Android-Based Text Message Security Application With Rivest Method, Shamir, Adleman (RSA)

Iwan Purnama, Sudi Suryadi, Ronal Watrianthos, Deci Irmayani, Marnis Nasution

Abstract: Security is very important in all aspects to protect data. Text messages on mobile phones, which is sms (short messages service) is one of the important data that needs a data security system. Data security is used to maintain the confidentiality of important data that we have on mobile devices. The encryption process is used so that messages cannot be read by other unwanted parties. While the decryption process is used so that the message can be read back by the intended party. Rivest Cryptography, Shamir, Adleman (RSA) is one of the asymmetric cryptographic algorithms that use a key pair, that is the public key and private key. The key length can be set, where the longer the key formation bit, the harder it is to solve because it is difficult to factor two very large numbers. This study applies the Rivest, Shamir, Adleman (RSA) algorithm for text message security applications based on Android. Based on the research that has been done, the author can draw conclusions, namely: Rivest, Shamir, Adleman (RSA) cryptographic algorithm can be implemented for text message security Android based. So it is safer to exchange text messages (SMS) so that user privacy is guaranteed

Index Terms: Android, Security, RSA

1 Introduction

In recent years there has been a rapid development of technology, one of which is cellular phones (cellphones). Starting from mobile phones that can only be used for talking and texting to "smartphones" that have various functions such as multimedia, multiplayer games, data transfer, video streaming, and others. Various software to develop cellphone applications has also emerged, including those that are quite widely known as Android. One of the facilities provided by mobile phones is to send data in the form of short messages via Short Message Service (SMS). But with the existing SMS facility, questions arise regarding information security if someone wants to send confidential information through the SMS facility[1]. Abroad, the use of SMS to send secret messages has already been developed. For example in the UK a cell phone operator company, StaaCium UK, issued a service called "stealth text" which can be used to send messages safely, that is by deleting messages automatically as soon as 40 seconds of messages are read or known as self-destruct text message[2].

2 Research Method

2.1 Rivest Cryptography, Shamir, Adleman (RSA)

Rivest cryptography, Shamir, Adleman (RSA) is one of modern cryptography which encoding in asymmetric keys[3]. In 1977, Ron Rivest, Adi Shamir, and Lonard Adleman formulated a practical algorithm that implemented a public key cryptographic system called Ron Rivest cryptography, Adi Shamir (RSA)[4]. Although in 1997 the National Cryptogrhapy published that Clifford Cock had formulated the Rivest, Shamir, Adleman (RSA) system 3 years earlier than Rivest, Shamir, and Adleman.

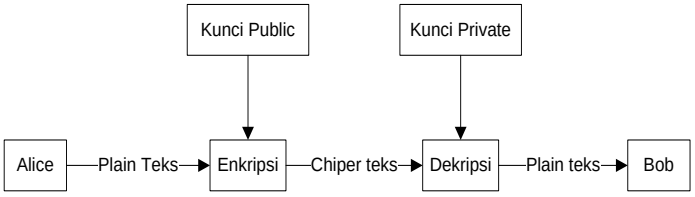

Figure.1 *Cryptography for network security*

As show Figure 1, There are 3 algorithms on the Rivest, Shamir, Adleman (RSA) cryptographic system, which is, as follows[5]:

I. Key generation algorithm

To use Ron Rivest, Adi Shamir (RSA), the descriptor (Bob) raised a key pair namely public key and private key at first. This key generation uses Algorithms. The first thing the key generator algorithm does is generate 2 large prime numbers. In order for the Rivest, Shamir, Adleman (RSA) cryptographic system to be safe, a large prime number is needed so that n = p x q is very difficult to factorize. The steps in the key generation are as follows:

1. Select two random prime numbers p and q.
2. Calculate n = p x q, with p ≠ q.
3. Calculate ϕ(n) = (p-1) (q-1)
4. Select public key e, which is relatively prime with ϕ (n).
5. Generate the private key d = 1+ k ϕ (n) / e or d = e-1 (1 + k.ϕ (n)).

II. Encryption Algorithm

Alice transmits her public key (n, e) Bob and keeps the key secret personal. Bob then wants to send a P message to Alice. Bob then calculates the ciphertext c according to *C=Pe mod n.* This can be done quickly using the exponentiation method by squaring it. Bob then sends c to Alice.

III. Decryption Algorithm

If Bob gets a password text that is encrypted with Bob's public key *P=Cd mod n* then Bob can use his private key to return the original text.

2.2 RSA Algorithm

RSA which was built by modular exponential function consists of three main processes, namely: key generation, encryption, and decryption[5]. Decryption must generate public and private keys in order to use RSA. Both of these keys require two large primes to make it difficult to be factored. The following RSA key generation algorithm is[6]:

Step 1. RSA Key Generation

p=47 and q=71 (both are prime)

n=p·q=3337

m=(p-1) (q-1) = 3220
Select e which is relatively prime to m, gcd (e, m) = 1
e=79→ gcd (79, 3337) = 1
Look for the value d, dxe = 1 mod (m)
dx79 = 1 mod 3220
dx79 mod 3220 = 1
d = 1019

So it gets:
1. Public key: (79, 3337)
2. Private key: (1019, 3337)

Step 2. RSA Encryption
After obtaining the above calculation, plaintext encryption will be done P = HARI INI. First, the plaintext is changed to ASCII format as follows:

The character of H A R I (SPACES) I N I
ASCII 72 65 82 73 32 73 78 73
P is broken down into six 3-digit blocks:
P1 = 726 P4 = 273
P2 = 582 P5 = 787
P3 = 733 P6 = 003 (plus 0)

After dividing the block, and then encrypted using the formula Ci = Pi ^ e mod n.
C1 = 726 ^ 79 mod 3337 = 215
C2 = 582 ^ 79 mod 3337 = 776
C3 = 733 ^ 79 mod 3337 = 1743
C4 = 273 ^ 79 mod 3337 = 933
C5 = 787 ^ 79 mod 3337 = 1731
C6 = 003 ^ 79 mod 3337 = 158

So, the obtained ciphertext is C = 21577617439331731158

Step 3. RSA Decryption

After the ciphertext from TODAY is obtained, to change it back to plaintext using decryption with the formula Pi=Ci ^ d mod n.
P1 = 215 ^ 1019 mod 3337 = 726
P2 = 776 ^ 1019 mod 3337 = 582
P3 = 1743 ^ 1019 mod 3337 = 733
P4 = 933 ^ 1019 mod 3337 = 273
Mod P5 = 1731 ^ 1019 3337 = 787
P6 = 158 ^ 1019 mod 3337 = 003

So, after decryption the results will be the same, which is, 7265827332737873, in ASCII characters, which is:
ASCII 72 65 82 73 32 73 78 73
Character of H A R I (SPACES) I N I

3 Result and Discussion

3.1 Testing the Mito 9800 Smartphone
Test on the Mito 9800 Smartphone to send the message "HARI INI" to number 08527710192 ie E1C + Tab 7 'tablet as the recipient of the message. Figure.2 are the results of the testing.

Figure.2 *Testing the Smartphone Mito 9800*

3.2 Testing Tablet Advance E1C
After sending from the Mito 9800 Smartphone, Figure.2 show the message in on the E1C Advance Tablet. To read the message, user must press the "Key" button and then press the "Message Decryption" button and the message "HARI INI" appears.

Figure.3 *Testing the Tablet Advance*

4 CONCLUSION
Based on the research that has been done, the author can draw conclusions, which are: Rivest, Shamir, Adleman (RSA) cryptographic algorithm can be implemented for the security of

Android-based text messages. So it is safer to exchange text messages (SMS) so that user privacy is guaranteed.

REFERENCES

[1] J. Calloway, I. Hemmans, J. C. Jimcalloway, and I. Hemmans, “The 411 on Texting for Lawyers,” in Techshow 2018, 2018.

[2] A. H. Kridalaksana, E. Arriyanti, and W. Widodo, “Aplikasi Pengaman SMS dengan Metode Kriptografi Advanced Encryption Standard (AES) 128 berbasis Android,” J. Sebatik, vol. 10, no. 1, pp. 8–14, 2013.

[3] B. S. Muchlis, M. A. Budiman, and D. Rachmawati, “Teknik Pemecahan Kunci Algoritma Rivest Shamir Adleman (RSA) dengan Metode Kraitchik,” SinkrOn, vol. 2, no. 2, pp. 49–64, 2017.

[4] A. R. ; D. Alvianto, “Pengaman Pengiriman Pesan Via SMS dengan Algoritma RSA Berbasis Android,” J. SAINS dan SENI ITS, vol. 4, no. 1, pp. 1–5, 2015.

[5] C. Paar and J. Pelzl, Understand Criptography, vol. 1. 2010.

[6] D. Rachmawati, A. Amalia, and Elviwani, “Combination of Rivest-Shamir-Adleman Algorithm and End of File Method for Data Security,” J. Phys. Conf. Ser., vol. 979, no. 1, 2018.