MINI PROJECT

On

ENCRYPTION AND DECRYPTON OF IMAGE

(CSE VI Semester MINI PRJOECT)

2021-2022

Submitted to:

Dr. INDERJEET SIR

(CC-CSE-C-VI-Sem)

Guided by:

Mr BP dubey,Ms Preeti Chaudhary ,

Ms Kiran Kumain

Submitted by:

Pawan Singh Koranga

Roll. No.: 1018541

CSE-C-VI-Sem

Session: 2021-2022

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

GRAPHIC ERA HILL UNVERSITY, DEHRADUN

ACKNOWLEDGMENT

I would like to express our gratitude to The Almighty , the most Beneficent and the most Merciful, for Successful completion of Project.

I wish to thank our parents for their continuing support and encouragement. We also wish to thank them for providing us with the opportunity to reach this far in our studies.

I would like to thank particularly my External Supervisor Mr. B. P. Dubey Sir for his patience, support and encouragement throughout the completion of this project.

I also acknowledge to my Class coordinator Dr. Inderjeet Sir and Subject Teacher Mr.Sawmitro Sir who help me to understand this course.

At last but not the least I greatly indebted to all other persons who directly or indirectly helped me during this course.

Pawan Singh Koranga

Roll No.- 1018541

CSE-C-VI-Sem

Session: 2021-2022

GEHU, Dehradun

TABLE OF CONTENTS

1. Inroduction

1.1 Definition

Encryption is a process which uses a finite set of instruction called an algorithm to convert original message, known as plaintext, into cipher text, its encrypted form. Cryptographic algorithms normally require a set of characters called a key to encrypt or decrypt data. With the help of key and the algorithm we can encrypt or Decrypt the plaintext into cipher text and then cipher text back into plaintext..

Nowadays, information security is becoming more important in data storage and transmission. Images are widely used in different-different processes. Therefore, the security of image data from unauthorized uses is important. Image encryption plays a important role in the field of information hiding. Image encryption method prepared information unreadable. Therefore, no hacker or eavesdropper, including server administrators and others, have access to original message or any other type of transmitted information through public networks such as internet.

We are very excited by the vast future possibilities that our project has to offer. Possible improvements include getting back the decrypted image in color. We are also looking forward to encrypt videos by extracting each frame and encrypting the images simultaneously. We know that all the videos have sound. So we are planning to encrypt frames and sound simultaneously. Finally after achieving all of the above, we are planning to create an app which will do all of the above. With two people having the app, one will become the sender and other the receiver at a time, based on the requirements of either of the two. This is future of our project we are looking at and looking forward to implementing all of the above successfully..

2.System Requirements

2.1

- OS: Win Xp 32
- Processor: Intel Pentium III / AMD Athlon MP
- System Memory: 256 MB RAM
- Storage: 75 MB Hard drive space
- DirectX 9 Compatible Graphics Card

3.Algorithm Used

3.1

RSA (Rivest–Shamir–Adleman) is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of the keys can be given to anyone. The other key must be kept private. The algorithm is based on the fact that finding the factors of a large composite number is difficult: when the factors are prime numbers, the problem is called prime factorization. It is also a key pair (public and private key) generator.

RSA involves a public key and private key. The public key can be known to everyone- it is used to encrypt messages. Messages encrypted using the public key can only be decrypted with the private key. The private key needs to be kept secret. Calculating the private key from the public key is very difficult.

3.2
Generating Public Key :

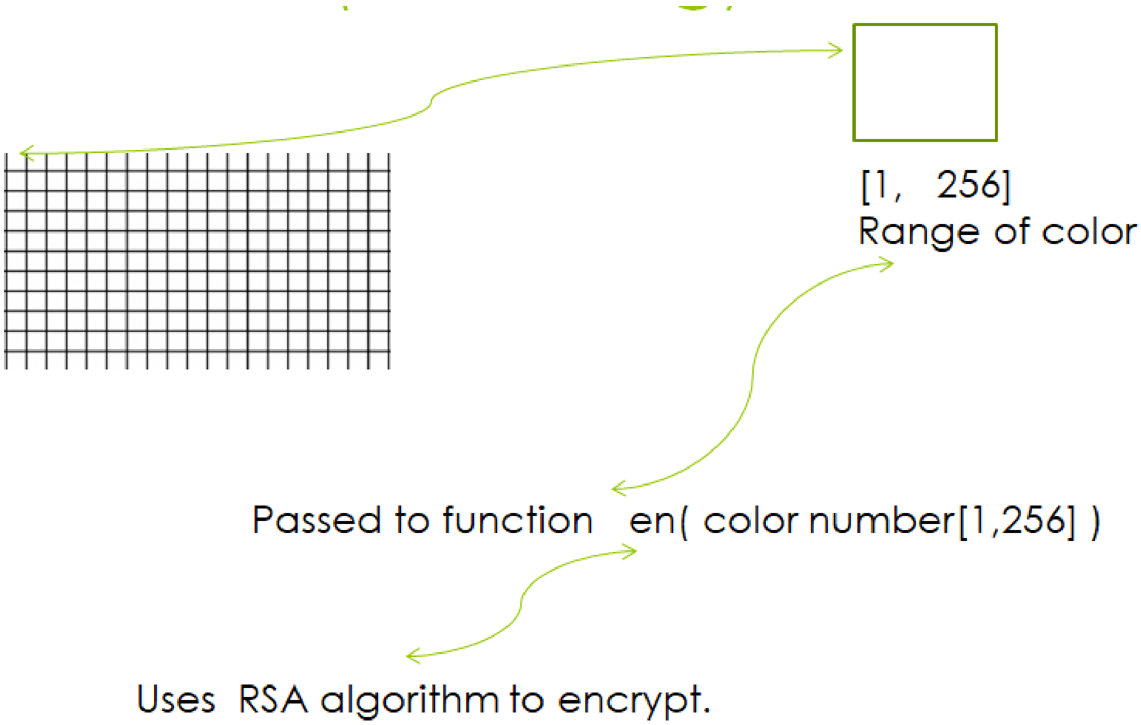
- Select two prime no's. Suppose **P = 53 and Q = 59.**
- Now First part of the Public key : **n = P*Q = 3127.**
-
- We also need a small exponent say **e** :
- But e Must be
    -
        - An integer.
        -
        - Not be a factor of n.
        -
        - **1 < e <** Φ(n) [Φ(n) is discussed below],
        - Let us now consider it to be equal to 3.
-
- Our Public Key is made of n and e

3.3
Generating Private Key :

- We need to calculate Φ(n) :
- Such that **Φ(n) = (P-1)(Q-1)**
- so, Φ(n) = 3016
-
- Now calculate Private Key, **d** :
- **d = (k*Φ(n) + 1) / e** for some integer k
- For k = 2, value of d is 2011.

4.How Software Works

4.1 Encryption



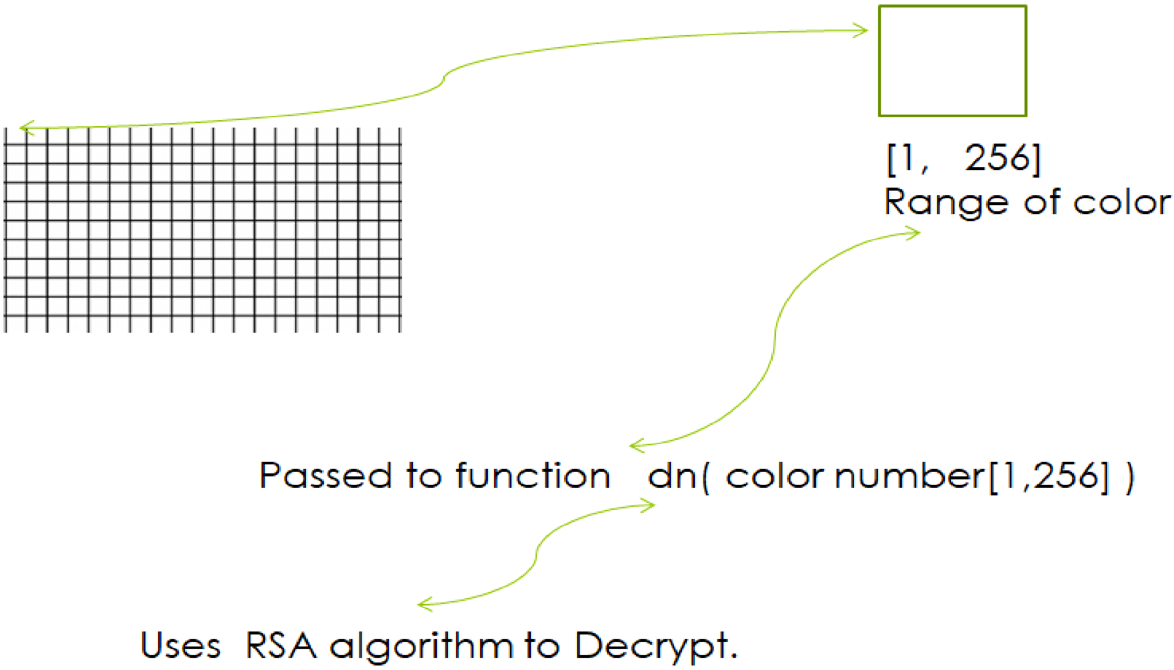
[1, 256]
Range of color

Passed to function en(color number[1,256])

Uses RSA algorithm to encrypt.

.

4.2 Decryption



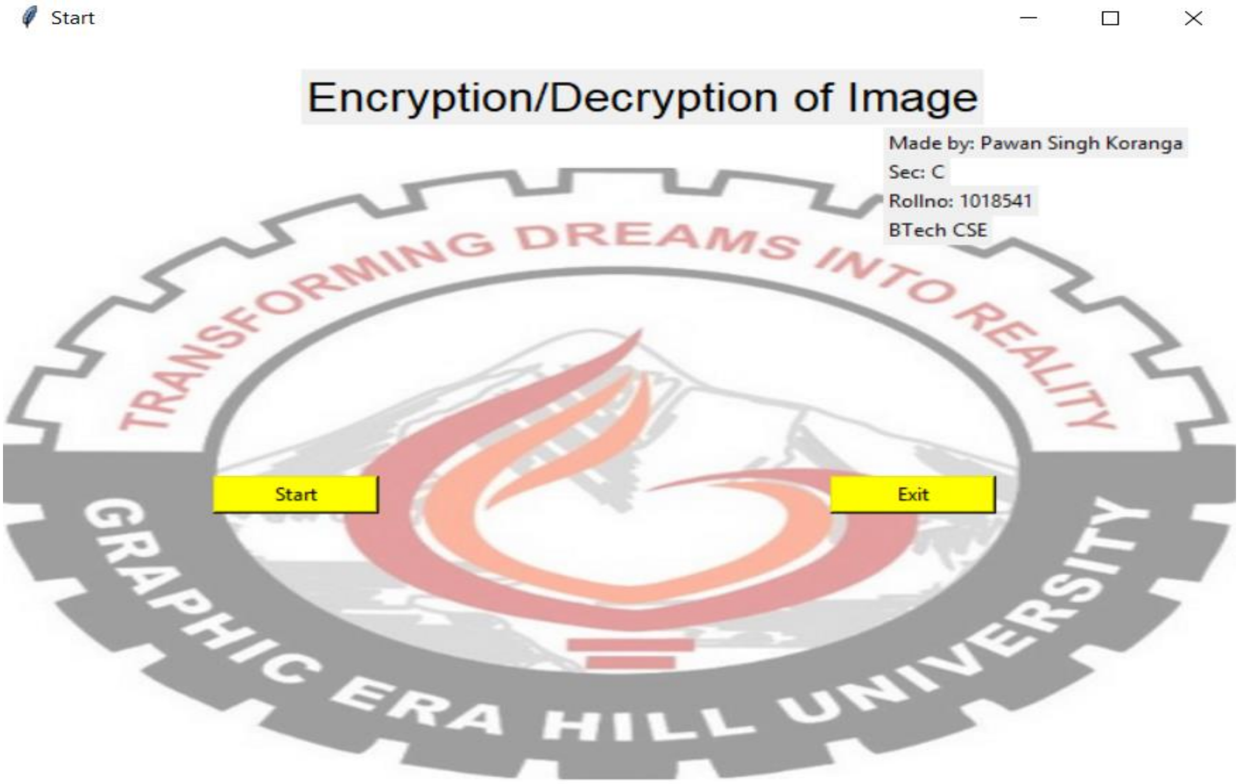
[1, 256]
Range of color

Passed to function dn(color number[1,256])

Uses RSA algorithm to Decrypt.

5.Snapshots of Project

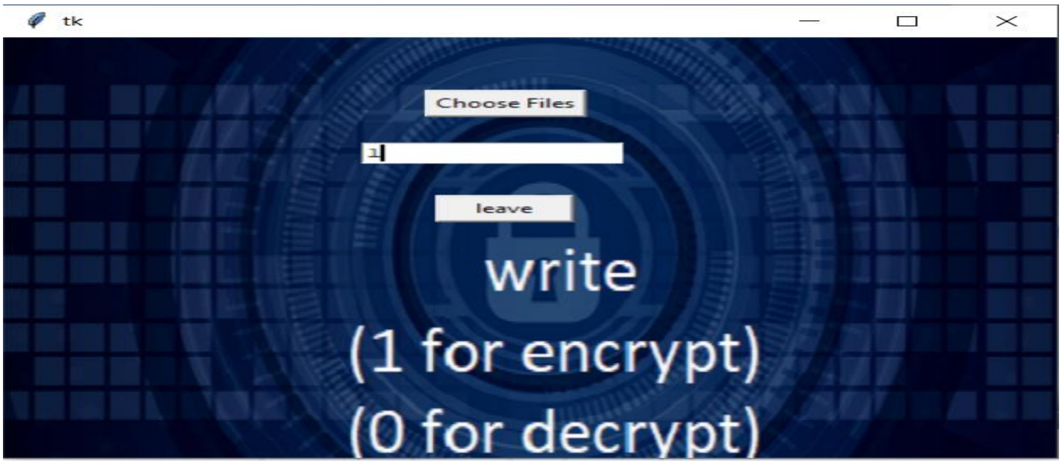
5.1 Front Page



Encryption/Decryption of Image

Made by: Pawan Singh Koranga
Sec: C
Rollno: 1018541
BTech CSE

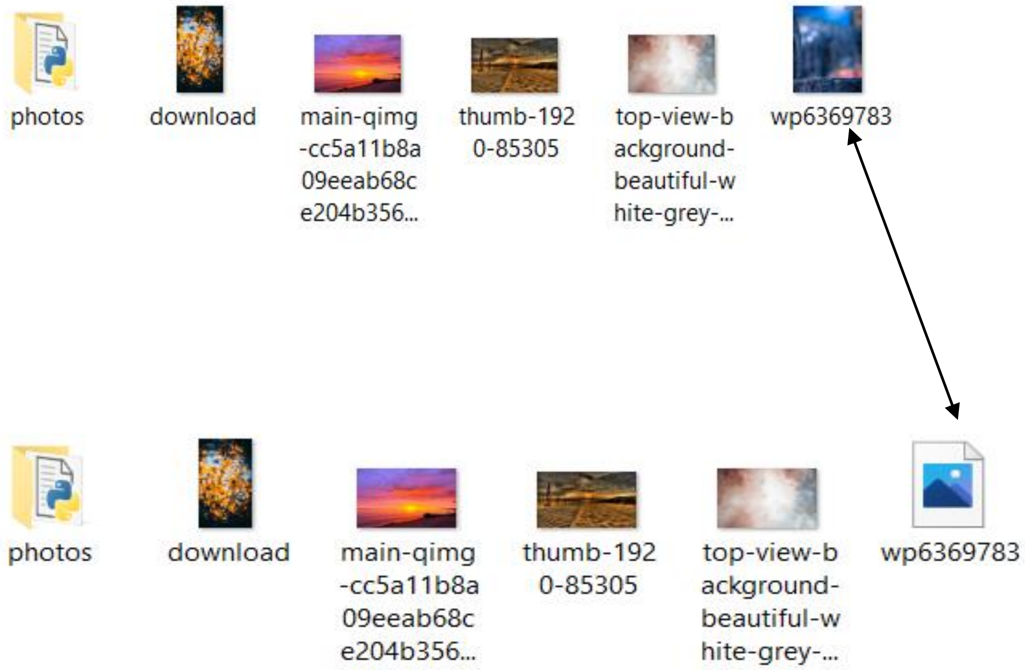
5.2 Encryption/Decryption Dialog Box



1

write
(1 for encrypt)
(0 for decrypt)

5.3 Encrypted/Decrypted Image


photos
download
main-qimg-cc5a11b8a09eeab68ce204b356...
thumb-1920-85305
top-view-background-beautiful-white-grey-...
wp6369783
photos
download
main-qimg-cc5a11b8a09eeab68ce204b356...
thumb-1920-85305
top-view-background-beautiful-white-grey-...
wp6369783

REFERENCE

1. Kurose Rose: Computer Networking a Top down approach, 7th Edition, Pearson Education.

2. Behrouz a Forouzan: Data communication and Networking, 4rd Edition, McGraw-Hill.

3. Etc.

Other resources include youtube/google/web.