UANL
UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

FCFM
FACULTAD DE CIENCIAS FÍSICO MATEMÁTICAS

Criptografía y Seguridad

Explicación y experiencia con métodos de criptografía
Grupo 032

Maestro Angel Salvador Pérez Blanco

Roberto Treviño Cervantes **#1915003**

Presentado el 30 de Octubre de 2023

Explicación y experiencia

Cifrado de César

Se seleccionó este método porque representa los principios y fundamentos de la criptografía y simboliza los comienzos del campo de estudio asi como nuestro curso. Programar el algoritmo del cifrado de César en Python fue bastante sencillo. La librería estándar de Python incluye por defecto un módulo llamado string, el cual exporta una variable llamada ascii_letters, que es el conjunto de las letras mayúsculas y minúsculas incluidas en el conjunto ASCII. Luego, podemos iterar sobre cada uno de los caracteres del mensaje de entrada y buscar el índice de este en el conjunto de caracteres ascii_letters y sumarle o restarle el número de la llave según se esté encriptando o desencriptando.

RSA

Se seleccionó este método porque es ampliamente utilizado en la criptografía moderna para firmar mensajes o transmitirlos de forma segura. Este algoritmo simboliza el avance de la criptografía hasta el punto actual puesto que se utiliza en gran medida aún hoy en día. Este algoritmo hace uso de un principio bastante sencillo e implica el uso de operaciones un poco más complejas por lo que representa un mejor reto para obtener una buena comprensión de la criptografía como área de estudio. Ahora bien, programar el algoritmo de RSA también fue bastante sencillo puesto que podemos aprovechar de nuevo la variable ascii_letters. Primero pedimos un par de números primos, verificamos que sean primos, calculamos su producto y la función phi de Euler. Después buscamos en un bucle entre *1* y *phi(n)* un coprimo para este último, y realizamos el algoritmo extendido de euclides para encontrar *d* que cumpla $(d * e) \bmod \varphi(n) = 1$. Estas son operaciones bastante sencillas de implementar y computacionalmente triviales para la magnitud de números con que estamos trabajando. Encriptar y desencriptar también es bastante sencillo puesto que sólo implicar a la llave privada o la llave publica el número que representa cada una de las letras ascii del mensaje.