UNSA

UNIVERSIDAD NACIONAL DE SAN AGUSTÍN DE AREQUIPA

FACULTAD DE INGENIERÍA Y PRODUCCIÓN DE SERVICIOS

ESCUELA PROFESIONAL DE CIENCIA DE LA COMPUTACIÓN

“AÑO DE LA UNIDAD, LA PAZ Y EL DESARROLLO”

SEGURIDAD EN COMPUTACIÓN

SEMESTRE: 2023 - B

CRIPTOGRAFÍA CLÁSICA

ESTUDIANTES:

Béjar Román Edson Bryan

Casaverde Aleman Moises Alejandro

Sumare Uscca Josue Gabriel

DOCENTE:

LUCY ANGELA DELGADO BARRA

Arequipa – Perú

2023

CRIPTOGRAFÍA CLÁSICA

Cifrado Alberti

El disco de Alberti, también conocido como "cipher wheel" en inglés, es reconocido como el pionero en la creación de sistemas polialfabéticos. En un sistema polialfabético, cada carácter se sustituye por otro carácter de manera diferente según un patrón específico. Esta característica hace que sea resistente a los intentos de desciframiento mediante análisis de frecuencia. Por ejemplo, si contamos cuántas veces aparece la letra 'a' en el mensaje cifrado, la letra original podría ser cualquier otra letra del alfabeto.

Se usa mediante dos discos concéntricos, cada uno con el alfabeto impreso, el anillo interno se puede girar en relación con el anillo externo. Para cifrar un mensaje, se selecciona una letra de la clave que indica la posición inicial en el anillo interno, luego, se encuentra la letra que corresponde en el anillo externo que se alineará con la letra deseada del mensaje verdadero.

La clave va a cambiar constantemente durante el cifrado siguiendo un patrón predeterminado o acordado previamente, por lo que esta rotación de la clave hace que sea un sistema poliafabético, lo que hace que sea dificultoso el descifrar el mensaje mediante el análisis de frecuencia. Para descifrar el mensaje, el destinatario debe entender y conocer el patrón de cambio de la clave y realizar un proceso inverso.

Cifrado homofónico

En los cifrados de sustitución tradicionales, se reemplaza cada letra del texto original con un símbolo diferente, pero este enfoque presenta un problema notable en el análisis criptográfico de frecuencias. El problema radica en que, al sustituir cada letra por un símbolo distinto, la frecuencia de las letras en el texto original se refleja en el criptograma. Como resultado, si conocemos la frecuencia de aparición de las letras en el idioma original, podemos obtener pistas útiles para descifrar el mensaje cifrado.

Los cifrados de sustitución homofónica representan una evolución de los cifrados de sustitución convencionales. Su objetivo principal es atenuar el efecto de las frecuencias de las letras en el mensaje cifrado. Tomando en cuenta esto, si tomamos el ejemplo de la letra "A", que es la letra más común en un idioma, en un cifrado homofónico, en lugar de reemplazarla por un único símbolo, la sustituimos por varios símbolos diferentes, que pueden también ser números aleatorios.

Link del repositorio:

https://github.com/GGDEEBOR/cifrado-alberti--descifrado-homof-nico