Documentación Visualizador RC4

Alejandro Barreiro Sisto - alejandro.barreiro@udc.es
Alejandro Fernández Fraga - a.fernandez3@udc.es
Alejandro García Tenreiro - a.garciat@udc.es

Ejercicio RC-4:

El programa está escrito en python3 y tiene dos modos de ejecución, normal y descifrado. Nótese que en modo descifradose podría encriptar texto, pero en modo normal no se podría descifrar ya que algunos valores de bytes no se podrían introducir por teclado.

Requisitos:

Es necesario tener el módulo curses.

En ubuntu viene por defecto pero en windows es necesario instalar windows-curses con el comando:

python -m pip install windows-curses

Curses da un error si el tamaño del shell no es suficiente así que se recomienda tenerlo abierto a pantalla completa para su ejecución.

Instrucciones de uso:

- **Modo normal:**

python rc4.py -k key

key es una lista de valores numéricos separados por comas (sin espacios) de hasta 256 elementos.
Los valores deben ser enteros entre 0 y 255 incluidos representando el valor decimal de un byte.
En caso de introducir una lista de más de 256 valores solo los primeros serán tomados en cuenta.
Ejemplo: ***python rc4.py -k 12,234,232,1,33,32,32***

Una vez iniciado el programa se imprimirá el vector S inicializado, la permutación inicial y a continuación con cada tecla pulsada por el usuario se trasforma en bytes que serán encriptados mostrando:

- La matriz permutada en dicha iteración con los valores permutados destacados.
- El resultado del cifrado del byte. Input XOR Key = Output

Para parar el programa usaremos Ctrl + C

- **Modo descifrado:**

python rc4.py -k key -d texto_cifrado
key es igual que para el cifrado.
El **texto_cifrado** es una lista de valores decimales separados por comas (sin espacios).
Ejemplo: ***python rc4.py -k 12,234,232,1,33,32,32 - d 37,100***

Una vez iniciado el programa se imprimirá el vector S inicializado, la permutación inicial y a continuación se muestra paso a paso el descifrado de cada byte.
En este caso la tecla que se pulse no influye, ya que los bytes a descifrar ya han sido introducidos.

Referencias:

- Documentación de curses - https://docs.python.org/3/howto/curses.html
- Pseudocódigo RC4 de referencia - https://campusvirtual.udc.gal/mod/resource/view.php?id=189279
- Read single character python 3 - https://stackoverflow.com/questions/510357/how-to-read-a-single-character-from-the-user