Information Security Lab Project Report

Submitted By :

17104011 Kapil Kumar Israni

17104012 Ayush Nagar

17104018 Akshara Nigam

Problem Statement :- The idea is to use an encryption-decryption system with secured user login. This application would encrypt any file, be it image(.png .jpg .jpeg), csv , text files(.doc .txt .rtf) etc.

Requirements:- Python 3.0 and above with libraries Tkinter, pyDes and crypto installed.

Implementation

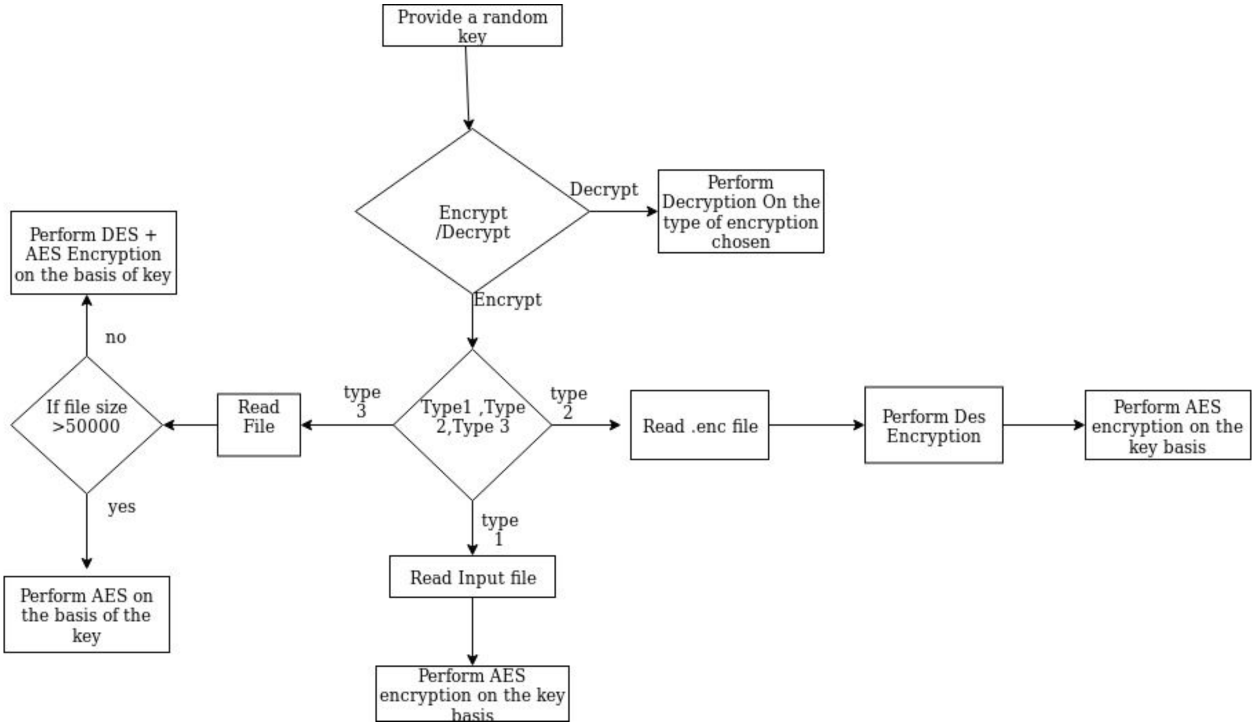
We have used two algorithms as mentioned below for encryption and decryption purpose. Initially the user is asked for the password, after which he has to enter the name of the file which he wants to encode. Correspondingly, the user is asked for his choice, if he selects AES then this encryption technique would be used. While if he selects AES + DES then two level encryption is done.

AES: The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It 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).
Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes.
Here we are using Cipher-Block Chaining (CBC) mode of AES, In CBC mode, the current plaintext block is added to the previous ciphertext block, and then the result is encrypted with the key.

DES : It is a block cipher, and encrypts data in blocks of size of 64 bit each, means 64 bits of plain text goes as the input to DES, which produces 64 bits of cipher text. The same algorithm and key are used for encryption and decryption, with minor differences. The key length is 56 bits. The DES satisfies both the desired properties of a block cipher. These two properties make cipher very strong.

- **Avalanche effect** − A small change in plaintext results in the very great change in the ciphertext.
- **Completeness** − Each bit of ciphertext depends on many bits of plaintext.

Flow Diagram:-


Provide a random key
Encrypt /Decrypt
Decrypt
Perform Decryption On the type of encryption chosen
Encrypt
Perform DES + AES Encryption on the basis of key
no
If file size >50000
Read File
type 3
Type1 ,Type 2,Type 3
type 2
Read .enc file
Perform Des Encryption
Perform AES encryption on the key basis
yes
type 1
Perform AES on the basis of the key
Read Input file
Perform AES encryption on the key basis