**Project report**

Image Cryptography

Bachelor of Technology



Department of Computer Science and Engineering

Graphic Era Deemed University

Dehradun

2021 – 2022

**Submitted by:**

Ananya Saini

E – 59

2016631

**Declaration**

I, Ananya Saini, hereby declare that this project entitled “**Image Cryptography**” submitted by me to MR. DEVESH PRATAP SINGH as Mini Project for my 4th semester in Computer Science and Engineering in **Graphic Era Deemed University, Dehradun** during the academic year 2021-2022 is a bona fide project work by me under the guidance of MR. AKSHAY RAJPUT.

**Dr. Devesh Pratap Singh**

**HOD (Computer Science)**

**ACKNOWLEDGEMENT**

Here by I am submitting the project report on “Image Cryptography” as per the arrangement of Graphic Era Deemed University, Dehradun.

I would like to give my sincere gratitude towards Mr. Akshay Rajput, Professor of Design and Analysis of Algorithms, for providing a congenial environment to work in and carry out our project.

I am thankful to all the faculty members of the Department of Computer Science and Technology, friends and our parents for their constant encouragement, support and help throughout the period of project conduction.

Ananya Saini

Roll No. - 2016631

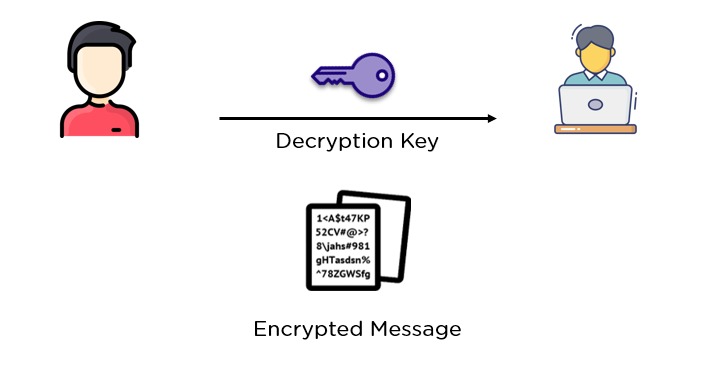
**Introduction**

Today, the Internet is the fastest growing communication medium and an essential part of the infrastructure. To cope with the growth of the Internet, it has become a constant battle to keep information secret and, in terms of profits, to protect data copyright.

Cryptography is a technique of storing and transmitting data in a form that only those it is intended for can read and process. It is a method of protecting information by encoding it into an unreadable format. It is an effective way of protecting sensitive information as it is stored on media or transferred through network communication paths.

Encryption

In cryptography, encryption is the process of encoding information in the form of unreadable file. This process changes the original layout of the information, known as plaintext, into an alternative form known as ciphertext. Technically, only authorized parties can decrypt a ciphertext back to plaintext and access the original information.



Decryption

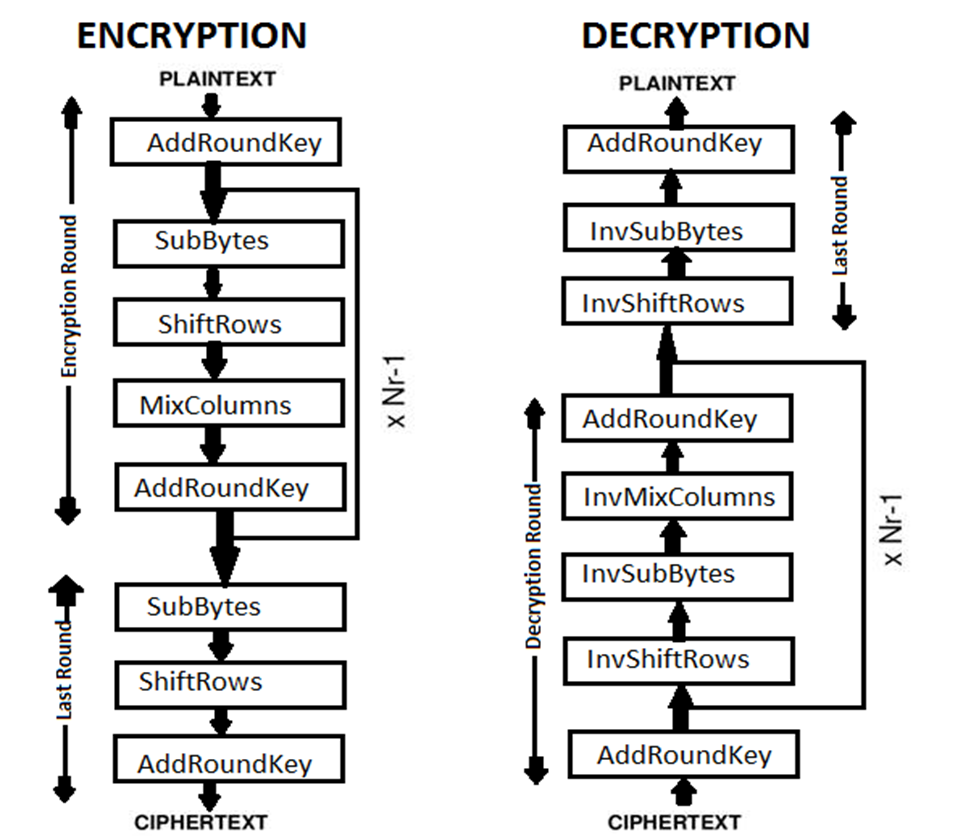
The conversion of encrypted data into its original or readable form is called Decryption. It is the reverse process of encryption. It decodes the encrypted file so that only an authorized user can decipher the encrypted data because decryption requires a secret key or password.

Diagram

Description automatically generated

Advanced encryption standard

Advanced Encryption Standard (AES) is an algorithm in cryptography that can be used rightly to secure data. The AES algorithm divides data into data blocks and works on these data blocks in the form of 4 x 4 matrix. Symmetrical ciphertext blocks can encrypt (encipher) or decrypt (decipher) files.

****

**Working**

1. *KeyExpansions*—round keys are derived from the cipher key using Rijndael’s key schedule. AES needs a distinct 128-bit or 192- bit or 256-bit key block for each round and another.
2. *InitialRound*
   1. AddRoundKey—each byte of the state is combined with a block of the round key using bitwise xor.
3. *Rounds*
   1. SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
   2. ShiftRows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
   3. MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
   4. AddRoundKey
4. *Final Round (no MixColumns)*
   1. SubBytes
   2. ShiftRows
   3. MixColumns
   4. AddRoundKey.

**Advantages**

* The image can only be viewed by the sender and the receiver as the image is encrypted using AES algorithm and the key is only known to the sender and receiver.
* Since the image is encrypted using the AES algorithm, it is more secure than the other techniques.
* Since the key size may be 128 bits or 192 bits, the encryption and decryption become more secure.

**Disadvantages**

* The encrypted format size to be transmitted becomes large.
* Since the file size is huge it can be suspected to contain some critical information.

**Bibliography**

* <https://www.simplilearn.com/tutorials/cryptography-tutorial/asymmetric-encryption>
* <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7406040&queryText=image%20aes&newsearch=true>
* <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5734951&queryText=image%20aes&newsearch=true>
* <https://www.scitepress.org/Papers/2018/89055/89055.pdf>
* <https://www.geeksforgeeks.org/advanced-encryption-standard-aes/>
* <https://en.wikipedia.org/wiki/Encryption>
* <https://economictimes.indiatimes.com/definition/decryption>