Messenger Program using RSA algorithm

Wooseok Kim

Abstract

By distributing widely the smartphone in the world, a protection of personal information security is more important than in the past. Some people are using instant message application on their smartphone instead of text message because use of the instant message application is more convenient than traditional use of text message. However, these days, the instant message application users knew that contents of conversation can be eavesdropped by the government or the provider of instant message application. To solve the issue, I will develop the messenger program instead of the instant message program using RSA algorithm which is one of security algorithm. Server can send encrypted message to client. The client can receive the encrypted message from the server and then decrypt the message. Naturally, the client can send encrypted message to the server.

1. Introduction

These days smartphone has come into wide use in the world. Naturally, they are not only conducting a lot of business on their smartphone but also are able to use the internet anytime anywhere on their smartphone. Although the people are more convenient than in the past by using the smartphone, their personal information is more dangerous than in the past. In some country, instant message application is more popular than traditional text message. This is because instant message application gives many advantages to the users. For example, the people can send and

reply instant message in real time without face to face, meanwhile the files, such as pictures, voice, video and etc., can be shared during the communication between the users of instant message application. In addition, the instant message can make a virtual conference without getting all the related people together in a physical meeting room. While there are many advantages, the security may not provide for the users.

In South Korea, there is an issue about the instant message application, Kakaotalk. Surprisingly, Korea government and prosecutors eavesdropped and monitored from conversation content of criminals to conversation content of innocent people through instant message application server. This means that Korea government and prosecutors can get access to online conversation through server. Of course, some Koreans are worrying about online privacy. More than two million Korean users of the Kakaotalk move to secure instant message application. After the issue, Kakaotalk CEO said that we will create message security system during conversation between the users until the end of year and will shorten the store time about the conversation contents in server.

By being motivated by South Korea issue above, This project is planned. The project will focus on the RSA algorithm and conversation encrypt when the users are talking. By encrypting the message, hackers are difficult to attack the message between the users.

2. Related knowledge for the program

To encrypt and decrypt the message, we should know security algorithm. Also, we should learn about network programming in order to do the project.

2-1. RSA algorithm

[1] The RSA scheme is a block cipher in which the plaintext and ciphertext are integers between 0 and n – 1 for some *n*. A typical size for *n* is 1024

bits, or 309 decimal digits. That is, *n* is less than 2^{1024}. RSA makes use of an expression with exponentials. Encryption and decryption are of the following form, for some plaintext block M and ciphertext block C.

$$\mathrm{C} = M^e mod\ n$$

$$\mathrm{M} = C^d\ mod\ n = (M^e)^d\ mod\ n = M^{ed} mod\ n$$

Both sender and receiver must know the value of n. The sender knows the value of e, and only the receiver knows the value of d.

3. Program Design

The challenge for the program is to send securely encrypted message and decrypt securely the message when the users are talking using the program.

In this section, we enumerate the approach and the central system of the program.

3-1. Design Principles

The program will be made by Java programming language. There will exist three parts, RSA class, server class and client class. Server class and client class will be provided by Java swing which is the primary JAVA graphical user interface (GUI) widget toolkit.

In RSA class, public key and private key will create in order to provide for the users, server and client. Also, we may check whether the pair keys are prime number or not. Thus, RSA class may include prime check program.

In Server, the program will be created at first. IP and port number of server is very important because the clients have to connect to the server. Before the program runs, the port number of server program will be inputted by the user. If the client class gets access from the server, the server will give the private key and the public key to the client.

In Client, the user can know the port number of server in advance in order to connect with server. When the client get access from the server, the client can get public key and private key. The client will use the private key

and the public key to send and receive the message. For example, Alice will encrypt the message using the private key and then Bob can decrypt the received message using her public key.

4. Total design of the program

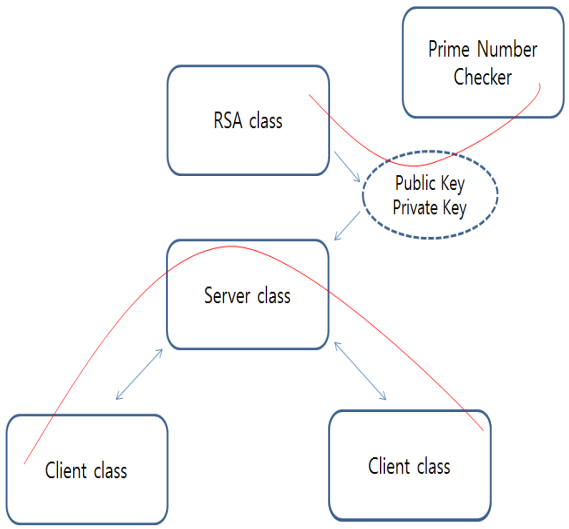

Figure 1. Class diagram of the program

At first, the program will execute the RSA class to make public key and private key. After yielding the public key and the private key, the user can check whether the pair key is prime number. If the given pair key is prime number, server class get the pair key. Once the client class is connected to server class, the server class gives the pair key to the client. If new client tries to get access from the server, the server class receives the public key and the private key from the RSA class and then the server can provide the pair key for the new client class. In the end, the clients can send and receive the message using the given pair key.

5. Conclusion

When the smartphone users use the instant message application, some provider of instant message does not provide message security to protect the users from the attackers. There are a lot of solutions for the issue. My solution is to encrypt and decrypt the message using the public key and the private key when the users communicate through the instant message application. What we discussed is computer program, not mobile program. However, we can include the idea or better ideas of security on the instant message application for the protection of the users' privacy.

In the future, the program should include message authentication and key distribution center. When sender

encrypts the message using private key in order to send encrypted message to client, the client cannot be sure what the received message is from the sender. Thus, message authentication should include.

Furthermore, server class distributes the public key and the private key. The client cannot certain whether the given key is fake or not as well. To address the issue, the program should include key distribution center in the future. The key distribution center need to be authenticated from qualified office in real such as government, bank and etc.

6. Reference

[1] William Stallings (2010), Cryptography and network security: principles and practice 5th edition, Prentice Hall, p. 278