IMAGE ENCRYPTION PROJECT

BY SANCHARI RAY

AIM: Network security

Objective: Image encryption using AES Algorithm and steganography

INTRODUCTION

In computing, encryption is the method by which plaintext or any other type of data is converted from a readable form to an encoded version that can only be decoded by another entity if they have access to a decryption key. Encryption is one of the most important methods for providing data security, especially for end-to-end protection of data transmitted across networks.

PURPOSE

The purpose of this software is provide the security of Data for which no one except the customer can see the private information.

USER INTERFACES

1. In this software, have two main buttons (Encrypt, decrypt) and a textbox for input paraphrase.
2. First tab i.e. encrypt tab will allow a user to select the image they wish to encrypt and provides the encrypted image.
3. Second tab i.e. decrypts option, will allow the user to decrypt the encrypted image.

SYSTEM FEATURES

- ⊡ Encryption
- ⊡ Decryption

ENCRYPTION

⊡ This system feature involves encrypting the image using Advanced Encryption System Algorithm which is symmetric.

⊡ Function Requirements:

⊡ 1. Firstly, the user types the paraphrase in the given input field.

⊡ 2. Select the file using Encrypt option that he wants to encrypt.

⊡ 3. Before pressing the Encrypt button, you must enter the key that helps to encrypt your file.

⊡ 4. After selecting your file successfully, it gives the encrypted file.

5. After encryption, file is saved in destination folder.

DECRYPTION

⊡ This system feature involves decrypting the image using the same paraphrase and AES algorithm.

⊡ Functional Requirement:

⊡ 1. Select file using Decrypt option that you want to decrypt.

⊡ 2. Enter the paraphrase value in key field; without entering the key value you cannot decrypt the image.

⊡ 3. Press the decrypt button to get the decrypted file.

PERFORMANCE REQUIREMENTS

Most cryptographic ciphers rely on high computational cost operations. Therefore, keeping performance considerations in mind, for data encryption/decryption computational effort to encryption/decryption using Asymmetric key is very powerful compared to symmetric key algorithm. It provides more security compared to symmetric key and also performance of encrypting file is very good. It is general purpose software. But, for simplicity reasons we have chosen symmetric algorithm.

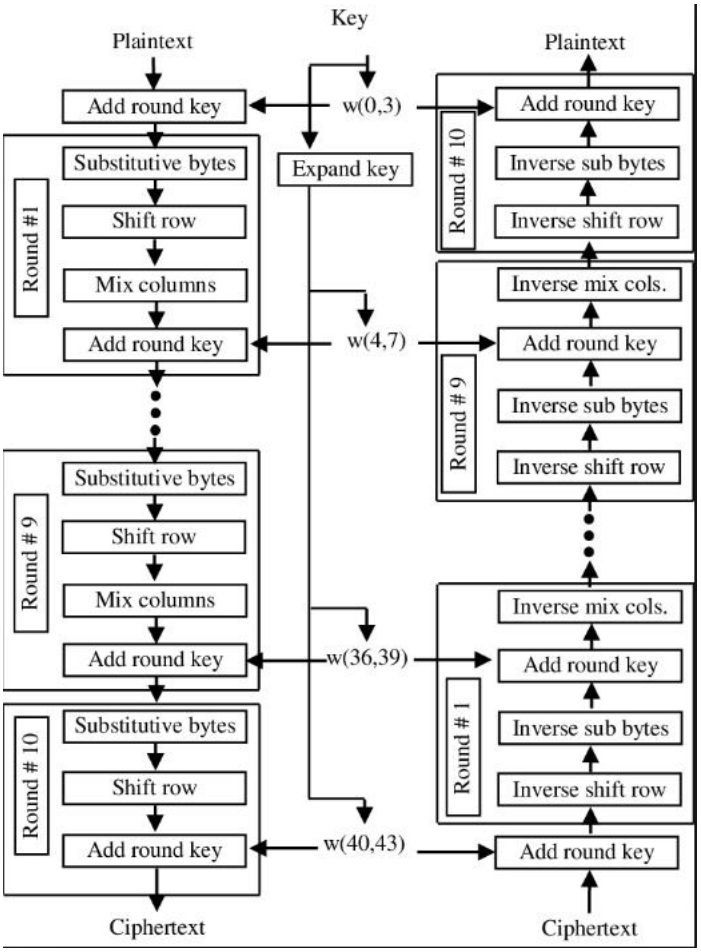
SECURITY REQUIREMENTS

User is required to remember his password that he/she used to encrypt data (or lock password safe) because most of secure cryptographic algorithms implemented in this suite are secure enough so that no algorithms better than brute-force can be used to recover lost password.

SOFTWARE QUALITY ATTRIBUTES

The source code should be properly documented, so that new developers will be able to understand the code as easily as possible. It should be easily available for every end user for better security.

WORKING OF AES



ENCRYPTION AND DECRYPTION

- ☑ For 1st step add round key.
- ⊡ Substitute byte
- ⊡ Shift Row
- ⊡ Mix Column
- ⊡ Add round key except for last step

DECRYPTION:

- ⊡ For 1st step add round key
- ⊡ Inverse shift row
- ⊡ Inverse substitute byte
- ⊡ Add round key
- ⊡ Inverse mix coulumn
- ⊡ Get plaintext