

“La alumna declara haber realizado el presente trabajo de

acuerdo a las normas de la Universidad Católica San Pablo”

CIENCIA DE LA COMPUTACIÓN

PRÁCTICA 2

ALGEBRA ABSTRACTA

MARÍA GRACIEL

CRUZ CÁCERES

3ER SEMESTRE

2020

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.

A close up of a white wall

Description automatically generated

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.

**Archivos**: VigenereClass.h, VigenereClass.cpp

1. 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,.

**Texto Cifrado:**

CufoBZRwtKlbXrAwBRlzvKvof nlFZevzLwef fCG lrEwkeO

FCqQVfzKb cosKsIRqFEr:nLbKANPlvThsgaApFSciBEddP,

INSVvzMdnN bJHKRwpToof bCGQ.wpTd ,oAwsI.wq

HlnvjpAS.DuyClP ozqGRDxBuaneoKsKlgzyoonyAnoMeeq

SuTdpKsRPvzvlrnlpCNURvIHv .atKGQVwJyv TsulNM.gyyc

LoAwoZbyzLh,nyAlNURgvLCe,lbKG Zfzyq .eAAHHdsq

1. Implementar el criptoanálisis del cifrado de Vigenere aplicando el método Kasiski

**Archivos**: Kasisiki.h, Kasisiki.cpp

1. 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.

**Archivo**: main.cpp

**Texto Cifrado:**

CufoBZRwtKDQHIjmwQlpELCvoQVTsQdsITpaf B.ggevzLwef fCOoFMJuCnbcipn

mUjaHsRrjmwQLDRiXIcosKsIRqFEDQHIp:NjNDDHfhoQVTsZRwJuCeftB.ggciBEddP,

IOoFMQMlrXtbymZmUjadzhlfCmZYsRiXIf bCGQ.wpTDQHIbKzNlpvCrsoQVTn

qpQOleatB.gg.DuyClP ozOoFMtAh VislNDmUjaq TlAnwDYsRiXInyAnoMeeq

DQHIQEsC.DvLfroQVTwAVvQErsnvB.ggRvIHv .atKOoFMJKlsgetKsRmUjawannpnvDM

RiXILoAwoZbyzLDQHIfjNXleQOhcoQVTsRliBEd gaB.ggZfzyq .eAAOoFMKBvoO

Xf

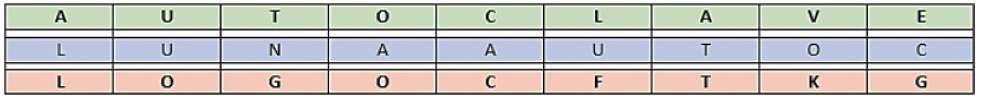
1. Modifique el cifrado de Vigenere realizando los siguientes pasos:
2. Se escribe la clave
3. Al llegar a la última letra de la clave, se continúa con el mensaje en claro

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

Mensaje: MODIFIQUE EL CIFRADO

Clave : SEGÚN

CIFRADO



**Archivos**: VigenereClass.h, VigenereClass.cpp

**Funciones**: string cifradoModified(string mensaje);

string descifradoModified(string mensaje);

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

**Debilidades:**

El cifrado Cesar al ser un cifrado Mono alfabético contiene una cantidad de claves limitadas el cual es muy sencillo de descifrar por un ataque de fuerza bruta, en el peor de los casos tendrá que codificar con cada una de las 26 posibilidades.

**Fortalezas:**

El cifrado Cesar es mucho más rápido de cifrar al ser uno de los algoritmos de cifrado más sencillo.

1. Cuáles son las debilidades y fortalezas del cifrado de Vigenere (cifrado poli alfabético)

**Debilidades:**

Se puede conocer la longitud de la clave al buscar patrones repetidos en el texto cifrado. El saber la longitud de la clave será sencillo dividir la cadena en subcadenas para posteriormente adivinar la clave y descifrarlo sin mucha dificultad (como realiza el método Kasiski)

**Fortalezas:**

A comparación del cifrado mono alfabético es un poco más complicado de descifrar porque contiene n alfabetos (n es la longitud de la clave).

Es sencillo y rápido de cifrar.