SECURITY E-MAIL MESSAGE USING ONE TIME PAD ALGORITHM FOR ENCRYPTION MESSAGE

by Turnitin 7

Submission date: 26-Oct-2023 02:03PM (UTC+0700)
Submission ID: 2207695252
File name: 11-_jeas_1119_8012_1_Security_robbi_rochim.pdf (361.52K)
Word count: 2147
Character count: 11439

VOL. 14, NO. 22, NOVEMBER 2019 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

SECURITY E-MAIL MESSAGE USING ONE TIME PAD ALGORITHM FOR ENCRYPTION MESSAGE

Robbi Rahim[1], Erlin Windia Ambarsari[2], Akbar Iskandar[3], Firman Aziz[4], Wildan Mahir Muttaqin[5], S Sujito[5], Folkes E. Laumal[6], Erna Hendrawati[7], Lusy Tunik Muharlisiani[7], Irwan Sugiarto[8], Endang Noerhartati[7] and Johny Sugiono[7]

[1]School of Computer and Communication Engineering, Universiti Malaysia Perlis, Arau, Malaysia
[2]Universitas Indraprasta PGRI, Indonesia
[3]STMIK AKBA, Makassar, Indonesia
[4]Universitas Pendidikan Indonesia, Bandung, Indonesia
[5]Department of English Language Education, IAIN Surakarta, Indonesia
[6]Politeknik Negeri Kupang, Kupang, Indonesia
[7]Universitas Wijaya Kusuma Surabaya, Surabaya, Indonesia
[8]Sekolah Tinggi Hukum Bandung, Indonesia
E-Mail: usurobbi85@zoho.com

ABSTRACT

The confidentiality of information in the digital age is very important, one of which is the confidentiality of e-mail messages so that they cannot be read by certain parties, especially e-mails that are under the domain of companies or institutions where e-mail admins can be read. The solution that can be given is to do the encryption and decryption process in e-mail messages so that only those who are entitled can read the e-mail message. One Time On is an algorithm that is suitable to be applied to the security of e-mail messages because the encryption process is done with keys in accordance with the length of e-mail messages and is very difficult to analyze.

Keywords: cryptography, mail security, security, one time pad.

INTRODUCTION

Electronic Mail or commonly called E-mail is one type of service that cannot be released from all activities that occur in cyberspace, email usage is not only for business but also for social networks, sending messages quickly, sending important files and other things related to the information transfer process [1], [2]. Microsoft Outlook and Mozilla Thunderbird are applications specifically for sending and receiving e-mails from third parties, sending e-mails will be easier if using applications such as outlook or thunderbird and reading e-mails will be easier because the message will be downloaded first so that it can be read offline.

E-mail messages are basically not encrypted except that the e-mail sending process is secured using SSL (Secure Socket Layer) [3] which is in accordance with the standard so that various types of mail servers can communicate with each other well, security weakness in e-mail messages [4] is one of the problems that the author discussed this research, to secure the message the author uses a One Time Pad algorithm [5]-[7] to encrypt so that secure e-mail messages from irresponsible parties if the e-mail message is successfully tapped.

One Time Pad is one of the best algorithms until now and it is uncrackable if the message are not with same pattern [8], the use of one time pad algorithm on email message security is very good because the message encryption process is perform with same length key and the key used in the security message is random generated so it doesn't have a special pattern and it is also make difficult to cryptanalysis to decipher the message, and one more advantage is that the encryption ciphertext has the same length of message as the plaintext so that it does not make heavy resources on the network.

THEORY

Security system

Security system is a process of making several work procedures by adding security aspects so as to produce a good system with integrated security features on the system [9]. Aspects relating to security [10], [11] requirements include:

a) Secrecy. Associated with access to reading data and information. Data and information in a computer system can only be accessed and read by people who are entitled.
b) Integrity. Connect with access to change data and information. Data and information that is inside a computer system can only be changed by the rightful person.
c) Availability. Associated with the availability of data and information. Data and information that is in a computer system is available and can be used by people who are entitled.

Cryptography

Cryptography is the science and art of storing messages, data, or information safely that is sent from somewhere to another [12], [13]. Cryptography is part of a branch of mathematics called Cryptology that deals with aspects of information security such as data confidentiality, data validity, data integrity, and data authentication [14], [15]. Cryptography aims to maintain

the confidentiality of information contained in the data so that the information cannot be known by unauthorized parties. But not all aspects of information security can be handled by cryptography.

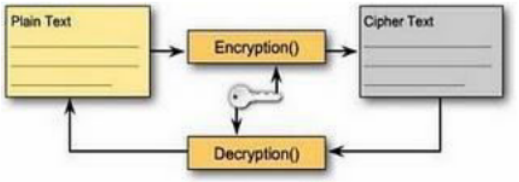

Figure-1. Cryptography Process Ilustration.

Cryptography can not be separated from key processing, symmetry and asymmetry is the key used in cryptographic algorithms. Simeteris cryptographic algorithms or also called conventional cryptography algorithms are algorithms that use the same key for encryption and decryption[6], [16]. The security of symmetry cryptography lies in the secrecy of the key, there are many modern cryptographic algorithms that are included in symmetry cryptography systems including DES (Data Encryption Standard), Blowfish, Twofish, Triple-DES, IDEA, Serpent, AES (Advanced Encryption Standard).

The advantages of symmetric key[17] algorithms or also called secret key algorithms are:

a) The operating speed is higher when compared to the asymmetric algorithm.
b) Because the speed is quite high, it can be used on real-time systems.

While the weakness of this symmetrical key algorithm is:

a) different types of messages with different users, different keys are needed, so that there will be difficulties in the management of the key.
b) The problem in sending the key itself is called "key distribution problem".

Asymmetric cryptography[18], [19] algorithm is using a different key for the encryption and decryption process or called public key algorithm because the key for encryption is made public or can be known by everyone, but the key for decryption is only known by the authorized person to know the data encoded or often called the private key.

One Time Pad

One Time Pad[5], [8], [20] is one example of a cryptographic method with a symmetry type algorithm where the key to the encryption process is the same as the key used for the decryption process. It was discovered in 1917 by Major Joseph Mouborgne and Gilbert Vernam in World War II. this algorithm has been claimed to be the only perfect cryptographic algorithm that cannot be solved. An algorithm is said to be safe, there is no way to find the plaintext and until now only the One Time Pad (OTP) algorithm has been declared unbreakable even though unlimited resources are given. The process of encryption and decryption on One Time Pad is almost the same as the process of encryption and decryption using the vigenere cipher algorithm. The encryption process can be done with mathematical equations as follows:

Ci = (Pi + Ki) Mod 26

While for the decryption process can be seen in the mathematical equation as follows:

Pi = ((Ci - Kr) + 26) Mod 26

From the above equation it can be seen:

Ci = character shift in ciphertext
Pi = character shift to text
Kr = Key in decimal form generated from the conversion table.

The part that distinguishes between one time pad and vigenere cipher is in key function. If the key usage in vigenere cipher can be repeated to adjust the length of the plaintext, then at one time pad this cannot be done because the number of keys used must be the same as the length of the plaintext.

RESULT AND DISCUSSIONS

Email usage has become a separate need and many email service providers make it easy for users to choose e-mails that are used, e-mail is usually used to communicate with one or more recipients of e-mail and one of the weaknesses that the e-mail function uses is encryption and decryption. e-mail so that anyone who has access to the mail server can read the e-mail, to overcome this problem an application can be made that can send encrypted e-mail by applying the One Time Pad algorithm as a process of encrypting and decrypting e-mail messages.

The following is a use case diagram modeling of a system prototype made.

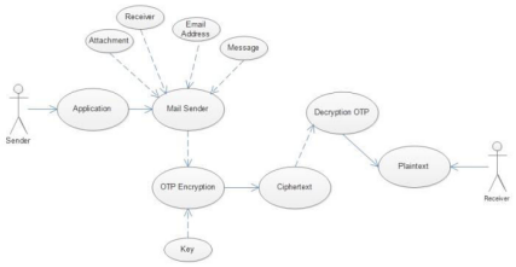

Figure-2. Use Case Diagram System.

Figure-2 is a use case diagram of the system that the author made, while the explanation is as follows:

a) The user runs the application

b) In the application, users can send email with some information such as messages, email addresses, recipient names and file attachments
c) The process of sending an email can be encrypted by using the OTP algorithm with a key whose length is the same as the message length, the key will be generated randomly so that it can adjust automatically with the message length.
d) Results of encryption produce a ciphertext that will be sent via email.
e) Ciphertext results can be decrypted by using a key that matches the encryption key to produce a plaintext.

In addition to use case diagrams there are also activity diagrams and from the system created, here is the diagram

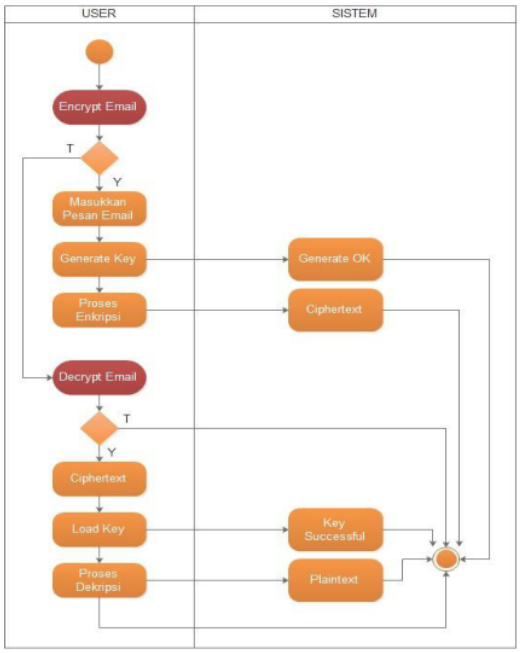

Figure-3. Activity Diagram System.

Use case diagrams and activity diagrams are working models of systems designed, here is the design of an e-mail sending application encrypted with the One Time Pad algorithm.

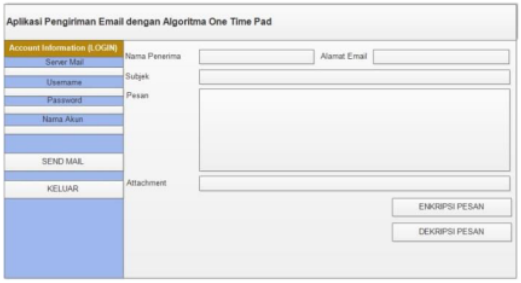

Figure-4. Interface System.

The main application that the author designs for sending email using the one time pad algorithm looks like in Figure-5 until 8 below.

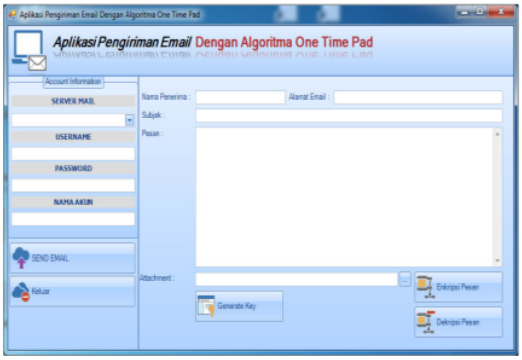

Figure-5. Main System.

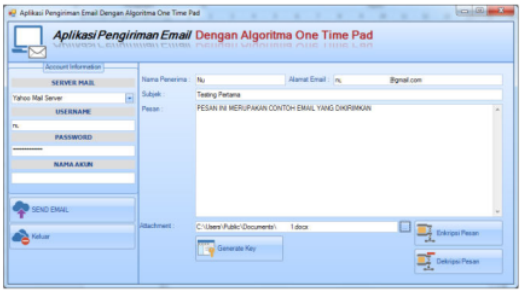

Figure-6. Sample Message.

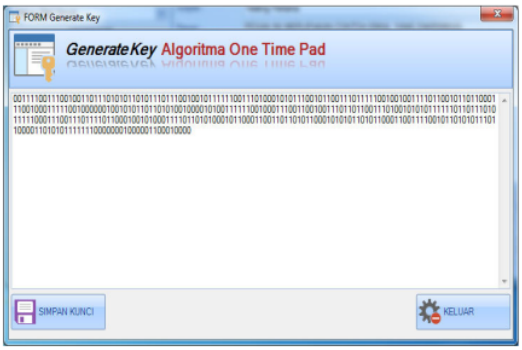

Figure-7. Key Generation.

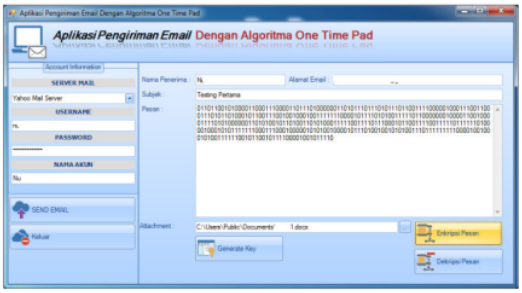

Figure-8. Encryption Message.

Based on the tests carried out in Figures 5 to 8, it is found that the message sent will be encrypted first with a randomly generated key so that it does not have the same pattern, the generated ciphertext will not be easily read easily and takes relatively little time longer to decrypt without knowing the key used.

CONCLUSIONS

The security of e-mail messages using the One Time Pad algorithm can be done well, one of the factors is the use of one time pad keys that are generated randomly so that the key pattern can be read, then to decrypt the cipher-text must use the same application so that the decryption process can be done well.

REFERENCES

[1] C. P. J. Koymans and J. Scheerder. 2008. Email. in Handbook of Network and System Administration.

[2] T. Heyd. 2008. Email hoaxes: Form, function, genre ecology. Email hoaxes: Form, function, genre ecology.

[3] C. Meyer and J. Schwenk. 2013. Lessons Learned From Previous SSL/TLS Attacks-A Brief Chronology Of Attacks And Weaknesses. IACR Cryptol. ePrint Arch.

[4] K. Pandove. 2010. Email Security. Int. J. Comput. Appl. (0975).

[5] F. Rubin. 1996. One-time pad cryptography. Cryptologia. 20(4): 359-364.

[6] R. Rahim, N. Kurniasih, M. Mustamam, L. Andriany, U. Nasution, and A. H. Mu. 2018. Combination Vigenere Cipher and One Time Pad for Data Security. Int. J. Eng. Technol. 7(2.3): 92-94.

[7] M. Iqbal, M. A. S. Pane and A. P. U. Siahaan. 2016. SMS Encryption Using One-Time Pad Cipher. IOSR J. Comput. Eng. 18(6): 54-58.

[8] D. Rijmenants. 2009. Is One-time Pad History?. Cipher Mach. Cryptol.

[9] R. Marty and B. Rexroad. 2017. Network security. in Building the Network of the Future: Getting Smarter, Faster, and More Flexible with a Software Centric Approach.

[10] R. A. Mollin. 2007. An introduction to cryptography. Chapman & Hall/CRC.

[11] S. Bruce. 1996. Applied cryptography.

[12] R. Rahim. 2017. 128 Bit Hash of Variable Length in Short Message Service Security. Int. J. Secur. Its Appl. 11(1): 45-58.

[13] R. Rahim *et al*. 2019. HASHING VARIABLE LENGTH APPLICATION FOR MESSAGE SECURITY COMMUNICATION. ARPN J. Eng. Appl. Sci. 14(1): 259-264.

[14] R. Rahim. 2017. Man-in-the-middle-attack prevention using interlock protocol method. ARPN J. Eng. Appl. Sci. 12(22): 6483-6487.

[15] A. Putera, U. Siahaan and R. Rahim. 2016. Dynamic Key Matrix of Hill Cipher Using Genetic Algorithm. Int. J. Secur. Its Appl. 10(8): 173-180.

[16] H. R. Ismaeel. 2010. Apply Block Ciphers Using Tiny Encryption Algorithm (TEA). Baghdad Sci. J. 7(2).

[17] M. Ebrahim, S. Khan, and U. Bin Khalid. 2014. Symmetric Algorithm Survey: A Comparative Analysis. 61(20): 12-19.

[18] S. Halevi and H. Krawczyk. 1998. Public-key cryptography and password protocols. in Proceedings

of the 5th ACM conference on Computer and communications security - CCS '98.

[19] H. Delfs and H. Knebl. 2-15. Symmetric-key cryptography. in Information Security and Cryptography.

[20] R. Rahim, R. Ratnadewi, D. Prayama, E. Asri and D. Satria. 2018. Base64, End of File and One Time Pad for Improvement Steganography Security. IOP Conf. Ser. Mater. Sci. Eng. 407: 012161.

SECURITY E-MAIL MESSAGE USING ONE TIME PAD ALGORITHM FOR ENCRYPTION MESSAGE

ORIGINALITY REPORT

22%	17%	16%	12%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	garuda.kemdikbud.go.id Internet Source	2%
2	1library.net Internet Source	1%
3	tel.archives-ouvertes.fr Internet Source	1%
4	Ida Bagus Ary Indra Iswara, I Ketut Sudarsana, Nurlaidy Joice Simamora, Vivi Novalia Sitinjak et al. "Application of Data Encryption Standard and Lempel-Ziv-Welch Algorithm for File Security", International Journal of Engineering & Technology, 2018 Publication	1%
5	www.matec-conferences.org Internet Source	1%
6	D Apdilah, M K Harahap, N Khairina, A M Husein, M Harahap. "A Comparison of One Time Pad Random Key Generation using Linear Congruential Generator and Quadratic	1%

Congruential Generator", Journal of Physics: Conference Series, 2018
Publication

7	Submitted to Victorian Institute of Technology Student Paper	1 %
8	jurnal.unimed.ac.id Internet Source	1 %
9	Submitted to Kingston University Student Paper	1 %
10	research.aalto.fi Internet Source	1 %
11	Submitted to Melbourne Institute of Technology Student Paper	1 %
12	ijsrst.com Internet Source	1 %
13	www.researchgate.net Internet Source	1 %
14	eudl.eu Internet Source	1 %
15	www.ijeat.org Internet Source	1 %
16	Umesh Kumar, Rohit Kumar Pathak, Arun Kumar. "Handling Secure Healthcare Data Streaming using R2E Algorithm", 2020	1 %

	International Conference on Electronics and Sustainable Communication Systems (ICESC), 2020 Publication	
17	www.scribd.com Internet Source	1 %
18	Fursan Thabit, Ozgu Can, Asia Othman Aljahdali, Ghaleb H. Al-Gaphari, Hoda A. Alkhzaimi. "A Comprehensive Literature Survey of Cryptography Algorithms for Improving the IoT Security", Internet of Things, 2023 Publication	1 %
19	es.scribd.com Internet Source	1 %
20	Submitted to uva Student Paper	1 %
21	Submitted to Universitas Wijaya Kusuma Surabaya Student Paper	1 %
22	Submitted to University of Kufa Student Paper	1 %
23	www.sciencepubco.com Internet Source	1 %

Exclude quotes	Off	Exclude matches	< 1%
Exclude bibliography	Off		