Image encryption using RSA Technique

PROJECT REPORT for Information and Network Security (IT - 407)

By

Sarthak Jain (2K19/ME/216)

Abhinav Mittolia (2K19/EN/003)

DEPARTMENT OF INFORMATION TECHNOLOGY

DELHI TECHNOLOGICAL UNIVERSITY

ACKNOWLEDGEMENT

This project has in due course helped us learn many important Network security concepts. We feel delighted to do this as our Information and Network Security (IT - 407) minor-project and Dr. Sonia as our project guide. We are thankful to her for her help and guidance. Finally, we would like to thank our family and friends who stood by us all the time and cooperated in the best way they could. There is a profound sense of satisfaction in completing this project.

SARTHAK JAIN

ABHINAV MITTOLIA

INTRODUCTION

Internet is the most important medium in the increasing growth of multimedia to transfer data from one place to another across the internet. There are many ways to transmit data over the internet such as e-mails, sending text and images, etc.

In the present communication images are widely use. One of the key issues with transferring data over the Internet is its security and authenticity. Encryption is one of the techniques which is used for securing the information. Similarly, in decryption no one can access the information without knowing the decryption key.

Image security is an utmost concern on the web. Cyber-attacks such as phishing and identity theft are becoming more serious. **Image encryption and decryption has applications in internet communication, military communication, medical imaging, multimedia systems, telemedicine, etc.** To make the data secure from various attacks the data must be encrypted before it is transmitted. The government, financial institution, military, hospitals deal with confidential images about their patients, their financial status, geographical areas as well as enemy positions. Most of this information is now collected and stored on electronic computers and transmitted over the network. If all these confidential images about enemy positions, patient and geographical areas get in the wrong hands can be catastrophic. **Protecting confidential images is a legal requirement.** One must make a strong encryption for an image so that it cannot be hacked easily. And the perfection in the original image can be re-obtained after decrypting it. Another use of internet could be transferring the secure data which may be very essential for a group of companies, the data should not be viewed by others.

Therefore, hiding sensitive data becomes very crucial in securing network information. The method used for securing data is known as encryption. After encrypting the data, with the help of internet it is transferred to the destination. At its destination encrypted data is decoded with the help of the provided algorithm which is known as decryption. The private or sensitive information will be hidden within an image, and it is transmitted with the secure keys which is then decrypted.

RSA is an algorithm which is used to provide an encryption and authentication system. It is an **asymmetric block cipher** cryptographic technique. This was developed by Ron Rivest, Adi Shamir, and Leonard Adleman in 1977. This algorithm is a very commonly used cryptographic algorithm. The RSA algorithm is one of the very first **public key cryptosystems**. In such a cryptosystem, the encryption key is a public one and the

decryption key is different, which is kept secret. In RSA, this asymmetry is based on the product of two large prime numbers, the factoring problem. The RSA encrypt key encrypts the image, so that it converts into cipher text format and it will be stored as a text file. The opposite method of encryption, the reverse process is computed by the decryption key of RSA algorithm and it decrypts the image from the cipher text. Finally, it will output the resultant image by the decryption techniques.

FUNCTIONALITY OF IMAGE CRYPTOGRAPHY

The image cryptography works as shown in the flow chart in the Fig.1. The Fig.1 is describing the step-by-step manner of processing in the encryption and decryption as done in the RSA encryption method (And also in our project).

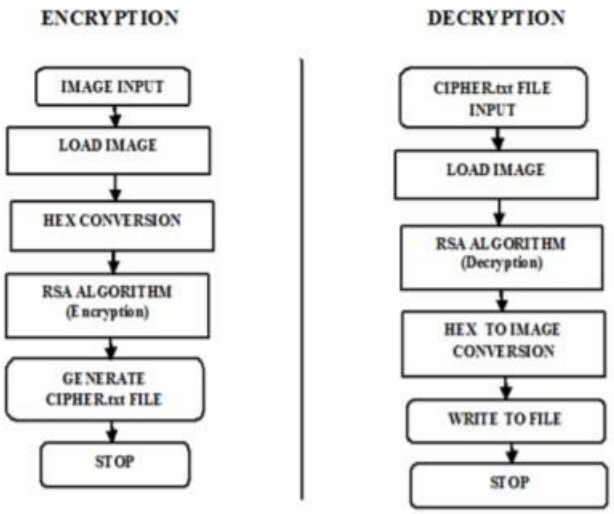

Fig. 1 Encryption and Decryption flow

IMAGE CRYPTOGRAPHY METHODOLOGY BY RSA

RSA is an algorithm is using in the modern computer environment to encrypt and decrypt the data in transform. The RSA algorithm is also called as an asymmetric cryptographic algorithm. Asymmetric cryptosystem means two different keys are using in the encryption and decryption. In the two keys one key is using for encryption and the second key is using for decryption. This RSA algorithm is also called as the public key cryptography. Because one of the secret key can be given to everyone which means public. The other key must be kept private. The RSA algorithm consists of three manor steps in encryption and decryption. The steps are following as,

1. Key Generation
2. Encryption
3. Decryption

Key generation

The key generation is the first step of RSA algorithm. The RSA involves a public key and a private key. On those keys the public key can be know everyone and it is use for encrypting messages. Messages encrypted with the public key can decrypt using the private key. The keys for the RSA algorithm is generated by the following steps,

1) First choose the two distinct prime numbers **p** and **q**.

2) For security purposes, the integer p and q should be chosen, and it should be the similar bit-length. Prime integers can be efficiently found by a primality testing.

3) Then compute the **n** value, **n** = **p** * **q**.

4) n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.

5) Compute **ϕ(n)** = **ϕ(p)ϕ(q)** = **(p – 1)(q – 1)** = **n - (p** + **q -1)**, where ϕ is **Euler's totient function**. This value is kept private.

6) Choose an integer **e** such that **1** < **e** < **ϕ(n)** and **gcd (e, ϕ(n))** = **1**; i.e., **e and ϕ(n) are co-prime**. e is released as the public key. e has a short bit-length and its small Hamming weight results in more efficient encryption. However, much smaller values of e have been shown to be less secure in some settings.

7) Determine d as **d ≡ e–1 (mod ϕ(n))**; i.e., d is the modular multiplicative inverse of e (modulo ϕ(n)). This is stated as, solve the d given **d·e ≡ 1 (mod ϕ(n))**. This is computed using extended Euclidean algorithm. It using the pseudo code in the Modular integers section, inputs a and n correspond to e and ϕ(n), respectively.

8) Exponent **d** is kept as the private key. **The public key consists of the modulus n and the public key e**. **The private key has the modulus n and the private key d**, and it is kept secret. **p, q, and ϕ(n) values are also kept secret** because they can be used to calculate d.

Encryption

We will explain the use flow of this encryption by an example.

Alice transmits her **public key (n, e)** to Bob and keeps the **private key d** secret. Bob then wishes to send the message **M** to Alice.

So, Bob first turns **M** into an integer **m**, such that **0 ≤ m** < **n**. Then it computes the cipher text **c**. This can be done efficiently, even the numbers are 500- bit numbers, it is using the Modular exponentiation. Bob then transmits c to Alice. At least nine values of m will yield a cipher text c equal to m.

$$c = m^e \pmod n$$

Decryption

Alice can recover m from c by using her private key exponent d via computing. Given m, she can recover the original message M by reversing the padding scheme.

$$m = c^d \pmod n$$

MAJOR APPLICATIONS OF IMAGE CRYPTOGRAPHY

- Core banking is a set of services providing by the group of networked bank branches. Bank customers may access their funds and perform the simple transactions from the member branch offices.
- The major issue in core banking is the authenticity of the customer. An unavoidable hacking of the databases on the Internet, it is always quite difficult to trust the information in Internet.
- To solve this problem of authentication proposing an algorithm based on image processing and image cryptography. The internet multimedia applications are becoming rapidly popular.
- The valuable multimedia content such as the image is vulnerable to unauthorized access while in storage and during transmission over a network. The image processing applications have been commonly found in the Military communication, Forensics, Robotics, Intelligent systems etc.

MERITS AND DEMERITS OF IMAGE CRYPTOGRAPHY

Merits

One advantage to encryption is that it separates the security if data from the security of the device where the data is transmitted over the Internet. And the advantages to implementing encryption include the pain that comes with data breach disclosures, the provision of strong protection for intellectual property. The people should keep in mind the standard email is not secure and is in fact tantamount to writing sensitive information on

postcards. The encrypted data that can only be read by a system or user who has the key to unencrypted the data means the system or user is authorized to read the data. Encrypted data cannot be accessed by the third parties. The encryption is come with the numerous advantages that need to protect the data. And some another benefit is there in using Image Cryptography.

There are,

1) **Peace of Mind**

2) **Identity Theft Protection**

3) **Safe Decommissioning of Compute**

4) **Unauthorized Access Protection**

5) **Compliance with Data Protection Acts**

Demerits

1. There are very few demerits of applying cryptographic security layer.
2. The encryption is an overly complex technology.
3. One big disadvantage of encryption with keys is that the security of data becomes the security of the encryption key. The data is lost effectively if one loses the keys.
4. Encrypting data and creating the keys necessary to encrypt and decrypt the data is computationally expensive.

RESULT AND DISCUSSION

For this project, many different raw images of varied sizes were encrypted and decrypted. One public key is needed to encrypt and another private key is needed to decrypt the image.

The image cryptography experiment is providing feasible security to the image. The data is not viewable to anyone without the knowledge of the private key.

The image consisted of valuable secrets and it is going to be encrypted.

Fig. 3 Original Image

The Original image is encrypted by the key which is generated by the RSA algorithm. It is converting the image into the cipher text. It is shown in Fig.4.

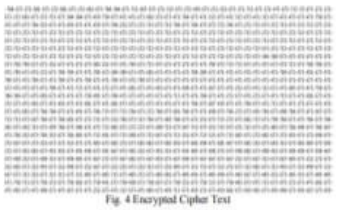

Fig. 4 Encrypted Cipher Text

Finally the cipher text is decrypted by another one decrypt key which also generated by the RSA algorithm. And it is convert the cipher text into the resultant image. It is shown in Fig.5.

Fig. 5 Decrypted Image

CONCLUSION

In the digital world, the security of images has become more important as the online communications have increased rapidly. All the techniques present in real-time image encryption could only ensure a risky level of security. Here, the image encryption algorithm used efficient and highly secure with elevated level of security and less computation. The results of the simulation show that the algorithm has advantages based on their techniques which can be easily applied on images. Hence it is concluded that this technique is good for image encryption and give decent security on open networks.

END