



Ejercicios:

Introducción a la seguridad informática

- 1.1. La frase que pronunció Julio César cuando decidió atravesar el Rubicón con sus legiones para llegar a Roma: "La suerte está echada", en lenguaje cifrado se escribe

DOHD MDFAD HXA

Descífrala para obtener la frase original en latín.

- 1.2. ¿Cuál de los siguientes criptogramas fue enviado por Julio César y cuál por César Augusto?

- a) DBGHQAHX IRVABQD MBBDA
- b) GFTVKOB MFOVF

- 1.3. Utilizando una scitula de ocho filas y seis columnas cifra:

La frase que coreaban los soldados de Julio César en su triunfo sobre las Galias:

"Ciudadanos, guardad vuestras mujeres: llevamos un libertino calvo"

VRBANI, SERVATE VXORES: MOECHVM CALVOM ADDVCIMVS

La frase que dijo de él Curio padre en un discurso:

"Marido de todas las mujeres y mujer de todos los maridos"

OMNIVM MVLIERVM VIRVM ET OMNIVM VIRORVM MVLIEREM

- 1.4. Encuentra el texto en claro correspondiente al criptograma

c=AE_NMHIIOMNRVIRSSE_STME_

sabiendo que se ha utilizado una scitula de ocho filas y tres columnas.

- 1.5. Utiliza el sistema de cifrado ADFGX para cifrar el mensaje

m=ARBEIT MACHT FREI

escrito en la entrada del campo de concentración de Auschwitz.

- 1.6. Enumera y describe a grandes rasgos qué tres aspectos fundamentales hay que garantizar para mantener un sistema seguro (o fiable).

- 1.7. Enumera y describe a grandes rasgos los tres principales elementos a proteger en cualquier sistema informático.

- 1.8. Enumera y describe a grandes rasgos los cuatro grandes grupos de amenazas a la seguridad.

- 1.9. Describe, brevemente, los términos criptografía, criptoanálisis y criptología.

- 1.10. La seguridad perfecta requiere que la longitud de la clave sea mayor o igual que la del texto en claro. ¿Por qué este resultado teórico hace que los criptosistemas con seguridad perfecta sean inútiles en la práctica?
-