Universidad del Valle de Guatemala
Seguridad en sistemas de computación
Catedrático: Melinton Navas
Pablo Viana – 16091

Algoritmos de transposición y sustitución

Para el presente trabajo se crearon tres algoritmos: uno de transposición, uno de sustitución y uno mixto.

El programa se corre con 6 banderas diferentes:

```
help = """ejecute los siguiente comandos para:
Encriptar con transposicion: python algo_encriptacion.py -transE
Desencriptar con transposicion: python algo_encriptacion.py -transD
Encriptar con sustitución: python algo_encriptacion.py -sustE
Encriptar con sustitución: python algo_encriptacion.py -sustD
Encriptar mixto: python algo_encriptacion.py -mixE
Encriptar mixto: python algo_encriptacion.py -mixD
"""
```

Dependiendo de la bandera, el programa pregunta al usuario que mensaje desea encriptar y utiliza el método escogido. Para la **generación de llave de transposición** se utiliza un número aleatorio entre 1 y la mitad con aproximación al decimal mas bajo de la longitud del mensaje a descifrar. Posteriormente, se guarda en un archivo de texto para ser utilizada en el paso de desciframiento. Para la **generación de llave de sustitución** se crea un diccionario desde la 'a' hasta la 'z' luego se revuelven los elementos de la lista y esta nueva sucesión de caracteres aleatorios es la llave para el cifrado por sustitución. Está, también se almacena en un archivo de texto para luego ser usada en el desciframiento. El método mixto emplea las mismas funciones que los otros dos, solo que de manera secuencial una después de la otra.

A continuación, capturas del funcionamiento de los distintos algoritmos:

- **Algoritmo de transposición**

```
C:\Users\Pablo Viana\OneDrive\Documentos\Universidad 2021\seguridad\al
mensaje a descifrar: hola me llamo pablo
texto cifrado:
hl elaopbooam lm al|

C:\Users\Pablo Viana\OneDrive\Documentos\Universidad 2021\seguridad\al
mensaje a descifrar: hl elaopbooam lm al
hola me llamo pablo
```

- **Algoritmo de sustitución**

```
C:\Users\Pablo Viana\OneDrive\Documentos\Univers
mensaje a descifrar: hola como estas
ueclzquihzdms

C:\Users\Pablo Viana\OneDrive\Documentos\Univers
mensaje a descifrar: ueclzquihzdms
holacomoestas
```

- **Algoritmo mixto**

```
C:\Users\Pablo Viana\OneDrive\Documentos\Universidad 2021\seguridad\al
mensaje a descifrar: hola mensaje final
encriptando por sustitución
encriptando por transposicion
uzthubbvrbffswec

C:\Users\Pablo Viana\OneDrive\Documentos\Universidad 2021\seguridad\al
mensaje a descifrar: uzthubbvrbffswec
decifrando por transposición
decifrando por sustitución
holamensajefinal
```