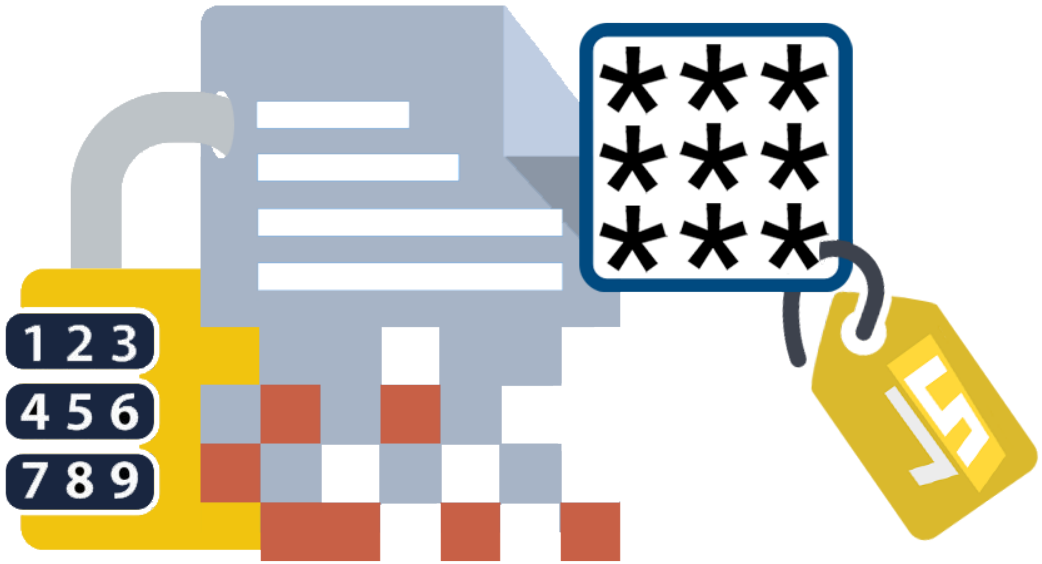
Curso de bastionado de redes y sistemas

areaproject

2. Administración de credenciales de acceso a sistemas

Aplicación de la criptografía a la seguridad de la información
Técnicas para el cifrado de información confidencial
Certificados digitales, gestión de una PKI
Aplicación de firma digital
Políticas y Procedimientos de seguridad para los procesos de autenticación
Autenticación de dos factores, utilización de tarjetas criptográficas
Sistemas de Single Sign On SSO

2.1.Aplicación de la criptografía a la seguridad de la información



Cifrado de información

- ✓ El cifrado se lleva a cabo mediante unos algoritmos que garantizan la confidencialidad (solo lo leen las personas autorizadas), autenticación (el emisor de un mensaje se puede verificar) y integridad (no se ha modificado) de la información.

- ✓ Los procesos de cifrado son capaces de convertir los datos de texto claro a texto cifrado y viceversa.

Técnicas para el cifrado de información

- ✓ Tipos de cifrados
  - Cifrado por sustitución
  - Cifrado por transposición
  - Cifrado simétrico / asimétrico
  - Cifrado Híbrido
  - Cifrado RSA
  - Curvas elípticas

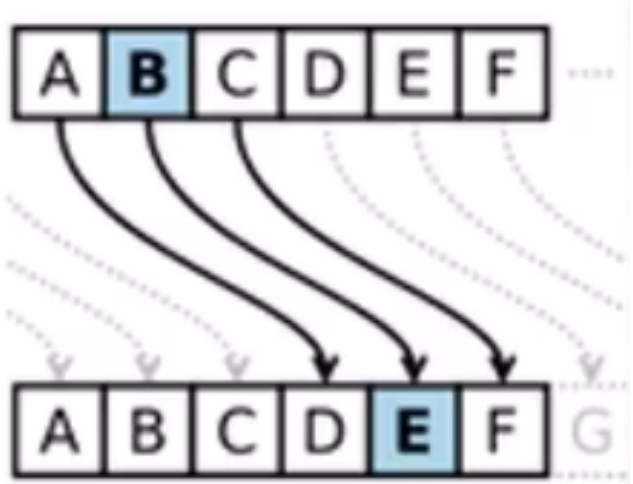
Tipos de cifrado: Sustitución

- ✓ Se sustituye cada carácter del texto plano por otro carácter en el texto cifrado (criptograma)

- ✓ Tipos:
  - Sustitución monográfica mono alfabeto (PE=CESAR)
  - Homófonos (Un carácter se cifra con más de uno)
  - Sustitución monográfica poli alfabeto (Utilizan sustituciones múltiples aplicando 2 o más alfabetos)
  - Sustitución poligráfica mono alfabeto [(se cifran por poligrama n>1) polybios, playfair, hill]

Tipos de cifrado: Sustitución (CESAR)

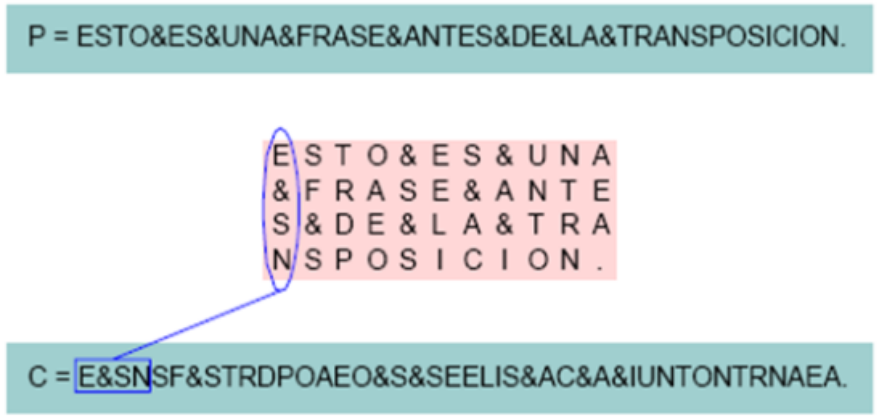
- ✓ Se aplica un desplazamiento constante igual a 3 caracteres sobre el texto a cifrar
- ✓ Ejemplo, la letra “B” será una “E” y la “C” será una“F”



Tipos de cifrado: Transposición

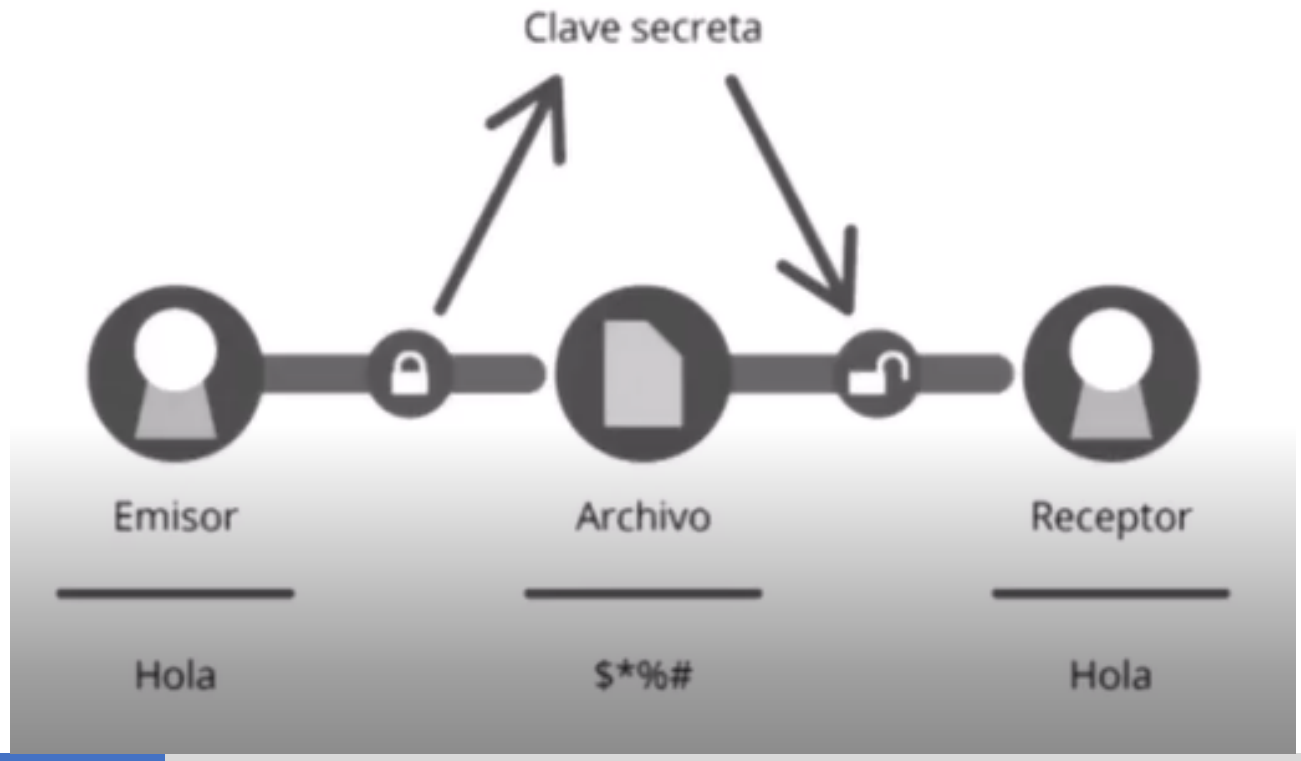
- ✓ Se reordenan los caracteres del texto en claro barajándolos siguiendo un esquema bien definido. Tipos:
  - ✓ Grupos: Por medio de permutaciones
  - ✓ Series: Se ordena el mensaje como cadena de submensajes
  - ✓ Columnas / Filas
  - ✓ Chino

- ✓ Ejemplo:



Tipos de cifrado: Simétrico

- ✓ Se cifra y descifra la información con una misma clave, la cual es conocida por el emisor y receptor previamente.



Simétrico: Ventajas-Desventajas

- ✓ Ventajas
  - ✓ La distribución de claves es muy sencilla
- ✓ Desventajas
  - ✓ La distribución de claves es poco segura
  - ✓ El numero de claves necesarias para comunicarse entre un grupo de personas es muy elevado, cada uno tendrá la suya propia

Algunos algoritmos y tecnologías de clave simétrica son:

DES, 3DES, RC4, RC5, RC6, AES, Blowfish, IDEA…

Híbridos: Cifrado simétrico por bloques

- ✓ Cifrado DES
  - Este algoritmo está diseñado para cifrar y descifrar bloques de datos que constan de 64 bits bajo el control de una clave de 56 bits (simétrico) Los otros 8 bits restantes se utilizan para comprobar la paridad.
  - Se considera inseguro actualmente.
- ✓ Cifrado AES
  - Es un algoritmo capaz de proteger información sensible el cual trabaja repitiendo la misma operación múltiples veces con un bloque fijo de 128 bits y tamaños de llave de 128, 192 o 256 bits
  - Actualmente no se conocen vulnerabilidades de este cifrado.

Híbridos: RCx

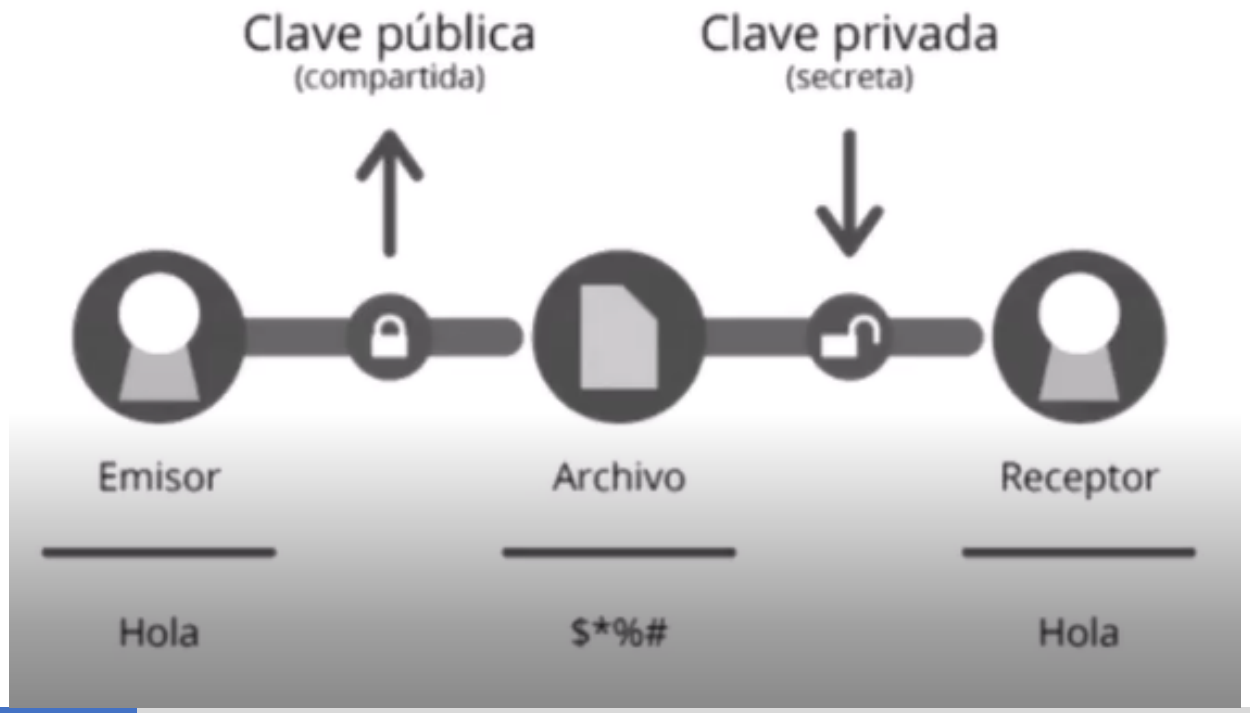
- ✓ RC4 es el sistema de cifrado de flujo con bytes orientados a operaciones, se emplean en algunos protocolos como SSL para proteger el tráfico o WEP para añadir seguridad en redes inalámbricas, pero es muy inseguro.

- ✓ RC5 es un algoritmo de cifrado por bloques con tamaño variable (34,68 o 128 bits) con un tamaño de llave variable, así como un numero variable de vueltas (0/255)

- ✓ RC6 es una unidad de cifrado por bloques de clave simétrica derivada a partir de RC5.

Tipos de cifrado: Asimétrico

- ✓ Emplea diferentes claves para cifrar y descifrar el mensaje.
- ✓ Se cifra con la clave pública y se descifra con la clave privada.



Asimétrico: Ventajas-Desventajas

- ✓ Ventajas
  - La distribución de claves es más segura. Se distribuye la clave pública manteniendo la privada para el uso exclusivo del propietario
- ✓ Desventajas
  - Para una misma longitud de clave y mensaje se necesita mayor tiempo para su procesamiento
  - Las claves deben ser de mayor tamaño que las simétricas
  - El mensaje cifrado ocupa más espacio que el original

Algunos algoritmos y tecnologías de clave asimétrica son:
RSA, DSA, ElGamal, Diffie-Hellman, Goldwasser-Micali

Tipos de cifrado: RSA

- ✓ Es un sistema criptográfico de clave pública (asimétrico)
- ✓ El cifrado RSA es ampliamente utilizado y de hecho es uno de los sistemas de cifrado estándar.
- ✓ Este sistema emplea aritmética modular y teorías de números elementales para realizar cálculos empleando dos números primos altos.
- ✓ Es el algoritmo más utilizado de este tipo y es válido tanto para cifrar como para firmar digitalmente.

2.2.Usos de cifrado en informática

GnuPG

- ✓ Software libre que funciona como herramienta de cifrado y firmas digitales que viene a remplazar a PGP
- ✓ No utiliza algoritmos de cifrado que estén restringidos por patente
- ✓ GPG cifra los mensajes usando pares de claves individuales asimétricas generadas por los usuarios
- ✓ Tiene un repositorio de claves donde guarda todas las que tenemos almacenadas en nuestro sistema ya sean públicas o privadas

Funciones Hash

- ✓ El nombre de **hash** se usa para identificar una **función criptográfica** cuyo **objetivo primordial consiste en codificar datos para formar una cadena de caracteres única.** Todo ello sin importar la cantidad de datos introducidos inicialmente en la función. **Estas funciones sirven para asegurar la autenticidad de datos, almacenar de forma segura contraseñas, y la firma de documento electrónicos.**
- ✓ Los hashes criptográficos **se utilizan principalmente para:**
  - ❖ **proteger las contraseñas y no guardarlas en texto claro en una base de datos**.
  - ❖ **para detectar malware**
  - ❖ **asegurar la integridad de los mensajes o ficheros.**

- ✓ Criptografia Algoritmos Hash

Usos comunes de cifrado

- ✓ Correo electrónico
- ✓ Navegación por Internet
- ✓ Firma electrónica
- ✓ Conexiones seguras a máquinas: SSH
- ✓ Intercambio de ficheros: SFTP, FTPS
- ✓ Introducción de información sensible en una BBDD




Usos comunes de cifrado: Correo electrónico

- ✓ Utilizan el estándar S/MIME basado en las normas PKCS#7
- ✓ Aplican cifrados simétricos con claves autogeneradas y luego dichas claves se cifran con algoritmos asimétricos.
- ✓ El cifrado email también puede incluir la autenticación.
- ✓ La mayoría de clientes de email proveen soporte nativo para S/MIME para resguardar la firma digital de emails y el cifrado de mensajes utilizando certificados.
- ✓ Otras opciones de cifrado incluyen PGP y GNU

Usos comunes de cifrado: Navegación por internet

- ✓ Uso del protocolo seguro HTTPS en lugar de HTTP.
- ✓ Se usan certificados para comprobar la veracidad de los sitios.
- ✓ Al usar HTTPS se solicita la clave pública del servidor y luego se establece la comunicación mediante algoritmos simétricos.
- ✓ En caso de ser interceptada la transmisión los datos al ir cifrados no serán legibles.

Usos comunes de cifrado: Firma electrónica

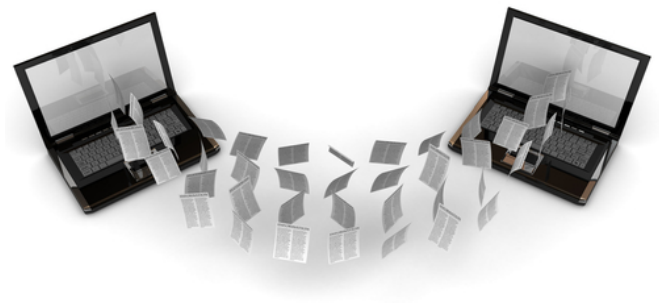
- ✓ Las funciones básicas son:
  - Identificar al firmante de manera inequívoca
  - Asegurar la integridad del documento firmado y que no ha sufrido alteración o manipulación. (Funciones Hash)
  - Asegurar el no repudio del documento firmado, los datos para firmar son únicos y exclusivos y al firmarse serían igual que documentos firmados en papel.

Usos comunes de cifrado: Conexiones seguras a máquinas con SSH

- ✓ Secure Shell o intérprete de órdenes seguro.
- ✓ Sirve para acceder a servidores privados y manejarlos por completo mediante un intérprete de comandos.
- ✓ SSH trabaja de forma similar a como se hace con telnet pero usa técnicas de cifrado que hacen que la información viaje segura evitando que puedan descubrir el usuario y contraseña de la conexión.

Usos comunes de cifrado: Intercambio de ficheros con FTPS, SFTP

- ✓ FTPS: FTP/SSL realiza transferencias FTP seguras, conlleva el uso de una capa SSL/TLS debajo del protocolo FTP para cifrar los canales de control y/o datos.
- ✓ SFTP: Es un protocolo nuevo, en sí no facilita la autenticación y seguridad, sino que espera que el protocolo subyacente asegure a este.



Usos comunes de cifrado: Bases de Datos

- ✓ Cada empresa valora que datos son críticos y valiosos como para ser cifrados teniendo en cuenta la caída de rendimiento que tendrá el sistema
- ✓ Pueden cifrar toda la base de datos, objetos y datos de usuarios
- ✓ Si cifran las aplicaciones de la organización y la base de datos al conectar con la aplicación, esta deberá proporcionar la clave de cifrado
- ✓ Si quieres cifrar la base de datos, debes crearla como cifrada
- ✓ Las técnicas para trabajar con una base de datos cifrada son iguales a las de trabajar con una no cifrada

Herramientas de cifrado de información

- ✓ VeraCrypt
  - Solución de cifrado Open Source basado en TrueCrypt
  - Utiliza la misma interfaz y características con la diferencia que incluyen un número mayor de posibilidades para el cifrado de la información.
  - Incluye algoritmos de cifrado tales como AES, Twofish y Serpent.

- ✓ DiskCryptor
  - Open Source para el cifrado de particiones y disco duro completo, podemos cifrar archivos, particiones, usb…
  - Usa algoritmos de cifrado como AES, Twofish y Serpen

Herramientas de cifrado de información

- ✓ OpenPuff / OpenStego
  - Herramienta Open Source para Windows
  - Fue una de las primeras herramientas de estenografía
  - Soporta imágenes BMP y JPG, archivos MP3 y WAV entre otros
  - Podemos enviar mensajes ocultos dentro de una imagen o cualquier archivo multimedia

Herramientas de cifrado de información

- ✓ OpenSSH
  - Herramienta Open Source de acceso remoto a través de IP.
  - Es una alternativa perfecta al protocolo Telnet.
  - Podemos conectarnos de manera segura a un dispositivo en la red al ir cifrada la conexión.

- ✓ GnuPG
  - Implementación libre de PGP (Pretty Good Privacy)
  - Permite el cifrado y firma de datos y de comunicaciones.

Herramientas de cifrado de información

- ✓ Tor Browser
  - Aplicación de código abierto que ayuda a mantener la privacidad al navegar por Internet conectándonos a una red P2P totalmente cifrada y usando el algoritmo AES.
- ✓ OpenSSL
  - Implementa Open Source del protocolo SSL.
  - Este protocolo permite el cifrado de información a través de la red.
  - Es utilizado para realizar de manera segura la mayoría de transacciones financieras en línea. Usado como solución de VPN, como alternativa al protocolo IPSEC.

Prácticas

Prácticas 2.1-2.5 Cifrado y Firma de datos

areaproject

Curso de bastionado de redes y sistemas