

CIENCIA DE LA COMPUTACIÓN

PRÁCTICA 2

ÁLGEBRA ABSTRACTA

SOL MORELIA

VELÁSQUEZ RODRÍGUEZ

3ER SEMESTRE

2020

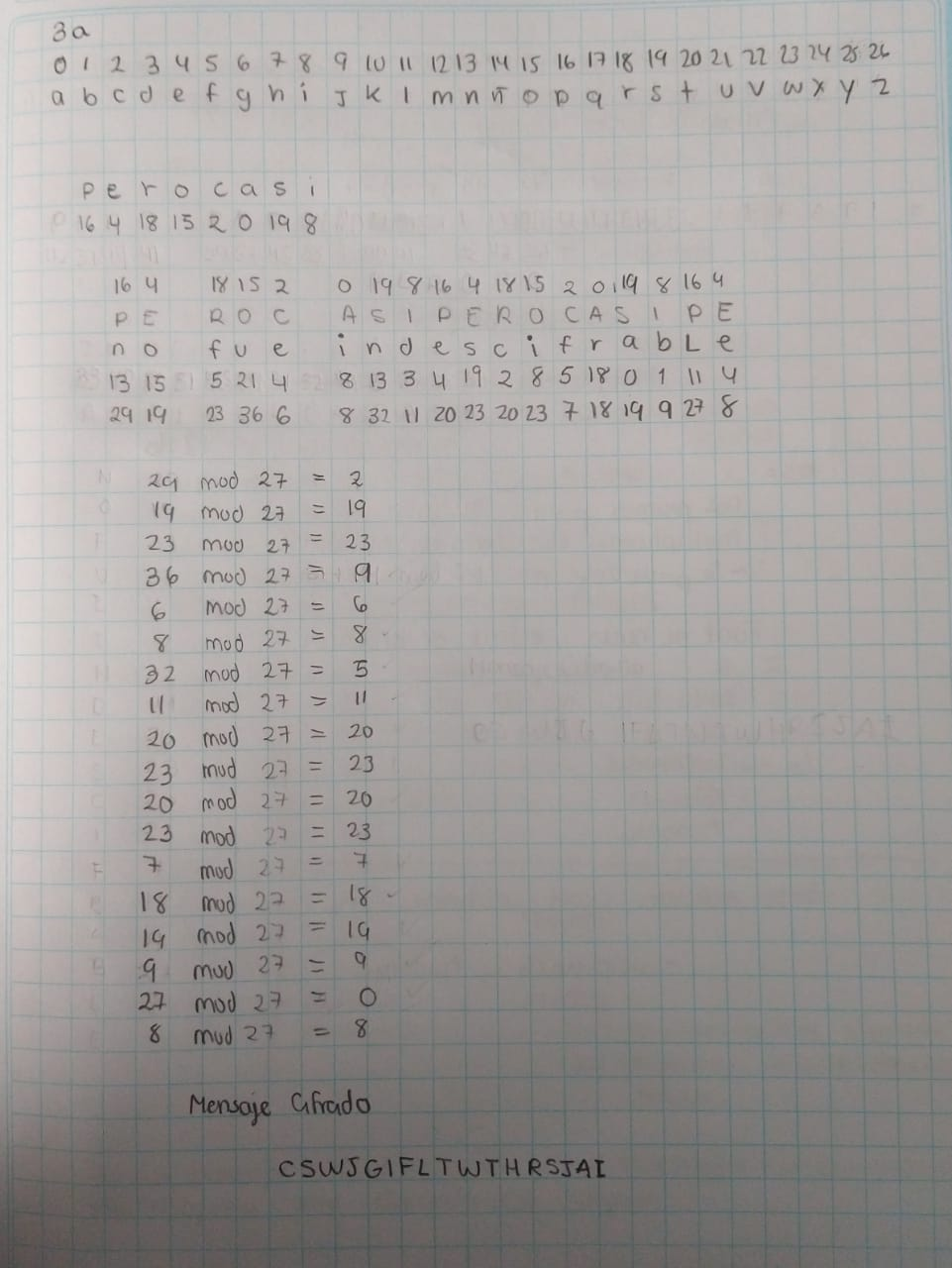
“La alumna declara haber realizado el presente trabajo de

acuerdo a las normas de la Universidad Católica San Pablo”

**SEGUNDA PRACTICA DE LABORATORIO**

CRIPTOGRAFIA POLIALFABÉTICA

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

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

Alfabeto: abcdefghijklmnopqrstuvwxyz(espacio)ABCDEFGHIJKLMNOPQRSTUVWXYZ,.

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

Clase Kasiski

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.

Funciones: inserteAqui();

quitarAqui();

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

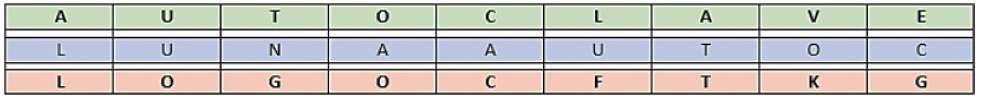
Por ejemplo, para el mensaje AUTOCLAVE con la clave LUNA, el proceso a realizar sería:

Mensaje: MODIFIQUE EL CIFRADO

Clave : SEGÚN

Funcion: cifrado2

CIFRADO



Conclusiones

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

La fortaleza es la forma simple de cifrarlo y descifrado, ya que solo se suma a la posición de letra el modulo del tamaño del alfabeto que vamos a utilizar.

La debilidad de este es que, si queremos descifrarlo y no tenemos la clave, se puede hacer por fuerza bruta es decir probando los valores de desplazamiento que es el tamaño del alfabeto o por análisis de frecuencias, en este se considera la letra que se usa mas según el alfabeto, en caso del español las que mas se repiten son la a y la e; el detalle el cuando queremos aplicar esto en mensajes cortos, ya que pueden aparecer varias palabras descifradas.

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

Las fortalezas es la forma simple de cifrado y descifrado, ya que también aplicamos el módulo, en la clave y el alfabeto.

La debilidad de este es en el descifrado sin clave, ya que existen métodos como Kasiski que pueden descifrarlo, aplicando análisis de frecuencias y MCD.