Encriptado de texto por el método afín

Daniel Eduardo Cobos Ayala, Laura Vanessa Méndez Rivera, César Luis Hurtado Rodríguez
22958- Autómatas y lenguajes formales - Grupo B1
Escuela de Ingeniería de Sistemas e Informática

Resumen

La criptografía es un ámbito de la criptología que se ocupa de las técnicas de cifrado destinadas a alterar el contenido de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no deseados.

En este proyecto se desarrolló el método de cifrado afín, este es un tipo de cifrado por sustitución en la que cada símbolo del alfabeto es sustituido por un símbolo del alfabeto cifrado siendo el numero de símbolos del alfabeto claro igual que el numero de símbolos del alfabeto cifrado.

Introducción

En este proyecto observamos como se implementa el método de cifrado afín en el encriptado de mensajes.

La criptografía surge como necesidad para que la información que se envié por escrito preserve su privacidad. El cifrado de mensajes es muy importante ya que este sirve para hacer las comunicaciones mas seguras, lo mismo se puede decir a la hora aplicarlo en internet.

La primera funcionalidad para conseguirlo es la de la privacidad y confidencialidad de los mensajes transmitidos, ya que al no ir descubiertos, cuando tu le envías algún mensaje a otra persona, los algoritmos criptográficos ayudan a que esta información no se pueda leer fácilmente si es que llega a ser interceptada en el camino.

En la actualidad esto ya se está implementando ya que si tu envías un SMS y se envía en texto plano, sin cifrar, y si un operador o alguna compañía interfiere el mensaje, puede leer toda la información que hay en ella. Sin embargo esto ya está solucionado porque aplicaciones como WhatsApp, Gmail, Telegram, etc… aplican cifrados para que el descifrarlos no sea tan sencillo

Proceso y método

En el cifrado afín, para hallar el símbolo del alfabeto cifrado que sustituye a un determinado símbolo del alfabeto claro, se implementa una función matemática afín en aritmética modular.
Para poder aplicar dicha función matemática lo primero que hay que hacer es asignar un orden que a cada símbolo de cada uno de los del alfabeto le asocie un numero de orden. Una vez establecido esto se usa la siguiente formula

$$F(m_i, k) = (k_1 * m_i) + k_2 mod 27$$

Figura 1..

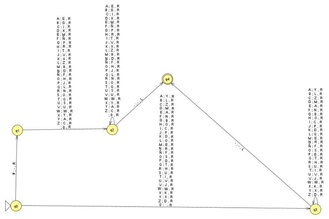


Figura 2. Título

Resultados

En este proyecto se analizó el ya mencionado método afín, una vez se ejecute el programa, este le dará una opción al usuario de ingresar una cadena de texto para luego encriptarla dando como resultado unos símbolos que a simple vista se ve ilegible pero claro, esa es la idea de el algoritmo. Ya que como ya sabemos esto genera seguridad y privacidad en ciertas comunicaciones cotidianas.

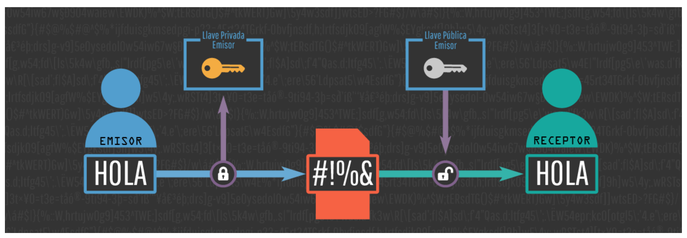
```
print("Bienvenido al cifrador por el metodo AFIN\n"
      "Para encriptar una cadena de texto por favor ingresela a continuación: \n")
mensaje = input()
mensaje = mensaje.upper()
mensaje = "#"+ mensaje
try:
    print(d.validate_input(mensaje))
except Exception as e:
        print("Por favor ingrese una cadena de texto valida.\n")
```

```
Bienvenido al cifrador por el metodo AFIN
Para encriptar una cadena de texto por favor ingresela a continuación:

Hola mundo
('q5', TMTape('-RHZE0BSDKH-'))
```

Imagen 1.

Imagen 2.



Conclusiones

- Se llego a la conclusión de que el cifrado afín es un método práctico pero tiene una desventaja que es que al ser un cifrado por sustitución es vulnerable a ataques criptoanalíticos, los mas habituales son, el análisis de frecuencias y la búsqueda en el espacio de claves.

Trabajo Futuro

Se quiere que este método de cifrado no sea vulnerable a diferentes ataques criptoanalíticos como los previamente mencionados ya que si se maneja una información muy importante y confidencial y es interceptada satisfactoriamente, puede generar serios problemas.

Información de contacto

Nombre Autor 1, Email:
Nombre Autor 2, Email:
Nombre Autor 3, Email:
Nombre Autor 4, Email:
Nombre profesor, Email:

Referencias Bibliográficas (en formato APA)

1. Lam Díaz, Rosa María. (2016). La redacción de un artículo científico. Revista Cubana de Hematología, Inmunología y Hemoterapia, 32(1), 57-69. Recuperado en 09 de agosto de 2020, de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S0864-02892016000100006&lng=es&tlng=es.
2.
3.
4.
5.
6.
7.
8.