Cryptography Implementation for electronic voting security

Suwarjono Suwarjono*, Lilik Sumaryanti, and Lusia Lamalewa

Department of Informatics, Faculty of Engineering, Universitas Musamus, Merauke 99600, Indonesia

Abstract. Electronic voting is done by recording election data centrally and presenting it into fast digital information. E-voting is an internet technology, which aims to improve the performance of the voting process, and is expected to be a breakthrough in technological development that helps human work. Security constraints in e-voting include the distribution of voting, for example voters who distribute voting rights, are illegitimate and can abuse voters' rights, because they know the voter's account to access the system. This study implements cryptographic methods as a password security for voter accounts, and the results of voting, so that the secrecy of the voters' data and the results of voting are maintained. RSA algorithm to implement cryptographic techniques based on two mathematical problems, namely factorization and modulo operations on composite numbers, which use two different keys for encryption and decryption processes. The public key is used encryption process to encode text, and the private key is used description process, namely translating ciphertext into plaintext.

Keywords: Cryptography; Electronic; Security

1 Introduction

E-voting system is an internet technology-based, which aims to improve the performance of the voting process, and is expected to be a breakthrough that can take place in accordance with the principle of election that is direct, general, honest and fair. Electronic voting is done by centrally recording election data and presenting it into fast and inexpensive digital information, because the process of selecting and counting votes consists of a simple process, and only requires a few workers [1]. Whereas conventional voting can lead to fraud and human error in the vote counting process, or the occurrence of problems such as a voter can give more than one vote. Besides the conventional system provides a loophole to manipulate or change the results of vote calculations for certain candidates. The application of technology based on the concept of the Internet of Things offers transparency in the implementation of voting activities and supports voters to vote via mobile and PC connected to the network [2]. The e-voting system has the advantage of providing easy access to vote, but security issues are a new obstacle in the voting machine [3]. Security problems in e-voting include the distribution of voting rights, for example voters who distribute voting rights, not their true identity can abuse, because they know the voter's account to access the system. The security of e-voting by performing the authentication process using face recognition, is used as a reliable and strong password for voters to be able to give their voting rights [4, 5]. The implementation of e-voting security uses biometric techniques as a non-

transferable physical characteristic, such as fingerprints and pattern recognition as identification of voters' identities [6].

Fair elections must be able to guarantee the confidentiality and integrity of the votes cast by voters, and have the ability to audit election results [7]. The privacy is guarantee for the owner of the vote can be done by using encryption techniques, that can maintain the secrecy of the voters' votes [8]. The application of e-voting based on surveys can increase voter participation to distribute voting rights, and tools to reduce apathetic voters, the system prioritizes the convenience of access to be able to distribute voting rights without being limited to polling stations, and presents accurate vote count results [9, 10]. This study implements cryptographic methods as a password security for voter accounts, and the results of voting, so that the secrecy of the voters' data and the results of voting are maintained. The stegano-cryptographic model is used to improve security in e-voting systems to prevent the possibility of fraud in electronic voting [11].

The application of e-voting must be carried out in accordance with the nature of the law, namely: suffrage is universal, everyone can choose; equality of votes: every voice is the same; freedom of choice: the autonomy of voters' decisions must be granted; secrecy of the vote; voting is direct, personal right to vote: a personal vote without representation must be granted, and an audit process can be carried out [12, 13]. The research to improve security of e-voting systems using one of the cryptographic methods namely blockchain techniques, shows that the system can provide security

---

* Corresponding author: suwarjono@unmus.ac.id

to avoid falsification of the results of voting [14]. Security methods using the blockchain encryption process can be applied to electronic voting and other applications [15, 16]. Encryption methods have been used to improve the security of voting using cellular media by applying a symmetric and hybrid algorithm, the Elliptic Curve Cryptography (ECC) algorithm, where voters' votes will be encrypted on the server administrator and will be read using RSA public key encryption [11].

2 Material and Methods

2.1 Cryptographic Methods for Information Security

The Information security is an activity to maintain confidentiality in the presentation of digital information from all electronic data usage for unauthorized users. Implementation of security in presenting data to protect the confidentiality and integrity of data can be done using cryptographic encryption methods.

Cryptography is one of the fields of computer information security technology that applies the method of sending personal information through open network communication. The security of cryptographic services such as: confidentiality, approval, integrity and accessibility of information presented through the process of encrypting information that is encrypted using a cryptographic key. The length and strength of cryptographic keys are important factors for the encryption and decryption process, so they can produce strong and reliable encryption. The application of cryptographic methods in daily life includes electronic voting, computer passwords, ATM cards, and electronic commerce. The stages of applying cryptographic techniques in this study are shown in Figure 1.

Fig. 1. Cryptography Implementation Diagram

Application of cryptographic techniques consists of two processes, namely encryption and decryption. The message or original data is called plaintext, which can be read and understood by anyone. While the plaintext message that has gone through the encryption process or the encoding process is referred to as ciphertext or encrypted data. The encryption and decryption process uses a special algorithm which involves the use of a key form called a cipher, which is a mathematical function

for the encryption and decryption process. The mathematical concept underlying the cryptographic algorithm is the relation between two sets containing plaintext elements and the set containing ciphertext. Encryption and decryption are functions that map the elements between the two sets. For example, P represents plaintext and C represents ciphertext, so that it can be determined [17]:

$E(P) = C \Rightarrow$ application of the E encryption function maps P to C

$D(C) = P \Rightarrow$ application of the decryption function D maps C to P

This study uses the RSA algorithm to implement cryptographic techniques on the results of voting with an e-voting system. In addition to voting results provided by voters, cryptographic techniques are also applied to the user name of the voter account, this is done to prevent unauthorized voters in the electronic voting process. Sender is an entity that has the right to choose and send messages or the results of voting to other entities. Whereas the receiver is the entity that receives the message or the voting committee.

2.2 RSA Algorithm

Cryptographic algorithms are divided into two categories, namely symmetric and asymmetric. Where the symmetric algorithm uses one key for the encryption and decryption process. While the Asymmetric Algorithm uses two different keys for the encryption and decryption process. The public key is used for the encryption process, which is the process of encoding or changing the original text data (Plaintext) to secret text (Ciphertext), and the private key is used for the decryption process, namely translating secret text (ciphertext) into original text (plaintext). Cryptography overcomes the problem of data security by using a key, which must be kept confidential. The key is the parameter used for encryption and decryption transformation. The key is usually a string or a string of numbers. By using a key, the encryption and decryption functions can be performed as the diagram shown in Figure 1.

RSA (Rivest Shamir Adleman) algorithm is an asymmetric cryptographic algorithm, where the key used to encrypt is different from the one used to decrypt it. Cryptographic security is implemented by the RSA method based on two mathematical problems, namely factorization and modulo operations on composite numbers. The public key is available to everyone, so users can encrypt data but cannot decrypt, the only person who can decrypt it is the person who has the private key. Theoretically it is very difficult to make a private key a public key, this makes the RSA algorithm a very popular choice in data encryption [17].

The step of applying the RSA algorithm begins with determining two prime numbers, p and q . Multiplication of two numbers called n which is a component of a large-value public key, numbers p and q cannot be extracted from more than 512 bits, that is, numbers greater than 10^{154} . Then the encryption key e is co-prime into a number [18]:

$m = \phi(n) = (p-1)(q-1)$, determination of the decryption key d such that $de \bmod m = 1$. Based on this rule we can generate public keys and private keys.

2.2.1 Encryption

The encryption process is done by determining $y = E(x)$ to be an encryption function where x is an integer and y is a form of data that is amplified from x , so to produce the value of y using the following equation [17, 18]:

$$y = x^e \bmod n.$$

2.2.2 Decryption

Presentation of information to the receiver through the decryption process, assuming that $X = D(y)$ becomes a decryption function, example y is an encrypted integer and X is a description form of y , so as to generate the value of X using the following equation [17, 18]:

$$X = y^d \bmod n$$

3 Results and Discussion

E-voting application was made to carry out an electronic voting process with a case study of student president and vice president elections. Presentation of information provided by the application includes: presentation of real time voting information, account data management for voters, validation of voter accounts sent by email, by encrypting the username and password, providing facilities to set start and end times voting process, facilities to activate and verify voter accounts, counting the results of voting in real time, encrypting the votes that have been given by voters and presenting the results of vote counting based on the number of voters who use their voting rights.

Application of cryptographic techniques in e-voting, for example voters or senders want to distribute their voting rights to the election committee, the system will encrypt the election results using the RSA algorithm with a scheme where the sender must get a receiver's public key pair (e, n) . The message sent is encrypted using pairs (e, n) . However, the message ' m ' must be represented as an integer in the interval $[0, n-1]$. To encrypt it, the sender only counts the number ' c ' where $c = m^e \bmod n$. Then sending the results of the election that has been coded c ciphertext to the committee.

Presentation of encrypted message information to the receiver using a private key by decrypting the c password text, the receiver needs to use his own private key d (decryption exponent) and modulus n . By calculating the value of $c^d \bmod n$, so that it returns the decrypted message (m). An example of applying encryption and decryption with RSA is explained as follows:

- Determine two values by choosing prime numbers $p = 3$ and $q = 11$
- Calculate the value of n by multiplying the values of p and q to be $n = p * q = 3 * 11 = 33$, then find the value of m with the equation

$$m = (p-1)(q-1) = (3-1)*(11-1) = 2 * 10 = 20$$

- Searching factor number by trying $e = 3$, so that $\gcd(3, 20) = 1$ indicates that e is co-prime to n .
- Finding the value of d where $1 \equiv d * e \bmod m \rightarrow 1 = K * m + d * e$, using Euclid's algorithm which shows that $1 = -1 * (20) + 7 * (3) \rightarrow$ generate value $d = 7$.
- Encryption process uses a public key example: let's say we want to encrypt numbers $x = 9$ use encryption function $y = x^e \bmod n$, so that

$$y = 9^3 \bmod 33 \rightarrow y = 729 \bmod 33 \equiv 3 \rightarrow E(9) = 3$$
- Presentation of messages using the private key by doing the decryption process y we use the function $X = y^d \bmod n$, where

$$X = 3^7 \bmod 33 \rightarrow x = 2187 \bmod 33 = 9 \rightarrow \text{value } x = 9 \text{ so the decryption process is successful}$$

Figure 2 shows the results of implementing e-voting for the encryption and decryption process.

Fig. 2. E-voting using security of cryptography

Application of the RSA algorithm is most widely used, because it allows one of two keys to encrypt a message and vice versa the opposite key to decrypt, thereby inviting confidentiality, integrity, authenticity, and non-integrity of data and Information and communications technology [19]. The use of two large prime numbers randomly chosen is used to calculate modulus n , to generate public key and private key. The strength of RSA lies in its key size, because it is not easy to find large prime number factors, to do encryption, consequently the calculations are slow and have some special compilation negatives related to cellular devices, because they require more battery resources and battery resources for the keys public, thus increasing device performance [17], RSA key strength is based on the selection of large prime numbers, thus causing the encryption process slower than using other algorithms to generate public keys [19]. Presentation of public interest services based on information, communication and technology, plays an important role in helping human work [20], both in agriculture and food and other fields [21, 22].

4 Conclusion

Electronic voting system security with cryptography techniques can be employed to maintain the confidentiality and data integrity of the voting for the legitimate user. RSA public key algorithm for encryption, which is the process encoding of plaintext

become ciphertext, and the private key is used to process descriptions that translate message into plaintext ciphertext. RSA well in addressing the security issues of data by using a key, which must be kept confidential, with the strength of RSA lies in the size of the key, because it is not easy to find large prime factor. This algorithm has the disadvantage that requires considerable time in finding the factors of primes, causing RSA is slower than the other algorithms in making public key.

References

1. K. M. AboSamra, A. A. AbdelHafez, G. M. R. Assassa, and M. F. M. Mursi, "A practical, secure, and auditable e-voting system," *J. Inf. Secur. Appl.*, vol. **36**, pp. 69–89, (2017).
2. L. Yuan, M. Li, C. Guo, W. Hu, and Z. Wang, "A verifiable e-voting scheme with secret sharing," *Int. J. Netw. Secur.*, vol. **19**, no. 2, pp. 260–271, (2017).
3. D. Springall *et al.*, "Security analysis of the estonian internet voting system," *Proc. ACM Conf. Comput. Commun. Secur.*, no. May, pp. 703–715, (2014).
4. Z. J. Mohammed Ameen, "Secure Electronic Voting Application Based on Face Recognition and Ciphering," *Res. Artic. J. Comput. Sci. Appl. Inf. Technol.*, vol. **3**, no. 2, pp. 1–11, (2018).
5. A. DeviS and A. JothiR, "Confidential E-Voting System Using Face Detection and Recognition," *Int. J. Eng. Tech.*, vol. **3**, no. 4, pp. 81–85, (2017).
6. T. U. Pavshere and S. V More, "A Survey on Secured E-Voting System Using Biometric," *Int. J. Advanced Res. Sci. Eng. Technol.*, vol. **3**, no. 3, pp. 1700–1704, (2016).
7. G. Uzedhe and J. Okhaifoh, "a Technological Framework for Transparent E-Voting Solution in the Nigerian Electoral System," *Niger. J. Technol.*, vol. **35**, no. 3, p. 627, (2016).
8. M. T. Afrin and K. J. Satao, "E-Voting System for on Duty Person Using RSA Algorithm with Kerberos Concept," *Int. J. Adv. Res. Comput. Eng. Technol. (IJARCET)*, vol. **2**, no. 7, pp. 2258–2261, (2013).
9. C. Sravani and G. Murali, "Secure electronic voting using blockchain and homomorphic encryption," *Int. J. Recent Technol. Eng.*, vol. **8**, no. 2 Special Issue 11, pp. 1002–1007, (2019).
10. A. Ampuni, A. Fitrianto, and R. Indrajaya, "E-voting infrastructure system for Indonesia," *Int. J. Innov. Technol. Explor. Eng.*, vol. **9**, no. 1, pp. 761–763, (2019).
11. D. V. R. Aditya B Kakde, "Mobile Voting System Secutrity Schema Based on Elliptic Curve Cryptography," *Int. J. Electr. Electron. Res.*, vol. **3**, no. 4, pp. 209–214, (2015).
12. O. O. M, A. O. T, O. E. O, and O. O. O, "Performance Assessment Of An Imperceptible And Robust Secured E-Voting Model," *Int. J. Sci. Technol. Res.*, vol. **3**, no. 6, pp. 127–132, (2014).
13. T. Lauer and T. W. Lauer, "The Risk of eVoting," *Electron. J. E-government*, vol. **2**, no. March, pp. 177–186, (2016).
14. A. Raj, G. T. George, P. Konnullu, and S. R. Nair, "Vote Blocks : A Block Chain Based E - Voting System," *Int. J. Comput. Sci. Trends Technol.*, vol. **7**, no. 3, pp. 49–54, (2019).
15. S. bindewari and J. Surana, "Design and Implementation a Smart E-Voting Model : Decentralization Using Blockchain," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. **5**, no. 4, pp. 109–114, (2019).
16. K. M. Khan, J. Arshad, and M. M. Khan, "Secure digital voting system based on blockchain technology," *Int. J. Electron. Gov. Res.*, vol. **14**, no. 1, pp. 53–62, (2018).
17. S. Nisha and M. Farik, "RSA Public Key Cryptography Algorithm A Review," *Int. J. Sci. Technol. Res.*, vol. 06, no. 07, pp. 187–191, (2017).
18. M. Preetha and M. Nithya, "A STUDY AND PERFORMANCE ANALYSIS OF RSA ALGORITHM," *Int. J. Comput. Sci. Mob. Comput.*, vol. **2**, no. 6, pp. 126–139, (2013).
19. I. Jahan, M. Asif, and L. Jude Rozario, "Improved RSA cryptosystem based on the study of number theory and public key cryptosystems," *Am. J. Eng. Res.*, vol. **4**, no. 1, pp. 2320–847, (2015).
20. L. Sumaryanti and N. Nurcholis, "Analysis of Multiple Criteria Decision Making Method for Selection the Superior Cattle," *INTENSIF J. Ilm. Penelit. dan Penerapan Teknol. Sist. Inf.*, vol. **4**, no. 1, pp. 131–141, (2020).
21. L. Sumaryanti, L. Lamalewa, and T. Istanto, "Implementation Of Fuzzy Multiple Criteria Decision Making For Recommendation Paddy Fertilizer," *Int. J. Mech. Eng. Technol.*, vol. **10**, no. 3, pp. 236–243, (2019).
22. L. Sumaryanti, T. K. Rahayu, A. Prayitno, and Salju, "Comparison study of SMART and AHP method for paddy fertilizer recommendation in decision support system," *IOP Conf. Ser. Earth Environ. Sci.*, vol. **343**, no. 1, (2019).