

CS 5158/6058 Data Security and Privacy, Fall 2022

Project 1: One-Time Pad

Margi Amin

M15219371

Software: Python 3.6.3 is required to run this if you're using Windows 10.

Program Location: ..\otp_m15219371\src

Files and structure:

Files included in program:

Data

-ciphertext.txt

-key.txt

-newkey.txt

-plaintext.txt

-result.txt

Src

-Decryption.py

-Encryption.py

-EncryptRunTime.py

-KeyFrequency.py

-main.py

-XOREncrypt.py

Description:

a) Encryption Function

This program generates the ciphertext using message from the plaintext.txt file in the data folder based on the key in the key.txt file of the data folder and stores ciphertext in the ciphertext.txt file in the data folder.

To change the message open the plaintext.txt file and enter the message.

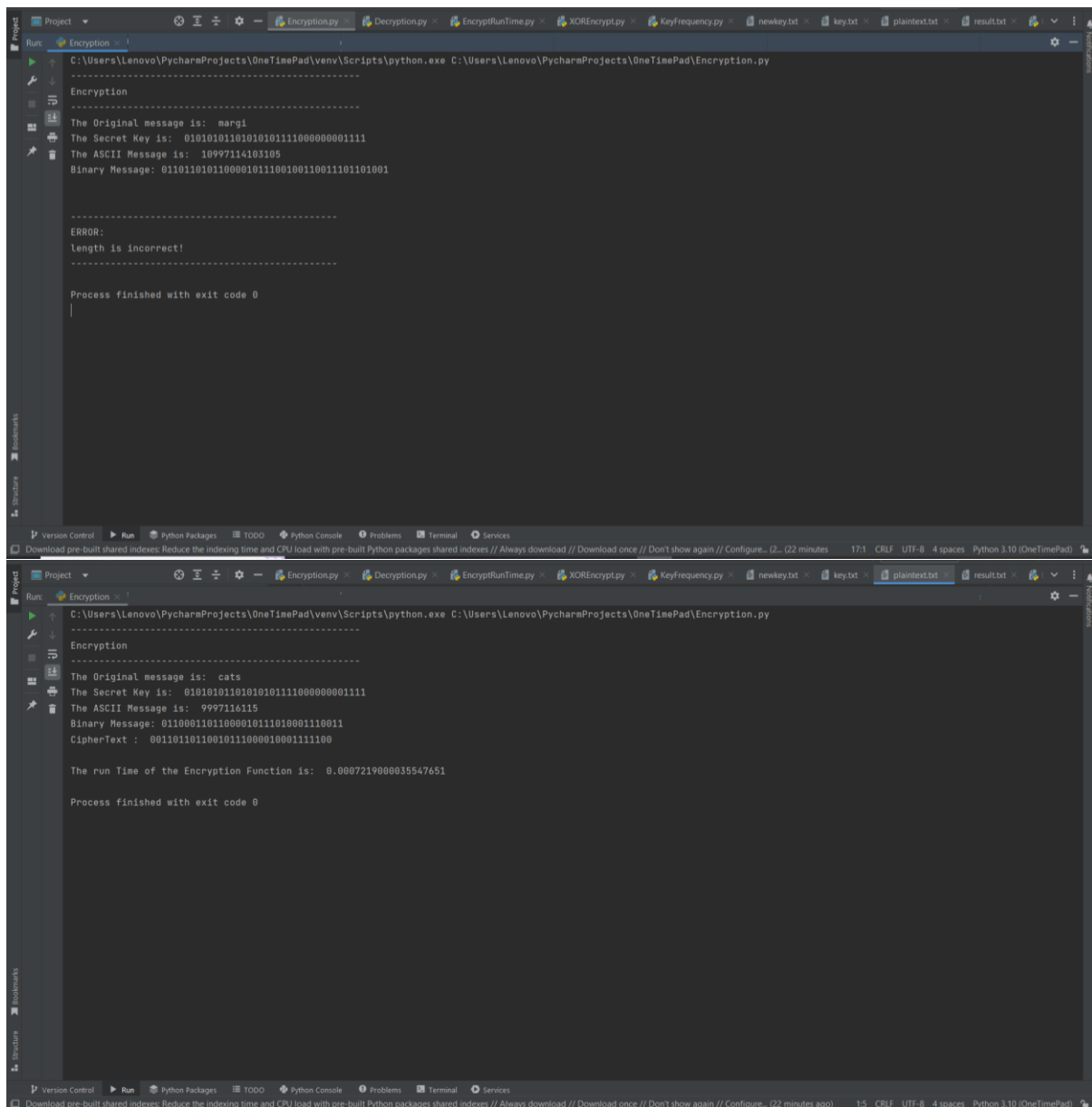
The key stored in the key.txt file is 32bit key given in the project details so if you pass a message longer than 32bits will generate error.

Command to run:

python src\Encryption.py

Output:

Here are screenshots of output of the encryption programs with different input i.e bear, eecs, cats, bike, rice which are 32bits and will generate the ciphertext. margi which is not 32bits will not generate ciphertext.



```
-----
Encryption
-----
The Original message is: margi
The Secret Key is: 01010101101010111100000001111
The ASCII Message is: 10997114103105
Binary Message: 0110110101100001011100100110011101101001

-----
ERROR:
length is incorrect!
-----

Process finished with exit code 0
```

```
-----
Encryption
-----
The Original message is: cats
The Secret Key is: 01010101101010111100000001111
The ASCII Message is: 9997116115
Binary Message: 01100011011000010111010001110011
CipherText : 00110110110010111000010001111100

The run Time of the Encryption Function is: 0.000721900035547651

Process finished with exit code 0
```

```
Project
Run: Encryption.py
C:\Users\Lenovo\PycharmProjects\OneTimePad\venv\Scripts\python.exe C:\Users\Lenovo\PycharmProjects\OneTimePad\Encryption.py

Encryption
-----
The Original message is: bear
The Secret Key is: 010101011010101111000000001111
The ASCII Message is: 9810197114
Binary Message: 01100010011001010110000101110010
CipherText : 0011011111001111001000101111101

The run Time of the Encryption Function is: 0.0007301000005099922

Process finished with exit code 0

Version Control Run Python Packages TODO Python Console Problems Terminal Services
Download pre-built shared indexes: Reduce the indexing time and CPU load with pre-built Python packages shared indexes // Always download // Download once // Don't show again // Configure... (22 minutes ago) 1.5 CRLF UTF-8 4 spaces Python 3.10 (OneTimePad)

Type here to search 70°F Sunny 09:33 21-09-2022

Project
Run: Encryption.py
C:\Users\Lenovo\PycharmProjects\OneTimePad\venv\Scripts\python.exe C:\Users\Lenovo\PycharmProjects\OneTimePad\Encryption.py

Encryption
-----
The Original message is: eecs
The Secret Key is: 010101011010101111000000001111
The ASCII Message is: 10110199115
Binary Message: 01100101011001010110001101110011
CipherText : 00110000110011111001001101111100

The run Time of the Encryption Function is: 0.000826300005428493

Process finished with exit code 0

Version Control Run Python Packages TODO Python Console Problems Terminal Services
Download pre-built shared indexes: Reduce the indexing time and CPU load with pre-built Python packages shared indexes // Always download // Download once // Don't show again // Configure... (23 minutes ago) 1.5 CRLF UTF-8 4 spaces Python 3.10 (OneTimePad)
```

```
OneTimePad | data | plaintext.txt
Run: Encryption
C:\Users\Lenovo\PycharmProjects\OneTimePad\venv\Scripts\python.exe C:\Users\Lenovo\PycharmProjects\OneTimePad\Encryption.py
Encryption
-----
The Original message is: bike
The Secret Key is: 01010101010101011100000001111
The ASCII Message is: 98105107101
Binary Message: 01100010011010010110101101100101
CipherText : 00110111100001110010101101101010

The run Time of the Encryption Function is: 0.001121600057174824

Process finished with exit code 0
```

```
OneTimePad | data | plaintext.txt
Run: Encryption
C:\Users\Lenovo\PycharmProjects\OneTimePad\venv\Scripts\python.exe C:\Users\Lenovo\PycharmProjects\OneTimePad\src\Encryption.py
Encryption
-----
The Original message is: rice
The Secret Key is: 01010101010101011100000001111
The ASCII Message is: 11410599101
Binary Message: 01110010011010010110001101100101
CipherText : 0010011110000111001001101101010

The run Time of the Encryption Function is: 0.000852999904567376

Process finished with exit code 0
```

b) Decryption Function

This programs generates the original message back from the ciphertext in the ciphertext.txt file and save this message in the result.txt file.

If the key value does not match the length of the ciphertext then it will display error.

Commands to run:

Python src\Decryption.py

Output:

Here are screenshots of output of the decryption programs with different plaintext encrypted. i.e bear, eecs, cats, bike, rice which are 32bits and will encrypt and will generate plaintext back by decryption.

margi which is not 32bits will not encrypt and will not generate plaintext back by decryption.

```
Project
Run: Encryption
C:\Users\Lenovo\PycharmProjects\OneTimePad\venv\Scripts\python.exe C:\Users\Lenovo\PycharmProjects\OneTimePad\Encryption.py

Encryption
-----
The Original message is: rice
The Secret Key is: 0101010101010111000000001111
The ASCII Message is: 11410599101
Binary Message: 01110010011010010110001101100101
CipherText : 00100111100001110010010110101010

The run Time of the Encryption Function is: 0.0007503000015276484

Process finished with exit code 0
```

```
Project
Run: Decryption
C:\Users\Lenovo\PycharmProjects\OneTimePad\venv\Scripts\python.exe C:\Users\Lenovo\PycharmProjects\OneTimePad\Decryption.py

Decryption
-----
The Secret Key is: 0101010101010111000000001111
The Ciphertext is: 001101111001111001000101111101
The deciphered bitStream is: 01100010011001010110000101110010
Message in ASCII is: 1650811250
Here is your Message: bear

Process finished with exit code 0
```

```
Project
Run: Decryption
C:\Users\Lenovo\PycharmProjects\OneTimePad\venv\Scripts\python.exe C:\Users\Lenovo\PycharmProjects\OneTimePad\Decryption.py

Decryption
-----
The Secret Key is: 0101010101010111000000001111
The Ciphertext is: 001100001100111100100110111100
The deciphered bitStream is: 01100101011001010110001101110011
Message in ASCII is: 1701143411
Here is your Message: eecs

Process finished with exit code 0
```

```
Project
Run: Decryption
C:\Users\Lenovo\PycharmProjects\OneTimePad\venv\Scripts\python.exe C:\Users\Lenovo\PycharmProjects\OneTimePad\Decryption.py

-----
Decryption
-----
The Secret Key is: 0101010101010111000000001111
The Ciphertext is: 0011011001001100001000111100
The deciphered bitStream is: 011000101100001011101000110011
Message in ASCII is: 1667331187
Here is your Message: cats

Process finished with exit code 0

Version Control Run Python Packages TODO Python Console Problems Terminal Services
Run selected configuration 15 CRLF UTF-8 4 spaces Python 3.10 (OneTimePad)
```

```
Project
Run: Decryption
C:\Users\Lenovo\PycharmProjects\OneTimePad\venv\Scripts\python.exe C:\Users\Lenovo\PycharmProjects\OneTimePad\Decryption.py

-----
Decryption
-----
The Secret Key is: 0101010101010111000000001111
The Ciphertext is: 001101111000011001010101010
The deciphered bitStream is: 0110001001101001011010100101
Message in ASCII is: 1651075941
Here is your Message: bike

Process finished with exit code 0

Version Control Run Python Packages TODO Python Console Problems Terminal Services
Download pre-built shared indexes: Reduce the indexing time and CPU load with pre-built Python packages shared indexes // Always download // Download once // Don't show again // Configure... (29 minutes ago) 15 CRLF UTF-8 4 spaces Python 3.10 (OneTimePad)
```

```
Project
Run: Decryption
C:\Users\Lenovo\PycharmProjects\OneTimePad\venv\Scripts\python.exe C:\Users\Lenovo\PycharmProjects\OneTimePad\src\Decryption.py

-----
Decryption
-----

ERROR:
length is incorrect!

Process finished with exit code 0

Version Control Run Python Packages TODO Python Console Problems Terminal Services
Download pre-built shared indexes: Reduce the indexing time and CPU load with pre-built Python packages shared indexes // Always download // Download once // Don't show again // Configure... (today 09:11) 16 CRLF UTF-8 4 spaces Python 3.10 (OneTimePad)
```

c) Key Genration Function:

This program generates a new key based on the number we input which must be between 1 and 128(given in the project details). The new generated key will be stored in the newkey.txt.

Command to generate key:

Python src\KeyGen.py (number between 1 and 128)

Example: Python src\KeyGen.py 16

Output:

Here is sceenshot of some generated key.

The screenshot shows a Windows PowerShell terminal window with the following content:

```

PS C:\Users\Lenovo\PycharmProjects\OneTimePad\venv\Scripts> activate.ps1 cannot be loaded because running scripts is disabled on this system. For more information, see
about_Execution_Policies at https://go.microsoft.com/fwlink/?LinkID=135170.
+ CategoryInfo          : SecurityError: ([]) ParentContainsErrorRecordException
+ FullyQualifiedErrorId : UnauthorizedAccess

PS C:\Users\Lenovo\PycharmProjects\OneTimePad> python src\KeyGen.py 1
The new Secret Key is: 1

PS C:\Users\Lenovo\PycharmProjects\OneTimePad> python src\KeyGen.py 16
The new Secret Key is: 1111101001100011

PS C:\Users\Lenovo\PycharmProjects\OneTimePad> python src\KeyGen.py 32
The new Secret Key is: 100000100010101101001011100001

PS C:\Users\Lenovo\PycharmProjects\OneTimePad> python src\KeyGen.py 128
The new Secret Key is: 0000110001010010011111011000010100001111000000011110000101010110100100110110001000011001001101000010100010000101001000
PS C:\Users\Lenovo\PycharmProjects\OneTimePad>
  
```

d) Distribution of Keys:

This program runs 5001 times to check how frequently the same newly generated 4-digit secret keys repeat themselves. It maintains a counter and provides a list of keys and a list of frequencies to show how many times the same keys were generated.

The list of Keys and Frequencies looks like this:

	Keys	Frequencies
	0000	351
	0001	307
	0010	343
	0011	307
	0100	275
	0101	306
	0110	330
	0111	299
	1000	325
	1001	255
	1010	295
	1011	344
	1100	320
	1101	317
	1110	314
	1111	314

Command to run:

Python src\KeyFrequency.py

e) Encryption runtime:

This program is used to run the Enc() function 10 times and find the average running time that the function for Encryption takes. It will return the average time that the function runs for.

Command:

```
python EncryptRunTime.py
```