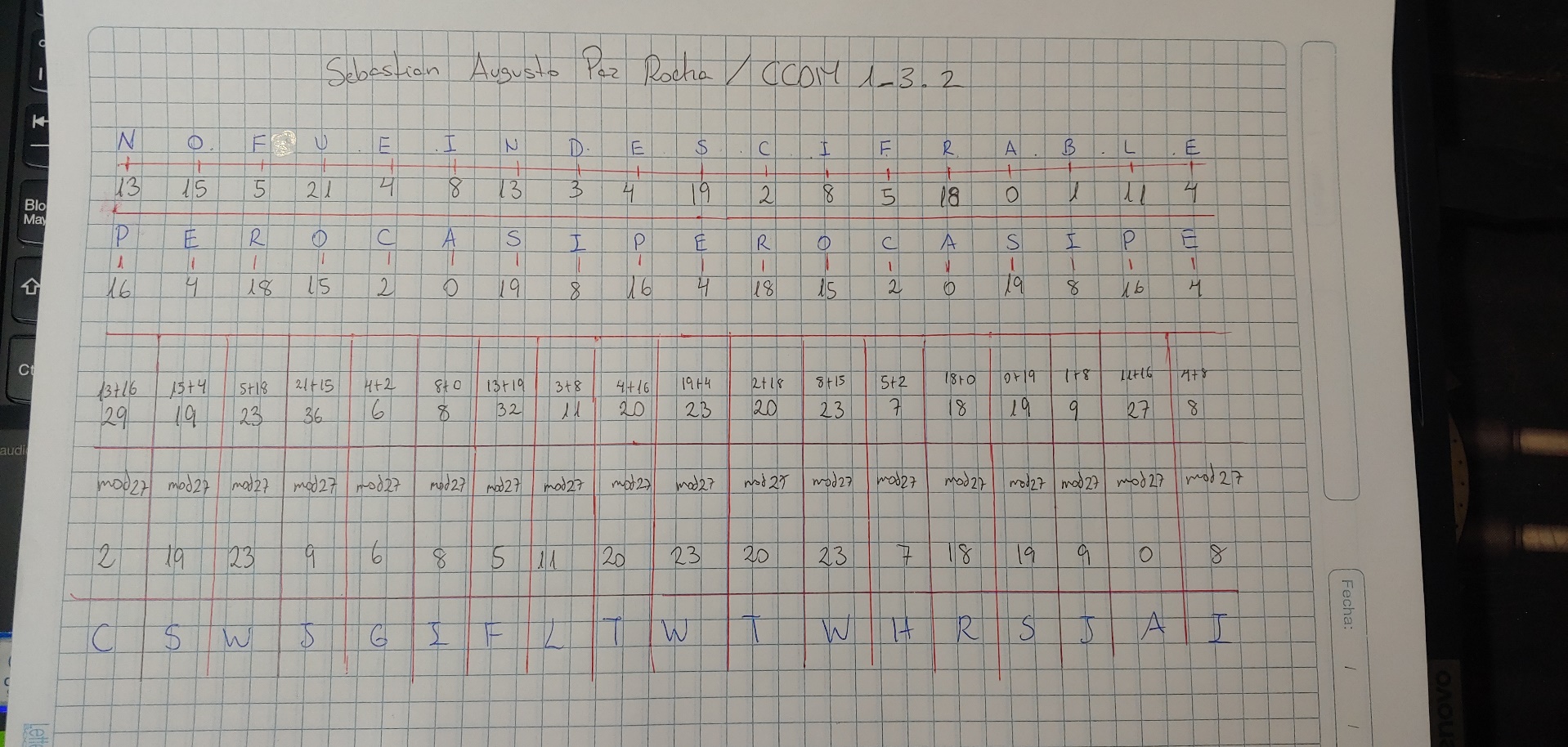
**SEGUNDA PRACTICA DE LABORATORIO**

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.

**En Github**

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.*

Clave: Pablo Neruda

Alfabeto: abcdefghijklmnopqrstuvwxyz(espacio)ABCDEFGHIJKLMNOPQRSTUVWXYZ,.

**En Github**

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.

**En Github**

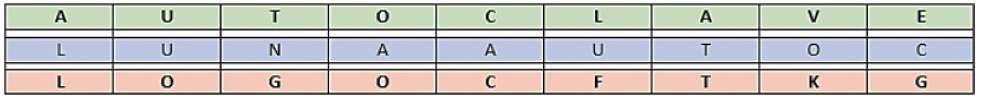
1. Modifique el cifrado de Vigenere realizando los siguientes pasos:
2. Se escribe la clave
3. Al llegar a la última letra de la clave, se continúa con el mensaje en claro

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

Mensaje: MODIFIQUE EL CIFRADO

Clave : SEGÚN

CIFRADO



**En Github**

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

Sus fortalezas es que es muy fácil de cifrar y entender cómo hacerlo. Puede ser efectivo cuando las personas que se quiere evitar que conozcan el mensaje no tienen idea de los conceptos básicos de criptografía.

Lamentablemente hoy en día este cifrado ya es bastante obsoleto, y su principal debilidad es que puede ser descifrado muy fácilmente por alguien que ya conoce este tipo de encriptación a través del análisis de frecuencia, comparando el mensaje con palabras comunes de un lenguaje que conozcamos.

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

Aunque no sea muy fácil cifrar un mensaje por medio de Vigenere, es bastante posible incluso sin el uso de máquinas; y es mucho más difícil de descifrar que el cifrado de Cesar, ya que utiliza diferentes alfabetos, dependiendo cada letra de la clave. Y esta se convierte en su principal fortaleza, ya que este cifrado fue considerado invulnerable por muchísimos años; sólo lo podían descifrar las personas que supiesen la clave con exactitud, y aún así, era bastante tedioso hacer las operaciones para descifrar, esta sería una de sus debilidades.

La otra debilidad apareció cuando Friedrich Kasiski encontró la forma de descifrar el mensaje aún sin conocer la clave previamente.