Securing Data through Amalgam of Cryptography and Steganography

PRESENTED BY

GADA, SHARANYA- TEAM LEAD

ATTULURI, SAI

MUDDANA, TULASI PALEM,
KISHORE

PERUMALLA, VENKATA KRISHNA MEHER KANJARA,

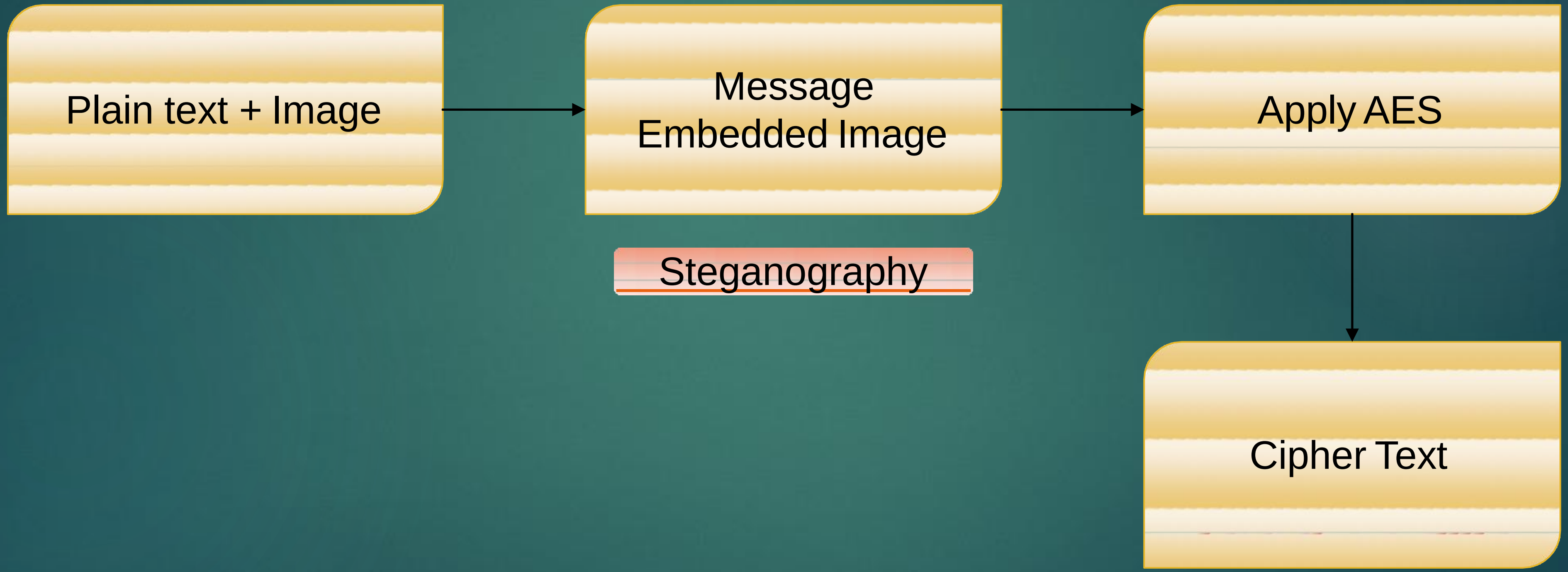
SABAREESH THIRUVEEDHI

Agenda

- Cryptography
- Steganography
- Advanced Encryption Standard (AES)
- Implementation
- Code Results
- Conclusion

Project Walk Thru

- Encryption



Plain text + Image

Message Embedded Image

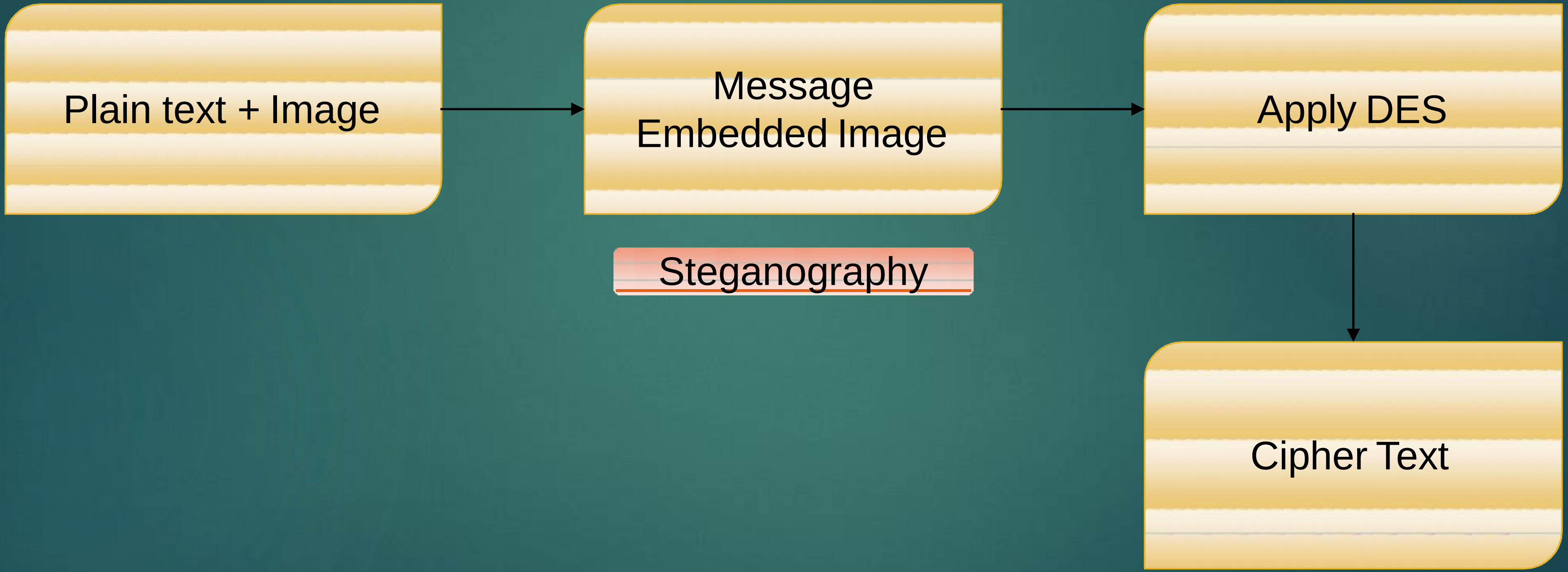
Steganography

Apply AES

Cipher Text

Project Walk Thru

- Encryption



Plain text + Image

Message Embedded Image

Steganography

Apply DES

Cipher Text

Steganography

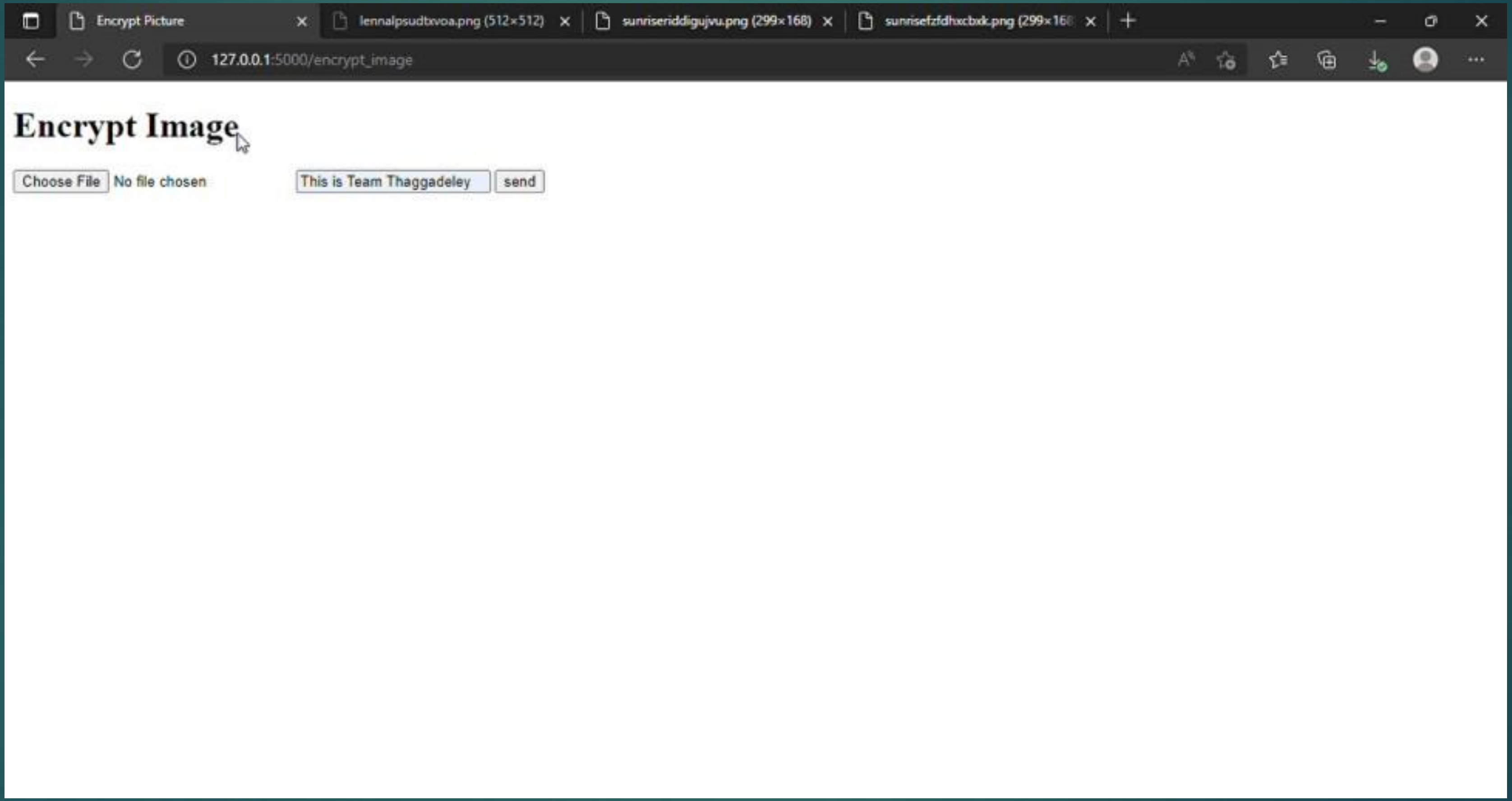
Least Significant Bit

Digital Image:

- A Digital image as represented is composed of X rows by Y columns.
- The coordinates: [a,b] of a point, such as $0 <= a < X$; $0 <= b < Y$, is called a pixel.
- A pixel represents a smallest addressable element of a picture.

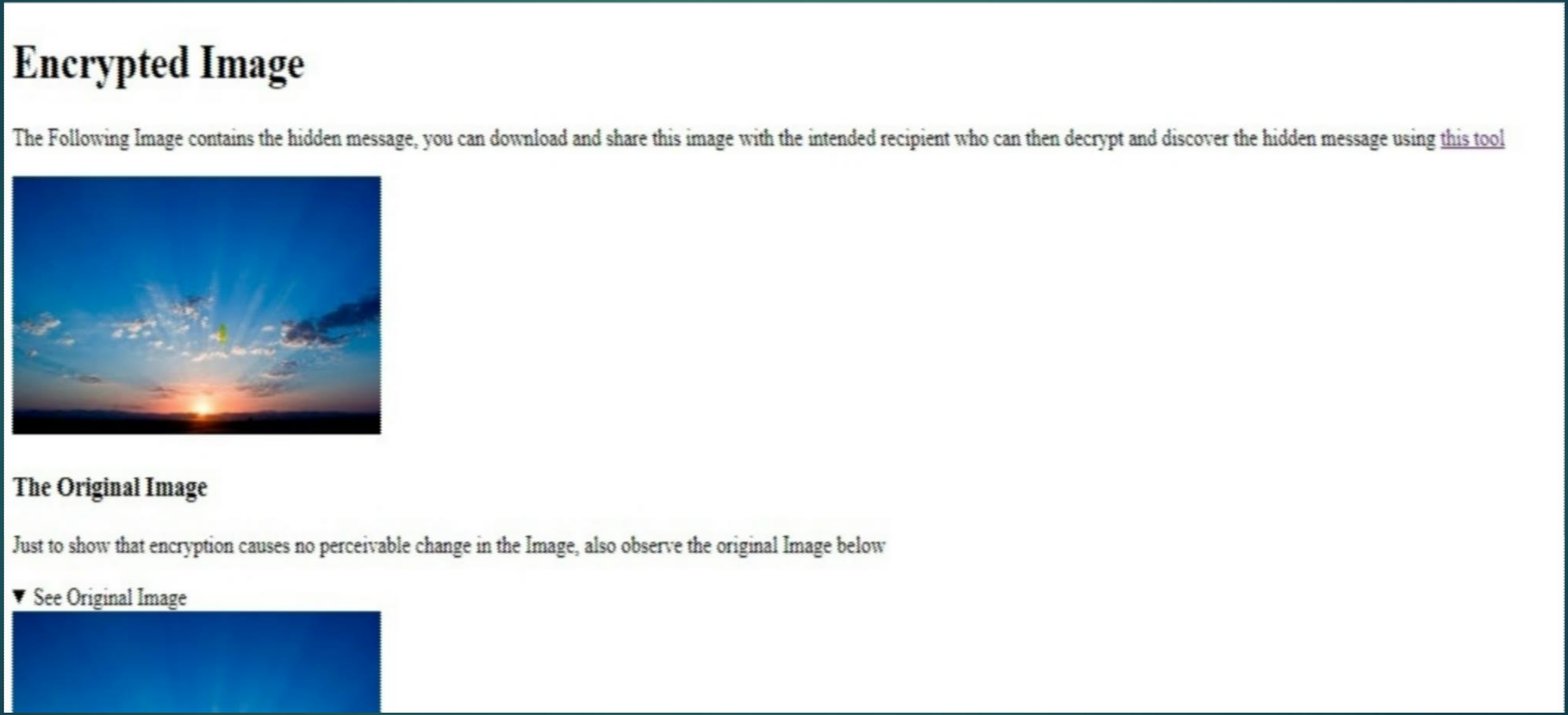
- Each pixel is assigned a color and is usually divided into three primary colors: red, green, and blue. Then specifying the pixel as a pixel (red, green, blue). This is called the RGB model.
- Red, Green, and blue intensities can vary from 0 to 255.
  WHITE = (255,255,255) and BLACK = (0,0,0).
- Pixels require 3 bytes of memory. 1 byte for each major component (hence the maximum
  value is 255).
- One byte consists of 8 bits representing a binary number (eg. 1010 0101).
- The maximum value a byte can take is 11111111, which is a decimal number of 255.

Steganography Demo


Encrypt Picture
lennalpsudtxvoa.png (512×512)
sunriseriddigujvu.png (299×168)
sunrisefzfdhxcbxk.png (299×168
127.0.0.1:5000/encrypt_image
Choose File
No file chosen
send

Encrypt Image

This is Team Thaggadeley



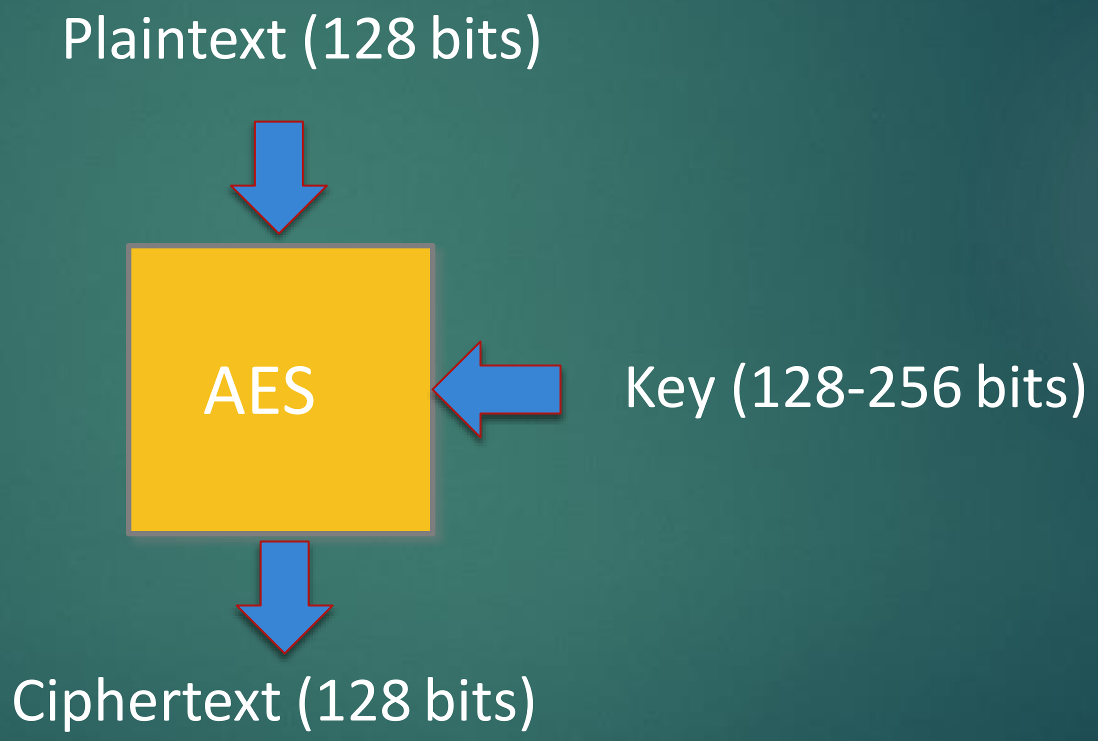
Encrypted Image

The Following Image contains the hidden message, you can download and share this image with the intended recipient who can then decrypt and discover the hidden message using this tool

The Original Image

Just to show that encryption causes no perceivable change in the Image, also observe the original Image below

Advanced Encryption Standard



Key Features

Key Expansion

- Round keys are derived from the cipher key using Rijndael's key schedule

Initial Round

- AddRoundKey : Each byte of the state is combined with the round key using bitwise xor

Rounds

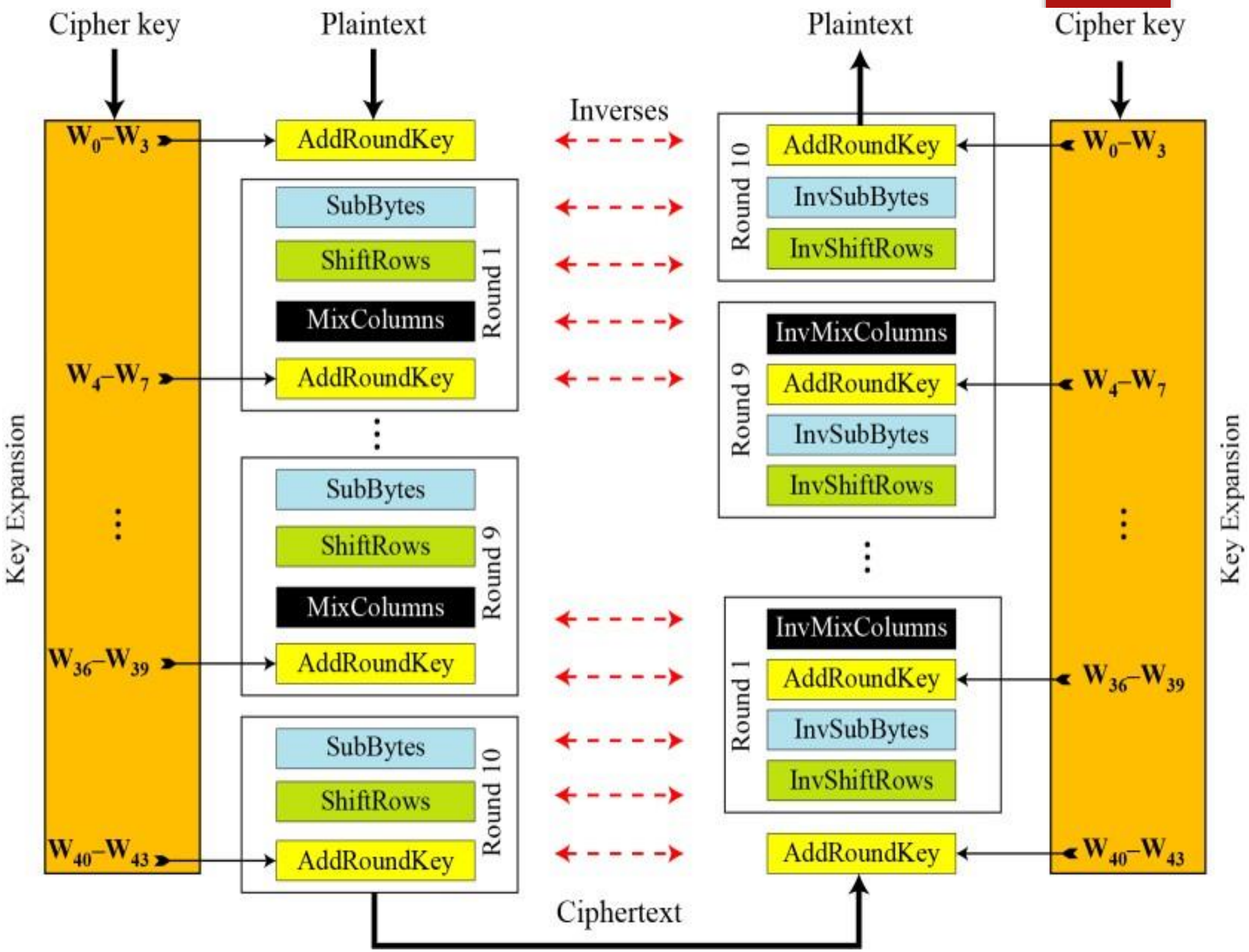
- SubBytes : non-linear substitution step
- ShiftRows : transposition step
- MixColumns : mixing operation of each column.
- AddRoundKey

Final Round

- SubBytes
- ShiftRows
- AddRoundKey

Overall Structure

- Encryption consists of 10 rounds of processing for 128-bit keys.
- Except for the last round in each case, all other rounds are identical.
- Each round of processing includes one single-byte based substitution step, a row-wise permutation step, a column-wise mixing step, and the addition of the round key. The order in which these four steps are executed is different for encryption and decryption.



- AES also has the notion of a word. A word consists of four bytes, that is 32 bits. Therefore, each column of the state array is a word, as is each row.

- The plain text is of 4 words same with cipher text and key. Therefore, we have 44 words key, each round in AES uses 4 words thus making it to 40 words and the remaining i.e., the initial 4 words are used in the initial stage of AES where we use it in pre addition stage along with plain text.

- The first four bytes of a 128-bit input block occupy the first column in the 4 × 4 array of bytes. The next four bytes occupy the second column, and so on

- The output state array produced by the last round is rearranged into a 128-bit output block.

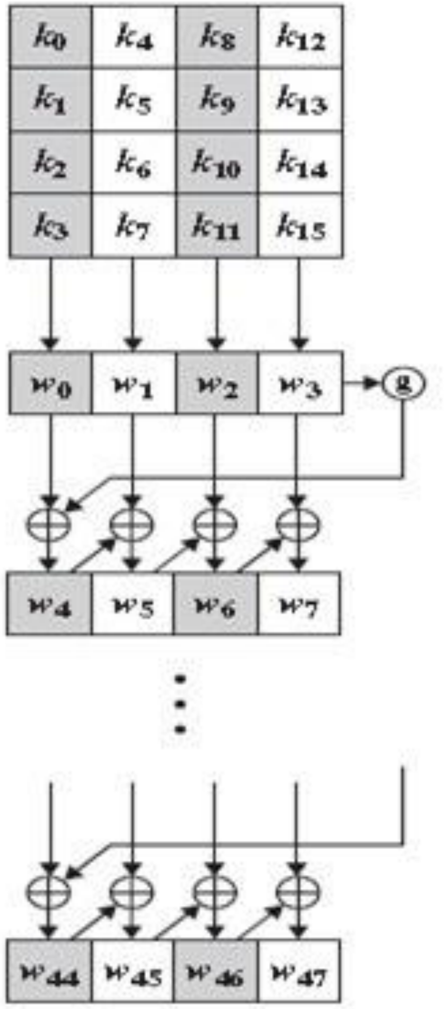
- The g function performs the one byte
- G-function:

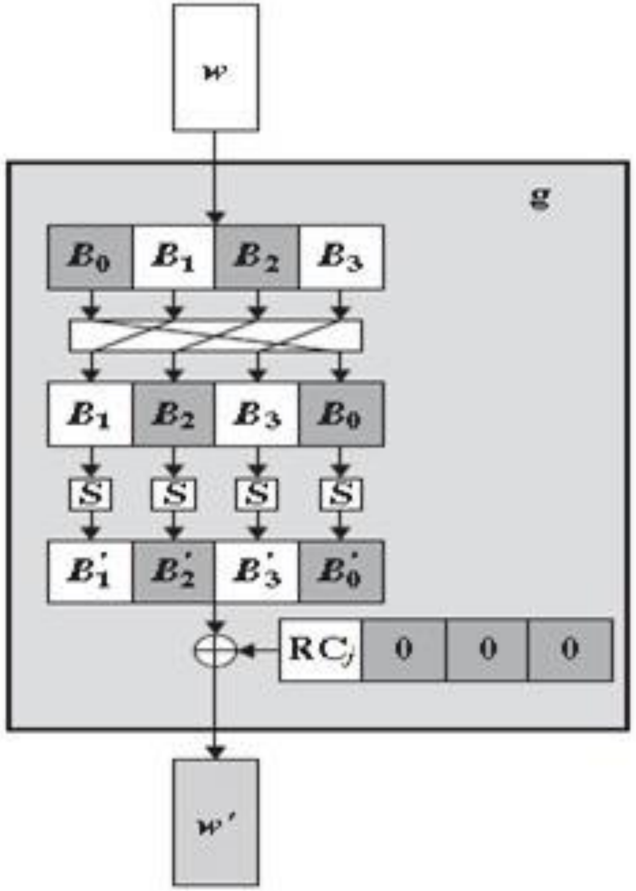
  It has sub functions

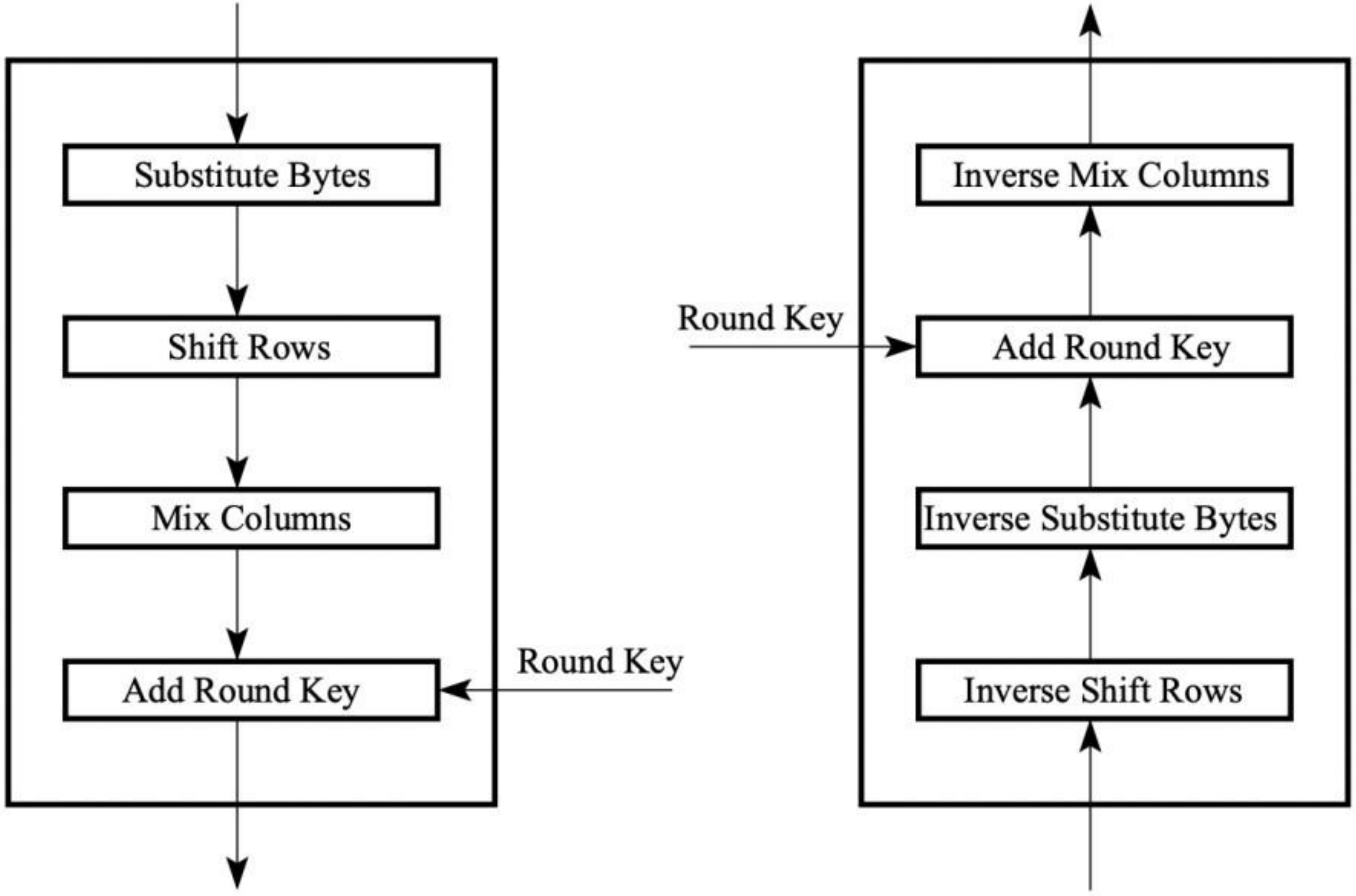
  a)one-byte circular left shift

  b)byte-substitution using s-boxes

  c)XOR function with the round-constant Rconst







Encryption Round

Decryption Round

THE FOUR STEPS IN EACH ROUND OF PROCESSING

- *SubBytes:*

  This step consists of using a 16 × 16 lookup table to find a replacement byte for a given byte in the input state array.

- *ShiftRows:*

  The state array bits are shifted accordingly as shown below which then is sent to mix columns.

  0th row – shifted 0 times; 1st row – shifted 1 times; 2nd row – shifted 2 times; 3rd row – shifted 3 times

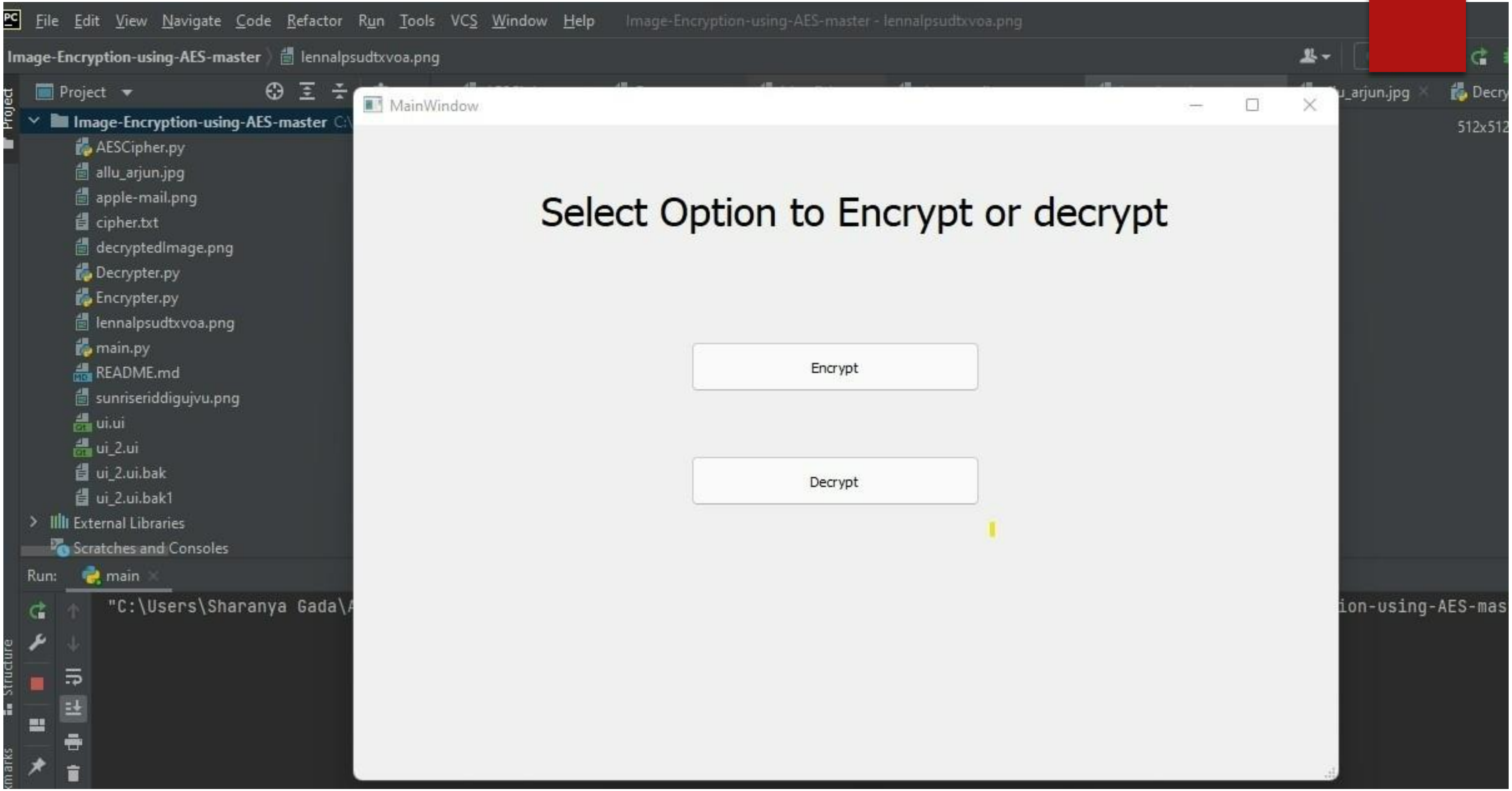
- *MixColumns*:

  In mix columns stage, each word (column wise) is multiplied with the following matrix and the resultant is stored in the state array.

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$

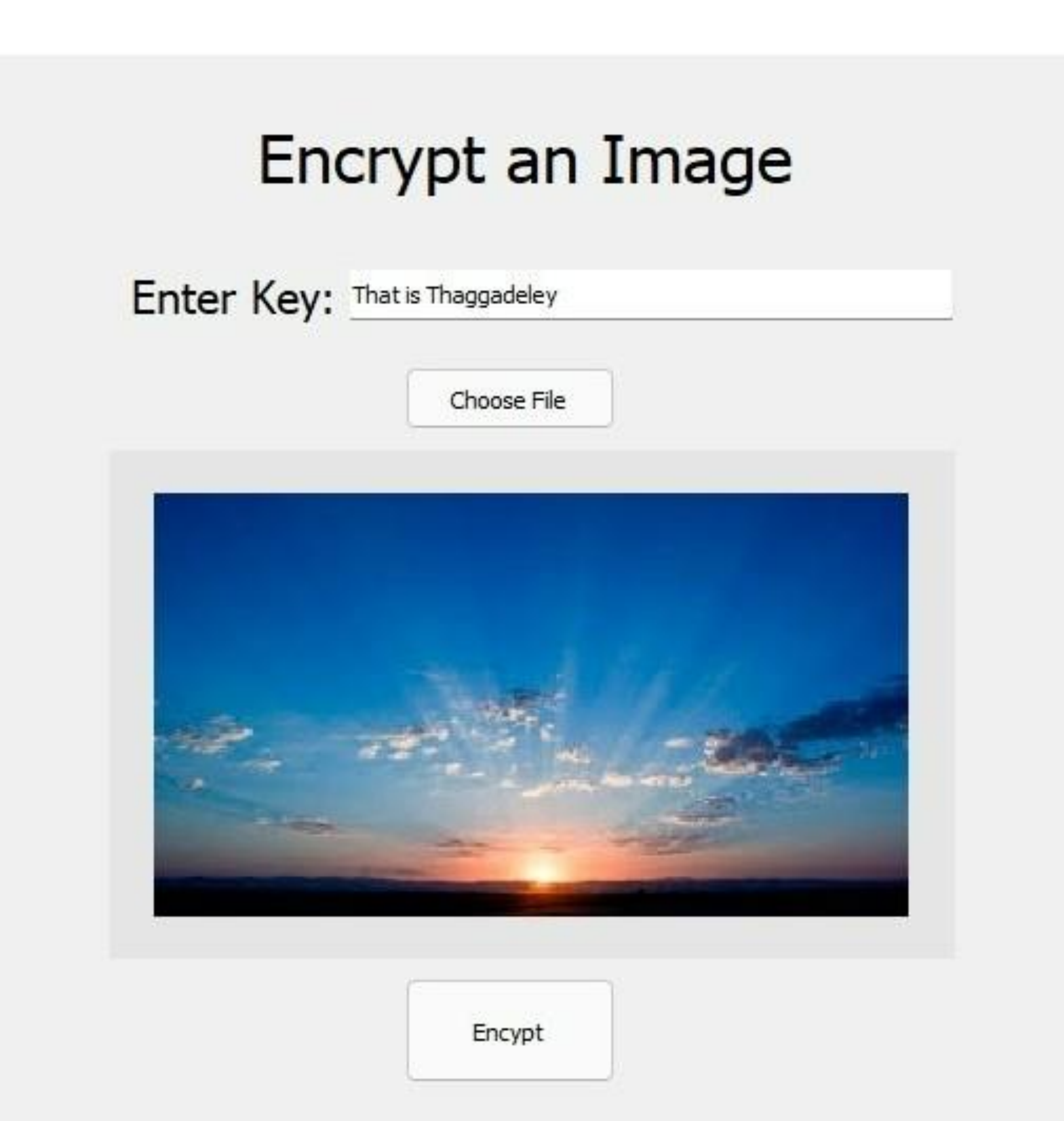
- *AddRoundKey:*

XOR state with 128-bits of the round key proceeds one column at a time. Adds a round key word with each state column matrix the operation is matrix addition



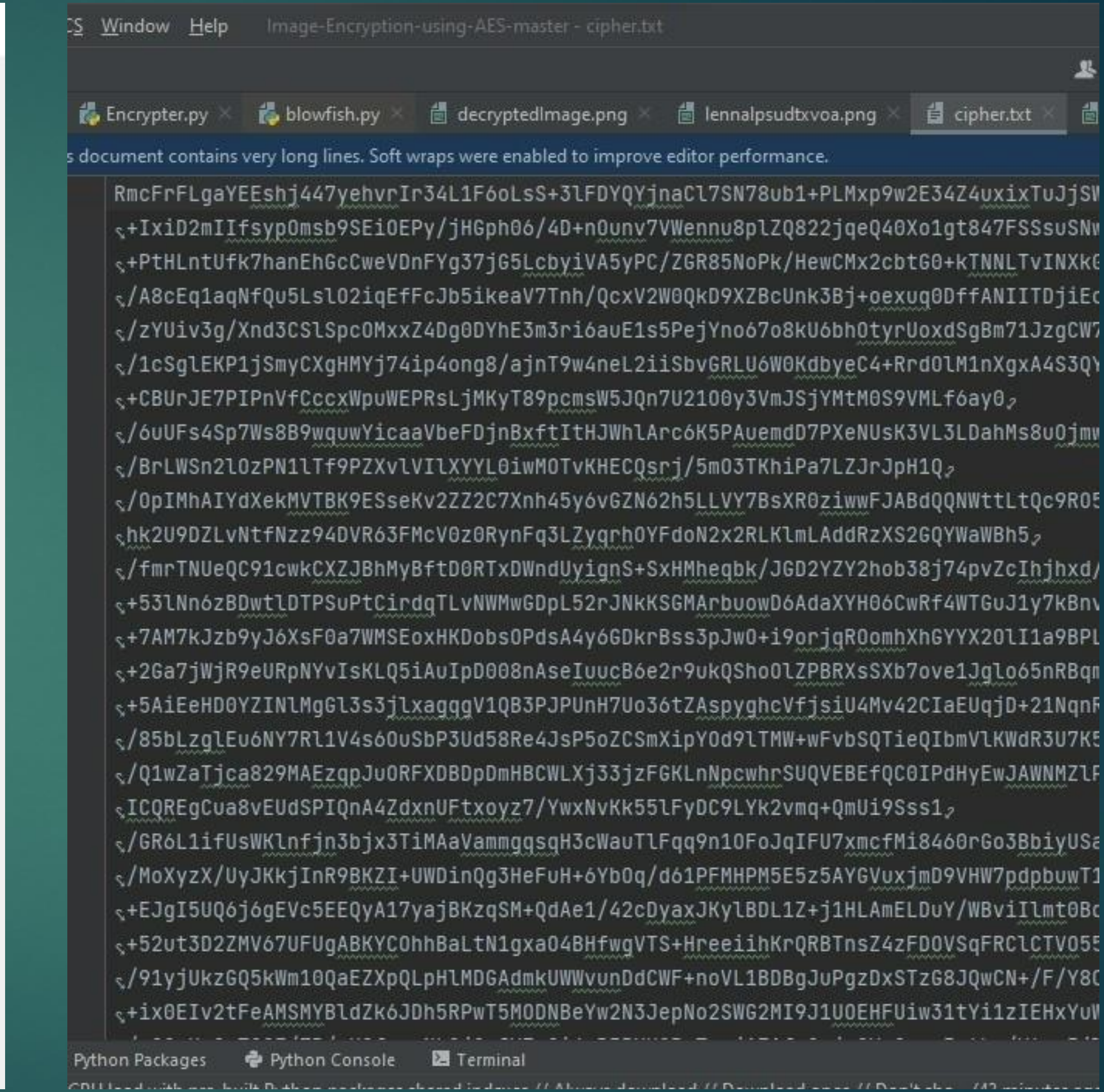
Select Option to Encrypt or decrypt

```
"C:\Users\Sharanya Gada\A
ion-using-AES-mas
```



Encrypt an Image

Enter Key: That is Thaggadeley



s document contains very long lines. Soft wraps were enabled to improve editor performance.

```
RmcFrFLgaYEEshj447yehvrIr34L1F6oLsS+3lFDYQYjnaCl7SN78ub1+PLMxp9w2E34Z4uxixTuJjSW
+IxiD2mIIfsypOmsb9SEiOEPy/jHGph06/4D+nOunv7VWennu8plZQ822jqeQ40Xo1gt847FSSsuSNw
+PtHLntUfk7hanEhGcCweVDnFYg37jG5LcbyiVA5yPC/ZGR85NoPk/HewCMx2cbtG0+kTNNLTvINXkG
/A8cEq1aqNfQu5Lsl02iqEfFcJb5ikeaV7Tnh/QcxV2W0QkD9XZBcUnk3Bj+oexuq0DffANIITDjiEc
/zYUiv3g/Xnd3CSlSpcOMxxZ4Dg0DYhE3m3ri6auE1s5PejYno67o8kU6bhOtyrUoxdSgBm71JzgCW7
/1cSglEKP1jSmyCXgHMYj74ip4ong8/ajnT9w4neL2iiSbvGRLU6W0KdbyeC4+Rrd0lM1nXgxA4S3QY
+CBUrJE7PIPnVfCccxWpuWEPRsLjMKyT89pcmsW5JQn7U2100y3VmJSjYMtM0S9VMLf6ay0
/6uUFs4Sp7Ws8B9wquwYicaaVbeFDjnBxftItHJWhlArc6K5PAuemdD7PXeNUsK3VL3LDahMs8uOjmw
/BrLWSn2lOzPN1lTf9PZXvlVIlXYYL0iwMOTvKHECQsrj/5mO3TKhiPa7LZJrJpH1Q
/OpIMhAIYdXekMVTBK9ESseKv2ZZ2C7Xnh45y6vGZN62h5LLVY7BsXR0ziwwFJABdQQNWttLtQc9RO5
hk2U9DZLvNtfNzz94DVR63FMcV0z0RynFq3LZygrhOYFdoN2x2RLKlmLAddRzXS2GQYWaWBh5
/fmrTNUeQC91cwkCXZJBhMyBftD0RTxDWndUyignS+SxHMheqbk/JGD2YZY2hob38j74pvZcIhjhxd/
+53lNn6zBDwtlDTPSuPtCirdqTLvNWMwGDpL52rJNkKSGMArbuowD6AdaXYH06CwRf4WTGuJ1y7kBnv
+7AM7kJzb9yJ6XsF0a7WMSEoxHKDobsOPdsA4y6GDkrBss3pJw0+i9orjqR0omhXhGYYX20lI1a9BPL
+2Ga7jWjR9eURpNYvIsKLQ5iAuIpD008nAseIuucB6e2r9ukQShoOlZPBRXsSXb7ove1Jglo65nRBqm
+5AiEeHD0YZINlMgGl3s3jlxagqgV1QB3PJPUnH7Uo36tZAspyghcVfjsiU4Mv42CIaEUqjD+21NqnR
/85bLzglEu6NY7Rl1V4s6OuSbP3Ud58Re4JsP5oZCSmXipYOd9lTMW+wFvbSQTieQIbmVlKWdR3U7K5
/Q1wZaTjca829MAEzqpJuORFXDBDpDmHBCWLXj33jzFGKLnNpcwhrSUQVEBEfQC0IPdHyEwJAWNMZlF
ICQREgCua8vEUdSPIQnA4ZdxnUFtxoyz7/YwxNvKk55lFyDC9LYk2vmq+QmUi9Sss1
/GR6L1ifUsWKlnfjn3bjx3TiMAaVammgqsqH3cWauTlFqq9n10FoJqIFU7xmcfMi8460rGo3BbiyUSa
/MoXyzX/UyJKkjInR9BKZI+UWDinQg3HeFuH+6Yb0q/d61PFMHPM5E5z5AYGVuxjmD9VHW7pdpbuwT1
+EJgI5UQ6j6gEVc5EEQyA17yajBKzqSM+QdAe1/42cDyaxJKylBDL1Z+j1HLAmELDuY/WBviIlmt0Bc
+52ut3D2ZMV67UFUgABKYCOhhBaLtN1gxa04BHfwgVTS+HreeiihKrQRBTnsZ4zFDOVSqFRClCTVO55
/91yjUkzGQ5kWm10QaEZXpQLpHlMDGAdmkUWWvunDdCWF+noVL1BDBgJuPgzDxSTzG8JQwCN+/F/Y8C
+ix0EIv2tFeAMSMYBldZk6JDh5RPwT5MODNBeYw2N3JepNo2SWG2MI9J1UOEHFUiw31tYi1zIEHxYuW
```

AES SECURITY

- AES was designed after DES.
- Most of the known attacks on DES were already tested on AES.
- *Brute-Force Attack*

  AES is definitely more secure than DES due to the larger-size key.
- *Statistical Attacks*

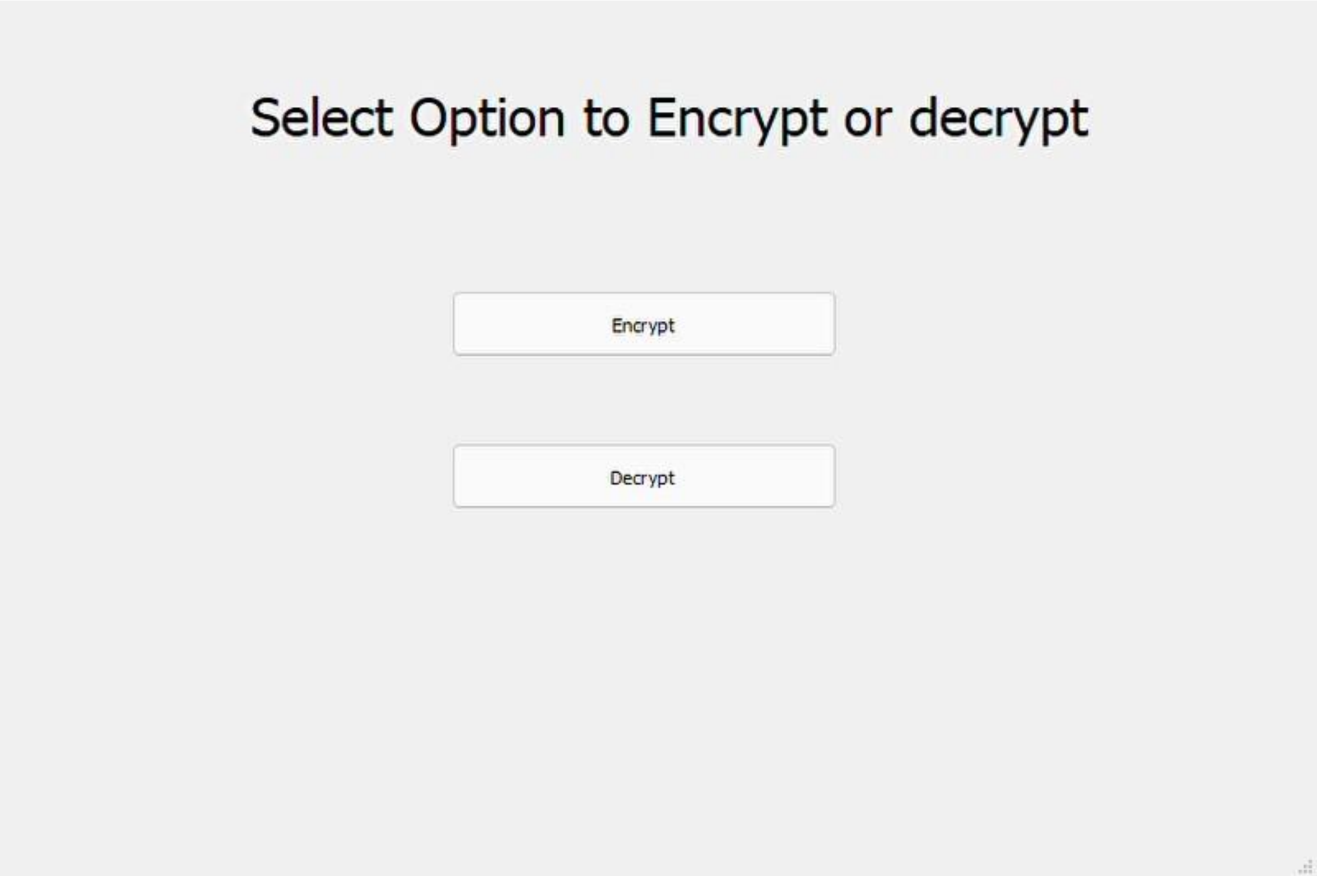
  Numerous tests have failed to do statistical analysis of the ciphertext
- *Differential and Linear Attacks*

  There are no differential and linear attacks on AES as yet.

DES VS AES

- Stronger & faster than Triple-DES
- A Replacement for DES was needed since the Key size was small
- AES is more secure than the DES cipher and is the de facto world standard.
- As DES was proven inadequate in terms of security, AES was introduced which is considered to provide the security needed.

Encryption



Select Option to Encrypt or decrypt

Implementation Parameters

- **Computational time**

  It is calculated by the time taken to produce a cipher text from a plain text i.e., total plain text in bytes encrypted divided by time taken to encrypt or decrypt the text.

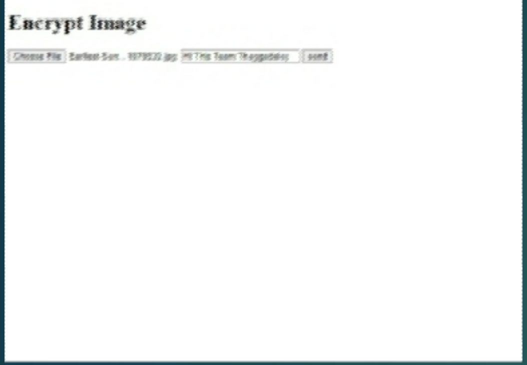
- **NPCR & UACI**

In general, it is one of the metrics used to assess the image encryption algorithm's security. Consider I1 and I2 as two pictures with a size of N ×M, and an array A with sizes that are comparable to I1 and I2.A(i,j)={ 0ifI1(i,j)=I2(i,j), 1ifI1(i,j)≠I2(i,j) }We can also calculate the percentage of pixels between two different images using,

$$NPCR=\sum N\times Mij-1D(i,j)N\times M\times 100\%$$

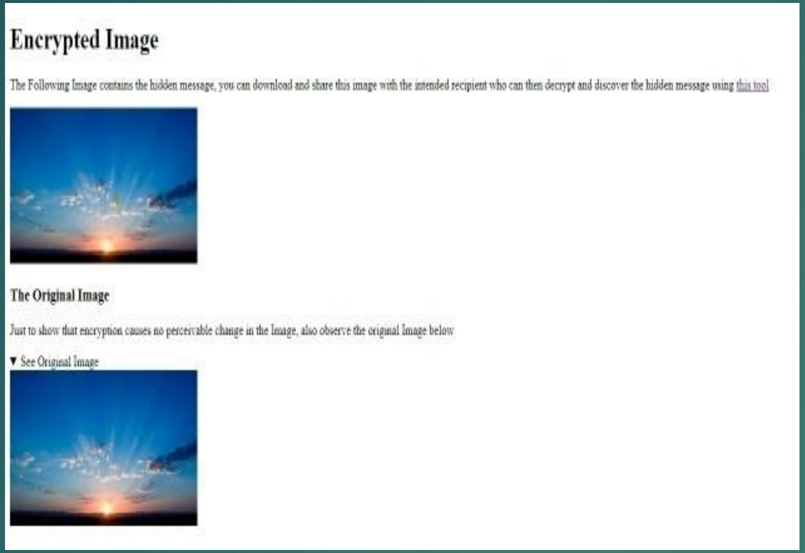
The two most popular variables used to measure the strength of picture encryption or decryption techniques are NPCR and UACI.A high value of those probably equates to a better resistance to assaults.

Parameters	DES Encryption Algorithm	AES Encryption Algorithm
Encryption Time (in sec)	215.9359	99.871
NPCR	99.6643	99.6399
UACI	51.2496	50.8584



Encrypt Image

Choose File Earliest-Sun... 1979533.jpg Hi This Team Thaggadeley send



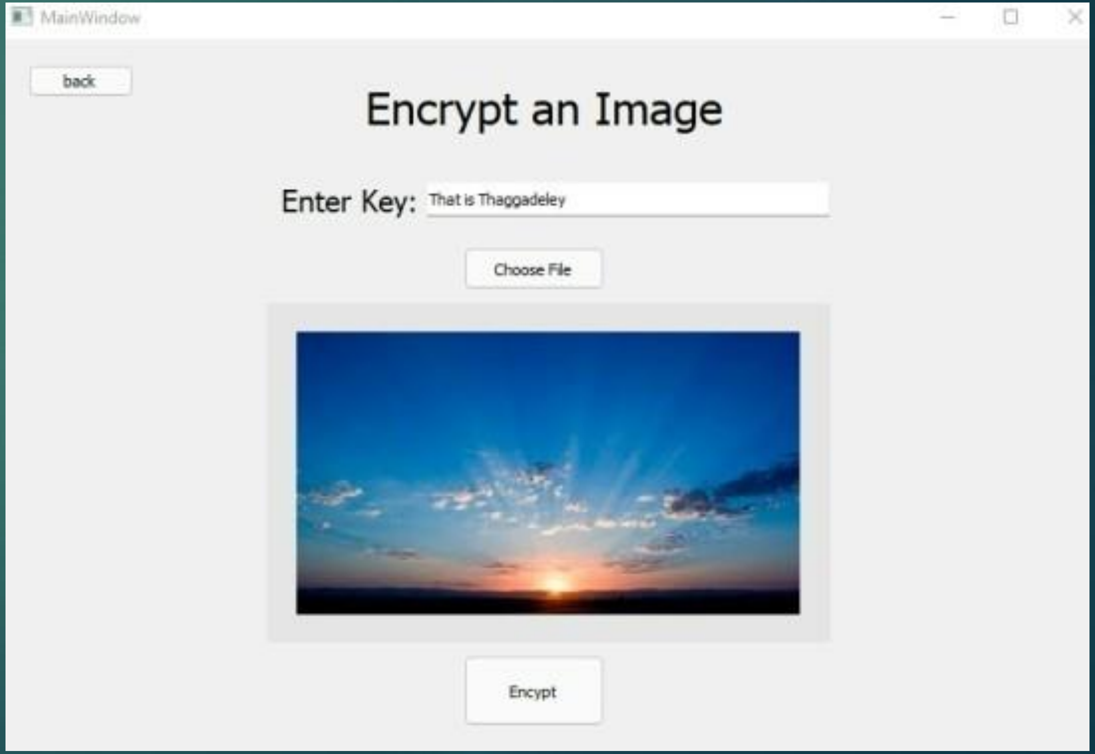
Encrypted Image

The Following Image contains the hidden message, you can download and share this image with the intended recipient who can then decrypt and discover the hidden message using this tool

The Original Image

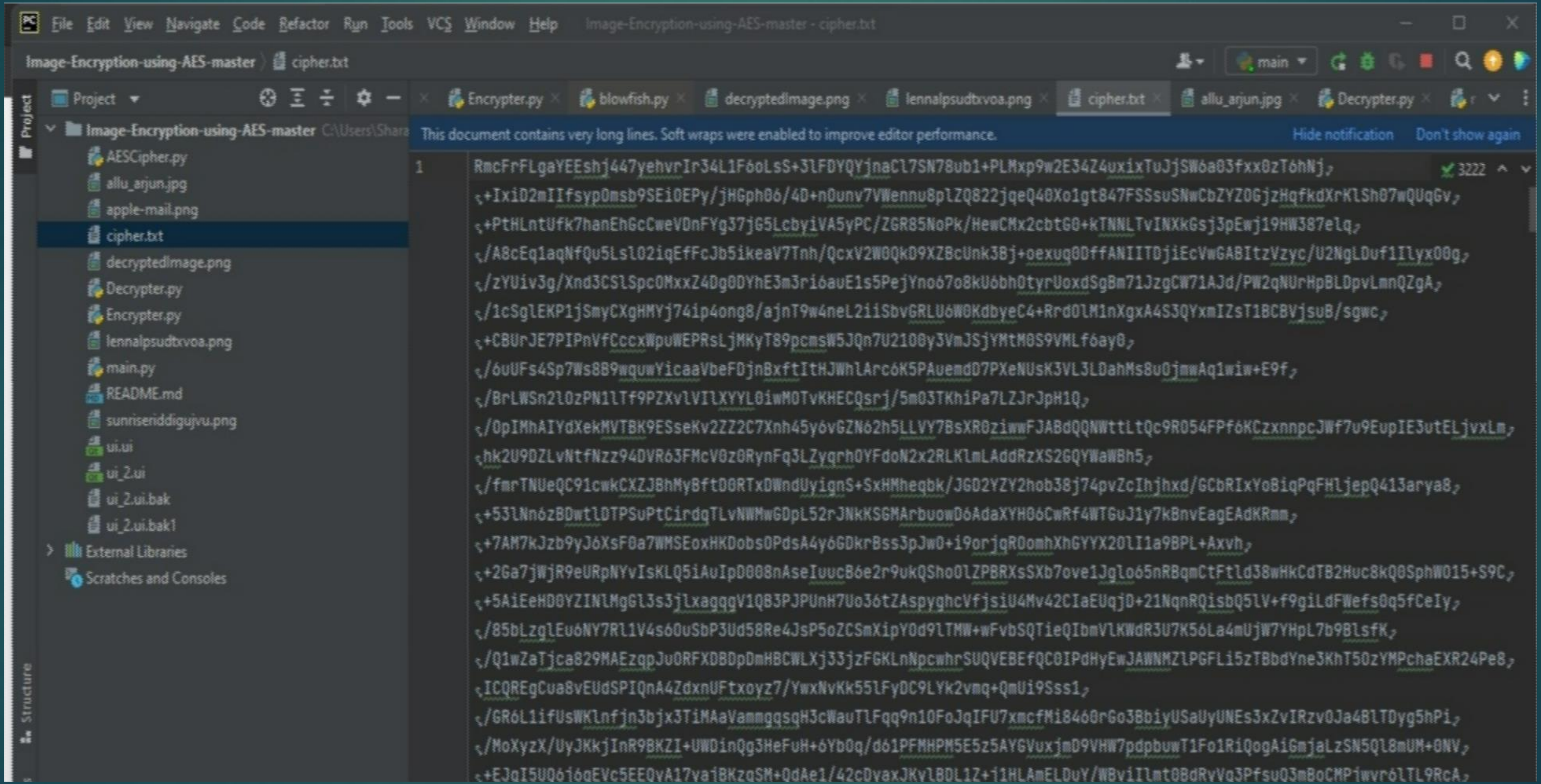
Just to show that encryption causes no perceivable change in the Image, also observe the original Image below

▼ See Original Image



Encrypt an Image

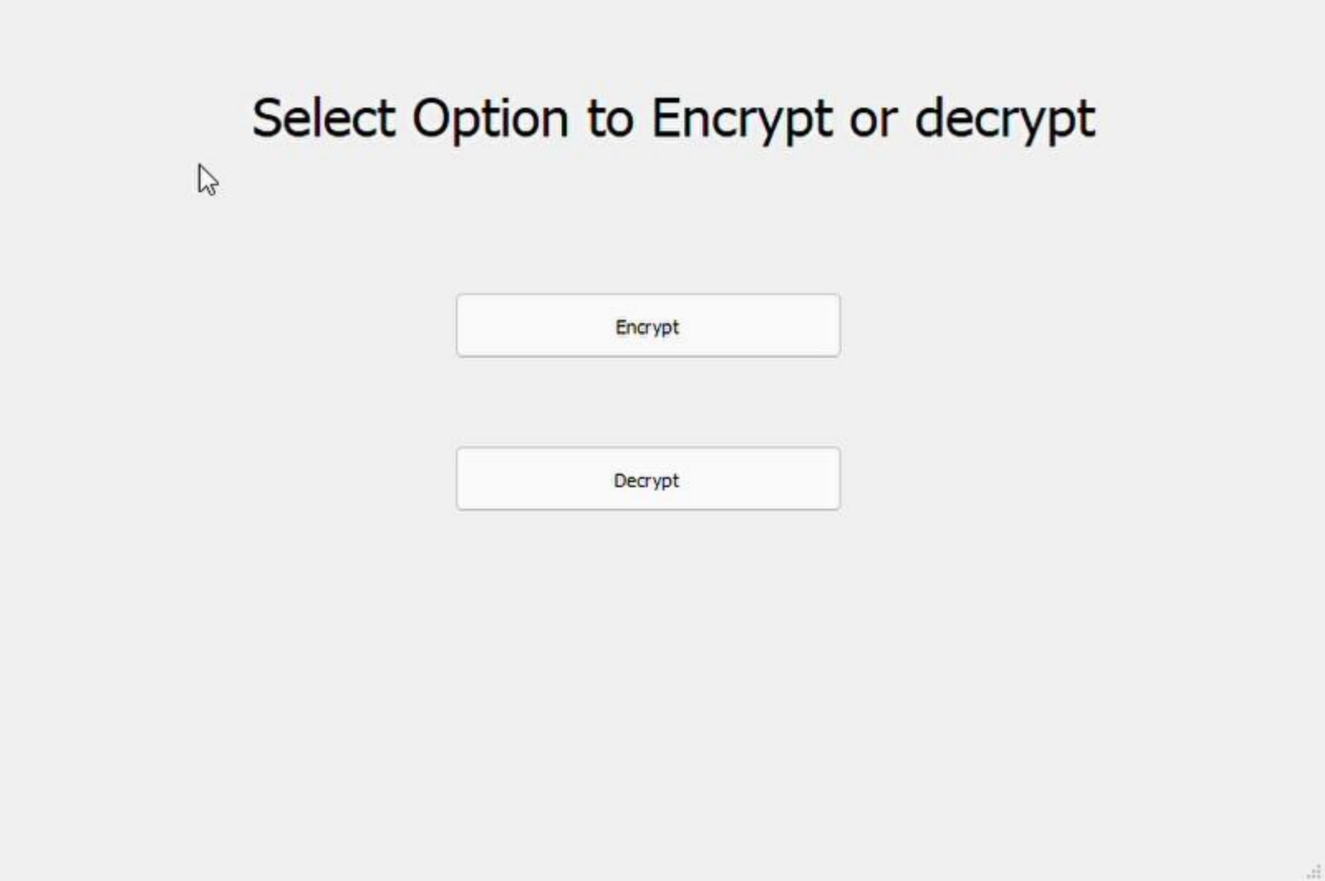
Enter Key: That is Thaggadeley



This document contains very long lines. Soft wraps were enabled to improve editor performance.

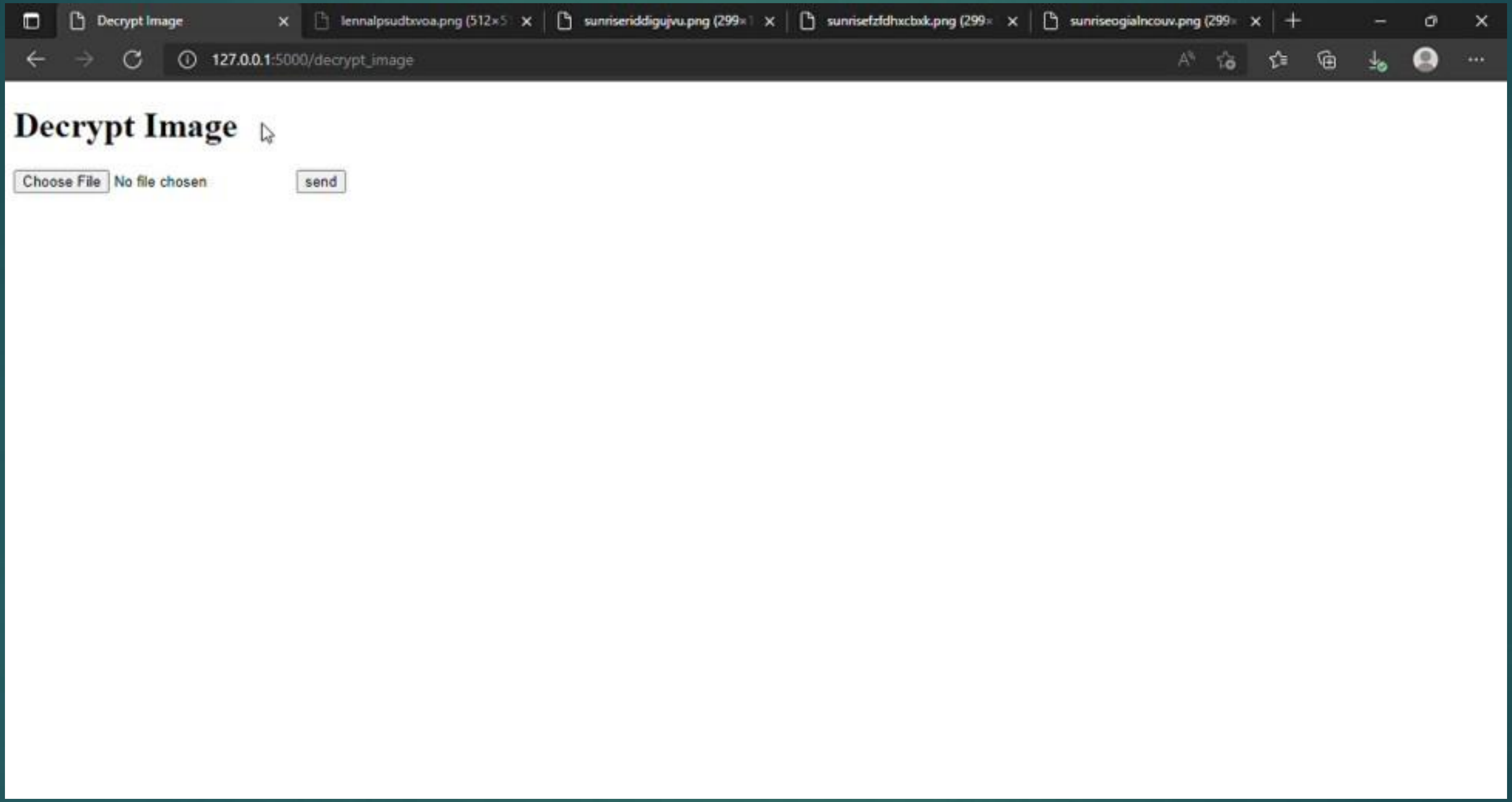
```
RmcFrFLgaYEEshj447yehvrIr34L1F6oLsS+3lFDYQYjnaCl7SN78ub1+PLMxp9w2E34Z4uxixTuJjSW6a03fxx0zT6hNj
+IxiD2mIIfsyp0msb9SEi0EPy/jHGph06/4D+n0unv7VWennu8plZQ822jqeQ40Xo1gt847FSSsuSNwCbZYZ0GjzHqfkdXrKlSh07wQUqGv
+PtHLntUfk7hanEhGcCweVDnFYg37jG5LcbyiVA5yPC/ZGR85NoPk/HewCMx2cbtG0+kTNNLTvINXkGsj3pEwj19HW387elq
/A8cEq1aqNfQu5Lsl02iqEfFcJb5ikeaV7Tnh/QcxV2W0Qk09XZBcUnk38j+oexuq0DffANIITDjiEcVwGABItzVzyc/U2NgLDuf1Ilyx00g
/zYUiv3g/Xnd3CSlSpc0MxxZ4Dg0DYhE3m3ri6auE1s5PejYno67o8kU6bh0tyrUoxdSgBm71JzgCW71AJd/PW2qNUrHpBLDpvLmnQZgA
/1cSglEKP1jSmyCXgHMYj74ip4ong8/ajnT9w4neL2iiSbvGRLU6W0KdbyeC4+Rrd0lM1nXgxA4S3QYxmIZsT1BCBVjsuB/sgwc
+CBUrJE7PIPnVfCccxWpuWEPRsLjMKyT89pcmsW5JQn7U2100y3VmJSjYMtM0S9VMLf6ay0
/6uUFs4Sp7Ws8B9wquwYicaaVbeFDjnBxftItHJWhlArc6K5PAuemd07PXeNUsK3VL3LDahMs8u0jmwAq1wiw+E9f
/BrLWSn2l0zPN1lTf9PZXvlVIlXYYL0iwM0TvKHECQsrj/5m03TKhiPa7LZJrJpH1Q
/0pIMhAIYdXekMVTBK9ESseKv2ZZ2C7Xnh45y6vGZN62h5LLVY7BsXR0ziwwFJABdQQNWttLtQc9R054FPf6KCzxnnpcJWf7u9EupIE3utELjvxLm
hk2U9DZLvNtfNzz94DVR63FMcV0z0RynFq3LZyqrh0YFdoN2x2RLKlmLAddRzXS2GQYWaWBh5
/fmrTNUeQC91cwkCXZJBhMyBftD0RTxDWndUyignS+SxHMheqbk/JGD2YZY2hob38j74pvZcIhjhxd/GCbRIxYoBiqPqFHljepQ413arya8
+53lNn6zBDwtlDTPSuPtCirdqTLvNWMwGDpL52rJNkKSGMArbuowD6AdaXYH06CwRf4WTGuJ1y7kBnvEagEAdKRmm
+7AM7kJzb9yJ6XsF0a7WMSEoxHKDobs0PdsA4y6GDkrBss3pJw0+i9orjqR0omhXhGYYX20lI1a9BPL+Axvh
+2Ga7jWjR9eURpNYvIsKLQ5iAuIpD008nAseIuucB6e2r9ukQSho0lZPBRXsSXb7ove1Jglo65nRBqmCtFtld38wHkCdTB2Huc8kQ0SphW015+S9C
+5AiEeHD0YZINlMgGl3s3jlxaqqqV1QB3PJPUnH7Uo36tZAspyghcVfjsiU4Mv42CIaEUqjD+21NqnRQisbQ5lV+f9giLdFWefs0q5fCeIy
/85bLzglEu6NY7Rl1V4s60uSbP3Ud58Re4JsP5oZCSmXipY0d9lTMW+wFvbSQTieQIbmVlKWdR3U7K56La4mUjW7YHpL7b9BlsfK
/Q1wZaTjca829MAEzqpJu0RFXDBDpDmHBCWLXj33jzFGKLnNpcwhrSUQVEBEfQC0IPdHyEwJAWNMZlPGFLi5zTBbdYne3KhT50zYMPchaEXR24Pe8
ICQREgCua8vEUdSPIQnA4ZdxnUFtxoyz7/YwxNvKk55lFyDC9LYk2vmq+QmUi9Sss1
/GR6L1ifUsWKlnfjn3bjx3TiMAaVammqqsqH3cWauTlFqq9n10FoJqIFU7xmcfMi8460rGo3BbiyUSaUyUNEs3xZvIRzv0Ja4BlTDyg5hPi
/MoXyzX/UyJKkjInR9BKZI+UWDinQg3HeFuH+6Yb0q/d61PFMHPM5E5z5AYGVuxjmD9VHW7pdpbuwT1Fo1RiQogAiGmjaLzSN5Ql8mUM+0NV
+EJqI5U06j6qEVc5EEQvA17vajBKzqSM+QdAe1/42cDvaxJKvlBDL1Z+j1HLAmELDuY/WBviIlmt0BdRvVq3PfsuQ3mBoCMPjwvr6lTL9RcA
```

AES Decryption



Select Option to Encrypt or decrypt

Steganography Decryption

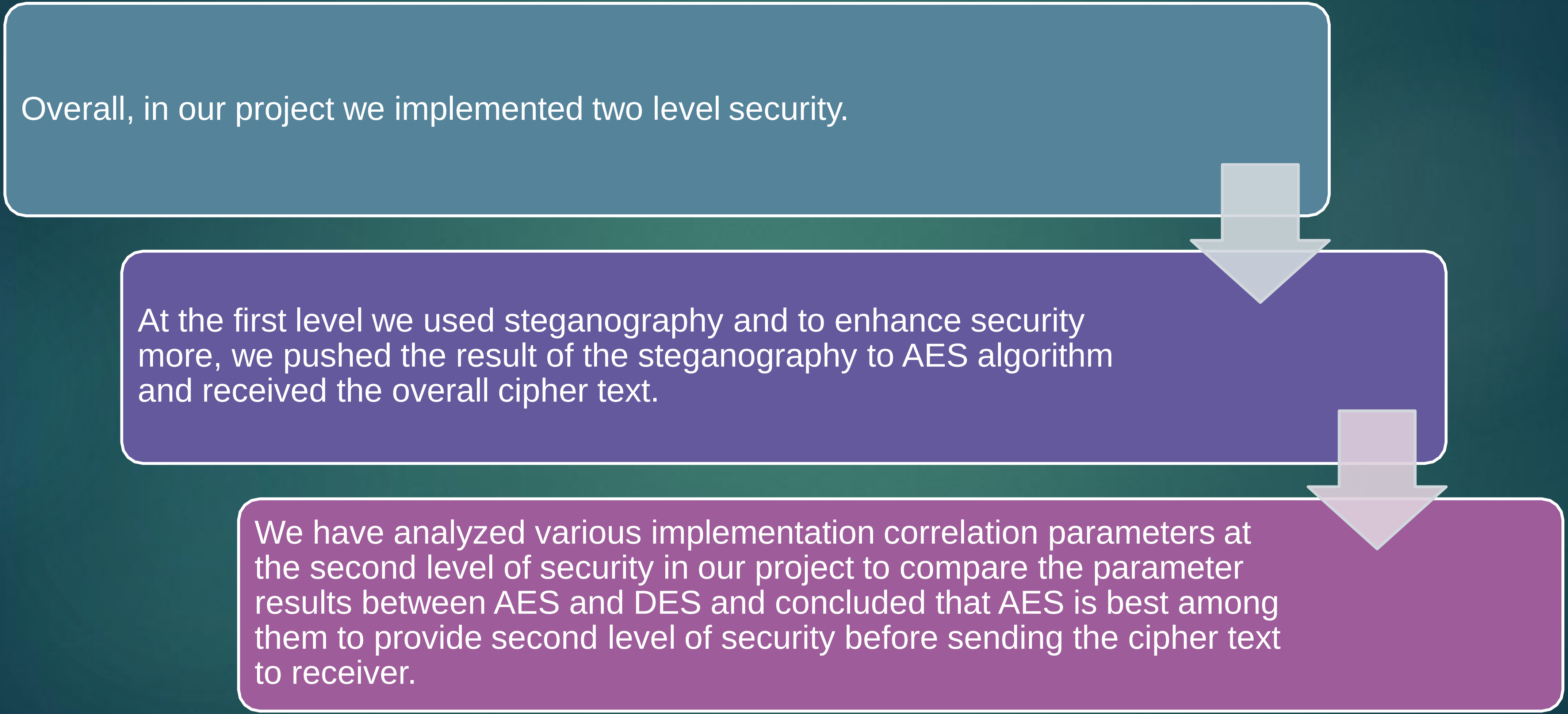


Decrypt Image
lennalpsudtxvoa.png (512×5
sunriseriddigujvu.png (299×
sunrisefzfdhxcbxk.png (299×
sunriseogialncouv.png (299×
127.0.0.1:5000/decrypt_image

Decrypt Image

Choose File No file chosen
send

Conclusion



Overall, in our project we implemented two level security.

At the first level we used steganography and to enhance security more, we pushed the result of the steganography to AES algorithm and received the overall cipher text.

We have analyzed various implementation correlation parameters at the second level of security in our project to compare the parameter results between AES and DES and concluded that AES is best among them to provide second level of security before sending the cipher text to receiver.

References

C. Liu, Q. Chen. (2016). Digital Watermarking Processing Technique Based on   Overcomplete Dictionary. Int. J. Pattern Recognit. Artif. Intell, 30, 1658002.

Hans, R. Bhanot. (2015). “A review and comparative analysis of various encryption algorithms”. Int. J. Secur. its Appl.,, 9, 289–306.

J. S. Pan, W. Li, C. S. Yang, L. J. Yan. (2015). Image steganography based on subsampling and compressive sensing. Multimed. Tools Appl, 74, 9191–9205.

L. Yao, C. Yan. (2015). An asymmetric color image encryption method by using deduced gyrator transform. Opt. Lasers Eng, 89, 72–79.

O. Purcell, J. Wang. (2018). Encryption and steganography of synthetic gene circuits. Nat. Commun, 9.