Information Security System Using RSA Cryptography

San San Lwin  
Department of Information Technology Engineering  
Technological University (Kyaukse)  
sansanlwinmost@gmail.com

Win Win Maw  
Faculty of Computer System and Technologies  
University of Computer Studies (Mandalay)  
winwinmaw.tukse@gmail.com

Aye Kyaing  
Department of Information Technology Engineering  
Technological University (Kyaukse)  
mimikyaing.it@gmail.com

Abstract

RSA (Rivest–Shamir–Adleman) algorithm proposed by Ron Rivest, Adi Shamir and Len Adlenman in 1977 is the most widely develop public key cryptography. It can be used in key management, digital signature and message encryption scheme. At the present day, it is used for securing web traffic, e-mail and some wireless devices. Since RSA is based on arithmetic modulo large numbers, it is can be slow in constrained environments. Especially, when the key length is increased, the RSA decryption can be slow. In this paper, RSA using Chinese remainder theorem (RSA-CRT) is implemented and the speed performance efficiencies of all algorithm are compared at decryption stage. In this system, the algorithm is used for message encryption scheme. To implement this system, Chinese remainder theorem is used. This system is implemented by using Mat-Lab.

Keywords - RSA, Cryptography, Matlab

1. Introduction

The key length for modern cryptographic algorithms is the principal security parameter. The user examines the different decryption schemes that were described with respect to speed and memory. Ancient people used various techniques to send messages during war times. Sending of messages safely and securely has been top priority for any organization that deals with confidential data.

As more and more techniques for hiding information are developed and improved, more and more different information detecting techniques are also developed. That has produced a strong need to create new techniques for protecting confidential information from hacker. There are numbers of data hiding techniques available for different purpose and applications like steganography, cryptography, and watermarking.

Public-key encryption schemes and digital signature schemes have been developed, whose strength is derived fully from the RSA problem. The strength of RSA come from the fact that factoring large number is difficult. The best-known factoring methods are still very slow. Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and non-repudiation.

Authentication is the process of verifying identity so that one entity can be sure that another entity is who it claims to be. Two parties entering into a communication should identify each other. An attacker can pretend to be someone else in order to get private information. Therefore, in a secure communication, the two parties may want to be sure of the identities of their entities.

Privacy is the property that information is not made available or disclosed to unauthorized entities, or processes. Secrecy is a term synonymous with confidentiality and privacy. Privacy service is a security that protects private data against unauthorized person. Non repudiation service is a security service that provides protection against false denial of involvement in a communication.

The goal of non-repudiation is to prove that a message has been sent and received. This is extremely important in breaking networks where financial transactions must be verifiably completed and in legal networks where signed contracts are transmitted. A fundamental goal of cryptography is to adequately address these four areas in both theory and practice. Cryptography is about the prevention and detection of cheating and other malicious activities.

Data integrity is the property that data has not been changed, destroyed or lost in an unauthorized or accidental manner. So it means the obtained data is the same as the sent data. Data integrity service is a security service that protects against unauthorized changes to data, including both intentional change or destruction and accidental change or loss by ensuring that changes to data are detectable.

2. Implementation of the System

The main aim of the proposed system is to provide the secure messaging system between two parties. To create the design of proposed system, RSA algorithm is used for encryption and decryption.
Figure 1. Flow chart to illustrate RSA cryptography for sender side

Figure 2. Flow chart to illustrate RSA cryptography for receiver side

When the cover coding is run, it can be seen as shown in Figure 3. Figure 4 will be seen when the main coding is run.

Figure 3. Running the cover coding

Figure 4. Running the main coding

When the next button is pressed, the interface for encryption will be shown in Figure 5. The encryption interface has generated key, encrypt message, next and back buttons. The back button is for cover interface, the generate key button for public key generation, encrypt message for message encryption and next button for decryption interface.

Figure 5. Encryption interface

In the encryption interface, there are three input fields for value of P, value of Q and input message. The fourth input field is public key generation and the final input field is cipher text generation. When encrypt message button is pressed warning message will be appeared in Figure 6, while input field is empty.

Figure 6. Empty inputs
The values of P and Q must be prime numbers or the proposed system will show warning message for prime numbers is shown in Figure 7.

![Figure 7. Prime numbers warning](image1)

When the user inputs proper inputs for P, Q and message but key generation is not done; the warning message for the key generation will be displayed in Figure 8.

![Figure 8. Key generation warning](image2)

After adding all proper inputs, the message of the cipher text will be generated as shown in Figure 9.

![Figure 9. Cipher text generation](image3)

When the user runs the main2 coding, the user can see as shown in Figure 10.

![Figure 10. Running the main2 Coding](image4)

After generation cipher text, the final interface is decrypted interface. The decrypted interface has three buttons, namely Show Private Key button, Decrypt Message button and Back button. Show Private Key button is private key generation, Decrypt Message is message decryption and Back is encrypted interface.

The decrypted interface has two input fields, the first key is private key and another is message decryption as shown in Figure 11.

![Figure 11. Decryption interface](image5)

When decrypt message button is pressed before private key is generated, the warning message will be displayed for private key generation as shown in Figure 12.
3. Summary

The proposed system design is firstly introduced and then the implementation results have been carried out. According to the proposed system, the users can securely send secret message to one another. The system asks the user to input P and Q values and secret message. Using public key of the receiver, the sender can encrypt the message to get cipher text. Then, the sender can send the resultant cipher text to the receiver. The cipher text can only be decrypted using the receiver’s private key. Due to the implementation results, the proposed system is effectively developed RSA algorithm.

4. Conclusion and Discussion

The key length is the principal security parameter for current cryptographic algorithms. The user compares the various decryption schemes which were described in terms of speed and memory. A big key will ensure a high degree of security but it will also take a long time and it will consume a lot of memory. Currently, the recommended key length for the big standard crypto system RSA is more than 512 bit. If 1024 bits or 2048 bits could be used that is safer This key length is believed to be secure regarding the current computing abilities of our computers. But this length will probably be sooner or later too short. Public key cryptography is one of the main parts of the security. RSA algorithm is the most popular algorithm in public key cryptography. It is useful in key management and digital signature as well as message encryption scheme.

In practical application, the RSA algorithm is used with the secret key algorithms and hash functions to reach the goal of the security. In this paper, RSA-CRT is implemented. Three different key lengths of 512-bits, 1024-bits and 2048-bits are used in this system. To implement the algorithm, many mathematical theorems and modulo arithmetic formulae are used. In key generation stage, the Fermat primality test and Rabin-Miller primality test are used to be sure the pseudo prime as prime. Extended Euclidean algorithm is used to find modular inverse of an integer. In the decryption stage of RSA-CRT, the Chinese remainder theorem and Garner’s algorithm are used to perform the decryption process. Left-to-right exponentiation is used to perform the modular exponentiation.

Acknowledgements

The authors would like to express gratitude to the committee of the (University Journal Computer Information Research 2020) (UJCIR 2020) for accepting this paper. The author is very thankful to the Editorial Board for editing this paper and effective true guidelines to publish this paper.

References


