**TEMA 1-SEGURIDAD LOCAL**

**(sistema seguro no existe pq no existe seguridad al 100%)**

Sistema Informático

● Hardware

● Software

● Humanware

● Información/datos

● Servicios (google, youtube...)

**\*CARACTERÍSTICAS PRINCIPALES:**

* **C**onfidencialidad: los elementos del sistema solo serán visibles a los usuarios o grupos autorizados.
* **I**ntegridad: los elementos del sistema sólo serán modificados por los usuarios o grupos autorizados.

(lo contrario de corrupto, se mantiene la info. principal)

* **D**isponibilidad: los elementos del sistema estarán disponibles solo para usuarios o grupos autorizados. (Datos e info siempre disponibles para todos)
* **A**utenticación:dar acceso al sistema solo a los usuarios o grupos autorizados.

(“verificar que de verdad es tal”)

* **N**o repudio (registro de la modificación..)
* **F**iabilidad

**\*CATEGORÍAS DE ATAQUE (MILF):**

* Intercepción: Interceptar un servicio .Contra confidencialidad.
* Interrupción: Parar un servicio,ataq ue . Contra disponibilidad.
* Modificación: Alteración o modificación de un archivo.Contra la integridad.
* Fabricación (me invento una info nueva), contra autenticación y fiabilidad.

**\*MEDIDAS DE SEGURIDAD (PRADA):**

* ***P****revención:* todas las medidas para prevenir algún ataque.
* ***R****estauración:* si ya ha causado problema y no lo hemos detectado, intentamos dejar las cosas tal cual estaban. (Copia de seguridad, puntos de restauración)
* ***A****nálisis forense:* investigar qué ha pasado/Datos para denunciar.

Ver de qué forma han entrado para que no vuelvan a suceder.

* ***D****etección:* cuanto antes se detecte un ataque antes podemos remediarlo.

**\*RIESGOS (FILOSOFA)**

* *Físicos* (meteorológicos, una subida de tensión)
* *Lógicos* (un programa que no esté del todo bien programado, windows 10)
* *Factor humano*
* Pasivo: no altera nada.
* Activo: si altera.

**\*MEDIDAS DE ACCESO (ELBIOLOFO)**

Lo que eres: huella dactilar

Lo que tienes: llave

Lo que sabes: código

1. **Físicas:** vallas, puerta, vigilante.
2. **Lógicas:** contraseña.
   * Contraseña BIOS
   * Usuario con contraseña del SO
     + Windows (administrador, usuario (adm), invitado)
     + Linux (root, usuario (adm))
3. **Biométricas:**huella dactilar, escáner de retina.
4. **Electrónicas:** el metro.

**\*MEDIDAS DE PROTECCIÓN DE LA INFORMACIÓN**

* + Usuarios y permisos
    - Windows (ACL’S→listas de control de acceso: para cada fichero se pregunta si el usuario tiene permiso o no, pero casi todo es accesible)
    - Linux (modelo ugoa-rwx)
  + Criptografía: escritura oculta, la información la alteró para que directamente no tenga ningún sentido, no se pueda entender, es reversible, solo para el que lo ha creado.
  + Información redundante, ej: te compras 2 pares de zapas x si te falla una. En vez de duplicar toda la información, se duplica parte, para poder recuperarla en caso de algún error/fallo.
    - Sistema de archivos (“diario”) Ej:NTFS
    - Checksum, CRC, códigos… (paridad, hamming): detectores/correctores de errores

**\*MEDIDAS DE RESPALDO DE LA INFORMACIÓN**

* + Copia de Seguridad (Backup)
  + Clonación
  + Congelación (snapshot)

**\*ALMACENAMIENTO SEGURO**

* + +RAID: Redundant Array of Independent Disks
  + Almacenamiento compartido

**\*PROTECCIÓN LÓGICA**

* + Actualizaciones
  + Antivirus (prevencion, deteccion, desinfección)

**\*RESTAURACIÓN**

* + Live cd/usb

**TEMA 2-CRIPTOGRAFÍA**

* **“ESCRITURA OCULTA”**
* **HISTORIA**
  + **Escítala (Espartanos):** El sistema consistía en dos varas del mismo grosor que se entregaban a los participantes de la comunicación. Para enviar un mensaje se enrollaba una cinta de forma espiral a uno de los bastones y se escribía el mensaje longitudinalmente, de forma que en cada vuelta de cinta apareciese una letra de cada vez. Una vez escrito el mensaje, se desenrollaba la cinta y se enviaba al receptor, que sólo tenía que enrollarla a la vara gemela para leer el mensaje original.
  + **César**

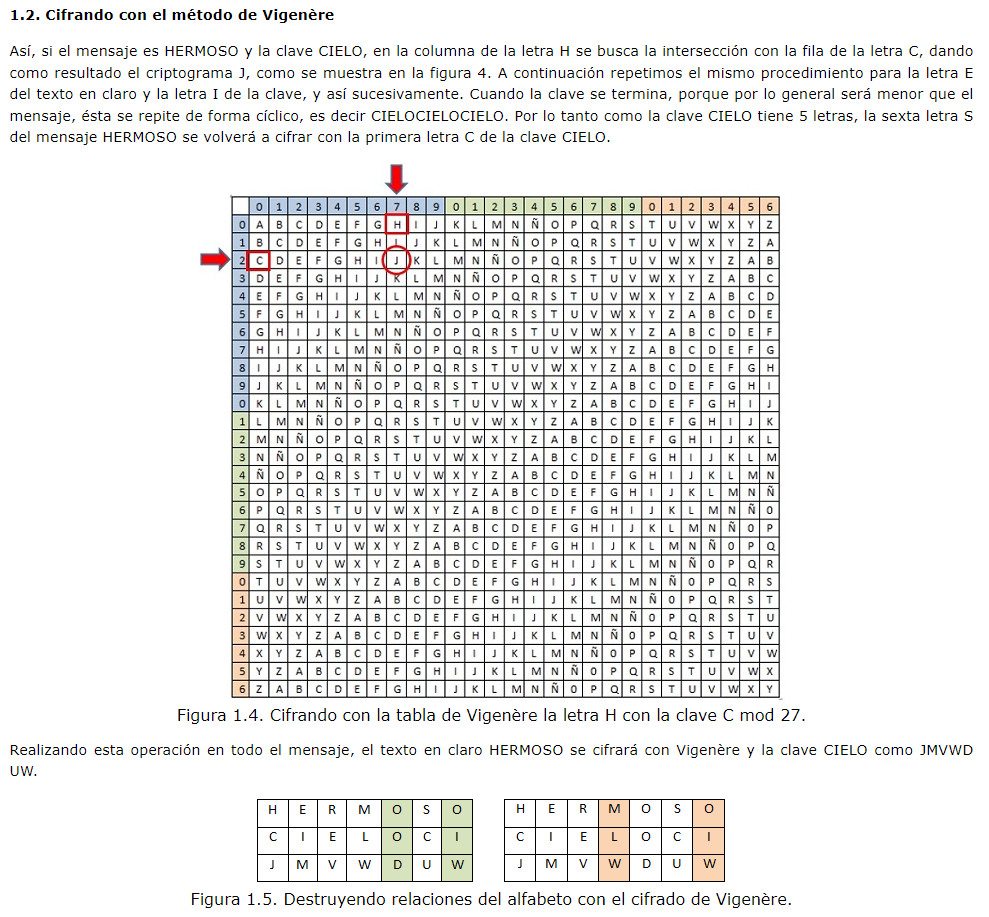
Ej: mensaje= hola buenos dias

coges el abecedario ABCDEFGHIJKLMNÑOPQRSTUVWXYZ

Y cambias cada letra por la tercera de la derecha:

H = K

O = R

* + **Blaise de Vigenère:** 
* **Máquina Enigma (Alan Turing) - Test de turing:** es un examen de la capacidad de una máquina para exhibir un comportamiento inteligente similar al de un ser humano o indistinguible de este. Alan Turing propuso que un humano evaluará conversaciones en lenguaje natural entre un humano y una máquina diseñada para generar respuestas similares a las de un humano. El evaluador sabría que uno de los participantes de la conversación es una máquina y los intervinientes serían separados unos de otros. La conversación estaría limitada a un medio únicamente textual como un teclado de computadora y un monitor por lo que sería irrelevante la capacidad de la máquina de transformar texto en habla. En el caso de que el evaluador no pueda distinguir entre el humano y la máquina acertadamente (Turing originalmente sugirió que la máquina debía convencer a un evaluador, después de 5 minutos de conversación, el 70 % del tiempo), la máquina habría pasado la prueba. Esta prueba no evalúa el conocimiento de la máquina en cuanto a su capacidad de responder preguntas correctamente, solo se toma en cuenta la capacidad de esta de generar respuestas similares a las que daría un humano.
* **TIPOS DE CIFRADO**
  + Simétrico: misma clave para cifrar y descifrar. (DES, 3DES, RC5, AES, Blowfish)
  + Asimétricos: una clave para cifrar, otra clave distinta para descifrar (Diffie-Hellman, RSA, DSA)

CLAVE:

* + - cifrar/descifrar pública (no sirve, cualquiera puede descifrar)
    - cifrar/descifrar privada (como un sistema simétrico)
    - cifrar pública, descifrar privada (“buzón”,ejemplo: banco, la gente cifra pero solo el banco descifra. A mi me llegan muchos mensajes pero solo los leo yo)
    - cifrar privada, descifrar pública (“firma”, asegurarte de q quien te lo ha enviado dice ser quien es)
  + Función hash, resumen o digest
    - Algoritmos: MD5, SHA1,...
    - Irreversible
    - Colisiones (cuando los cifrados coinciden en el mismo cifrado)
* **ATAQUES**
  + Clave: fuerza bruta, diccionario, ingenieria social…, keyloggers
  + Cifrado: estadística, criptoanálisis
* **PROTOCOLOS SEGUROS**
  + DSS, PGP/GPG, SSL, SSH, TLS

**PYTHON**

¿Cómo cifrar un fichero? Sintaxis y comandos

Gedit

***Emulador***

python “fichero” o incluir la ruta, abres la carpeta click derecho emulador:

*python ej01py*

***Conversión de variables***

• str(variable) caracteres (de número a texto para que sean compatibles)

• int(variable) número entero

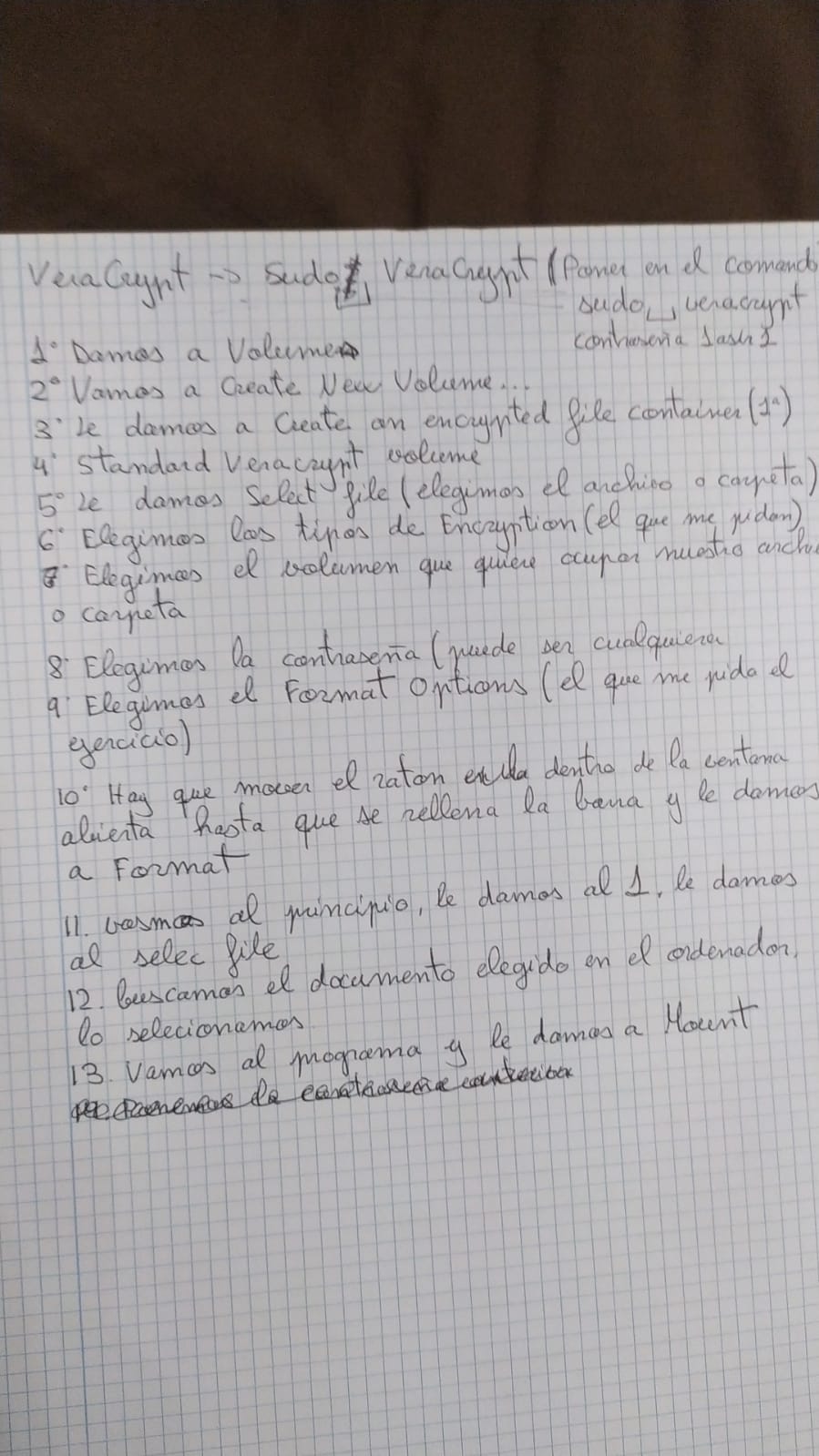
• float(variable) número decimal

• bool(variable) booleano (true/false)

Depende de la versión si es la versión 3 es solo input si es otra raw\_input

**VERACRYPT**

1. Iniciamos y seleccionamos la opción *Create Volumen*
2. Siguiente
3. En la ventana *Volume Location,* tenemos que introducir una cifra
4. En *Volume Sire* tenemos que indicar *el tamaño*
5. En *Volume Password,* tenemos que introducir una *contraseña y repetirla*
6. Nos aparecerá un mensaje de peligro pero, haremos click en SÍ
7. En *Format Option,* elegimos el formato para cifrar los archivos
8. *Cross Platform support,* indicamos que se pueda o no descifrar desde otra plataforma
9. *Mover el ratón por la pantalla* hasta que se llene por completo y click en *Format*
10. Un cuadro, introducimos la contraseña
11. Abrimos otra vez Veracrypt y hacemos click en un volumen y una vez seleccionado, click *Select File*
12. Nos abrirá un gestor de archivos, donde seleccionaremos el archivo creado en veracrypt

****