

CRIPTOGRAFÍA
Ejercicios de Criptografía Clásica – parte B

Afin – Afin

Ejercicio 1

Descifre el siguiente criptograma AQ8S1 MqVTu 1QyqT DWG6Zñ zcñKYG
Si para su cifrado se utilizó un alfabeto de longitud 64 (alfabeto en español alternando mayúsculas y minúsculas y al final los dígitos del 0 al 9), $a=13$ y $Kw=M1ST3rios0$

Ejercicio 2

Descifre el siguiente criptograma 636D5 y escriba una frase con el texto descubierto
Considere que se utilizó un alfabeto de longitud 64 (alfabeto en español alternando mayúsculas y minúsculas y al final los dígitos del 0 al 9), $a=17$ y $Kw=Rodar$

Ejercicio 3

En una palabra defina "seguridad" y cifre la palabra considerando $a=11$
Usted decida el alfabeto a utilizar y la Kw

→ Después de haber visto todos los tipos de algoritmos Afines ¿porqué considera que no se utilizan en el desarrollo de aplicaciones de seguridad informática?

Playfair

Ejercicio 1

Cifre y descifre el Mcla " EL PERÍODO ELECTORAL SERÁ UN RETO PARA LA SEGURIDAD" , use $Kw=PARTIDO$.

Ejercicio 2

Cifre y Descifre el Mcla " LA TAREA MÁS IMPORTANTE DEL SER HUMANO ES SER FELIZ" , use $Kw=AMARANTO$.

→ Después de realizar los ejercicios 1 y 2 ¿cuáles son los pros y contras de este algoritmo?

Hill

Ejercicio 1

Con base en el alfabeto inglés cifre la palabra FAMILIA utilizando $Kw = ENTRETENIMIENTOS$.

Ejercicio 2

El criptograma JDQTHH se obtuvo al cifrar un Mcla con una $K=FRUJXDCLN$, y $n=26$ ¿cuál es el mensaje cifrado?

Ejercicio 3

El criptograma FÑCHÑQ se obtuvo al cifrar un mensaje secreto como clave la palabra CONVERSAR ¿cuál es el mensaje secreto?

→ Después de realizar los ejercicios 1, 2 y 3 ¿cuáles son las ventajas y desventajas del algoritmo de Hill?