Department of Digital Business
Journal of Artificial Intelligence and Digital Business (RIGGS)
Homepage: https://journal.ilmudata.co.id/index.php/RIGGS
Vol. 1 No. 2 (2023) pp: 11-18
P-ISSN: 2963-9298, e-ISSN: 2963-914X

Implementation of Encrypt National ID Card in Sinovi Application Use Waterfall Methodology

Teguh Rijanandi[1], Ayu Silvia[2], Bintang Abillah Safna[3], Rima Dias Ramadhani[4]
[1,3] Software Engineering, Fakultas Informatika, Institut Teknologi Telkom Purwokerto
[2] Sistem Informasi, Fakultas Informatika, Institut Teknologi Telkom Purwokerto
[4] Sains Data, Fakultas Informatika, Institut Teknologi Telkom Purwokerto
[1]19104008@ittelkom-pwt.ac.id*, [2]20103011@ittelkom-pwt.ac.id, [3]21104067@ittelkom-pwt.ac.id, [4]rima@ittelkom-pwt.ac.id

Abstract

In this era of increasingly rapid technology, the development of information systems is also growing rapidly, because information systems provide what users need. Information is a very valuable thing. When information or data falls into irresponsible hands, it will bring disaster to the owner, and there have been many cases of data leaks in the past that have harmed several parties. There are various ways to protect data or information. Therefore, data security techniques are needed, the message security process is very diverse, including using cryptography. Cryptography aims to scramble messages so that they are difficult to read by unauthorized parties. In this study, we will use the AES 256 encryption method with the waterfall research method to secure KTP images on the Sinovi application, Sinovi is a copyright registration application at the Telkom Institute of Technology Purwokerto. The results of this study are the AES method will convert data or information in the form of plain text into cipher-text then stored in a file to replace the image file so that in this way the image cannot be viewed directly because it must pass the decryption technique first and the research data will be presented. in a table of blackbox testing. It is hoped that a security system like this can protect data from unauthorized parties and further research is expected to have research that tests AES 256 with different methods. https://github.com/teguh02/T-Encryption

Keywords: AES 256, Sinovi, KTP, Waterfall Methodology

1. Introduction

Advances in information technology have increased the need for data security regarding the confidentiality of information exchanged over the Internet, especially when the data resides on a computer network connected to another network [1]. This obviously poses a risk when irresponsible people access sensitive or valuable information. If this happens, it is likely to harm not only the sender of the message, but also the organization. Also, hacked data can be corrupted or lost, leading to huge losses [2], [3].

The author wants to implement this security encryption on the Sinovi application, Sinovi is an application for copyright registration and commercial application of Telkom Institute of Technology Purwokerto in the form of a website accessible to teachers and students. This app stores some important data like emails, addresses and IDs.

Not long ago, news about personal data, email addresses, addresses, phone numbers, ID and other cases of private data leakage appeared non-stop. [4]. For example Tokopedia e-commerce hacked by hackers. Tokopedia was reported to have been hacked, in fact the number was estimated at 91 million accounts and 7 million merchant accounts, no longer 15 million as previously reported. Whereas in 2019, Tokopedia revealed that there were around 91 million active accounts on its platform (Suyanto, 2003). This means that almost all accounts on Tokopedia have been successfully retrieved by hackers. The perpetrators sell data on the dark web in the form of user ID, email, full name, date of birth, gender, cellphone number and password that are still encrypted. All are sold at a price of US $5,000 or around Rp.74,000,000.00 (seventy-four million rupiah). There are even 14,999,896 Tokopedia accounts whose data can now be downloaded [5], In addition, previous research revealed that consumers who were harmed due to leaks stored by the online marketplace could file a lawsuit with the Minister of Communication and Information of the Republic of Indonesia to demand accountability for the online marketplace as the Electronic System Operator, this is in accordance with the ITE Law, PP PSTE, and Permenkominfo PDPSE [6].

Therefore, to prevent this from happening, the author uses the AES encryption algorithm while encrypting

Accepted: 14-11-2022 | Received in revised: 20-11-2022 | Published: 01-01-2023

and describing the data. Encryption has become an integral part of cyber security systems and one of the ways to encrypt data is the Advanced Encryption Standard (AES) [7], AES is the first and only cipher approved by the US National Security Agency (NSA) to protect classified information [8]. AES was originally named after its two developers, Belgian cryptographers Vincent Rijman and Joan Daemen Rijndael [9]. This study will use the waterfall research method, Waterfall is an approach to systematic and sequential software development starting from problem analysis, design, implementation, testing and maintenance [10]. The reason we use Waterfall is because it is easy to use, sequential processes from analysis to support, each process does not overlap [11], At the testing stage, the researcher will present data in the form of a table from the blackbox testing process, Black box testing or also known as Behavioral Testing is a test carried out to observe the input and output results of the software without knowing the code structure of the software. This test is carried out at the end of making the software to find out whether the software can function properly [12].

Writer use the PHP programming language. The hypertext preprocessor (PHP) is an interpreted programming language that translates lines of code into programs that a computer can understand at runtime [13], [14]. PHP is a very popular and easy to use server programming language. Many people use PHP to build different types of websites [15], [16]. This study uses an encryption library written in PHP programming language which was introduced earlier, in this library all ciphers are converted into one so that users can use it more easily [17]. The wirter have a plan and idea to secure a national id card, the author wants to change a sensitive image saved into a random text that cannot be opened by the responsible party, after the ID card image is encrypted, the random word will be stored in a file to replace the previous ID card image, so that irresponsible parties will find it difficult to guess someone's ID card [18] and in this research writer will try to use this encryption library to secure national id card are stored in sinovi application.

The hope is that with this research, the data in the Sinovi application will be more secure, and overcome data leaks to irresponsible parties, if data leaks no one can find out except the person who created the data security key. The author also hopes that this research can be a theoretical basis for other research

2. Research Methods

As explained in the previous chapter, this research uses the waterfall research method [10]. The waterfall method involves successive stages of software development, from analysis, design, coding and testing. The research stage is organized so that the research activities carried out are planned, organized and systematic and the research objectives can be achieved. Figure 1 below shows the research phase for implementation [19], the steps of the method can be seen in the image below.

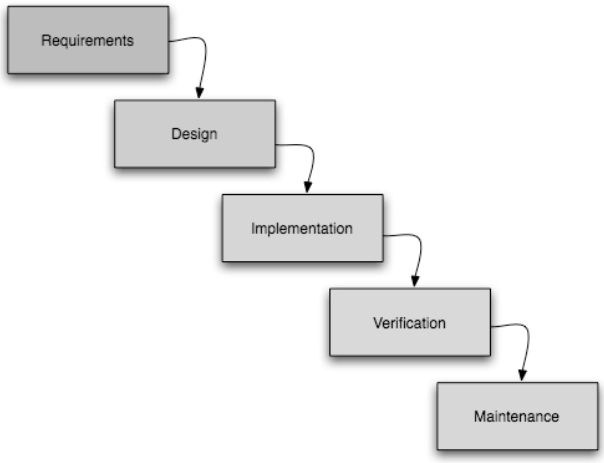

Figure 1 Waterfall Software Development Life Cycle

In figure 1, it is explained that the research will carry out 5 stages, namely:

a. Requirements
   In this steps, writter will collect all requirements for the next step, such as the main problem for the discussion from sinovi application and download several fake national id card from internet for as a sample.
b. Design
   In steps two, writer will design a simple encryption system, and writer will show to you the random strings are must create from the encryption process.
c. Implementation
   In steps three writer will start to code a encryption system use a PHP encryption library, because to make easy the encryption process and we don't to code from zero because we will too many time for that's, and writer will copy several fake national id card images inside a folder (one location from the PHP code) and the code will read all images one by one use loop, and encrypt them as random text.
d. Verification (Testing)
   In steps four, the writer will check again for the encryption results. Is same as a design steps or not. If not, writer will re-check the encryption process one by one, the test was performed using the black box test method. This test will test the functionality of the National ID card encryption system

DOI: https://doi.org/10.31004/riggs.v1i2.15

e. Maintenance
For the last steps, the writer will fix for future error in this encryption process. So anyone can't see the original image from national identity card. And the national identity card are safe.

3. Results and Discussions

a. Requirements
In this stage, the formation of the problem that we are going to solve is explained. In the field of technology, every company must build a security system. Because data is very important, there is very important private data in the Sinovi app, one of which is the service user ID card. Unfortunately, the Sinovi service does not set up strong enough encryption for the ID card, and I am concerned that the data will be leaked and irresponsibly distributed to users.

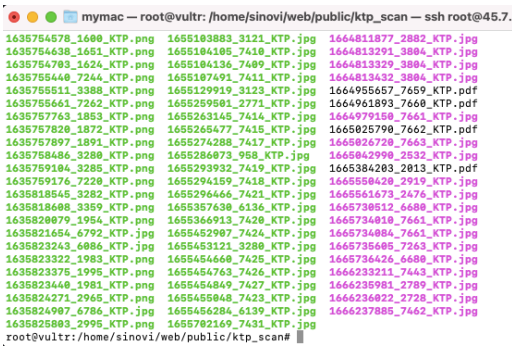

Figure 2 Not encrypted National ID Card in sinovi

In figure 2, the ID card of the user of the Sinovi application is not encrypted, so the data is feared to be seen by irresponsible parties, for example

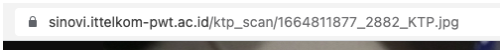

Figure 3 URL to identify National ID Card image

To display a national id card, sinovi will give a URL like in figure 3. The URL is divided into 3 parts, part one is the main domain, part two is a folder and part three is a filename with file extension and the response will be like this

Figure 4 National ID Card sample from sinovi app

Figure 4 is a sample of national id card are stored and not encrypted in the sinovi application, so many national id card are stored in sinovi (see in figure 3) and not encrypted (figure 4 are blurred by author for protect the author national identity card) , and if someone can guess the URL address (in figure 3) they can see another national id card. This method is often referred to as brute force. In cryptography, a brute force attack is a technique used to attack computer security systems by testing all keys [20], [21] . Attackers systematically check all possible passwords and passphrases until they find the correct one [22]. Not only password guessing, if someone tries to guess the sinovi app URL, it can also be considered as brute force [23], [24]. So in this research will use several images as a sample encryption test.

b. Design
In this step, the author will use a simple php command line application to code multiple images as shown in the previous step and the application folder structure will be like this

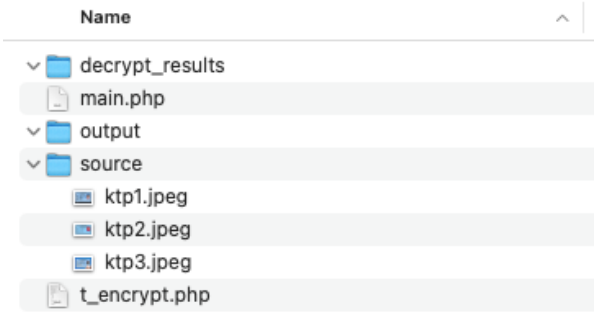

Figure 5 project folder structure

DOI: https://doi.org/10.31004/riggs.v1i2.15

The function of each folder is as follows :

1) Decrypt_results for store all decrypted file results
2) Main.php for the main command line program
3) Output for storing all encrypted files from the original file
4) Source folder is fake of national id card images

And how about for running the application like this in figure 6, the writer will execute main file from the command line, and the application will read all fake national id card images and encrypt them one by one.

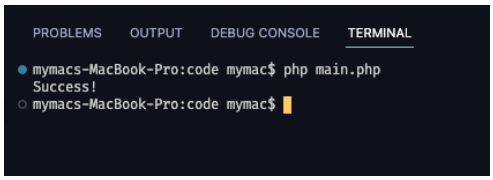

Figure 6 simple command line encryption app

When the program finishes encrypting all images, it will say success and the results must will be a random string, like in figure 7. So when the results in implementation steps later are same at this step, so the experiment was successful, and when not the writer will check again until the result are the same at this step. Because according to the abstract and introduction protecting data is very important.

Figure 7 encrypted file results

c. Implementation

The AES-256 key is 256 bits long and supports the largest bit size. Based on current computing power, it is almost impossible to impose hard restrictions and is the strongest encryption standard [25]. AES 256 need a secret key like a password for encrypt and decrypt the hashed string (figure 8).

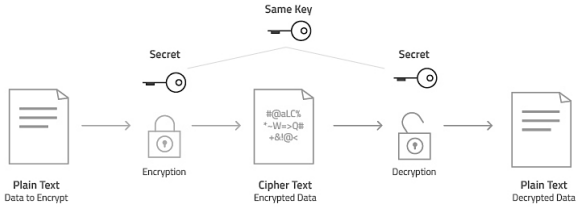

Figure 8 how AES 256 works

At this research the php command line program will works like in figure 9, for loop will scan all files inside of source folders, and the program will convert a original national id card to a random string. So not anyone can open for a hashed national id card.

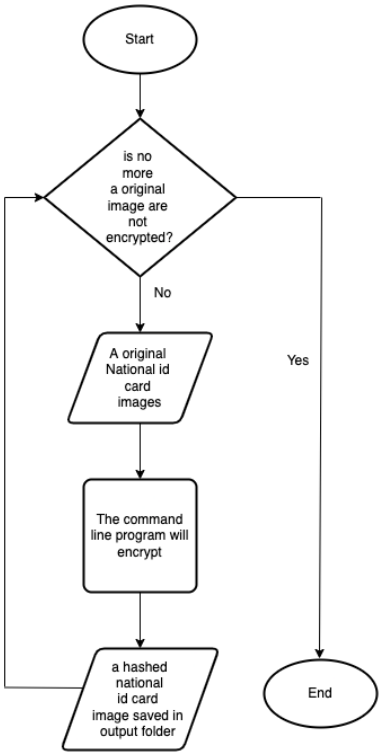

Figure 9 the encryption program flowchart

After all original images are successfully encrypted and the program said success, in the output folder, must be like in figure 10, there are several encrypted national id card images, and if someone opens that file, they will see a random string (figure 11).

DOI: https://doi.org/10.31004/riggs.v1i2.15

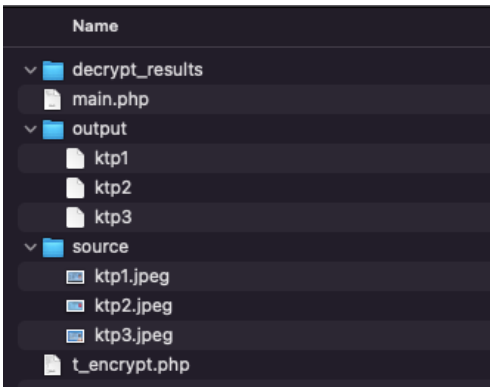

Figure 10 structure folder after the program says success

Figure 11 random string from a hashed national id card

d. Verification (Testing)

In the first test, the writer will edit the master file to decrypt all encrypted national ID cards, and the writer will re-run the master file and the program will convert it back as an image, so anyone can see the original national id card image. Figure 12 is the project's structure folder after the program is successfully executed there are some image files in decrypt_results, all images in the decrypt_results folder must be the same as the source image, see figure 13 for the decryption results.

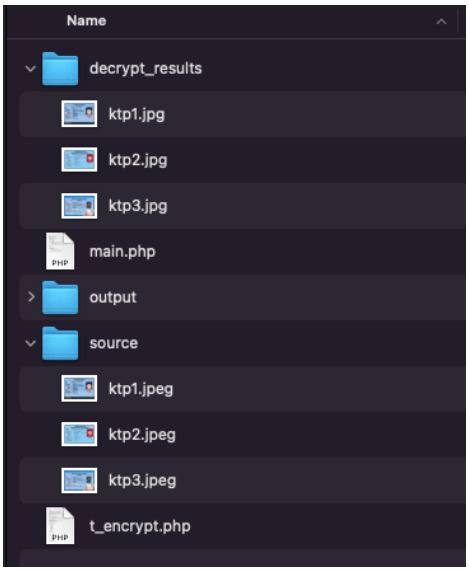

Figure 12 Projects folder after the decryption process

Figure 13 A decrypted images results

In the second step of the test, the author will uploads the encoded results to the sinovi server and brute force them one by one the URL without login into sinovi as an admin user (like in figure 3), to ensure the author can guess another national id card or not, if the author failed to guess another national id card, and finally this research are successful, and when the author tries to guess the URL address of someone else's ID that is stored in the sinovi server, the author sees as in figure 14, only random words that are difficult to guess appear.

DOI: https://doi.org/10.31004/riggs.v1i2.15

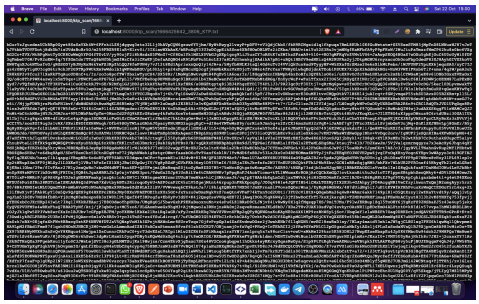

Figure 14 random string from encrypted National ID Card

If the author sees a random sentence given by the sinovi server, then the irresponsible party also cannot see the original version of the national id card that has been secured, no one can open the security except someone who has secured it and someone who creates a security password for the ID card. This way, data security is higher, and can prevent data leakage to unauthorized parties. As explained in the design stage, which requires that the output of the encryption process is a random word that cannot be easily guessed by someone, at this trial stage it has been in accordance with the previous design stage. So this step can be said to be complete and successful, and the writer summarize all testing steps in table 1 below

Table 1. Blackbox testing results

No	Tested features	Expected Results	Conclusion
1	Image encryption	Image converted to random string and secured with a password	Valid
2	Image file	Random string stored as txt file	Valid
3	Image results	Random string can be converted again to image	Valid
4	Server Response from a national id card URL	Return as a random string	Valid
5	Not authorized users	Not authorized users can't see original national id card image	Valid

e. Maintenance
When all stages have been passed and when the verification process is in accordance with the design process, at this stage the author will carry out monitoring and improvement so that the Sinovi application can run normally and the encryption system that has been designed previously runs well without any problems.

4. Conclusion

The conclusion obtained from this research is that data is an important asset for a person and for a company, so that everyone must protect their own data and companies must also have their own security systems to protect customer data. For example, as in this study, which uses the AES 256 method to secure the ID card data of users of the Sinovi service to make it more secure and anticipate data leaks to irresponsible parties. The limitation of the research in this study is only the scope of KTP data on the Sinovi application belonging to the Telkom Institute of Technology Purwokerto, and in this study the researcher has contributed to others in the form of having created an encryption library using the PHP programming language named t_encrypt so that other people can encrypt the data they have, are the same as those described in this study.
It is hoped that people or a company that is making an application service must perform data encryption, the authors hope that this research can be useful as a theoretical basis for anyone who wants to research about data security and ID card encryption, and the author hopes that there will be more research developed that is the same as this research, even the researcher hopes that there will be future research that uses the library that the author has made before, to speed up their research and have research that tests AES 256 with different methods research

DOI: https://doi.org/10.31004/riggs.v1i2.15

Reference

[1] H. M. Mohammad and A. A. Abdullah, "Enhancement process of AES: a lightweight cryptography algorithm-AES for constrained devices," *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 20, no. 3, pp. 551–560, 2022, doi: 10.12928/TELKOMNIKA.v20i3.23297.

[2] D. Darwis, R. Prabowo, and N. Hotimah, "Kombinasi Gifshuffle, Enkripsi AES dan Kompresi Data Huffman untuk Meningkatkan Keamanan Data," *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 5, no. 4, p. 389, Oct. 2018, doi: 10.25126/jtiik.201854727.

[3] M. A. Budiman, D. Rachmawati, and Jessica, "Implementation of Super-Encryption with Trithemius Algorithm and Double Transposition Cipher in Securing PDF Files on Android Platform," in *Journal of Physics: Conference Series*, Mar. 2018, vol. 978, no. 1. doi: 10.1088/1742-6596/978/1/012088.

[4] D. R. Destriani Firmansyah Putri Universitas Pembangunan Nasional Veteran Jakarta Jalan Fatmawati, P. Labu, J. Selatan, D. Jakarta, and M. R. Helmi Fahrozi Universitas Pembangunan Nasional Veteran Jakarta Jalan Fatmawati, "UPAYA PENCEGAHAN KEBOCORAN DATA KONSUMEN MELALUI PENGESAHAN RUU PERLINDUNGAN DATA PRIBADI (STUDI KASUS E-COMMERCE BHINNEKA.COM)," 2021. [Online]. Available: https://tirto.id/jumlah-pelanggan-e-commerce-tercatat-meningkat-383-selama-

[5] D. Komalawati, M. Dewi, M. R. Dan, R. D. Kartika, and I. Artikel, "KEJUTAN PULUHAN MILIAR TOKOPEDIA DITENGAH KASUS KEBOCORAN DATA," *Jurnal Syntax Admiration*, vol. 2, no. 1, 2021.

[6] K. Dio Ramadi Natha, I. Nyoman Putu Budiartha, and N. Gusti Ketut Sri Astiti, "PERLINDUNGAN HUKUM ATAS KEBOCORAN DATA PRIBADI KONSUMEN PADA PERDAGANGAN ELEKTRONIK LOKAPASAR (MARKETPLACE)," vol. 3, no. 1, pp. 2746–5039, doi: 10.22225/jph.3.1.4674.143-148.

[7] T. Hidayat, "ENCRYPTION SECURITY SHARING DATA CLOUD COMPUTING BY USING AES ALGORITHM: A SYSTEMATIC REVIEW," vol. 2, no. 2, 2019.

[8] X. Chen, "Implementing AES Encryption on Programmable Switches via Scrambled Lookup Tables," in *Proceedings of the 2020 ACM SIGCOMM Workshop on Secure Programmable Network Infrastructure, SPIN 2020*, Aug. 2020, pp. 8–14. doi: 10.1145/3405669.3405819.

[9] T. Hidayat and R. Mahardiko, "A Systematic Literature Review Method On AES Algorithm for Data Sharing Encryption On Cloud Computing," *International Journal of Artificial Intelligence Research*, vol. 4, no. 1, Apr. 2020, doi: 10.29099/ijair.v4i1.154.

[10] T. Rijanandi *et al.*, "Web-Based Application with SDLC Waterfall Method on Population Administration and Registration Information System (Case Study: Karangklesem Village, Purwokerto)," *Jurnal Teknik Informatika (JUTIF)*, vol. 3, no. 1, pp. 99–104, 2022, doi: 10.20884/1.jutif.2022.3.1.145.

[11] W. Steven Dharmawan *et al.*, "Penerapan Metode SDLC Waterfall Dalam Perancangan Sistem Informasi Administrasi Keuangan Berbasis Desktop," vol. VI, no. 2, 2018.

[12] R. F. Ramadhan and R. Mukhaiyar, "Penggunaan Database Mysql dengan Interface PhpMyAdmin sebagai Pengontrolan Smarthome Berbasis Raspberry Pi," *JTEIN: Jurnal Teknik Elektro Indonesia*, vol. 1, no. 2, pp. 129–134, 2020, doi: 10.24036/jtein.v1i2.55.

[13] I. M. Sudana, N. Qudus, and S. E. Prasetyo, "Implementation of PHPMailer with SMTP protocol in the development of web-based e-learning prototype," in *Journal of Physics: Conference Series*, Nov. 2019, vol. 1321, no. 3. doi: 10.1088/1742-6596/1321/3/032027.

[14] S. Hartati and Salamudin, "Membangun Katalog Online Toko Plastik Pedoman Menggunakan PHP Dan MYSQL," *Jurnal Informatika*, vol. 9, no. 1, pp. 75–87, 2020, [Online]. Available: http://www.ejournal.lembahdempo

[15] "ANALYZE MULTIPLE CHOICE ITEMS USING PHP PROGRAMMING LANGUAGE (Case Study: SMAN 1 Klari Karawang)", doi: 10.37200/IJPR/V24I7/PR270390.

[16] A. M. S. Huda and Y. Fernando, "E-Ticketing Penjualan Tiket Event Musik Di Wilayah Lampung Pada Karcismu Menggunakan Library Reactjs," *Jurnal Teknologi dan Sistem Informasi (JTSI)*, vol. 2, no. 1, pp. 96–103, 2021, [Online]. Available: http://jim.teknokrat.ac.id/index.php/JTSI

[17] I. Dewa, P. Gede, W. Putra, and D. W. Aristana, "PERANCANGAN DESAIN RUANGAN DATA CENTER MENGGUNAKAN STANDAR TIA-942 (STUDI KASUS : UPT SIMJAR STMIK STIKOM INDONESIA)," Online, 2019. [Online]. Available: http://jurnal.stiki-indonesia.ac.id/index.php/jurnalresistor

[18] R. Nuraini, D. Alamsyah, R. S. Septarini, A. Aristo, and J. Sinlae, "Completion of Multi-Criteria Decision Making Using the Weighted Product Method on the Server Maintenance Vendor Selection System," 2022.

[19] F. Adline, T. Tobing, and J. R. Tambunan, "Analisis Perbandingan Efisiensi Algoritma Brute Force dan Divide and Conquer dalam Proses Pengurutan Angka," *52 ULTIMATICS*, vol. XII, no. 1, 2020.

[20] D. Rachmawati, M. A. Budiman, and F. Atika, "PDF file encryption on mobile phone using super-encryption of Variably Modified Permutation Composition (VMPC) and two square cipher algorithm," in *Journal of Physics: Conference Series*, Mar. 2018, vol. 978, no. 1. doi: 10.1088/1742-6596/978/1/012115.

[21] Z. Abidin, A. Wijaya, and D. Pasha, "Aplikasi Stemming Kata Bahasa Lampung Dialek Api Menggunakan Pendekatan Brute-Force dan Pemograman C#," *JURNAL MEDIA INFORMATIKA BUDIDARMA*, vol. 5, no. 1, p. 1, Jan. 2021, doi: 10.30865/mib.v5i1.2483.

[22] R. Kesuma Dinata, N. Hasdyna, and R. Mahendra, "KOMBINASI ALGORITMA BRUTE FORCE DAN STEMMING PADA SISTEM PENCARIAN MASHDAR," 2020.

DOI: https://doi.org/10.31004/riggs.v1i2.15

[23] A. Susanto, "Image encryption using vigenere cipher with bit circular shift," 2021.

[24] N. Rachmat and Samsuryadi, "Performance analysis of 256-bit aes encryption algorithm on android smartphone," in *Journal of Physics: Conference Series*, Apr. 2019, vol. 1196, no. 1. doi: 10.1088/1742-6596/1196/1/012049.

DOI: https://doi.org/10.31004/riggs.v1i2.15