International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

Vol. 42 No. 1 December 2023, pp. 173-183

Study and Analysis of End-to-End Encryption Message Security Using Diffie-Hellman Key Exchange Encryption

Abdillah Imam Julianto[1], H.A Danang Rimbawa[2], Yudistira Dwi Wardhana Asnar[3]

[1]Program Studi Rekayasa Pertahanan Siber,
Universitas Pertahanan, Bogor, Indonesia ,
Email : abdillahimamjulianto@gmail.com

[2]Program Studi Rekayasa Pertahanan Siber,
Universitas Pertahanan, Bogor, Indonesia ,
Email : hadr71@gmail.com

[3]Program Studi, Teknik Informatika,
Institut Teknologi Bandung, Bandung, Indonesia
Email : yudis_asnar@yahoo.com

Abstract – The development of the field of communication has progressed rapidly. One example is a message exchange application like Whatsapp. The advancement of technology and innovation in the field of communication has allowed us to connect with people around the world in an easier and faster way. However, with advances in communication technology, new challenges arise related to information security and privacy of messages that have been sent. One solution to overcome this problem is to apply Cryptographic Techniques. In cryptography, data sent over the network will be disguised in such a way with encryption techniques so that even if the data can be read, it cannot be understood by unauthorized parties. The data to be sent without being encoded is known as plaintext, and after being disguised in an encoding way, this plaintext will turn into ciphertext. The method chosen for this journal is the Diffie-Hellman Key Exchange. In this journal, an analysis will be carried out regarding the end-to-end process of securing encrypted messages using the Python programming language.

Keywords – Diffie-Hellman, Encryption, End-to-End Encryption Message Security, Instant Messaging.

I. INTRODUCTION

The development of the field of communication has progressed rapidly. One example is a message exchange application like Whatsapp. Advances in technology and innovation in the field of communication have enabled us to connect with people around the world in an easier and faster way.

However, along with the rapid development of this communication technology, new challenges arise related to information security and privacy of messages that have been sent. in several cases that have happened at this time, especially wiretapping related to sent text messages, it is one of the warnings that we care about the security of data transmission. Generally, a lot of information available on the internet today is confidential and can only be accessed by certain parties.

Knowledge of cryptography is an alternative solution to address problems related to information security. The purpose of cryptography is to maintain message security when sending it to another party. That makes a message-sending application mandatory to ensure the security of the process of exchanging data from information. One application that applies the concept of end-to-end cryptographic security is the WhatsApp application. This feature allows only the sender and recipient to access the

Corresponding Author: Abdillah Imam Julianto

information exchanged on the application. The importance of a message is optimally encrypted on message delivery. The author conducted an experiment to apply

II. STUDY LITERATURE

2.1 Related Work

According to a study from Statista. 2016, mentioned that in defining a private situation, it is necessary to define who has access to what under which circumstances. The privacy of private chatting on Facebook represents a good example of the complexity of the restrictions that must be placed on a privacy situation. As of the third quarter of 2016, Facebook had 1.79 billion monthly active users. Chatting is one of the most favorite features of Facebook because, in a chat room, user can share their private content information. With this massive amount of users, the demand for Facebook user data will increase linearly with the value of the information itself. For many reasons and purposes, worldwide governments requested Facebook users' data up to 60,000 times in the first half of 2016. By giving private users' information to another without permission, Facebook, Inc. as a social media platform provider will be a serious threat to Facebook user privacy.

Encryption is the scrambling of plaintext messages, turning them into unreadable code that can only be deciphered by those who have the secret key. End-to-End Encryption (E2EE) is one of the most commonly used technologies to secure and send information across the internet. Hardware embedded into phones and computers allows for the random locks and keys that make E2EE only work on the devices involved in the conversation. According to [4], it is estimated that there were about 276 million internet users in the United States in 2014, and that number is predicted to rise. With this many users, the incentive for hackers to execute attacks and steal personal information increases.

According to a Javelin Strategy and Research Report in 2012, one in every four people who have a breach in their online data becomes a victim of identity theft as a result of that [5]. End-to-End Encryption provides an effective way to prevent these attacks, and if it had been implemented properly by Yahoo Inc., it could have prevented large-scale attacks like the one Yahoo suffered in 2016 and 2013, where almost 500 million, and more than 1 billion accounts were respectively compromised.

Governments and secret services on the other hand are asking encrypted messaging services like WhatsApp to allow them access to their users' data. There is a growing risk to public safety as organized crime, terrorists, and child pornographers are drawn to the use of E2EE apps like WhatsApp that are technically impossible to access. According to, a defendant in a serious felony case told another individual on a recorded jailhouse call that "end-to-end encryption is another gift from God". Criminal defendants across the United States are benefiting from E2EE while the safety of all other American communities is in peril. However, providing a backdoor would not only be a breach of privacy to WhatsApp users but creating a way for the authorities to read encrypted messages would also make the system vulnerable to cyber-attacks from criminals and other hackers.

In 2014 May, H.C. Chen et al. exhibited another idea about Mobile Text Chat utilizing a revolution session key-based transposition cryptosystem plan. Their proposed conspire just manages the safe content transposition for the mobile chat framework. It acclimatized the technologies of classical block cipher, substitution, and transposition. Also, the new session key can be created by the network pivot innovation. It could be easily applied to transmit via mobile devices using the quick encryption algorithm.

An ongoing study on the use of encryption and decentralized communication tools is being conducted via the H2020 CAPS (Collective Awareness Project) project NEXt-generation Techno-social Legal Encryption Access and Privacy (NEXTLEAP).1 NEXTLEAP seeks to address, in an interdisciplinary manner, the recent erosion of public trust in the Internet as a secure means of communication that has been prompted by the Snowden revelations. The core objective of NEXTLEAP is to improve, create, validate, and deploy communication protocols that can serve as pillars for a secure, trustworthy and privacy-respecting Internet able to ensure citizens‟ fundamental rights. For this purpose, NEXTLEAP seeks to develop an interdisciplinary internet science of decentralization as the basis on which these protocols can not only be built but become fully (and meaningfully) embedded in society. In this regard, the social aspect of end-to-end encryption must be included in the overall analysis of trust and decentralization at the heart of Internet Science.

The purpose of the Diffie-Hellman protocol is to enable two parties to securely exchange a session key which can then be used for the next symmetric encryption of messages. The idea of the Diffie-Hellman protocol is to calculate a session key by the communicating entities based on public parameters that are shared in the initial phase. This type of protocol is called key

agreement protocol. Diffie-Hellman's effectiveness comes from the difficulty of calculating discrete logarithms. However, the protocol can only be used for exchanging secret data without authenticating two parties. This is the reason why Diffie-Hellman is insecure against man-in-the-middle attacks. The solution for this vulnerability is to use a digital signature. Variants of Diffie-Hellman protocols are proposed since its introduction to overcome different issues and vulnerabilities including the aforementioned one. We can consider the key exchange or establishment protocols from two perspectives: cost/efficiency and security. Cost includes both processing and communication costs. To get low processing costs, researchers should avoid employing public key encryption schemes such as RSA, ECC, and ElGamal

According to research from A. Abusukhon, and B. Hawashin (2015) say that There are several techniques based on asymmetric encryption like RSA cryptosystem, the scheme of Diffie-Hellman key exchange (DH), the scheme of Elliptic Curve Cryptography (ECC), the specific Elliptic Curve Diffie-Hellman (ECDH), and ElGamal cryptosystem. In, the authors presented a hybrid encryption technique.

In 2002, the work of A.joux showed the use of Weil couplings on elliptical curves to make a three-party key exchange. If the Diffie-Hellman mechanism is used, it requires the establishment of a secure channel between each pair. the authors presented a generalization of in order to guarantee the exchange of keys between an arbitrary number of entities using a cryptographic multilinear application.

From the previous research above, the authors had the idea to conduct research related to the use of the Diffie-Hellman method to encrypt text communications with the concept of end-to-end security.

2.2 Data and Information Security

Information security is divided into 3 aspects, namely confidentiality, integrity, and availability. The following is an explanation of the 3 aspects of information security:

a. Confidentiality

Restrictions related to access and disclosure of information, including means to protect privacy. The loss of confidentiality is a gap for information to be opened without permission

b. Integrity

Apart from confidentiality, the second principle is integrity. This principle relates to changing information or data from a system. In the principle of integrity, your computer system is said to be safe if information or data can only be changed by authorized parties.

c. Availability

The next principle is availability or availability. This principle refers to the availability of the right data and information when needed. In the principle of availability, your system can be said to be safe if any information or data in the computer system is available and can be accessed by people who are given access rights.

2.3 Cryptography

Displayed equations Cryptography is the science and art of maintaining the secrecy of messages by encoding them in a form that the meaning can no longer be understood. In cryptography, there are two processes, namely encryption and decryption. The message to be encrypted is referred to as plaintext (plain text). So-called because this information can easily be read and understood by anyone. The algorithms used to encrypt and decrypt plain text involve the use of some form of key. Plaintext messages that have been encrypted (or encoded) are known as ciphertext (ciphertext). Cryptography can be a solution in securing data using a key, in which case the algorithm is not kept secret, but the key must be kept confidential. The key (key) is a parameter used for encryption and decryption transformation. Keys can usually be strings or strings of numbers. By using the kK key, the encryption, and decryption functions can be written as a schema.

2.4 Diffie-Hellman Algorithm

The Diffie-Hellman algorithm is an encryption method that has the unique characteristic of exchanging secret keys when communicating. Diffie and Hellman is referred to as public key cryptography and is commonly called the Diffie Hellman key

exchange or the Diffie Hellman protocol. According to Hendarsyah & Wardoyo, the purpose of this algorithm is to allow 2 application users to exchange keys safely and can be used to encrypt and decrypt messages. The following is the encryption process using the Diffie-Hellman key:

a. Suppose Alice and Bob are parties who will communicate with each other. At first Alice and Bob will agree on 2 large numbers (preferably using prime numbers) P and Q, so that P < Q. The values of P and Q do not need to be kept secret. Even Alice and Bob can talk over insecure channels though

b. Alice generates a large random integer x and sends the following computation results to bob

c. Bob generates a large random integer y and sends the following results to Alice :

d. Alice calculates K = Y mod Q

e. Bob Calculates K = X mod Q

If the calculation is done correctly then K = K. Thus Alice and Bob already have the same key without the other party knowing.

2.5 Asymmetric Encryption

Asymmetric encryption, also known as public-key cryptography, is a type of encryption that uses a pair of keys to encrypt and decrypt data. The pair of keys includes a public key, which can be shared with anyone, and a private key, which is kept secret by the owner. In asymmetric encryption, the sender uses the recipient's public key to encrypt the data. The recipient then uses their private key to decrypt the data. This approach allows for secure communication between two parties without the need for both parties to have the same secret key. Asymmetric encryption has several advantages over symmetric encryption, which uses the same key for both encryption and decryption. One of the main advantages is that it eliminates the need to exchange secret keys, which can be a challenging process, especially when communicating with multiple parties. Additionally, asymmetric encryption allows for the creation of digital signatures, which can be used to verify the authenticity of data. Asymmetric encryption is commonly used in various applications, including secure online communication, digital signatures, and secure data transfer. Examples of asymmetric encryption algorithms include RSA, Diffie-Hellman, and Elliptic Curve Cryptography (ECC). Asymmetric encryption, commonly known as public-key cryptography, employs two distinct keys for encryption and decoding. The private key is a separate key from the public key that is kept private by the owner of the public key while the public key is made available to everyone. Anyone can encrypt a message using the public key, but only the holder of the private key can unlock it. With no chance of the communication being intercepted and read by a third party, anyone can send a secure message to the public key's owner. Asymmetric encryption is frequently used for secure internet communication, including email encryption, e-commerce, and online banking. Digital signatures, which are used to confirm the legitimacy of digital documents and messages, are another application for it.

The two participants in the asymmetric encryption workflow are the sender and the receiver. Each has its own pair of public and private keys. First, the sender obtains the receiver's public key. Next, the plaintext message is encrypted by the sender using the receiver's public key. This creates ciphertext. The ciphertext is sent to the receiver, who decrypts it with their private key, returning it to legible plaintext. Because of the one-way nature of the encryption function, one sender is unable to read the messages of another sender, even though each has the public key of the receiver.

2.6 Symetric Encryption

Symmetric encryption is a type of encryption where only one key (a secret key) is used to both encrypt and decrypt electronic data. The entities communicating via symmetric encryption must exchange the key so that it can be used in the decryption process. This encryption method differs from asymmetric encryption where a pair of keys - one public and one private - is used to encrypt and decrypt messages.

By using symmetric encryption algorithms, data is "scrambled" so that it can't be understood by anyone who does not possess the secret key to decrypt it. Once the intended recipient who possesses the key has the message, the algorithm reverses its action so that the message is returned to its original readable form. The secret key that the sender and recipient both use could be a specific password/code or it can be a random string of letters or numbers that have been generated by a secure random number

generator (RNG). For banking-grade encryption, the symmetric keys must be created using an RNG that is certified according to industry standards, such as FIPS 140-2.

Symmetric encryption work that is encrypted and decrypted using a single key. That key, password, or passphrase is shared among the parties involved, and they can use it to decrypt or encrypt whatever messages they wish. It belongs to the public key infrastructure (PKI) ecosystem because it turns plain text, or readable data, into unreadable ciphertext, allowing secure communications to be sent over an insecure internet.

Some of the most common symmetric cryptography algorithms are the Data Encryption Standard (DES), which uses 56-bit keys; Triple DES, which repeats the DES algorithm three times with different keys; and the Advanced Encryption Standard (AES), which the US National Institute of Standards and Technology recommends for securely storing and transferring data.

Advantages of Symmetric Encryption :

- Exceptionally safe

Symmetric key encryption can be highly secure when it employs a secure algorithm. As recognized by the US government, the Advanced Encryption Standard is one of the most extensively used symmetric key encryption schemes. Using ten petaflop machines, brute-force guessing the key using its most secure 256-bit key length would take about a billion years. Because the world's fastest computer, as of November 2012, runs at 17 petaflops, 256-bit AES is virtually impenetrable.

- Speed

One of the disadvantages of public-key encryption methods is that they require very complex mathematics to function, making them computationally intensive. It's pretty simple to encrypt and decrypt symmetric key data, resulting in excellent reading and writing performance. Many solid-state drives, which usually are pretty fast, use symmetric key encryption to store data inside, yet they are still quicker than traditional hard drives that are not encrypted.

- Acceptance

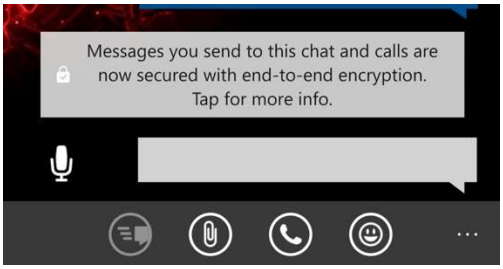
Because of their security and speed benefits, symmetric encryption algorithms like AES have become the gold standard of data encryption. As a result, they have enjoyed decades of industry adoption and acceptance.

- Minimizes message compromises

A distinct secret key is utilized for communication with each party, preventing a widespread message security breach. Only the messages sent and received by a specific pair of sender and recipient are affected if a key is compromised. Other people's communications are still safe.

2.7 End-to-End Encryption

End-to-end encryption is a technique for securing the transmission of information by encrypting content in any form of chat. End-to-end encryption sends information across a network that only the sender and receiver know. One application of end-to-end encryption is found in the WhatsApp application. Information on end-to-end message implementation will appear automatically and can be seen in Figure 2.



The general flow regarding end-to-end encryption can be seen in Figure 3.

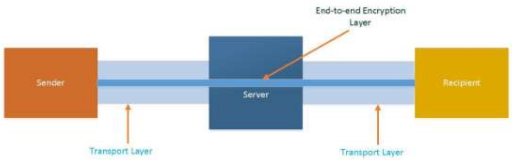


Figure 3. End-to-End Encryption Flow

Figure 3 explains that the encryption feature uses an end-to-end technique that has its own communication line. However, this line of communication is term only. This is because the end-to-end communication path is a wrapper for data security in communication between users. In this study, the authors conducted an experiment to apply the End-to-end Encryption concept to a simple messaging application using Python.

III. RESEARCH METHOD

A. End-to-End Encryption Using Diffie-Hellman

Digital encryption utilizing the Diffie-Hellman key exchange, commonly referred to as an exponential key exchange, makes cracking codes statistically unfeasible by using numbers raised to specific powers to construct decryption keys.

For example Let's assume as a prerequisite that both parties, let's say Alice and Bob, have securely imported each other's public keys. At key signing events, this can be done in person. The protocol is also fairly easy to understand and follow. This protocol's foundation is PGP, and as a result, the sender will encrypt and sign all data packets sent over the network to the recipient. Handshake and ciphertext data will be transferred above that layer. An ephemeral session key will be exchanged as part of a Diffie-Hellman key exchange before Alice or Bob can communicate with each other. The succeeding communications will utilize symmetric encryption with this key algorithms for encryption. Timestamps and sequence numbers that are randomly initialized are appended to handshake packets and message packets to thwart replay attacks.

B. Design System

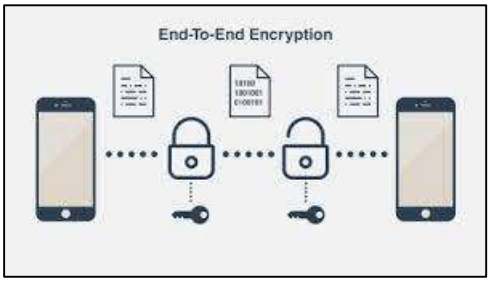


Figure 4. Design System

The following is the system design used in this study. shown in figure 4. shown in figure 4. two devices exchanging messages. messages sent from the device a will be encrypted using the diffie-hellman method. later this method will act as a place to exchange encrypted message keys.

C. Implementation

Figure 5 - 7 shows the code for system configuration, server.py to create a chat server to process encryption for each user. And client.py to create client users so they can communicate with each other.

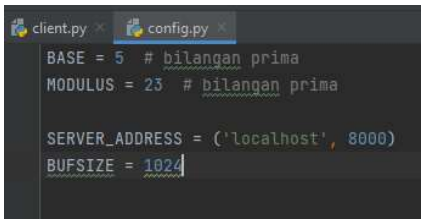


Figure 5. Config Code

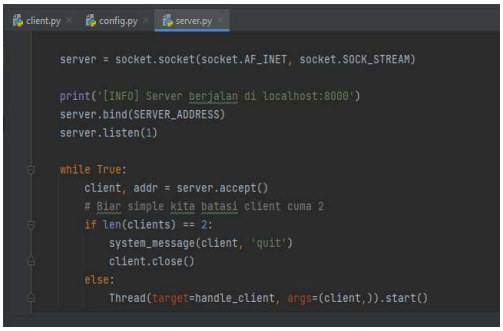


Figure 6. Server.py Code

Figure 7. Client.py code

Following are the implementation results of the system, to run the system run the chat server first

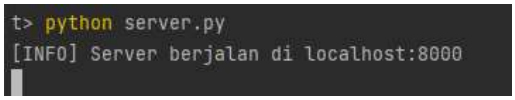


Figure 8. Running the Chat Server

Next, Create User1. To create user1 you can run code in figure 9.

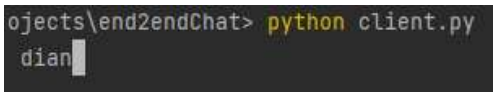


Figure 9. Creating a User Client 1

The public key has been automatically generated and is waiting for client 2 to connect to the system.

Figure 10. Waiting for Chat opponents

To create a new client so we can communicate with each other, type python client.py client 2 named Diane. If information appears as shown in Figure 10. then the process of sending messages to each other with end-to-end encryption is ready to run.

Figure 11. Successful End-to-End Chat System

Figure 12 presents the overall results of the program that has been implemented

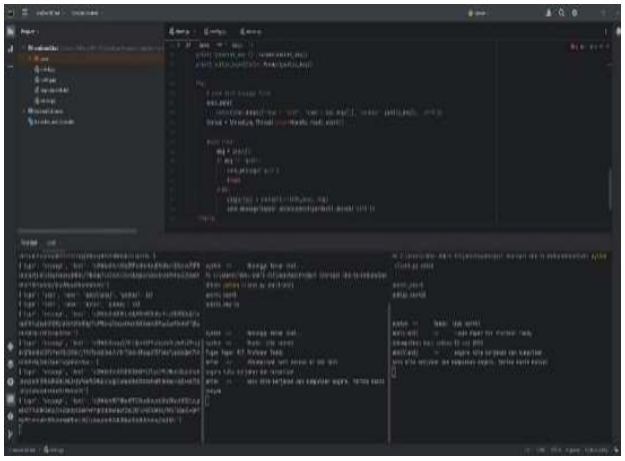


Figure 12. Some Implementation Code Snippets

IV. ANALYSIS AND RESULT

The results of the implementation using end-to-end encryption have been carried out and then tested and seen based on the output issued. Figure 13 shows the message Diane sent to Diana . Figure 14 shows the results of end-to-end encryption using Diffie-Hellman. And the results of the decryption are shown in Figure 15.

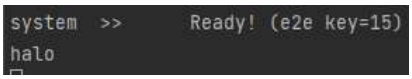


Figure 13. Send a message to Diana

Figure 14. Encryption Results

Figure 15. The result of the decryption of the message sent by Diane

V. CONCLUSION

In conclusion, the successful implementation of the End-to-End Encryption Message Security Using Diffie-Hellman Key Exchange Encryption highlights the following findings:

- The Python implementation of the End-to-End Security Concept serves as a successful proof of concept for Diffie-Hellman Key Exchange Encryption.
- The Diffie-Hellman Encryption Method effectively exemplifies the robustness of the End-to-End concept in secure communication.
- The emphasis on key value exchange and the consistent mathematical process in the Diffie-Hellman algorithm further strengthens its reliability in secure data transmission.

Future work can focus on Performance Optimization, exploring techniques to enhance the computational efficiency of the Diffie-Hellman algorithm, such as algorithmic optimizations and hardware acceleration.

REFERENCE

[1]. Fitrianti, U., & Ula, M. (2017). Implementasi algoritma levenshtein distance dan algoritma knuth morris pratt pada aplikasi asmaul husna berbasis android. Jurnal Sistem Informasi, 1(2).

[2]. Jamaluddin, Jamaluddin, Roni Jhonson Simamora, and Karyawati Sitepu. "Konsep Pengamanan Pesan dengan Teknik Enkripsi End to End pada WhatsApp Messenger." (2016).

[3]. Santria, Ummi, and Nira Arsoetar. "Penggunaan Enkripsi End-to-End dalam Pengamanan Pesan dan Video Call pada Whatsapp."

[4]. Zvika Brakerski and Vinod Vaikuntanathan, "Efficient fully homomorphic encryption from (standard) \$LWE\$", *SIAM Journal on Computing*, vol. 43, no. 2, pp. 831-871, 2014.

[5]. H. O. Alanazi, B. B. Zaidan, A. A. Zaidan, H. A. Jalab, M. Shabbir and Y. Al-Nabhani, "New Comparative Study Between DES, 3DES and AES within Nine Factors," JOURNAL OF COMPUTING, vol. 2, no. 3, pp. 152-157, 2010.

[6]. R. Anup and R. Suchithra, "Image Encryption using Triple DES Algorithm," Imperial Journal of Interdisciplinary Research (IJIR), pp. 969-974, 2017.

[7]. P. Jindal and B. Singh, "Study and Performance Evaluation of Security-Throughput Tradeoff With Link Adaptive Encryption Scheme," Department of Electronics and Communication Engineering, pp. 1-14, 2012.

[8]. S. Potteti and N. Parati, "Secured Data Transfer For Cloud Using Blowfish," International Journal of Advances In Computer Science and Cloud Computing, vol. 3, no. 2, pp. 17-22, 2015.

[9]. S. Gurjeevan and K. S. Ashwani, "Throughput Analysis of Various Encryption Algorithms," International Journal of Computer Science and Technology, vol. 2, no. 3, September 2011.

[10]. S. A. E. Diaa and M. A. K. Hatem, "Evaluating the Performance of Symmetric Encryption Algorithms," International Journal of Network Security, vol. 10, no. 3, pp. 216-222, May 2010.

[11]. K. Aman, J. Sudesh and M. Sunil, "Comparative Analysis between DES and RSA Algorithm's," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 2, no. 7, pp. 386-391, July 2012.

[12]. K. Ermoshina, F. Musiani and H. Halpin, "End-to-End Encrypted Messaging Protocols: An Overview," INSCI 2016, LNCS 9934, p. 244–254, 2016.

[13]. M. Nabeel and Q. Doha, "The Many Faces of End-to-End Encryption and Their Security Analysis," in 2017 IEEE 1st International Conference on Edge Computing, 2017.

[14]. M. A. Hameed, N. Asanka and G. Arachchilage, "Understanding the influence of Individual's Self-efficacy for Information Systems Security Innovation Adoption: A Systematic Literature Review," pp. 1-19, 2018.

[15]. W. Bai, M. Pearson, P. G. Kelley and M. L. Mazurek, "Improving Non-Experts' Understanding of End-to-End Encryption: An Exploratory Study," University of Maryland, pp. 1-15, 2020.

[16]. P. Tarigan, H. Sunandar, B. Sinuraya, Z. A. Matondang and G. Ginting, "Implementation Of Triangle Chain Cipher Algorithm in Security Message of Social Media," Journal of Physics, pp. 1-10, 2020.

[17]. J. B. Awotunde, A. O. Ameen, I. D. Oladipo, A. R. Tomori and M. Abdulraheem, "Evaluation of Four Encryption Algorithms for Viability, Reliability and Performance Estimation," NIGERIAN JOURNAL OF TECHNOLOGICAL DEVELOPMENT, vol. 13, no. 2, pp. 74-82, 2016.

[18]. Ermoshina, K., Musiani, F., Halpin, H. (2016) End-to-end encrypted messaging protocols: An overview. In: International Conference on Internet Science. Springer, Cham. pp. 244-254.

[19]. Garfinkel, S. (1994) PGP: Pretty Good Privacy. O'Reilly Media, California.

[20]. Diffie, W., Hellman, M. (1976) New directions in cryptography. IEEE Transactions on Information Theory, 22(6): 644-654.

[21]. Günther, C.G. (1989) An identity-based key-exchange protocol. In: Workshop on the Theory and Application of Cryptographic Techniques. Springer, Berlin, Heidelberg. pp. 29-37.

[22]. Sun, H.M., Hsieh, B.T., Hwang, H.J. (2005) Secure e-mail protocols providing perfect forward secrecy. IEEE Communications Letters, 9(1): 58-60.

[23]. Borisov, N., Goldberg, I., Brewer, E. (2004) Off-the-record communication, or, why not to use PGP. In: ACM workshop on Privacy in the electronic society. Washington. pp. 77- 84. [7] Suprihanto, D., Priyambodo, T.K. (2017) The Implementation of Pretty Good Privacy in eGovernment Applications (Case Study on the Official Scripts Electronic Applications in Bantul). International Journal of Information Engineering and Electronic Business, 9(4): 1-6.

[24]. Elkins, M. (1996) MIME security with pretty good privacy (PGP). RFC 2015.

[25]. Tripathi, S., Biswas, G.P. (2010) Secure E-Mail Messaging to Selected Group Members Using PGP Technique. International Journal of Computer Applications, 975, 8887: 76- 80.

[26]. Kurniawan, Y., Albone, A., Rahyuwibowo, H. (2011) The design of mini PGP security. In: Proceedings of the 2011 International Conference on Electrical Engineering and Informatics. Bandung. pp. 1-4.

[27]. Espinoza, A.M., Tolley, W.J., Crandall, J.R., Crete-Nishihata, M., Hilts, A. (2017) Alice and bob, who the FOCI are they?: Analysis of end-to-end encryption in the LINE messaging application. In: 7th USENIX Workshop on Free and Open Communications on the Internet. Vancouver. pp. 1-9.

[28]. R. W. Zhu, X. Tian and D. S. Wong, Enhancing ck-model for key compromise impersonation Resilience and Identity-based Key Exchange, Cryptology ePrint Archive: Report 2005/455, 13 December 2005. [Online]. Available: http://eprint.iacr.org/2005/455. [Accessed 3 11 2014].

[29]. H. Elkamchouchi and M. Eldefrawy, An efficient and confirmed protocol for authenticated key agreement, in Radio Science Conference, 2008. NRSC 2008. National, Tanta, 2008.

[30]. Q. Cheng, G. Han and C. Ma, Analysis of Two Authenticated Key Exchange Protocols, in Multimedia Information Networking and Security, 2009. MINES '09. International Conference on, Hubei, 2009.

[31]. J. Kar "Low Cost Scalar Multiplication Algorithms for Constrained Devices", International Journal of Pure and Applied Mathematics, Vol.102, No.3, pp.579-592, 2015.

[32]. M. R Mishra, J. Kar & B. Majhi, "Practical deployment of One-pass key establishment Protocol on Wireless Sensor Networks", International Journal of Pure and Applied Mathematics, Vol(100), No-4, pp 531-542, 2015

AUTHOR'S BIOGRAPHY

Abdillah Imam Julianto

Abdillah Imam Julianto works daily in the IT Department of the Indonesian Navy Headquarters with activities to carry out data center security management and also monitor data traffic and security traffic in the Indonesian Navy.

Teddy Mantoro

Teddy Mantoro is currently a professor at Sampoerna University, Jakarta, Indonesia. He obtained a Ph.D., an MSc, and a BSc, all in Computer Science/Computer Engineering, and his Ph.D. was from the School of Computer Science, the Australian National University (ANU), Canberra, Australia. He has secured 20+ research projects, won several international research awards, and filed 4 patents in Computer Science areas. He is a Senior Member of IEEE, Chair of the IEEE-Computational Intelligence Society-Indonesia Chapter, a Professional Member of ACM, and a member of the Asia-Pacific Neural Net Society (APNNS).