Secure SMS Encryption Using RSA Encryption Algorithm on Android Message Application

[1]Hüseyin Bodur and [1]Resul Kara
*[1]Faculty of Engineering, Department of Computer Engineering Düzce University, Turkey

Abstract

The rapid development of communication technology, on the one hand, is bringing many technological conveniences with it and simplifying our lives. On the other hand, it has disadvantages on hiding the information that is continuously roaming through various communication media resources between senders and receivers and on not sharing them with third people.

The aim of eliminating these disadvantages via specific security methods and algorithms is related to the discipline called cryptography, which includes information security.

In this study, how RSA encryption algorithm and the secure messaging process on the SMS channel are realized in the devices with the Android operating system is examined thanks to the developed application. The advantages and the disadvantages of the application are demonstrated. The solution proposals are presented.

The application is tested with different key sizes for fast and powerful messaging. The different key sizes which can be used for key generation processes and changes occurring on encrypted messages are mentioned. Also, existing alternative solutions to be used for the encryption process in secure messaging are stated.

Key words: Cryptology, RSA Encryption, SMS Encryption, Secure Communication

1. Introduction

Security issues have an important place in today's communication technologies. Since mutual communication must be done through secure channels that don’t allow third people to intervene, it is very important to make the security levels of these channels as high as possible.

Mutual communication is provided by talking, messaging and so on, and during the communication process that is realized via these ways, various security methods can be implemented by the service provider firms or software companies without making users aware of them. Of all security methods, the encryption algorithms have a great importance.

*Corresponding author: Address: Faculty of Engineering, Department of Computer Engineering Düzce University, 81620, Düzce TURKEY. E-mail address: huseyinbodur@duzce.edu.tr, Phone: +903805421036/4660 Fax: +903805421037

These algorithms are ranked according to their complexity and resist by the rate of their complexity and power from the moment seized by third people who can penetrate mutual communication.

As a result of the rapid developments in mobile communications, SMS messaging is widely used in both the business world and the social environments.

People can share their private information which are related to their social relationships or works easily and quickly with a total of 1120 bits if each character of SMS which is up to 160 character [7] is created by 7 bits [1]. If you pay attention to the architecture of the SMS messaging method in Fig 1, it is seen that SMS is never delivered directly from sender to receiver [2].

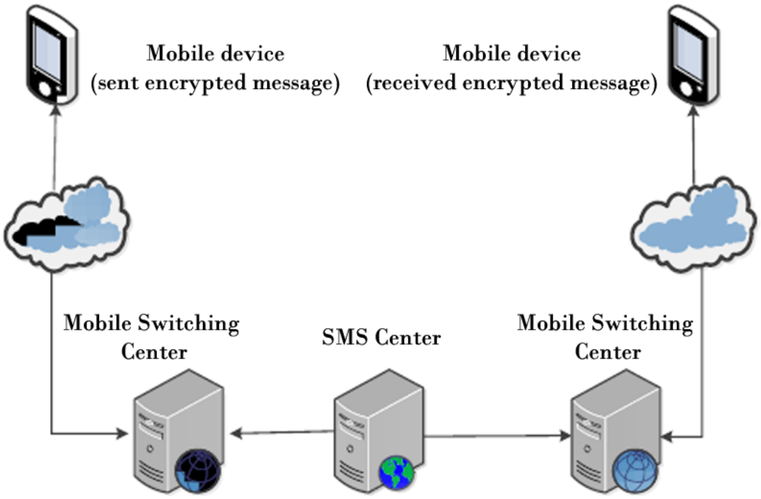


Figure 1. SMS architecture

Firstly, sent SMS passes from the mobile switching center that performs the message routing process. Then it is stored in the SMS center and directed for the transmission process [3]. Messages are transmitted as clear text between mobile switching stations and SMS centers. Namely, they aren't subject to any encryption or hiding processes during transmission. This case causes a number of disadvantages.

These disadvantages can be listed as follows;

- Before reaching the receiver from the sender, message contents are stored in the operator's system as clear text.
- Message contents can be read by the operator staffs.
- It is unclear that how reliable the operator system which stores message contents is against external threats.
- When message contents are requested by the courts from the related operators if it is necessary, they can easily be brought out.

Encryption algorithms can be utilized to remove such cases and to provide secure messaging environment. Thus, messages will circulate as encrypted form in transmission medium, not as clear text. Somebody who has seized encrypted data does not obtain original message from the encrypted data unless they possess the necessary method or a key. Encryption methods are divided into the following categories: private key cryptography and public key cryptography.

In a symmetric key algorithm, the sender and receiver must have a shared key set up in advance and keep secret from all other parties; the sender uses this key for encryption, and the receiver uses the same key for decryption. In this case, except for transmitted encrypted message, encryption key must also be submitted confidentially, which is one of the disadvantages of private-key cryptography [4].

If a third person who has managed to enter the system operator or listen to transmission medium seizes the key value, s/he can turn the encrypted data into original data. The most important feature of public key cryptography which is another method is that the key value used to encrypt the message is different from the key value used to decrypt the message. Each user has two keys in this method: public key and private key. The public key of the user can be viewed by anyone. The private key is kept secret by the user. When someone wants to send a message to user, they use the user's public key and create the encrypted message and then send the encrypted data to user. The user decrypts the encrypted data with her/his private key and obtains a meaningful message.

The data which has been encrypted by the user's public key is only solved with the user’s private key [4]. When the user wants to send a message, s/he reaches the public key library. S/he takes the public key of somebody to which s/he wants to send a message and encrypts the message and then s/he sends the encrypted message to the receiver. The only thing that the receiver must do is to solve the message with his/her own private key.

RSA algorithm, which is one of the public-key encryption methods and more reliable than the private key encryption algorithms, is used in this study for secure messaging via SMS.

2. RSA Algorithm

RSA encryption algorithm, which is based on the idea of ensuring the secure transfer of data in the digital environment and the algorithmic difficulty of separating the integer factorization, is a type of public-key encryption method [5]. Nowadays, it is also known as both the most commonly used encryption method and the method that allows digital signatures. It was created by Ron Rivest, Adi Shamir and Leonard Adleman [9] in 1978. Prime numbers are used for key generation process in RSA encryption method.

This makes it possible to create a safer structure. How the encryption and decryption processes are done with RSA algorithm is shown in Fig. 2.

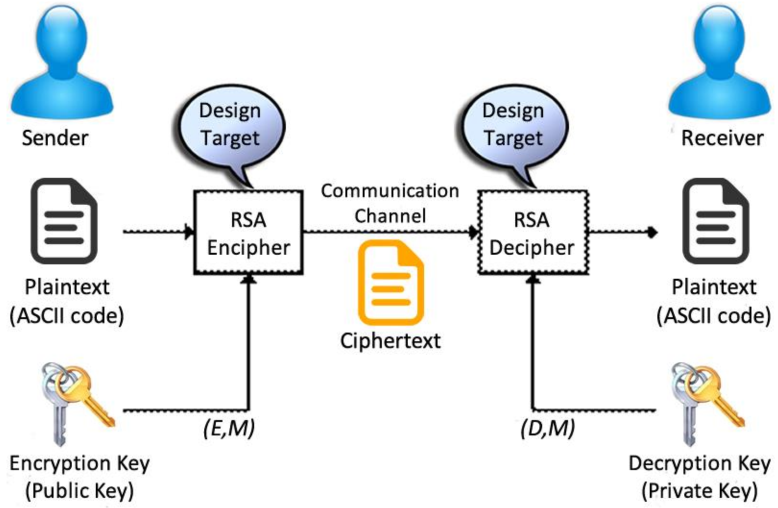


Figure 2. RSA algorithm structure

2.1. Algorithm Structure

- Choose two very large random prime integers: p and q.
- Compute n and $\varphi(n)$: $n = pq$ and $\varphi(n) = (p-1)(q-1)$.
- Choose an integer e, $1 < e < \varphi(n)$ such that: gcd(e, φ(n)) = 1 (where gcd means greatest common denominator)
- Compute d, $1 < d < \varphi(n)$ such that: $ed \equiv 1 \pmod{\varphi(n)}$.
- The public key is (n, e) and the private key is (n, d), the values of p, q and φ(n) are private, e is the public or encryption exponent, d is the private or decryption exponent.

After creating public and private keys, information which must be sent is encrypted with the public key.

Encryption and decryption processes are done as follows:

- The cypher text C is found by the equation $'C = M^e \bmod n'$ where M is the original message.
- The message M can be found from the cypher text C by the equation $'M = C^d \bmod n'$.
- A text encrypted with the public key can only be solved with the private key.

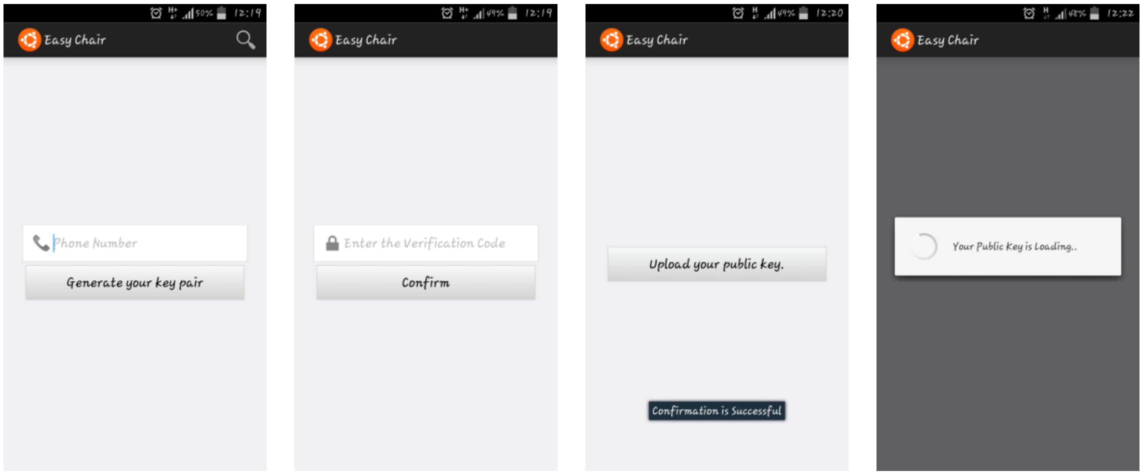
3. Related Work

An application has been developed on the Java platform in order to use the RSA encryption algorithm on Android-based mobile devices in the process of sending messages via SMS. Similar studies in which encryption algorithms are used in SMS messaging are available.

In one of these studies, encryption methods were written by means of AES and 3D-AES, which are private key (symmetric) encryption algorithms and the performance of these methods were compared. It was emphasized in the result of this comparison that the performance of the AES algorithm is higher when the length of the clear text is in the range of 0-256 bits while the performance of 3D-AES algorithm is higher in the cases of 256 bits and over [3].

In another study, the advantages of private and public key (asymmetric) encryption methods according to each other were examined and then RSA and ECDH algorithms, which are two public-key encryption algorithms, were compared and analyzed in terms of their performances and security issues [6]. The main result which is obtained from this study and similar studies is that the security levels of public key systems are higher than the security levels of private key systems.

Our difference from this study and similar studies is that we fixed the number of characters on the cipher text which would be allocated to blocks. Detailed information on this issue is reached by examining Tab 1. Fixing the number of characters makes it easy to allocate the cipher text into blocks for the sender side and to unit blocks for the receiver side. This reduces the complexity of process. As shown in Fig. 3 and Fig. 4, in the developed application each user must determine their public and private key and install their public key in the key library before beginning the encryption process with the RSA algorithm. Using the user's phone number information as the public key name will make it easy to determine which public key belongs to which user.

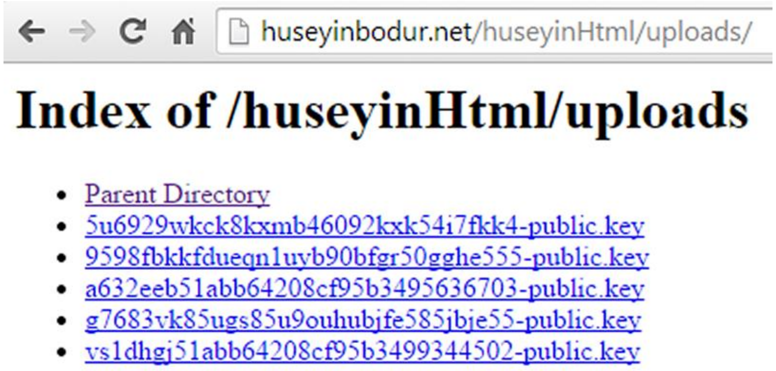


Confirmation is Successful

Your Public Key is Loading..

Figure 3. Generating key pairs and installing the public key to the library

Public and private key are generated only once. The application doesn't want the user to form two key values and to install public key in the key library again. After the public key is installed, the user selects a person to whom s/he wants to send a message from user's guide.



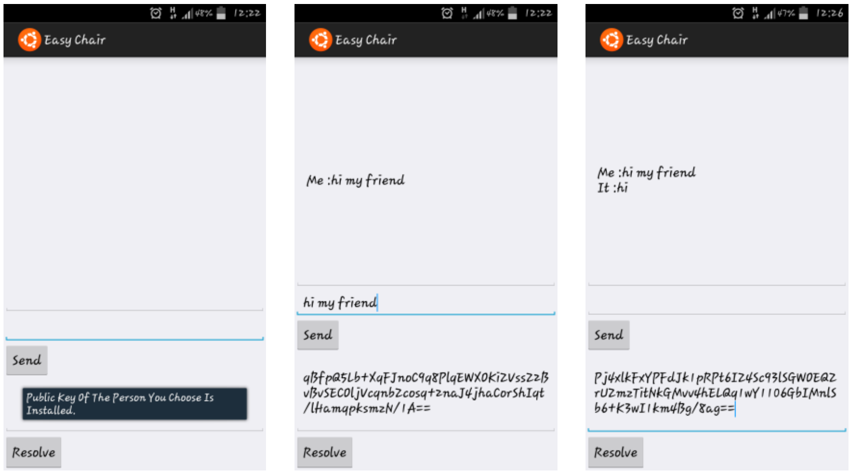
huseyinbodur.net/huseyinHtml/uploads/

Index of /huseyinHtml/uploads

- Parent Directory
- 5u6929wkck8kxmb46092kxk54i7fkk4-public.key
- 9598fbkkfduegn1uyb90bfgr50gghe555-public.key
- a632eeb51abb64208cf95b3495636703-public.key
- g7683vk85ugs85u9ouhubjfe585jbje55-public.key
- vs1dhgj51abb64208cf95b3499344502-public.key

Figure 4. Public keys installed in the key library.

If that person uses the application (if its public key is installed in the library), the person's public key is taken from the library, this key is loaded into the device's file system and the user is redirected to the page in which s/he sends a message. S/he writes and sends the message through this page. A simple screen design was created to display the encrypted message content in Fig. 5. When the message reaches the other side, the only thing that the other side needs to do is to turn on the application and to press the solve button. If the public key of the other side to whom the user wants to send a message is not installed in the library, it means that the other side does not use the application.



Public Key Of The Person You Choose Is Installed.

Me :hi my friend

hi my friend

qßfpQ5Lb+XqFJnoC9q8PlqEWX0KiZVssZzß vßvSECOljVcqnbZcosq+znaJ4jhaCorShIqt /lHamqpksmzN/1A==

Me :hi my friend
It :hi

Pj4xlkFxYPFdJk1pRPt6IZ4Sc93lSGW0EQZ rUZmzTitNkGMvv4hELQq1wY1106GbIMnlS b6+K3wI1km4ßg/8ag==

Figure 5. The installation of the other side's public key and the beginning of encrypted messaging

After the user has loaded her/his public key in the key library and installed the public key of the other side to whom the user wants to send a message into her/his system, there is no need in sending and receiving key packets over the internet for the next messaging in the application again. Internet is required only for the first match period. After the application initialization process has been completed, the parties can begin mutual messaging. The general structure of applied encryption processes is like the one in Fig. 6.

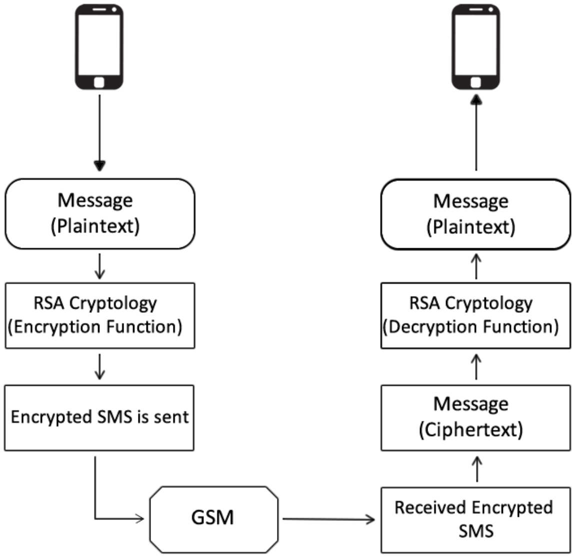


Figure 6. The general structure of sending encrypted SMS

4. Performance Evaluation

To prevent any problem in sending the message via the SMS channel, binary data must be encoded with Base64 structure, which is the encoding scheme that allows binary data to transmit and to store at the media using ASCII characters. Base64 structure brings a standard for the message's encrypted form. According to these standards, the message's encrypted form has the same size no matter how many characters the content of the message has unless it exceeds the number of characters in a certain block. For example, the message length which will be encrypted for the 512-bit key value is in the range of 0-64 character as shown in Tab. 1. The reason for this is that 512 bits (each character is 8 bits) is equivalent to the length of 64 characters. So, a 512-bit RSA key can encrypt a message up to maximum 64 characters. If the message's content includes more than 64 characters, what must be done is to allocate clear text into blocks. Encrypted data length obtained from a message which is in the range of 0-64 characters will be 88 characters. When the key size is 1024, the text can be encrypted in the range of 0-128 characters and the cipher text’s size includes 172 characters. When the key size is 2048, the text can be encrypted in the range of 0-256 characters and the cipher text size’s includes 344 characters. The message's length and the encrypted data's length are shown in Tab. 1 for the other key sizes.

Table 1. Maximum Message Length That Can Be Sent In Different Key Sizes

Size	Message length	Password length
256 bits	0-32 character	44 character
512 bits	0-64 character	88 character
1024 bits	0-128 character	172 character
2048 bits	0-256 character	344 character
3072 bits	0-384 character	512 character
4096 bits	0-512 character	684 character
8192 bits	0-1024character	1368 character

Another thing to be careful about is that with how many characters in maximum the data will be sent via SMS. A clear text message which is not subjected to any encryption algorithm can transmit up to 1120 bits [1], that is 160 characters level.

When the 1024 or 2048-bit key size of a message is used as shown Tab. 1, it is seen that the encrypted data consists of 172 and 344 characters. In this case, the encryption with a RSA key which has 1024 or 2048-bit key value is not suitable for the transmission of SMS messages on SMS encryption if any compression algorithm is not used. Since the encrypted message includes 88 characters for 512-bit RSA key value, it is better to select 512-bit as key size. The disadvantage of this situation is that transmission of message can be done up to maximum 64 characters for single-block message because the key size is 512 bits (64 characters). There are two ways to remove this disadvantage. Firstly, message can be allocated into blocks up to 64 characters before the encryption process. For this allocation process, how many blocks the message must be divided into is given in Fig. 7 as a pseudo code.

For a 512-bit key size;

```
$If\ (\,message\_size > 64\ and\ message\_size\ mod\ 64\ = 0)$
    $blocks\_number = message\_size/\,64;$
$else\ If(message\_size > 64\ and\ message\_size\ mod\ 64\ != 0)$
    $blocks\_number = (\,(Integer) message\_size/64\,) + 1;$
```

Figure 7. Block Number Finder Pseudo Code

The second way is to use the 1024 or 2048-bit key size because both the security level and the maximum number of characters that can be transmitted increase as the key size increases. However, the compression process must be applied on the clear text or the encrypted data of message because SMS restriction is constant with 160 characters. The average calculation durations of the different key sizes are shown in Tab. 2.

Table 2. The Average Calculation Durations Of Different Key Bits

Key size	Time (milliseconds)
256 bits	27
512 bits	84
1024 bits	411
2048 bits	2041
3072 bits	6010
4096 bits	14630
8192 bits	174115

Increasing the length of the encryption key has advantages in terms of raising both security levels and the number of characters that can be transmitted. The disadvantage of increasing the key length is that it requires more mathematical operations and raises the processing costs for the encryption and decryption processes.

5. Conclusion and Future Work

The communication method by means of SMS has a huge disadvantage in terms of security that the message content is not transmitted directly from sender to receiver and that it passes through the combination of several routers and central structures and that the sent message circulates as clear text between these structures. Using the structures of encryption is the right approach in order to eliminate this disadvantage. In this way, the message's security level can be increased.

But the biggest dilemma at this point is that the size of the message which can be transmitted via SMS is limited. That the encrypted data of the original message is larger than itself causes the message with maximum number of characters to be smaller. To solve this problem, both realizing the compression process on a message and allocating the contents of the message into the blocks will be right decision according to the maximum number of characters which correspond to the key size after selecting the appropriate key size to security level. Even if larger encrypted message sizes are created with RSA encryption algorithm compared to symmetric encryption algorithms, RSA algorithm is stronger than symmetric algorithms in terms of the security of encrypted messages. Storing the public key in a library requires that the device must be connected to the internet even if only a few times. The need of internet connection to send SMS message is another disadvantage. This disadvantage can be removed by doing the messaging over the internet entirely and eliminating the SMS technology. This is also a solution to the problem of limited message transmission of SMS technology.

However, using symmetric algorithms [8] can be another solution for encryption method. In this case, firstly key sharing might be realized between the two sides that will send messages to each other and then encrypted messages might be sent. Receiver can solve the content of the message with the key which is sent to her/him. If third people who listen to the communication channel or malicious operator staffs capture the value of this key and the message, they can decode the encrypted data. Therefore, receiver and sender must do key sharing in high-security environments.

6. References

[1] PEERSMAN, Gert, et al. A tutorial overview of the short message service within GSM. Computing & Control Engineering Journal; 2000; 11.2: 79-89.

[2] PEERSMAN, C., et al. The global system for mobile communications short message service. Personal Communications, IEEE; 2000; 7.3: 15-23.

[3] ARIFFI, Suriyani, et al. SMS Encryption Using 3D-AES Block Cipher on Android Message Application. In: Advanced Computer Science Applications and Technologies (ACSAT), 2013 International Conference on. IEEE; 2013, p. 310-314.

[4]Advantages and Disadvantages of Asymmetric and Symmetric Cryptosystems. http://www.uobabylon.edu.iq/eprints/paper_1_2264_649.pdf Access date: 01 December 2014

[5] RIVEST, Ronald L.; SHAMIR, Adi; ADLEMAN, Len. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM; 1978;21.2: 120-126.

[6] Neidhardt, Eric. "Asymmetric Cryptography for Mobile Devices."

[7] N. Saxena, N. S. Chaudhari, and J. Thomas. Solution to an attack on digital signature in SMS security. in Modeling, Simulation and Applied Optimization (ICMSAO), 2013 5th International Conference on, ed; 2013, pp. 1-6.

[8] SAXENA, Neetesh; CHAUDHARI, Narendra S. EasySMS: A Protocol for End-to-End Secure Transmission of SMS. 2014.

[9] RIVEST, Ronald L.; SHAMIR, Adi; ADLEMAN, Len. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM; 1978; 21.2: 120-126.