2016 1st International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE), Yogyakarta, Indonesia

RSA Implementation for Data Transmission Security in BEM Chairman E-Voting Android Based Application

Fransiskus Panca Juniawan
Information Engineering Department
STMIK Atma Luhur
Jl. Jend. Sudirman, Selindung Baru, Pangkalpinang 33117 Indonesia
fransiskus.pj@atmaluhur.ac.id

***Abstract*—Voting is a process that should be do in terms of leadership. In case, voting still use conventional methods which are less effective in terms of cost, governance, and working time. The possibility of calculation errors and fraud in the calculation process can also occur. STMIK Atma Luhur still using the conventional voting method in the election of the chairman of BEM. With the development of today's technology, we can make electronic voting system based on Android to solve the problems of conventional voting. E-voting security becomes fundamental things that must be considered. RSA cryptographic methods can be a solution to ensure the security. RSA choses because it has the advantage of difficulty level in factoring numbers into prime numbers. More difficult factoring the numbers, it will be more difficult to break the encryption. Another advantage is the form of higher security than symmetric algorithm. This algorithm is also resistant to various forms of attack, such as brute force. The security testing are using Wireshark and Eclipse LogCat. The result is the establishment of an e-voting system based on Android that is safe and confidential, so the students can do the voting quickly, whenever and wherever.**

Keywords—E-Voting; RSA Algorithm; Cryptography; Mobile; Android

I. INTRODUCTION

Voting is making decision process in terms of leadership. STMIK Atma Luhur today still using conventional election methods that less effective in terms of cost, governance, time, and security. Conventional election method make possible the calculation error and fraud in the calculation process. Today, technology has been growing rapidly, and Android phone usage is also increasing. With these condition, it can be proposed election of BEM chairman using Android mobile phone. There are many benefit of using mobile e-voting like computerized voting counting process so that becomes faster, more precise, and more accurate. The cost of implementing voting can also be reduced. Users are also able to vote anywhere and anytime with their own Android phone. The possibility of fraud and error calculation can also be avoided. Security of e-voting become the fundamental things that must be considered. There are four things that must be considered, namely accurate, democracy, privacy, and verifiability [1]. To fulfill these security aspect, cryptographic methods are needed to keep safe the security of that information. There are several methods of cryptography, one of which is RSA (Rivest-Shamir Adleman). This algorithm is an asymmetric cryptographic algorithms that perform with different encryption and decryption keys. This algorithm chosen because it has the form of a higher security than symmetric algorithms. In addition, this method is used for applications requiring fast digital data [2]. This algorithm is also resistant to various forms of attack, especially brute force. Other advantages are the degree of difficulty in factoring numbers into primes [3].

The purpose of this study is to make mobile e-voting system based on Android with RSA algorithm method in data transmission security.

II. RELATED WORK

Research by Al-Anie [4] conducted a study that the implementation of e-voting security protocol based on public key cryptosystem encryption. Nawindah [5], his work resulted the implementation of e-voting with MD5 encryption and election results were immediately visible. Handoyo [6] conducted a study that resulted the design of e-voting system with a cryptographic hash function without encryption and decryption. Kerem [7] resulted the use of NFC in mobile voting. Stradiotto [8] conducted the election process through the SMS protocol using web 2.0 tools and prototype system that can send voters data to the web service. Wisnu [9] resulted election-app with Hash Algorithm-1 and RSA key pair digital signing security method. Adnan [10] resulted multicore utilization for application of local e-voting purpose.

III. RIVEST SHAMIR ADLEMAN (RSA)

The RSA algorithm consist from four steps : key generation, key distribution, encrytion, and decription. RSA have basic principle which are find three very large positive integers *e*,*d*, and *n* with modular exponentiation (*m*).

A. Key Generation

The RSA algorithm using a public key (*e*,*n*) to encrypt the plaintext message. To decrypt the ciphertext, RSA using private key (*d*,*n*). The following are formula to compute *C* which is ciphertext and *M* which is plaintext.

B. Key Distribution

To distribute public and private key, User A transmit the public key (*n, e*) to User B via general way, but not the private key. The private key is never distributed.

C. Encryption

To calculate C (ciphertext), we can use formula (1) as shown as below :

$$C = M^e \bmod n \qquad (1)$$

- C is calculation result into ciphertext (encrypted number).
- M represent the plaintext that has been converted into ASCII code.
- The value of e and n is a public key pair that has been generated through the key generation process.

Here are the following RSA encryption flowchart shown as figure 1 :

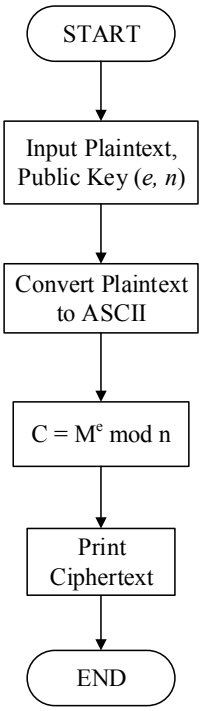


Fig. 1: RSA encryption Flowchart

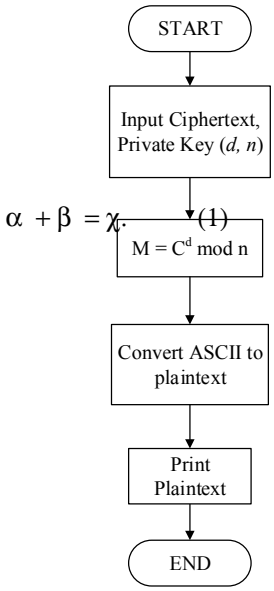
D. Decryption

To calculate M (plaintext), we can use formula (2) as shown as below :

$$M = C^d \bmod n \qquad (2)$$

- M is calculation result the value that to be returned into plaintext.
- C represent of the ciphertext or encrypted message that will be converted into plaintext.
- The value of d and n are pairs of private key that have been generated through the key generation process.

The following figure 2 shows RSA decryption flowchart :



$\alpha + \beta = \chi.$ (1) (1)

Fig. 2 RSA decryption Flowchart

IV. IMPLEMENTATION

A. Data Transmission Using RSA

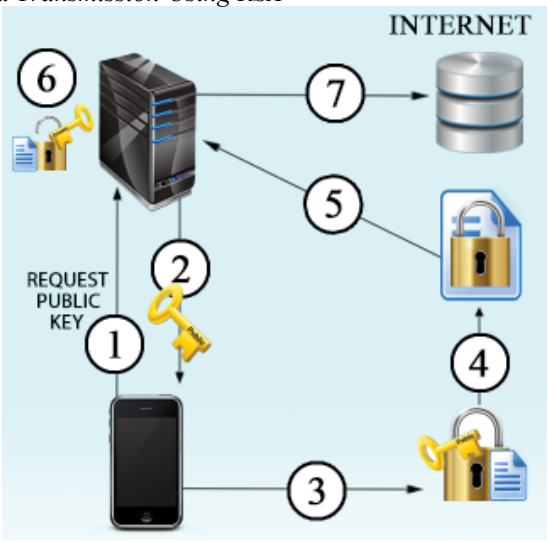


Fig. 3 : RSA Data Transmission Process

The following are explanation according figure 3 about RSA implementation on sending data process:

- Step 1 : Android Application make request to the server for public key.
- Step 2 : Servers generates the key primes p and q then performs calculations to determine the public key and private key. Then server sends the public key to the application.
- Step 3 : Application encrypts the message M to ASCII numbers. The encrytped data that sent candidate numbers. Messages ASCII M then converted into ciphertext C using the public key obtained.
- Step 4 : Applications sending ciphertext C to the server using URL function.
- Step 5 : The server accepts the ciphertext C.
- Step 6 : Server make the process of decryption with a private key with the PHP function. server then matches the decrypted form of the message M.
- Step 7 : Server save the data obtained to MySQL.

B. Data Process Analysis

In this voting application, there are four (4) candidates. To save the voting's results, each candidate is represented by a sequence number of 1 (one), two (2), 3 (three), and 4 (four). This application sends data preferred number and voters NIM to the server, but only preferred number data encrypted. So there are four possible encrypted data in terms with the serial number of candidates. Prime numbers are also selected randomly automatically in any electoral process to avoid fraud in the form of wiretapping. Due to the prime numbers are selected using random method, then the user will be used for the calculation of prime numbers is specified, namely 61 and 53. The following is the calculation process RSA encryption and decryption of the beginning :

- Determining the size of key encryption length is 1024. At this time the suggested key length for security RSA is 1024 bits.
- Determining the value of p and q randomly where p and q are primes free number. For example, manual calculations we have p = 61 and q = 53. These numbers were selected as a prime because not too big and not too small numbers. Prime numbers p and q in the calculations have been randomly selected because the application generate numbers p and q automatically so making it difficult to detect a selected number of applications.
- Calculate the modulus **n** (public key) and Euler's Totient function **Φ(n)** with formula **n = p * q**.

n = 61 * 53 = 3233
Φ(n) = (p-1)(q-1)
= (61-1)(53-1)
= 60* 52
= 3120

- Find e, where **1 < e < Φ(n)** and **GCD (Φ(n), e) = 1.**

TABLE I. E VALUE

e	GCD (25456, e)	Fermat = $2^{2^x} + 1$
e = 3	GCD (25456, 3) = 1	$2^{2^0} + 1 = 3$
e = 5	GCD (25456, 5) = 1	$2^{2^1} + 1 = 5$
e = 17	GCD (25456, 17) = 1	$2^{2^2} + 1 = 17$
e = 257	GCD (25456, 257) = 1	$2^{2^3} + 1 = 257$
e = 65537	GCD (25456, 65537) = 1	$2^{2^4} + 1 = 65537$

Table I. results that we have to choose e = 17 because that numbers included in the first five Fermat numbers so can make modular exponentiation process be faster.

- Calculate d with formula **d * e mod Φ(n) = 1** *d* * 17 mod 3120 = 1

Euclidean
3120 = 183 (17) + 9
17 = 1 (9) + 8
9 = 1 (8) + 1

Back Substitution
1 = 9 – 1 (8)
1 = 9 – 1 (17 – 1 (9))
1 = 9 – 1 (17) + 1 (9)
1 = 2 (9) – 1 (17)
1 = 2 (3120 – 183 (17)) – 1 (17)
1 = 2 (3120) – (2 * 183 (17)) – 1 (17)
1 = 2 (3120) – 366 (17) – 1 (17)
1 = 2 (3120) – 367(17)
d = 3120 – 367
d = 2753
So, e = (17, 3233) dan d = (2753, 3233).

Data encryption process conducted with formula **$Ci = Mi^e$ mod n.** With Mi = Nilai ASCII so get calculation described in the table below.

TABLE II. ENCRYPTION CALCULATION

Mi	ASCII	$Ci = Mi^e$ mod n	Value
1	49	49^{17} mod 3233	2906
2	50	50^{17} mod 3233	538
3	51	51^{17} mod 3233	368
4	52	52^{17} mod 3233	529

Table II. shows encryption calculation for each candidates number. So, for the first candidate with the serial number 1 will sent data with value 2906. For the second candidate with the number 2 will sent the data with value 538. The third candidate with the number 3 will sent the data with value 368, and for a fourth candidate with the number 4 will sent data with value 529.

Data decryption process is the reverse of the encryption data process which cipher text obtained from the encryption will be processed by the formula $Mi = C^{id}$ mod n to get the

original plaintext. The following table outlines the calculation of the data decryption.

TABLE III. DECRYPTION CALCULATION

Ci	Mi = Ci^d mod n	Nilai ASCII	Hasil
2906	2906^{2753} mod 3233	49	1
538	538^{2753} mod 3233	50	2
368	368^{2753} mod 3233	51	3
529	529^{2753} mod 3233	52	4

Table III. shows decryption calculation from ciphertext value. So, once decrypted, the ASCII value of the ciphertext is obtained, then the ASCII value are converted into the original value. The results are 2906 for result 1, 538 for results 2, ciphertext 368 for result 3, and the ciphertext 529 for result 4.

C. *System Architecture Analysis*

Figure 4 explains about voting system architecture that be used. the voting system architecture consists of three parts, such as the interface, Android Smartphone, and the server. At the appearance of the user interface describes the application form of authority permissions for users. In the android smartphone models explain the RSA algorithm that used. Server section describes the model RSA algorithm that used with data sources such as MySQL databases applications.

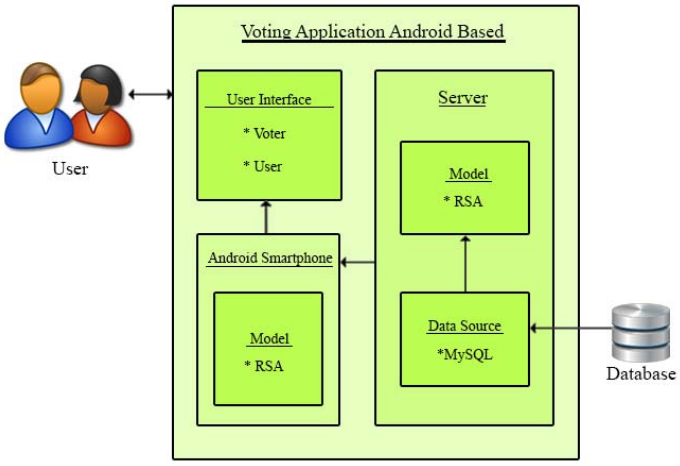


Fig. 4 System's General Architecture

D. *Analysis and System Design*

System analysis process describe what should be done by system to meet the users needs. Figure 5 shows system use case that describe system function from user perspective.

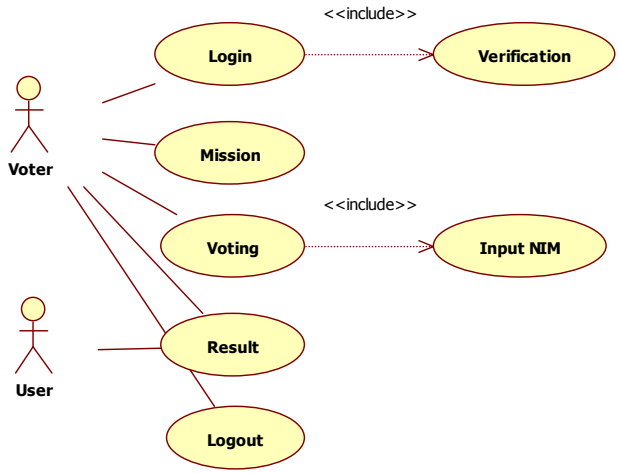


Fig. 5 System Use Case

Figure 6 show the class diagram in this system. The class consists of three table, that is mahasiswa, calon, and rincian.

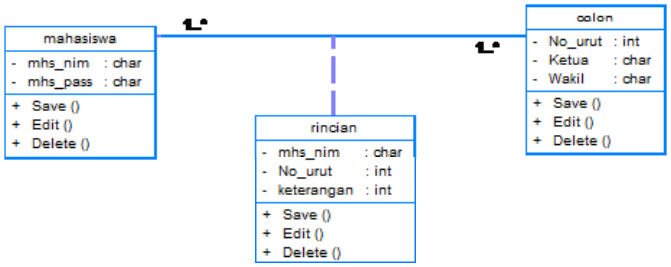


Fig. 6 System Class Diagram

Figure 7 shows activity's diagram voting. Voter initiate to start the application and go to homepage, then entering login page. Voter input the username and password. This step occur loop process. Then voter can choose the candidates and make the election. Finally, voting data will be saved in the server.

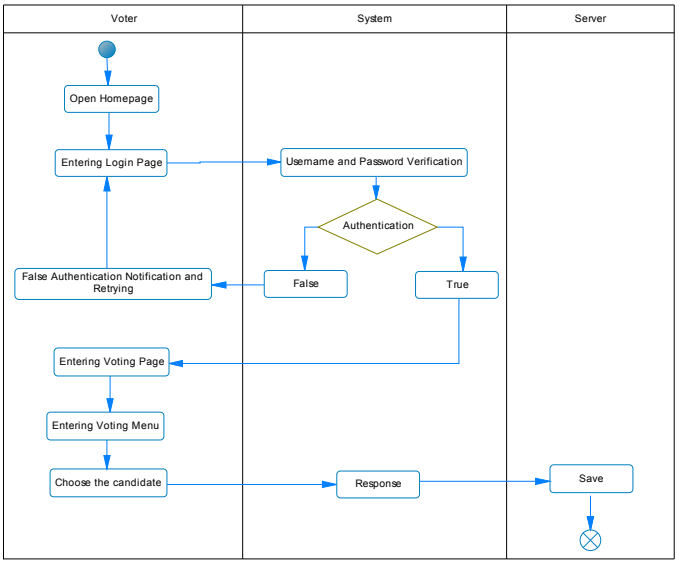


Fig. 7 Activity Diagram's Voting

Figure 8 show sequence diagram's voting.

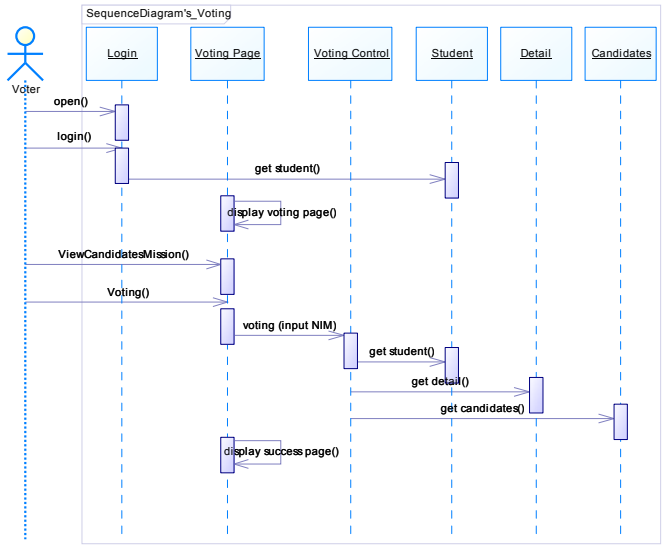


Fig. 8 Sequence Diagram's Voting

E. *Database Construction*

Mobile voting database is build using the MySQL database. software that used to design is phpMyAdmin. This tool provides data modeling, SQL development and database server configuration.

192.168.23.23:3306 » novalhe1_vote » calon

Browse | Structure | SQL | Search | Insert | Ex

#	Name	Type	Collation	Attributes	Null	Default	Extra
1	No_urut	int(1)			No	None	
2	Ketua	varchar(25)	latin1_swedish_ci		No	None	
3	Wakil	varchar(25)	latin1_swedish_ci		No	None	

Fig. 9 Candidate's Entity

Calon table consists of field No_urut with integer, Ketua with varchar, and Wakil with varchar.

F. *User Interface*

Fig. 10 Candidates Page

Figure 10 shows candidates page, there are four candidates. Click the candidates to the next step.

Fig. 11 Voting Page

Figure 11 shows voting page and candidates mission, insert voter's NIM and click Vote Button to deal it.

G. *Security Testing*

At this stage, conducted choosing process prime numbers with LogCat Eclipse and security testing with wireshark. Figure 12 is a display of enrcyption primes p and q in Logcat Eclipse. Figure 13 is a display of prime number that choosen randomlyand automatically on the application. Figure 14 show data testing results interception that has been encrypted using wireshark. Its results obtained random bytes data number encrypted with the RSA algorithm.

```
Prime exponent p : 11571345705632016433222156114637125071920588
88121625974643054262353126410065906852501166488335374455610877
26826452350612479816619395380250710164999474494298 7
Prime exponent q : 11201461649182603574214928380232757078273599
82594144318388886684939550919797772412898253443784476325916453
57055544259441310180287765414231561274211898713707
```

Fig. 12 LogCat Eclipse

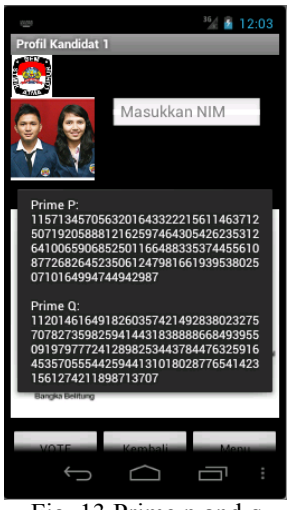


Fig. 13 Prime p and q

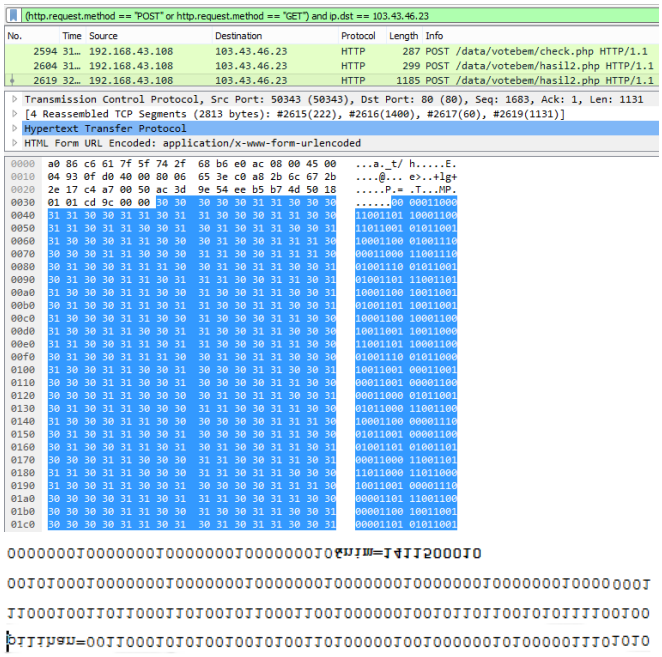


Fig. 14 Wireshark Interception Results

V. Conclusion

Based on RSA voting data transmission security on android-based research, it can be concluded as follows :

- The use of RSA algorithm in the data transmission security on the android-based smartphone get a good result. This is because the RSA algorithm is very good method of securing the security level.
- This android-based mobile voting with RSA algorithm can prevent the occurrence of rigging the election results because it has been encrypted.
- From the wireshark security testing results, it can be proved that the election data is sent encrypted properly. This makes the actual data can not be seen.

References

[1] C. Lambrinoudakis, *Secure Electronic Voting: Trends and Perspectives*. 2002.

[2] D. Boneh, *Twenty Years of Attacks on the RSA Cryptosystem*. 1999.

[3] P. S. . Pardede, "Analisis dan Perancangan Keamanan Informasi Pada Electronic Voting Menggunakan Algoritma Kriptografi Kunci Publik," 2012.

[4] H. K. Al-Anie, M. A. Alia, and A. A. Hnaif, "E-Voting Protocol Based on Public-Key Cryptography," *Int. J. Netw. Secur. Its Appl.*, vol. 3, no. 4, 2011.

[5] Nawindah and A. Sofwan, "Analisa Perancangan dan Implementasi Sistem Informasi E-Voting untuk Pemilihan Ketua BEM pada Himpunan Mahasiswa Jurusan Teknik Grafika dan Penerbitan," *Pros. Semin. Nas. Multidisiplin Ilmu Univ. Budi Luhur*, 2014.

[6] A. B. Handoyo, "Sistem Pengamanan Data Pemilihan Umum e-Voting dengan Menggunakan Algoritma SHA-1," *Makal. IF3058 Kriptografi - Sem. II*, 2013.

[7] K. Ok, V. Coskun, and M. N. Aydin, "Usability of Mobile Voting With NFC Technology," 2013.

[8] C. R. K. Stradiotto, T. C. . Bueno, and V. O. Mirapalheta, "Web 2.0 E-Voting System Using Android Platform," 2014.

[9] D. A. M. G. Wisnu, A. Suharsono, and D. S. Rusdianto, "Rancang Bangun Sistem E-Voting dengan Menerapkan Hash dan Digital Signature untuk Verifikasi Data Hasil Voting," 2013.

[10] Adnan, "Kinerja Tanda Tangan Digital RSA 1024 bit pada Simulasi E-Voting Menggunakan Prosesor Multicore," *Semin. Nas. Apl. Teknol. Inf.*, 2014.