utiliza una clave pública para cifrar y una privada para descifrar

HONEYPOT

es un mecanismo de detección de posibles ataques al sistema consiste en datos que parecen ser una parte legítima que parece contener información o un recurso de valor que los atacantes podrían usar para sus fines.
se cree que lo utilizan las policías o medios de inteligencia es como una especie de sebo.

honeypots de produccion:

- *dan poca información de los atacantes
- *son fáciles de implementar
- *son utilizados por las grandes corporaciones.

Un **hacker de sombrero negro** (o **hacker de sombrero negro**) es un pirata informático que viola la seguridad informática para beneficio personal o malicia.

honeypots de investigación:

son utilizados para recopilar información sobre motivos y tácticas de los de sombrero negro se utilizan para detectar vías de posibles ataques para que las empresas recopilen información sobre donde mejorar la seguridad.

SEGURIDAD EN REDES TELEMÁTICAS

Los 7 servicios de seguridad son

- *Autenticación de entidades
- *Confidencialidad de datos
- *Integridad de datos.
- *Control de acceso
- *El no repudio
- *Disponibilidad
- *Anonimato

FIREWALL

Cortafuegos y firewall es lo mismo

Tipos de cortafuegos:

- *Cortafuegos de pasarela
- *Cortafuegos de capa de red
- *Cortafuegos de Aplicación
- *Cortafuegos Personales

investigar conceptos como honeypots,UTM

MALWARE

malware es el nombre colectivo para referirse a diferentes tipos de software malicioso,consiste en código desarrollado por ciberatacantes,diseñado para causar un daño extensivo a datos o sistemas o para ganar acceso no autorizado a una red.

normalmente se entrega en forma de enlaces y que requiere que el usuario clique,al clicar se instala el archivo con el software malicioso .

Tipos de malware

-Virus:causan daño al núcleo del sistema,corrompiendo ficheros y bloqueando el sistema(ordenadores al usuario) al usuario.

-Worms(gusanos):ellos parten de un ordenador infectado y continúan su infección rápidamente a otros sistemas a través de USB u otros dispositivos.

-Spyware:estos a través de tu teclado pueden almacenar información de lo que tu tecleas y así poder recolectar información de contraseñas,etc

-Trojanos: son software que abren puertas traseras para que otros malware se instalen.así como los griegos introdujeron un caballo en forma de regalo en la ciudad de troya

-Ransomware:este es un tipo de malware que tiene como objetivo las grandes empresas de hoy en día. El ransomware te bloquea el acceso hasta que pagues una cuota de dinero por el rescate de tu ordenador.