**SEGUNDA PRACTICA DE LABORATORIO**

CRIPTOGRAFIA POLIALFABÉTICA

1. **Objetivos**

* Implementar un algoritmo de cifrado polialfabético: cifrado de Vigenere, usando valores numéricos, ASCII
* Realizar criptoanálisis al cifrado de Vigenere mediante el método Kasiski

1. **Conceptos básicos**
   1. **Cifrado de Vigenere**

En francés Blaise Vigenere (XVI) propone uno de los métodos más conocidos de cifrado polialfabético y que fue invulnerable por más de 300 años.

Usa una tabla con **alfabeto** en mayúsculas y consiste de una matriz cuadrada de nxn elementos, siendo n el número de letras del alfabeto. La primera fila está formada por el alfabeto, empezando por la letra A, la segunda fila inicia con B, y así sucesivamente.

La **clave** está constituida por una secuencia de letras del alfabeto k={k0, k1, …, kd-1} de longitud “d”, que no debe de tener letras repetidas, ni debe ser mayor que el tamaño del alfabeto.

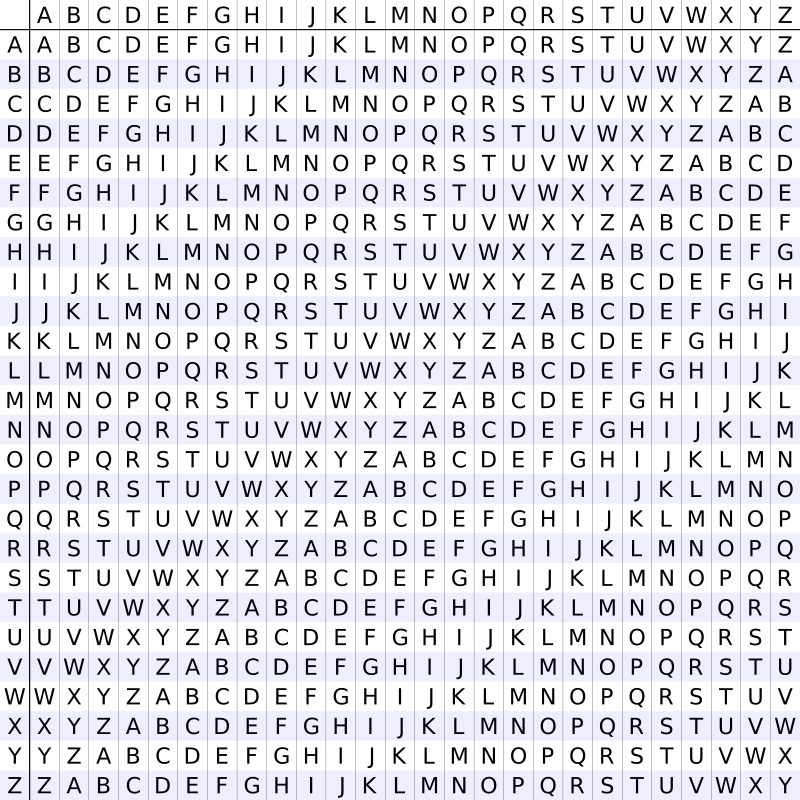


Figura 1: Tabla de Vigenere

* + 1. **Cifrado**

Se buscará la posición correspondiente del texto plano en las columnas de la tabla.

Las filas corresponden para la clave, repetida cíclicamente tantas veces como se necesite.

Por ejemplo, si el texto plano es HERMOSO y la clave es CIELO. En la columna de la letra H se busca la intersección con la fila de la letra C, dando como resultado el criptograma J

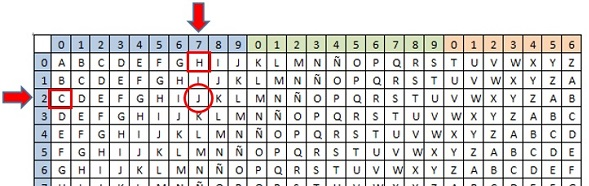


Figura 2[[1]](#endnote-1): : Cifrado de la letra H con la clave C

Realizando esta operación para todo el texto plano, se tiene:

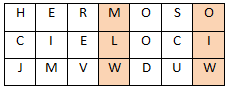


Figura 3: Mensaje Cifrado

**Matemáticamente, como sería la función de Cifrado?**

Función de Cifrado es:

**ci = mi + kl mod n**

Donde: i = al carácter i-ésimo del texto plano

l = al carácter l-ésimo de la clave

n = al tamaño del alfabeto



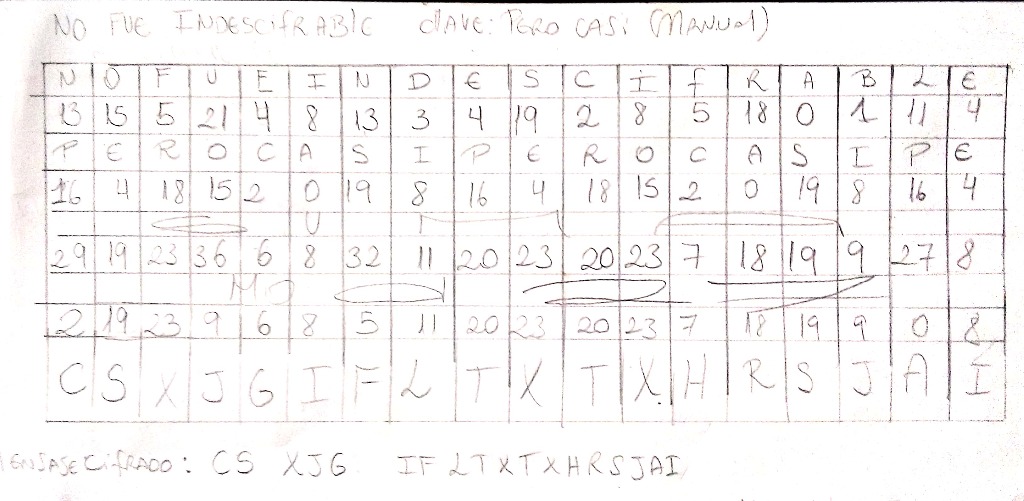


* + 1. **Descifrado**

Función de Descifrado es:

**ci = mi - kl mod n**

1. **Indicaciones de desarrollo para el cifrado de Vigenere**
2. Cifre manualmente el **mensaje** NO FUE INDESCIFRABLE con la **clave** PERO CASI. Para el alfabeto español.



1. Implementar el cifrado de Vigenere, donde se pueda seleccionar el alfabeto (numérico, ASCII, HEX), ingresar el texto plano (por archivo o interface) y genere el cifrado y descifrado.
2. Verifique el cifrado para el siguiente mensaje:

*Puedo escribir los versos mas tristes esta noche.*

*Escribir, por ejemplo: La noche esta estrellada,*

*y tiritan, azules, los astros, a lo lejos.*

*El viento de la noche gira en el cielo y canta.*

*Puedo escribir los versos mas tristes esta noche.*

*Yo la quise, y a veces ella tambien me quiso.*

Clave: Pablo Neruda

Alfabeto: abcdefghijklmnopqrstuvwxyz(espacio)ABCDEFGHIJKLMNOPQRSTUVWXYZ,.

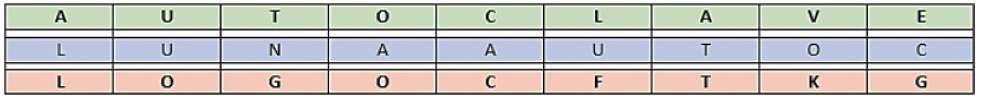
1. Implementar el criptoanálisis del cifrado de Vigenere aplicando el método Kasiski
2. Volver a procesar el mensaje insertando la cadena AQUI cada 10 caracteres, el texto resultante deberá contener un número de caracteres que sea múltiplo de 4, si es necesario rellenar al final con caracteres W según se necesita. Cifre y Descifre el mensaje.
3. Modifique el cifrado de Vigenere realizando los siguientes pasos:
4. Se escribe la clave
5. Al llegar a la última letra de la clave, se continúa con el mensaje en claro

Por ejemplo, para el mensaje AUTOCLAVE con la clave LUNA, el proceso a realizar sería:

Mensaje: MODIFIQUE EL CIFRADO

Clave : SEGÚN

CIFRADO



1. Conclusiones
2. Cuáles son las debilidades y fortalezas del cifrado de Cesar (cifrado monoalfabético)
3. Cuáles son las debilidades y fortalezas del cifrado de Vigenere (cifrado polialfabético)

|  |
| --- |
|  |

|  |
| --- |
| Cesar |
|  |

|  |
| --- |
| Ventajas: |
|  |

|  |
| --- |
| -Es mucho más fácil de codificar y decodificar. |
|  |

|  |
| --- |
| -Solo es necesario tener una clave para descifrarlo. |
|  |
|  |

|  |
| --- |
| Desventajas: |
|  |

|  |
| --- |
| -Cómo es tan facil de descifrar, alguien podría descubrir nuestro mensaje. |
|  |

|  |
| --- |
| Vigenere |
|  |

|  |
| --- |
| Ventajas: |
|  |

|  |
| --- |
| -Su cifrado es un poco complejo, por lo tanto, es un poco difícil de descifrar. |
|  |

|  |
| --- |
| -Para mí resultaría muy díficil descifrarlo sin la clave. |
|  |

|  |
| --- |
| Desventajas: |
|  |

-Si se nos pierde la clave, no se podría descifrar con facilidad.

1. http://www.criptored.upm.es/crypt4you/temas/criptografiaclasica/leccion9.html [↑](#endnote-ref-1)