Dept. of Information Technology, DTU

SUBMITTED TO

Mr. Kapil Sharma,
HOD of Dept. of Information Technology

SUBMITTED BY

Akaash Nidhiss 2K19/IT/008
Anasuya Mithra 2K19/IT/018

Image Encryption & Decryption using AES Algorithm

Table of Contents

I Introduction

There has been a recent increase in the number of people who use computers and other gadgets for communication and data transmission. Along with these individuals, there has been an increase in the number of unauthorised users who are attempting to gain access to data through deception. As a result, the issue of data security arises. Images are transferred across an unsecured transmission channel from a variety of sources; some image data contains classified data, and some images are very sensitive; hence, protecting them from assault is crucial.

To fix this, we encrypt and decrypt images using the AES method. Unauthorized users cannot read this encrypted data. It can be delivered across the network and decrypted at the receiving end using AES. As a result, the image transmission is secured.

I AES

AES is based on ‘substitution–permutation network’. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations). AES is widely used today as it is a much stronger than DES and triple DES despite being harder to implement.

Key Points

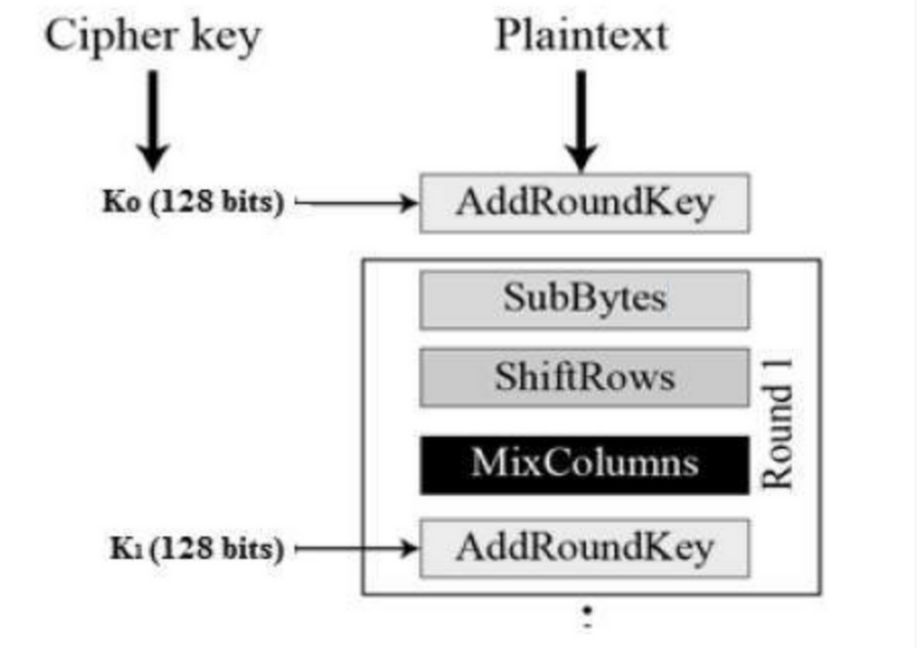
- AES is a symmetric block cipher.
- The key size can be 128/192/256 bits.
- Encrypts data in blocks of 128 bits each.
- Stronger and faster than Triple-DES
- The number of rounds depends on the key length as follows :
  - 128 bit key – 10 rounds
  - 192 bit key – 12 rounds
  - 256 bit key – 14 rounds

I Operation of AES

- AES uses bytes rather than bits to conduct operations. The cipher handles 128 bits (or 16 bytes) of input data at a time since the block size is 128 bits.
- These 16 bytes are arranged in 4 columns and 4 rows for processing as a matrix.
- The number of rounds in AES is variable and depends on the length of the key. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

I Encryption

- AES considers each block as a 16 byte (4 byte x 4 byte = 128) grid in a column major arrangement.
- Each round comprises of 4 steps:
  - SubBytes
  - ShiftRows
  - MixColumns
  - Add Round Key
- The last round doesn't have the MixColumns round.
- The SubBytes does the substitution and ShiftRows and MixColumns performs the permutation in the algorithm.



I Decryption

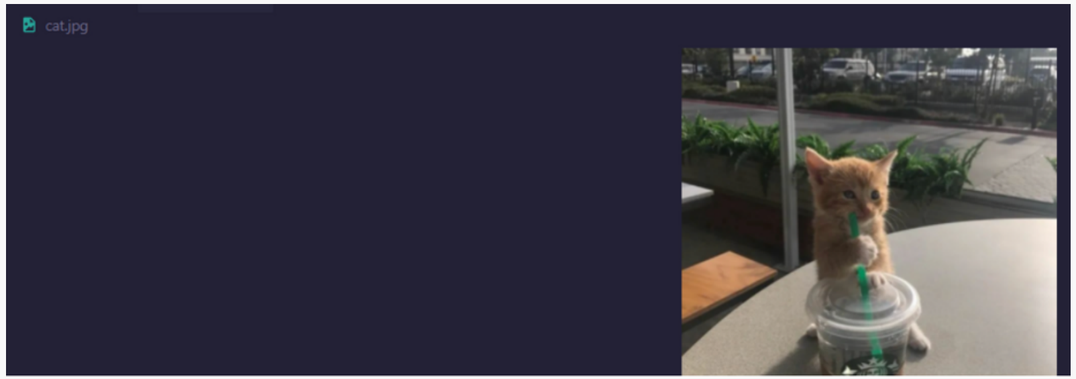
- The stages in the rounds can be easily undone as these stages have an opposite to it which when performed reverts the changes. Each 128 blocks goes through the 10,12 or 14 rounds depending on the key size.
- The stages of each round in decryption is as follows :
  - Add round key
  - Inverse MixColumns
  - ShiftRows
  - Inverse SubByte

- Since sub-processes in each round are in reverse manner, unlike for a Feistel Cipher, the encryption and decryption algorithms needs to be separately implemented, although they are very closely related.

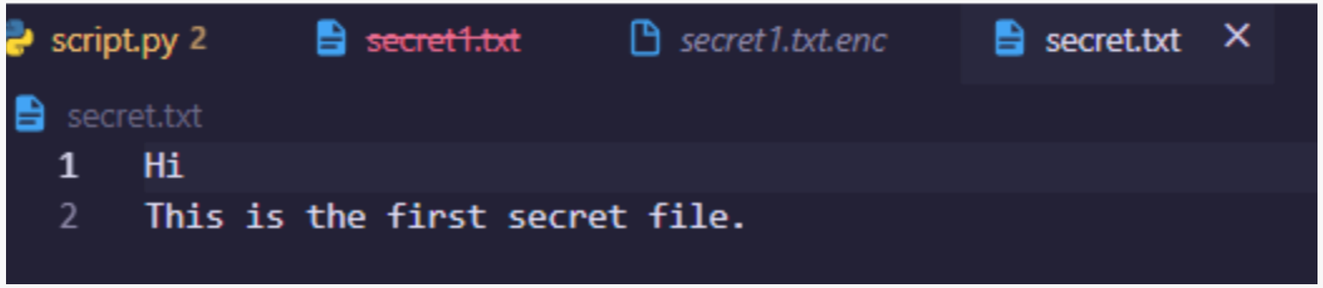
CODE

II Output Screenshots

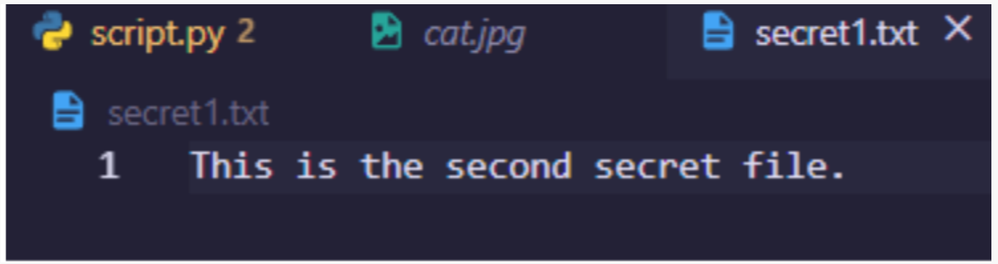
- The root folder contains the following files; script.py, secret.txt, secret1.txt, cat.jpg.
  - cat.jpg



  - secret.txt



  - secret.txt

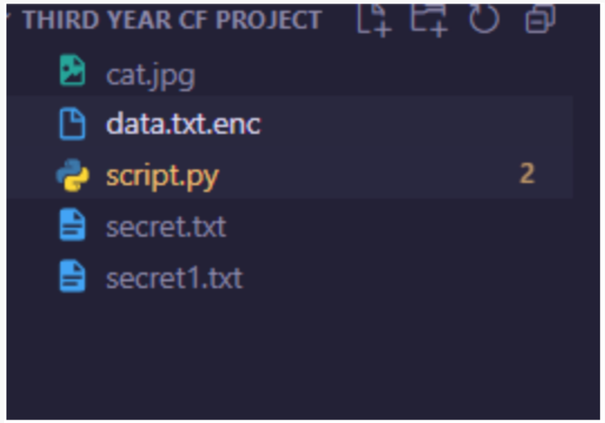


II Output Screenshots

- When we run ‘script.py’ for the first time, we have:

```
PS D:\University Project Folders\Third Year CF Project> py script.py
Please enter a password. It will be used to encrypt and decrypt your files: cyberforensics
```

- After running the following code, the data.txt.enc file is created which contains the password, ‘cyberforensics’



- The encrypted file appears like this.

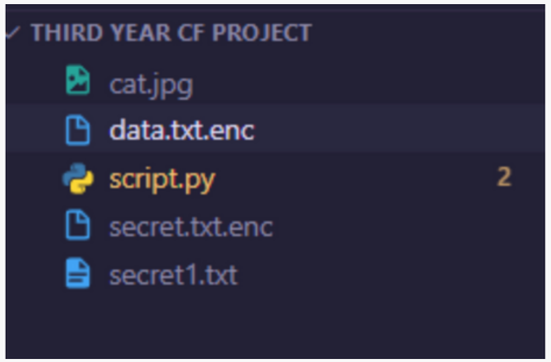
II Output Screenshots

- Once we run the script.py file again, the code prompts us for the password.

```
PS D:\University Project Folders\Third Year CF Project> py script.py
Enter the password: cyberforensics
```

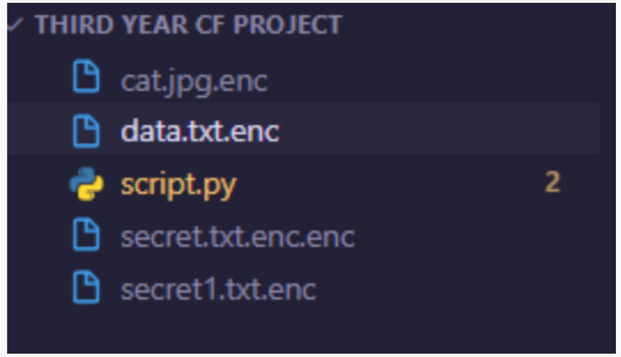
```
PS D:\University Project Folders\Third Year CF Project> py script.py
Enter the password: cyberforensics
Enter your choice of action:
        1. Encrypt file.
        2. Decrypt file.
        3. Encrypt all files in the directory.
        4. Decrypt all files in the directory.
        5. Exit.
1
Enter the name of the file you wish to encrypt: secret.txt
```

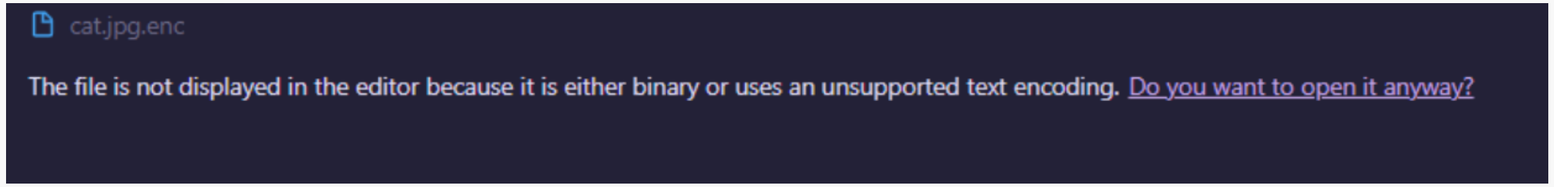
- Thus the secret.txt file is encrypted.

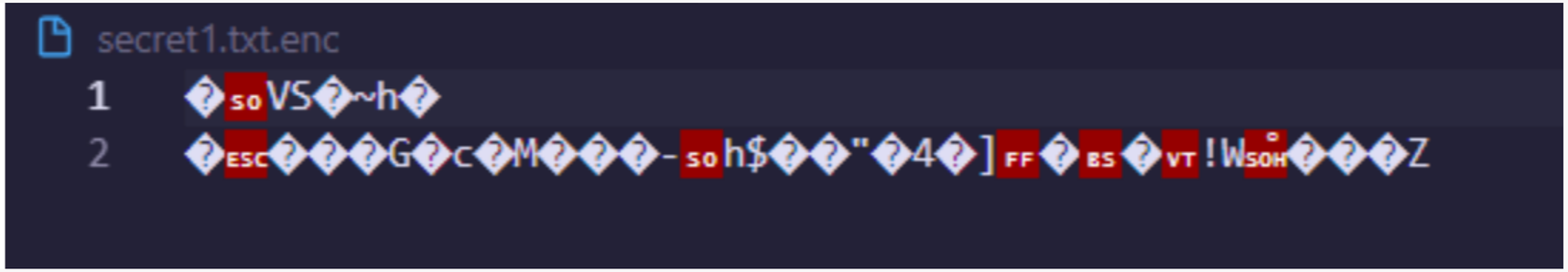


II Output Screenshots

- When we choose to encrypt all files in the directory.

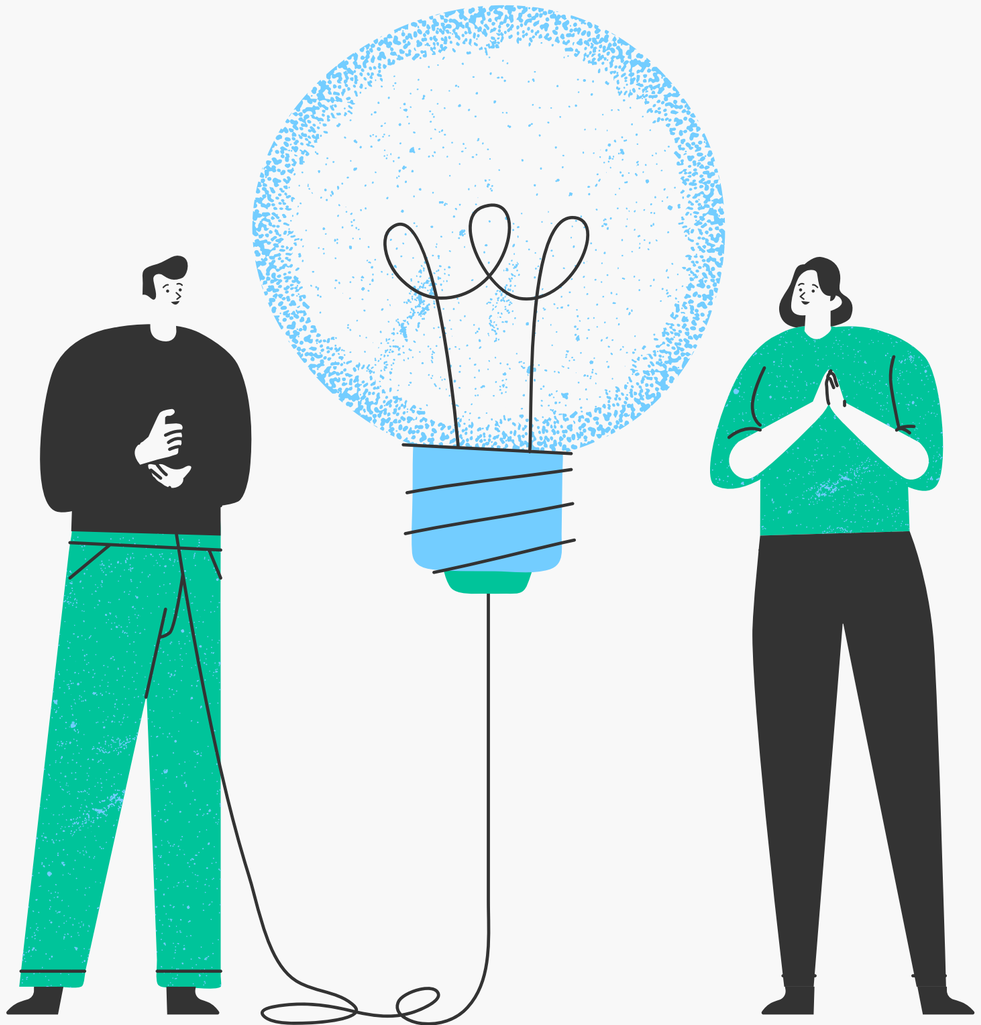






II Conclusion

- The system encrypts the provided file into an unreadable format. This is accomplished through the use of the AES encryption algorithm.
- The system decrypts the encrypted file and converts it to a readable format. This is accomplished through the use of the AES decryption mechanism. The produced image should be identical to the original.
- The mechanism ensures that the image is safely sent via any medium. Because unauthorised access is not permitted, a third-party system cannot make changes to the file being delivered.



Thank you for listening!