Development And Implementation Of The Rijndael Algorithm And Base-64 Advanced Encryption Standard (AES) For Website Data Security

Fathurrahmad, Ester

Abstract: The security of a website is absolutely analyzed and improvements are made to the web development framework to prevent data leakage, this study analyzes and modifies the Advanced Encryption Standard (AES) algorithm which can later be implemented on a website and tested and compared with the Advanced Encryption Standard (AES) algorithm. will be modified with the model that the researcher plans. The research objectives were, among others, to develop an algorithm that was modified from Base64 and Rijndael. The research stages consisted of a survey, implementation, and comparative analysis of the proposed modified algorithm. The results of research carried out through the encryption and decryption process by integrating the Base64 and AES Rijndael algorithms with the proposed algorithm so that it is known to improve data security better. If it is seen from the level of efficiency that the proposed algorithm can be used as a substitute for the Base64 algorithm. Whereas in the implementation, the proposed algorithm speed has good speed, it can be seen from the encryption process and the description and the resulting bits do not have a significant impact.

Index Terms: Security Analysis; Algorithm Development; Advanced Encryption Standard (AES); Rijndael; Base-64; Security Data; Website.

1 INTRODUCTION

Data security and information exchange both carried out on various platforms must have detailed security and are serious in their development, this is to protect every existing data (Zulham, 2017). Implementation of the use of the Advanced Encryption Standard (AES) has been widely used for message security (Prayitno and Nurdin, 2017), audio media (Santoso and Fakhriza, 2018), document files (Padede, Manurung, and Filina, 2017), as well as on a web network. (Hayati, Budiman, and Sharif, 2017). The security of a website is very important because the website is an information portal and an identity of an institution or institution. In addition, the website is not only used as a service to provide static information but has developed with the addition of features for online transactions (Wali et al, 2019; Wali et al, 2020). Until now, no website can be said to be completely secure. Likewise on the website of the AMIK Indonesia institution, according to the Head of Information and Technology AMIK Indonesia (Fathurrahmad et al, 2020), there were 23 attacks of various types in the form of defaces in 2019, and this also occurred on several campuses in Indonesia. Based on these problems, it is necessary to analyze and modify the Advanced Encryption Standard (AES) Algorithm which can later be implemented on a website and tested and compared with the Advanced Encryption Standard (AES) Algorithm which will be modified with the model that the researcher is planning. Modification of the Advanced Encryption Standard (AES) which is modified by embedding the Rijndael Encryption Algorithm and the addition of the Base-64 algorithm that the author developed as a better security enhancement. No web is completely secure, this is a paradigm for every website security developer in the world today. This research tries to develop a web security algorithm with Advanced Encryption Standard (AES) which will be modified and tested on the website which will be a new finding to strengthen the website's security system. Advanced Encryption Standard (AES) is a cryptographic algorithm that can be used to encrypt data. The AES algorithm is a symmetric ciphertext that can encrypt and decrypt information. Encryption converting data that can no longer be read is called ciphertext; conversely, decryption is changing the ciphertext data into its original form which we know as plaintext. AES has input and output blocks and keys 128 bits, 192, and 256 bits in a 4 × 4 byte rectangular state. The 128bit Advanced Encryption Standard algorithm can encode the header of a compressed file so that it can secure the file. (Putra et al, 2013). The grouping of this AES type is based on the length of the key used. AES-128 uses 10 rounds, AES-192 uses 12 rounds, and AES-256 uses 14 rounds. AES has fixed block sizes of 128 bits and key sizes of 128, 192, or 256 bits. Unlike Rijndael, which blocks and keys can be in multiples of 32 bits with a minimum size of 128 bits and a maximum of 256 bits. The Rijndael algorithm designated as AES has special characteristics that have earned it this status. In this case, this algorithm needs to be studied because there are many uses in everyday life and this will be useful in the development of cryptographic technology in order to find new breakthroughs.

Protecting data from attacks is difficult. One way to secure data from attacks is to use encryption. One of them uses the AES encryption method that has been described in this paper. Designed to replace DES (launched late 2001), using a variable-length block chipper, key length: 128-bit, 192-bit, 256-bit, applicable to smart cards. The Rijndael algorithm designated as AES has special characteristics that have earned it this status. In this case, also, this algorithm needs to be studied because there are many uses in everyday life and this will be useful in the development of cryptographic technology in order to find new breakthroughs. The main purpose of cryptography is to protect the information, as well as AES which is a series of steps or rounds carried out using symmetric keys. The use of AES is not only used in simple terms, but its role is very crucial in software or in other cases where AES is used.

- *Fathurrahmad is a lecturer in Department of Informatics, Faculty Informatics of Management, AMIK Indonesia. E-mail: fathurrahmad@amikindonesia.ac.id*
- *Ester is a lecturer in Department of Informatics, Faculty Informatics of Management, AMIK Indonesia. E-mail: ester@amikindonesia.ac.id*

Related research by Singh, G. (2013) states that system security needs to be improved by refining it with several data encryption algorithms and arranging them in an appropriate order. By analyzing security algorithms, it makes the best security system (Prasetyadi et al, 2019). Combining Advanced Encryption Standard with others can form a strong web (Selent, 2010; Canright, 2005), with the specifics of their respective security being enhanced. Likewise, the use of base-64 as an algorithm to improve data security (Abood & Guirguis, 2018, Du et al, 2007).

2 PROPOSED ENCRYPTION STANDARD (AES) RIJNDAEL AND BASE-64 MODIFIED

In the proposed encryption model uses Base-64 and AES Rijndael which then passes the previously entered secret key. In this study, two stages are used for encryption and decryption with stages; Stage 1: Encrypts the first character of plain text, the corresponding value of the first character of Plain Text (Pi) and key (Ki) obtained from using the secret code entered under the name "SECRET_KEY" and added and then the resulting value is again obtained character which will be the first character of the ciphertext. Stage 2: The encrypted results are then re-encrypted using Base64-encode and Rijndael from the ciphertext results from Plaintext (Pi) and key (Ki), the previous ciphertext namely Ci-1 is also added to Pi and Ki.

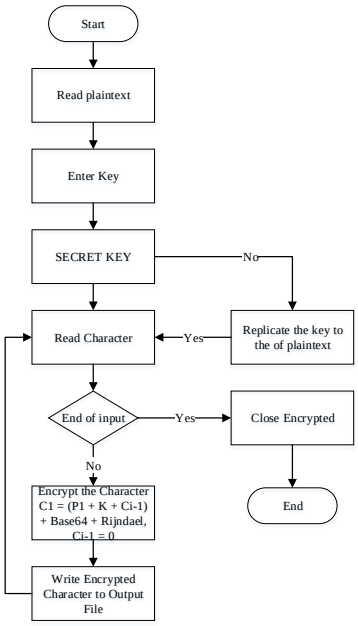

***Fig. 1**. Flowchart of Encryption Process*

As in Figure 1, the first step of each plaintext is read and entered a key with the name "SECRET KEY". If the keys match, it will proceed to the next stage. If the key names do not match, it will be repeated until the keys match. If the first step succeeds in reading the first text, the encryption process will be carried out by applying the equation by embedding Base64 + Rijndael encryption as well. (1) and produce output. This stage will run until all the characteristics of the entered file are encrypted.

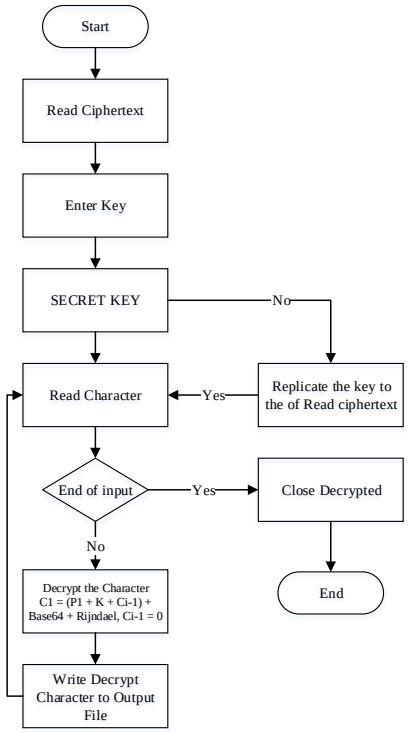

***Fig 2.** Flowchart of the Decryption Process*

In Figure 2 it is clear that the first step the initial text or file is entered using the "SECRET KEY" key. If the key entered is correct, it will continue with the next stage, if not the same, it will be repeated so that the keys are the same. In the next stage, the first character read from a file will be decrypted by applying eq. (2) and generate a file in the output. This stage will be repeated until every character that is decrypted is complete.

3 RESULTS AND AND ANALYSIS

3.1 Proposed Implementation

The encryption algorithm used is the Base64 algorithm and the Rijndael algorithm. Researchers surveyed a number of AES, DES, TRIPLEDES, BLOWFISH, BLOWFISH-compact, RIJNDAEL-256, R4, SERPENT, and TWOFISH encryption algorithms and were selected based on the popularity and efficiency used today for web security development in the world. For this reason, the researchers compared the three algorithms with the algorithms they built. In experimental tests, researchers used an Intel® Core ™ i5-4210U @ 1.70Ghz 4.00 GB RAM and 64-bit Windows OS in the encryption and decryption process in this study.

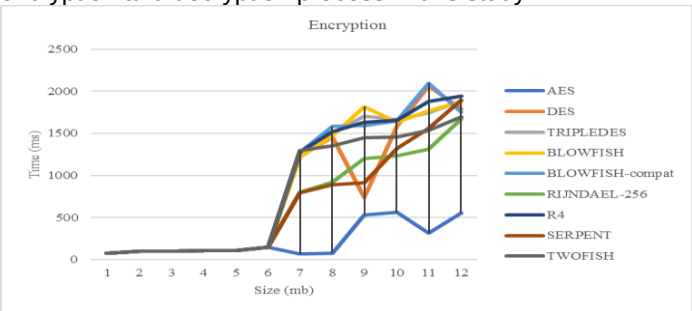

***Fig. 3**. Time Taken to Encrypt File*

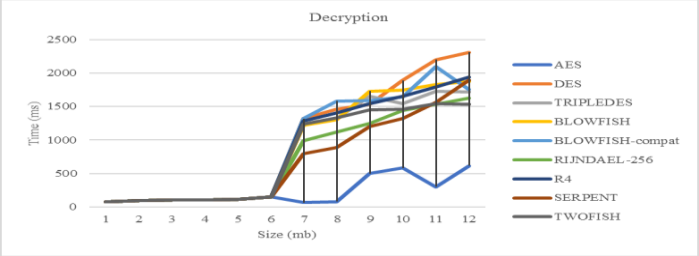

***Fig. 4**. Time Taken to Decrypt File*

If seen from Figures 3 and 4, then AES is the best algorithm for data encryption & decryption, this is also in agreement with the research conducted (Singh, 2013). The figures shown in Figures 3 and 4 show the encryption process and description of the algorithm under study, RIJNDAEL-256 in the second position in the problem. Meanwhile, the R4 algorithm has a long time. Each file is 79 Mb, 99 Mb, 103 Mb, 107 Mb, 111 Mb, and 149 Mb. Whereas the description process starts from the file that has been encrypted and re-encrypted, resulting in time (ms) in Figure 4

3.2 Experimental Results

The encryption algorithm is applied to files containing the text "WEBSITE DATA" and the encryption steps are carried out as follows :

1) Stage-1: using "WEBSITE DATA" conversion string using Base64 algorithm, to "zry/IdXpTtNWf9xU6s7xIsWfbg ==" by applying key K = "SECRET_KEY".
2) Stage-2: using RIJNDAEL-256 AES encryption algorithm, convert the string "zry / IdXpTtNWf9xU6s7xIsWfbg ==" to "¤‹! Óá „ì ° ãµÁ! / <Åâ¡ * çqûÚ {Ú¸; 0ö ..."

Meanwhile, the decryption process follows the reverse order steps from the encryption process to obtain the original text, namely "WEBSITE DATA". The proposed algorithm can also be applied to files containing large data and text data usage in website development at AMIK Indonesia.

3.3 Comparative Analysis of Proposed Modified Algorithms

At this stage of research, then the researcher has compared the proposed encryption algorithm by comparing the Base64 Algorithm and Rijndael AES to see the performance of the developed algorithm. We use text with the name "WEBSITE DATA" as plain text and "SECRET_KEY" as the key for all tested cases. Each case is considered by looking at the level of efficiency and the results that are encrypted from the proposed algorithm. As a consideration, we use a different case for the change of "TEXT" and amended by not using "SPACE" in the text.

Case 1 - Character Change in Middle of Text: No spaces in the text.

***Table 1**. Changed middle character of plaintext*

	Encryption Techniques		
	Base64	AES Rijndael	Modified Cipher
Text	WEBSITE DATA	WEBSITE DATA	WEBSITE DATA
Key	SECRET KEY	SECRET KEY	SECRET KEY
Encrypted text	zry/ IdXpTtNWf9xU6s 7xIsWfbg==	“¤‹!Óá„ì°ãµÁ!/<Åâ¡* çqûÚ{Ú¸;0ö…	E– vÁl¦..• ×aÿÀ.Kù}Î½. O_.ò..ÍtD³
Modified text	WEBSITEDATA	WEBSITEDATA	WEBSITEDATA
Modified encrypted text	1Co7BhWOcPhl YbfbS6m52g==	G.årQA×Ú^u0û]³• ` Ï.Õ.Ú¾o4;VzZ×d.ï	o.˜.Vgày!.<.¨ú.¡.œ Ø• Íùòô• í1ÛpÚGf
No. of bits flipped	16	32	32

It can be seen in table 1 that the input text has different results on the changed text. The avalanche effect varies according to the input text. In certain cases, the Vigenere Cipher shows a high avalanche effect compared to the proposed Modified Vigenere Code shown in Table III, but further results show that we propose the modified Vigenere Cipher has a high avalanche effect as compared to the Vigenere Cipher.

Case 2 - Last Key Character Changed: Here, only the last character is added.

***Table 2.** Changed last character of key*

	Encryption Techniques		
	Base64	AES Rijndael	Modified Cipher
Text	WEBSITE DATAS	WEBSITE DATAS	WEBSITE DATAS
Key	SECRET KEY	SECRET KEY	SECRET KEY
Encrypted text	h6QNYnJr +jUuB9ZS Id9kjA==	×4äƒÔ‡5 §KÁ+9´•Â ‹3ëØMˆo« %GÂ©Eµ 8ª	y_‰¥Ãm• •• næL(í|Gj• Hö r\.
Modified text	WEBSITE DATAZ	WEBSITE DATAZ	WEBSITEDATAZ
Modified encrypted text	/nt6PWI0 YibaIjDVZ BM6pw==	• DBÄ€®³ ã!Z3,RÑé³ ³¡NW27ð %72ÄëG	)WXÀ3-“¶³-Üÿ¿îWPGm™ •wBöS,öm
No. of bits flipped	32	32	32

Table 2 shows the absence of the number of bits from adding the original text to "WEBSITE DATA" shown in table 2.

5. CONCLUSION

Based on research that has been carried out through encryption and decryption processes using Base64 and AES Rijndael and the proposed algorithm by integrating the Base64 and AES Rijndael algorithms can improve data security better. If it is seen from the level of efficiency that the proposed algorithm can be used as a substitute for the Base64 algorithm. Whereas in the implementation, the proposed algorithm speed has good speed, it can be seen from the encryption process and the resulting description and bits do not have a significant impact. However, further, development is also needed regarding the use of the SHA 2 or SHA-256 algorithms to be integrated with the proposed algorithm.

ACKNOWLEDGMENT

Thank you to the Indonesian Ministry of Education, and the Directorate General of Research and Technology Strengthening and Development of the Ministry of Research, Technology and Higher Education (DITLITABMAS), as research funders for the 2020 Beginner Lecturer Research Grant (PDP). Laboratory Research Support Team as well as the lecturers and academics of AMIK Indonesia who always provide support to carry out this research in accordance with the author's expectations.

REFERENCES

[1] Abood, O. G., & Guirguis, S. K. (2018). A survey on cryptography algorithms. International Journal of Scientific and Research Publications, 8(7), 410-415.

[2] Canright, D. (2005, August). A very compact S-box for AES. In International Workshop on Cryptographic Hardware and Embedded Systems (pp. 441-455). Springer, Berlin, Heidelberg.

[3] Du, P., Kibbe, W. A., & Lin, S. M. (2007). nuID: a universal naming scheme of oligonucleotides for illumina, affymetrix, and other microarrays. Biology direct, 2(1), 16.

[4] Fathurrahmad, F., Yusuf, S., Iqbal, T., & Abdus, S. I. I., (2019). Source Code Library (SCL): Software Development Learning Application. International Journal of Scientific & Technology Research, 8(11), 175-182

[5] Hayati, N., Budiman, M.A. and Sharif, A., (2017). Implementasi Algoritma RC4A dan MD5 untuk Menjamin Confidentiality dan Integrity pada File Teks. SinkrOn, 1(2).

[6] Padede, A.M.H., Manurung, H. and Filina, D., (2017). Algoritma Vigenere Cipher Dan Hill Cipher Dalam Aplikasi Keamanan Data Pada File Dokumen. Jurnal Teknik Informatika Kaputama, 1(1), pp.26-33.

[7] Prasetyadi, G., Hantoro, U. T., Mutiara, A. B., Muslim, A., & Refianti, R. (2019, October). Heresy: A Serverless Web Application to Store Compressed and Encrypted Document in the Form of URL. In 2019 Fourth International Conference on Informatics and Computing (ICIC) (pp. 1-5). IEEE.

[8] Prayitno, A. and Nurdin, N., (2017). Analisa Dan Implementasi Kriptografi Pada Pesan Rahasia Menggunakan Algoritma Cipher Transposition. Jurnal Elektronik Sistem Informasi dan Komputer, 3(1), pp.1-10.

[9] Putra, M.D., (2018). Enkripsi Dan Dekripsi Gambar Dengan Menggunakan Perpaduan Algoritma Base64 Dan RC4. Semnasteknomedia Online, 6(1), pp.2-14.

[10] Santoso, H. and Fakhriza, M.F.M., (2018). Perancangan Aplikasi Keamanan File Audio Format Wav (Waveform) Menggunakan Algoritma RSA. Algoritma: Jurnal Ilmu Komputer Dan Informatika, 2(1).

[11] Selent, D. (2010). Advanced encryption standard. Rivier Academic Journal, 6(2), 1-14.

[12] Singh, G. (2013, December). Modified Vigenere encryption algorithm and its hybrid implementation with Base64 and AES. In 2013 2nd International Conference on Advanced Computing, Networking and Security (pp. 232-237). IEEE.

[13] Wali, M., Akbar, R., Iqbal, T., & Al-Bahri, F. P. (2019). Development Of An Android-Based Tourism Guide (A Case Study: Sabang City, Indonesia). International Journal of Scientific and Technology Research, 8(11), 887-893.

[14] Wali, M., Ahmad, L., Akbar, R., & Abdus, S. I. I., (2020). Source Code Library (SCL): Software Development Learning Application. International Journal of Scientific & Technology Research, 8(11), 175-182.

[15] Zulham, M., Kurniawan, H. and Rahmad, I.F., (2017, October). Perancangan Aplikasi Keamanan Data Email Menggunakan Algoritma Enkripsi RC6 Berbasis Android. In Seminar Nasional Informatika (SNIf) (Vol. 1, No. 1, pp. 96-101).