# Lab 1 – Encriptado y Decriptado de Texto

Competencias a desarrollar

* Implementar el uso de funciones para encriptar y decriptar un texto cifrado
* Identifica los requisitos para un análisis de fuerza bruta por frecuencia.

Problemas a resolver

1. Implementar las funciónes de encriptado y decriptado para un texto plano en castellano (27 letras) para los siguntes métodos (30 puntos)
   1. Cifrado Caesar

A computer screen shot of a black screen with white text

Description automatically generated

* 1. Cifrado afín

A screenshot of a computer program

Description automatically generated

* 1. Cifrado Vigenére

A computer screen shot of a program

Description automatically generated

1. Implementar el uso de funciones para encriptar y decriptar un texto cifrado. (30 puntos)

**Sugerencias:**

* Para construir una función que calcule las distribución de los caracteres que aparecen en el texto cifrado, se espera que su la función calcule las probabilidades **(las frecuencias divido el total de caracteres)**. (Es recomendable completar las letras que no aparezcan en su texto, con probabilidad 0.)

Cesar

A screenshot of a computer

Description automatically generated

Afin

A screenshot of a computer

Description automatically generated

Vigenere

A screenshot of a computer

Description automatically generated

1. Implementar una función para comparar la distribución encontrada contra la distribución teórica de las letras del castellanos. (40 puntos)

A graph of a number of letters

Description automatically generated

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Letra** | **A** | **B** | **C** | **D** | **E** | **F** | **G** | **H** | **I** |
| Porcentaje | **12,53%** | **1,42%** | **4,68%** | **5,86%** | **13,68%** | **0,69%** | **1,01%** | **0,70%** | **6,25%** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Letra** | **J** | **K** | **L** | **M** | **N** | **Ñ** | **O** | **P** | **Q** | |
| Porcentaje | **0,44%** | **0,02%** | **4,97%** | **3,15%** | **6,71%** | **0,31%** | **8,68%** | **2,51%** | | **0,88%** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Letra** | **R** | **S** | **T** | **U** | **V** | **W** | **X** | **Y** | **Z** | |
| Porcentaje | **6,87%** | **7,98%** | **4,63%** | **3,93%** | **0,90%** | **0,01%** | **0,22%** | **0,90%** | | **0,52%** |

Caesar corrimiento de 3

A screenshot of a computer screen

Description automatically generated

Mensaje: hola como te encuentras el día de hoy?

Mensaje encriptado: krñd fror wh hpfxhpwudv hñ gld gh krb?

En esta comparación de distribución de frecuencia se puede observar claramente un patrón en la distribución del texto cifrado, en donde justamente 3 posiciones delante de una letra con un porcentaje alto en la distribución teórica, se encuentra un porcentaje alto para la letra correspondiente al cifrado, este probablemente es en el cifrado donde se pueda observar de una manera más sencilla este patrón debido a la simpleza del cifrado cesar.

Afin con a = 7; b = 3

A screenshot of a computer screen

Description automatically generated

Mensaje: hola como te encuentras el dia de hoy?

Mensaje encriptado: yazd qaga ie enqoeniudb ez xfd xe yap?

En este cifrado se logra observar una distribución con un patrón que podría parecer a primera vista menos obvio, sin embargo, sabiendo que los porcentajes de que aparezcan ciertas letras son tan altos en las posiciones a, d y e esto nos da a entender que estas pueden representar algunas de las letras que mas se repiten en la distribución del castellano, lo cual lo hace una posible vulnerabilidad.

Vigenere con clave “cypher”

A screenshot of a computer screen

Description automatically generated

Mensaje: hola como te encuentras el dia de hoy?

Mensaje encriptado: jnah tqke xv ccjyvorhhw gj kmr bt lga?

En este cifrado se puede observar una distribución de letras mucho mas complicada de leer a comparación de las dos anteriores, debido a que estas se encuentran distribuidas mas uniformemente, lo que podría hacer la realización de un criptoanálisis mucho mas complicada. Por lo que se podría decir que el cifrado vigenere es el mas seguro de estos tres en cuanto a el estudio de las distribuciones de letras se refiere.