Institut Riset dan Publikasi Indonesia (IRPI)
MALCOM: Indonesian Journal of Machine Learning and Computer Science
Journal Homepage: https://journal.irpi.or.id/index.php/malcom
Vol. 4 Iss. 2 April 2024, pp: 670-677
ISSN(P): 2797-2313 | ISSN(E): 2775-8575

File Encryption and Decryption Using Algorithm Aes-128 Bit Based Website

Dola Irwanto

Informatics Engineering Study, Faculty of Computer Science, Pamulang University,
South Tangerang City, Indonesia

E-Mail: dosen01115@unpam.ac.id

Received Dec 26th 2023; Revised Mar 05th 2024; Accepted Mar 30th 2024
Corresponding Author: Dola Irwanto

Abstract

Digital data security has become very important in the current information era. One way to maintain data security is to use encryption and decryption techniques. The Advanced Encryption Standard (AES) algorithm has been proven effective in protecting data with a high level of security. This research aims to implement the AES-128 bit algorithm for online file encryption and decryption via a website. The method used in this research includes developing a website that provides a user interface for uploading and encrypting files, as well as for decrypting files that have been previously encrypted. The AES-128 bit algorithm is used to carry out the file encryption and decryption process. Users can choose their own encryption key or use a random key generated by the system. The result of this research is a website that can be used to efficiently secure sensitive files using the AES-128 bit algorithm. By using this website, users can easily encrypt the files they want to protect and also decrypt files that have been encrypted previously. The security of user data is guaranteed through the use of strong encryption algorithms and well-managed keys.

Keyword: AES-128 Bit, Data Security, Decryption, Encryption, Website

1. INTRODUCTION

Data stored and transmitted over the internet network is vulnerable to attacks and theft by unauthorized parties. Therefore, effective steps are needed to secure this data. One technique commonly used to maintain data security is encryption. Encryption is the process of converting data into a form that cannot be directly understood without a suitable encryption key. In the context of digital files, encryption allows data to be stored or transmitted securely without the risk of reading by unauthorized parties.

The Advanced Encryption Standard (AES) algorithm is one of the most widely used and internationally recognized encryption algorithms. AES offers a high level of security and efficiency in carrying out the encryption and decryption process. By using the right encryption key, data can be encrypted with AES so that only recipients who have the right key can decrypt and access hidden information.

Confidentiality of data or information is a complete service that is created to ensure that stored information cannot be read or opened by unauthorized parties. Efforts to maintain the confidentiality of this information data have been around since ancient times, specifically in Roman times, with the method of shifting letters or characters based on certain values.

In the modern era based on computer technology, these efforts have developed using algorithms created by many experts, but this can still be solved by irresponsible parties, therefore the development of cryptographic algorithms is increasingly rapid for data security. The concept of protecting information data can be done with an encryption and decryption system using a predetermined algorithm. The encryption process here is defined as the process of changing an original message (plain text) into a protected message, in this case an encrypted message (cipher text), while the decryption process is a process of returning a protected encrypted message to the original data form of the message.

The application of the AES algorithm for encryption and decryption of files online via a website offers advantages in terms of convenience and accessibility. Using an easy-to-access web interface, users can quickly and easily secure their sensitive files without needing to install additional software or have in-depth technical knowledge of cryptography.

In the context of technological innovation, the development of a website-based file encryption and decryption system using the AES-128 bit algorithm is a relevant and useful step. This will provide an effective

solution for individuals and organizations that prioritize data security in the use and exchange of digital files online.

Several studies on encryption and description include the first research simulating the Tiny encryption algorithm for encryption and description of text messages using Criptool2 [1]. The second research uses encryption for images and text with the Diffie Helman and El Gamal algorithms [2]. Short Message Service Encryption and Decryption Using the Blowfish Method [3]. Encrypt and decrypt files with the RC4-One Time algorithm on a LAN Network [4]. Fifth research aes-rijndael for encryption and Decription of sms data on android based phones [5]. Encryption and decryption are used to protect documents using Triple DES, which utilizes a USB flash drive for additional security [6]. The process of securing data using the AES-128 algorithm on various types of files involves encryption and decryption steps to protect information security [7]. The encryption and decryption procedure uses the SIMON algorithm on the QR Code to secure and restore information [8]. Encryption and decryption use the Speck algorithm to maintain security and access data stored in the QR Code [9]. The process of securing and recovering data in a file using the Twofish algorithm for encryption and decryption.[10]. Comparison between DES, AES, IDEA, and Blowfish algorithms in carrying out data encryption and decryption processes [11]. Encryption and decryption of text data using AES and RC4 algorithms in the CrypTool 2 environment [12]. Creation of cryptographic applications to secure document, audio and image files using the DES algorithm [13]. Research and evaluation of the Rivest Code 6 (RC6) algorithm in the data encryption and decryption process [14]. Implementation of the ElGamal public key cryptography algorithm to carry out the encryption and decryption process to maintain the security of data in files[15]. Implementation of the file encryption and decryption process using the Advanced Encryption Standard (AES-128) method [16]. Developing an application to secure image files using the ElGamal algorithm [17]. Analysis and design of cryptography-based Advanced Encryption Standard (AES) file security systems [18]. Performance analysis of encryption and decryption algorithm [19]. Cryptanalyzing a bit-level image encryption algorithm based on chaotic maps [20]. An optimized chaotic S-box for real-time image encryption scheme based on 4-dimensional memristive hyperchaotic map [21].

2. MATERIALS AND METHOD

The method in this research uses a flowchart on the image which consists of starting, identifying needs, designing, implementing the website and testing.

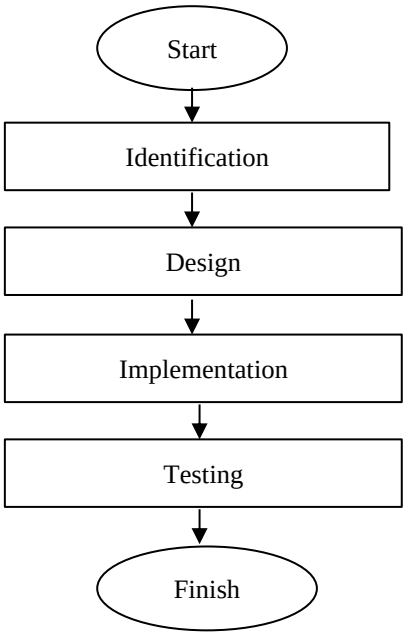

Figure 1. Research Methodology

This research uses identification which is a requirement for a file encryption and decryption system using the AES-128 bit algorithm. Design a website-based system to implement the AES-128 bit algorithm, by interacting with users for file upload, encryption and decryption. This is also done by defining workflows for file encryption and decryption. Website implementation is carried out by building a user interface. Integration with libraries or frameworks for the AES-128 bit algorithm. Testing The test was carried out with encryption and decryption running as expected. In general, an overview of cryptography in encryption and decryption can be seen in the following picture:

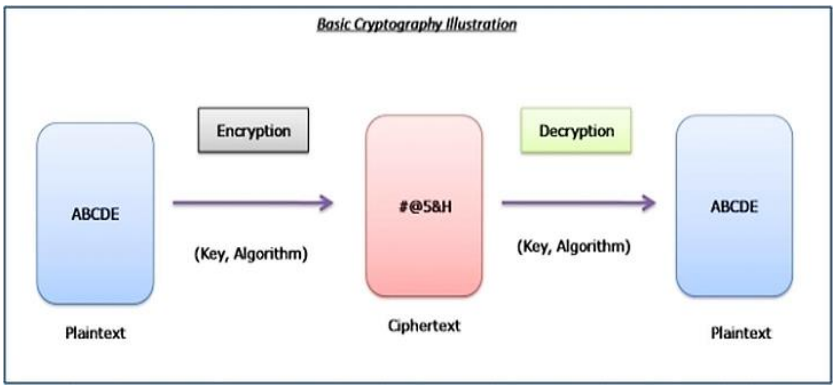

Figure 2. Illustration of Cryptography

How Advanced Encryption Standard (AES) works:

1. Add Round Key
   Add Round Key is basically combining an existing text cipher with a cipher key that is a cipher key with an XOR relationship. The chart can be seen in the Figure 3.

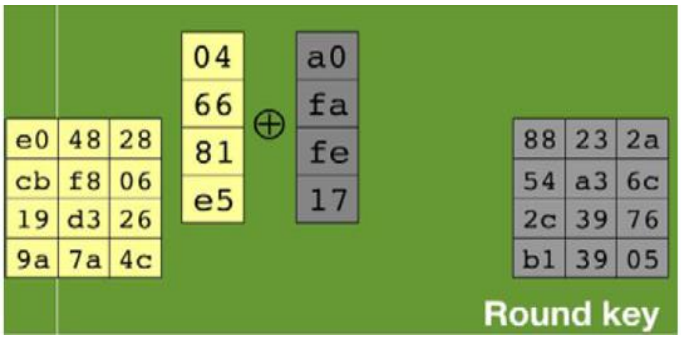

Figure 3. Round Key

   In the image above, on the left is the text cipher and on the right is the round key. XOR is done per column, namely column-1 of the text cipher is XORed with column-1 of the round key and so on.

2. Sub Bytes
   The Sub Bytes principle in the Advanced Encryption Standard (AES) algorithm is an important stage which aims to replace each byte in a data block with the corresponding byte from a substitution table. In this stage, each byte is changed individually according to a predefined substitution table. This substitution table is specifically designed to ensure that each byte value changes non-linearly, which significantly improves encryption security. This principle creates chaos in data blocks, so that even small changes in the input data will result in large changes in the output data. Therefore, the Sub Bytes Principle becomes a vital step in the AES encryption process, which helps improve security and resistance to cryptanalysis attacks. The principle of Sub Bytes is to exchange the contents of an existing matrix/table with another matrix/table called Rijndael S-Box. The figure 4 and igure 5 is an example of Sub Bytes and Rijndael S-Box.
   In the Sub Bytes illustration, there are column numbers and row numbers. As previously mentioned, each box in the cipher block contains information in hexadecimal form consisting of two digits, which can be numbers, letters, or letters, all of which are listed in the Rijndael S-Box. The step is to take one of the contents of the matrix box, match it with the left digit as a row and the right digit as a column. Then by knowing the columns and rows, we can retrieve the table contents from the Rijndael S-Box. The final step is to change the entire cipher block into a new block whose contents are the result of exchanging all the contents of the block with the contents of the steps mentioned previously

	1	2	3	4	5	6	7	8	9	0a	0b	0c	0d	0e	0f	
0	52	9	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
10	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
20	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
30	8	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
40	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
50	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
60	90	d8	ab	0	8c	bc	d3	0a	f7	e4	58	5	b8	b3	45	6
70	d0	2c	1e	8f	ca	3f	0f	2	c1	af	bd	3	1	13	8a	6b
80	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
90	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
a0	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
b0	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
c0	1f	dd	a8	33	88	7	c7	31	b1	12	10	59	27	80	ec	5f
d0	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
e0	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
f0	17	2b	4	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

Figure 4. Illustration of Sub-Bytes

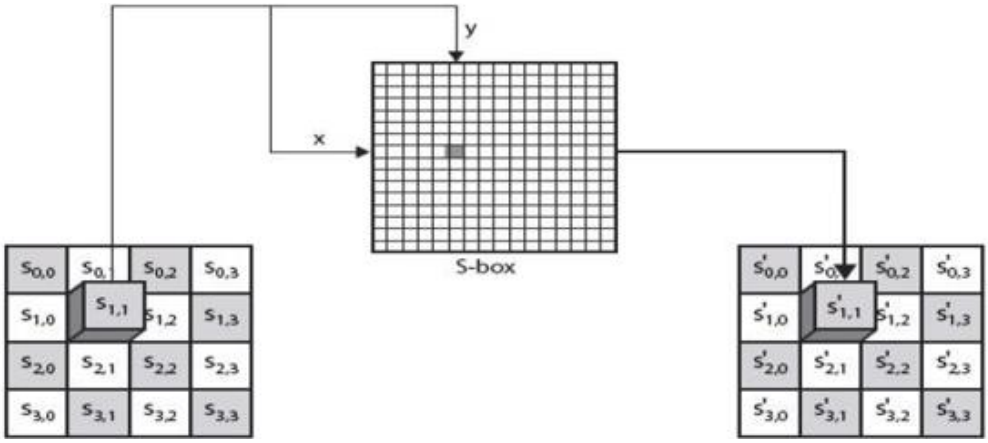

Figure 5. Illustration of S-Box

3. Shift Rows
   Shift Rows, as the name suggests, is a process that shifts each block/table element per row. Namely, the first line is not shifted, the second line is shifted by 1 byte, the third line is shifted by 2 bytes, and the fourth line is shifted by 3 bytes. The shift seen in a block is a shift of each element to the left depending on how many bytes are shifted, every 1 byte shift means a shift to the left once

4. Mix Column
   What happens when Mix Column is multiplying each element of the cipher block with the matrix shown in Table 1. The table has been determined and is ready to use. Multiplication is carried out like ordinary matrix multiplication, namely using dot product, then the two multiplications are entered into a new cipher block. The illustration in Table 1 will explain how this multiplication should be done. In this way, the entire series of processes that occur in AES have been explained and the next step is to explain the use of each of these processes.

Table 1. Matrix Multiplication

02	01	01	03
03	02	01	01
01	03	02	01
01	01	02	03

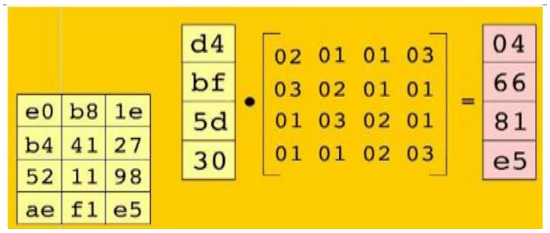

Figure 6. Illustration of Mix Column

5. AES Flowchart
   As can be seen, all the processes previously explained are in the diagram. What this means is that starting from the second round, continuous repetition is carried out with a series of Sub Bytes, Shift Rows, Mix Columns, and Add Round Key processes, after which the results of that round will be used in the next round using the same method. However, in the tenth round, the Mix Columns process is not carried out, in other words the sequence of processes carried out is Sub Bytes, Shift Rows, and Add Round Key, the results of the Add Round Key are used as the AES ciphertext.

Figure 7. AES 2 Flow Diagram

3. RESULTS AND DISCUSSION

In implementing the Advanced Encryption Standard (AES) algorithm, I created a file encryption and decryption website using the PHP programming language.

1. Login Page

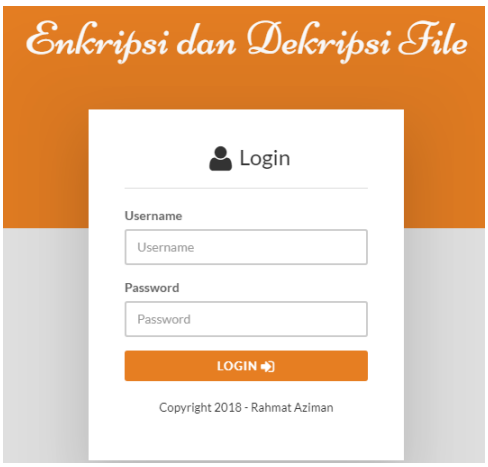

Figure 8. Login page

The home page of the website displays a login page, here I create a user with username: admin, password: admin.

2. Dashboard Page

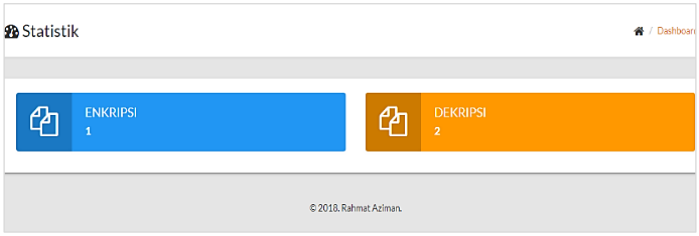

Figure 9. Dashboard Page

The dashboard page/website interface displays statistics on files that are already in the database, whether they have been encrypted or decrypted.

3. Files Page

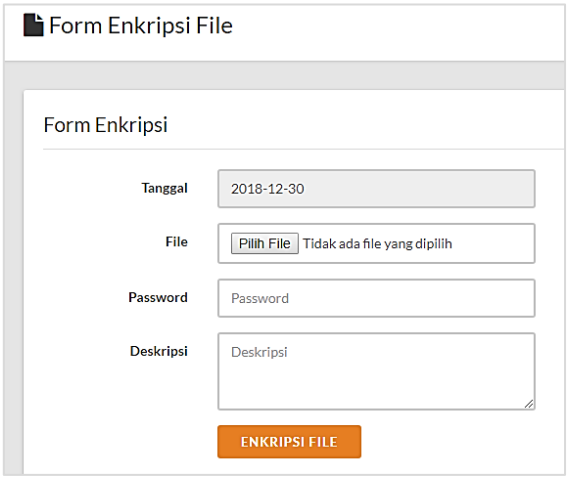

Figure 10. Encryption Page

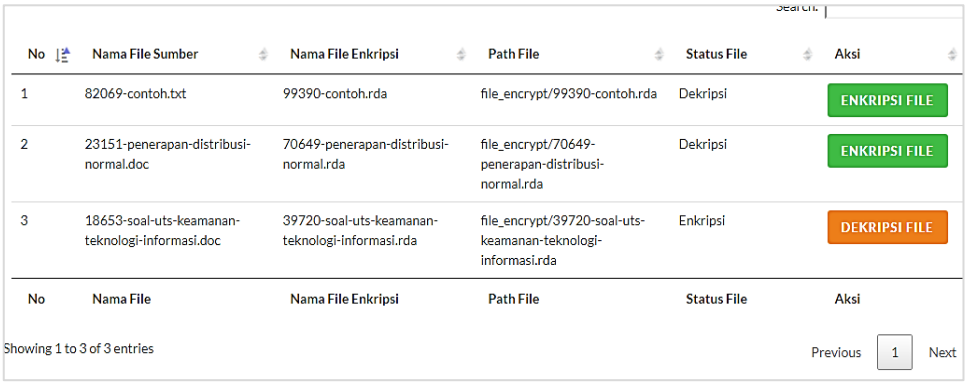

Figure 11. Decryption Page

The File page has 2 sub-menus, namely the encryption and decryption menus. The encryption menu functions to upload files to be encrypted, while the decryption menu functions to decrypt (return to original form) files contained in the database that have been encrypted.

4. List List Page

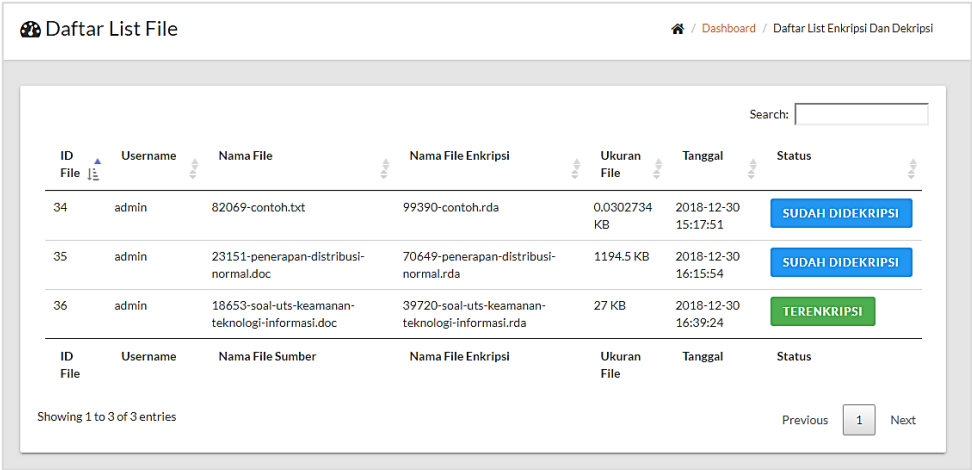

Figure 12. List List Page

The encryption and decryption file list is a collection of information that records all files that have undergone the encryption or decryption process in a system or project. Each record in this list generally includes details such as the file name, storage location, encryption or decryption status, and the date and time the process was executed. This list has a very important role because it helps users or system administrators in tracking and managing files that have undergone this process. Apart from being a management tool, this list also functions as an audit tool to ensure the success and security of the encryption and decryption process. By maintaining an organized and well-documented list of encryption and decryption files, users can increase the level of security as well as orderliness in the management of sensitive data. The list page contains information on all files in the database.

4. CONCLUSION

The Advanced Encryption Standard (AES) algorithm has proven to be very effective in maintaining a high level of data security. This research succeeded in applying the AES-128 bit algorithm for the process of encrypting and decrypting files via a website. This research adopts a structured methodology, starting from requirements identification to testing, using a flowchart that includes the steps of identification, design, implementation and testing. Through the provided user interface, users can upload files to be encrypted and decrypt previously encrypted files. The encryption and decryption process is carried out through a prepared database, ensuring data security and integrity. By using this website, users can easily protect their files with strong encryption as well as decrypt files as needed. This ensures the security of user data by using reliable encryption algorithms and well-managed keys.

REFERENCES

[1] M. F. Mulya and N. Rismawati, “ANALISIS DAN SIMULASI ALGORITMA TEA (TINY ENCRYPTION ALGORITHM) UNTUK ENKRIPSI DAN DEKRIPSI PESAN TEXT,” vol. 3, no. 1, 2019.

[2] L. Nisa, T. Indriyani, M. Ruswiansari, P. Studi, T. Informatika, and F. T. Informasi, “Aplikasi Enkripsi Citra dan Teks Menggunakan Algoritma Diffie-Hellman dan ElGamal,” vol. 1, no. 1, pp. 8–17, 2020.

[3] W. Fahriah and T. Febrianto, “Aplikasi Enkripsi dan Dekripsi Short Message Service di Android Menggunakan Metode Blowfish,” vol. 02, no. 01, pp. 1–5, 2019.

[4] P. Sihombing and W. Ginting, “Perancangan dan Implementasi Enkripsi dan Dekripsi File dengan Algoritma RC4 – One Time Pad pada Jaringan LAN,” vol. 02, no. 01, pp. 1–10, 2020.

[5] J. Vol, N. Juli, I. Algoritma, and A. U. Enkripsi, “Jurnal Vol. 10 No. 2 Juli 2019,” vol. 10, no. 2, 2019.

[6] A. Enkripsi *et al.*, “Jurnal Coding , Sistem Komputer Untan Jurnal Coding , Sistem Komputer Untan ISSN : 2338-493X,” vol. 04, no. 2, pp. 1–12, 2016.

[7] R. Visdya, H. Chandra, A. Kusyanti, and M. Data, “Analisis Performa Proses Enkripsi dan Dekripsi Menggunakan Algoritme AES-128 Pada Berbagai Format File,” vol. 3, no. 1, 2019.

[8] N. Putu, R. Novandra, A. Kusyanti, and K. Amron, “Implementasi Algoritme SIMON untuk Enkripsi dan Dekripsi Berbasis QR,” vol. 3, no. 11, pp. 10721–10728, 2019.

[9] Y. S. Fatmala, A. Kusyanti, and M. Data, “Implementasi Algoritme Speck untuk Enkripsi dan Dekripsi pada QR Code,” vol. 2, no. 12, pp. 6253–6260, 2018.

[10] A. Try, P. L. L. B, and F. Fattah, "Penerapan Enkripsi dan Dekripsi File Menggunakan Algoritma Twofish," vol. 2, no. 2, pp. 72–77, 2021.

[11] "Jurnal Teknologi Terpadu Perbandingan Algoritma DES , AES , IDEA Dan Blowfish dalam Enkripsi dan Dekripsi Data Donzilio Antonio Meko Program Studi Teknik Informatika , STIMIK Kupang Jurnal Teknologi Terpadu," vol. 4, no. 1, pp. 8–15, 2018.

[12] R. N. Fitriana, D. Djuniadi, and K. Kunci, "Analisis Perbandingan Algoritma AES Dan RC4 Pada Enkripsi Dan Dekripsi Data Teks Berbasis CrypTool 2," vol. 7, no. 2, pp. 1–7, 2021.

[13] F. Teknologi and I. Universitas, "PENGEMBANGAN APLIKASI KRIPTOGRAFI FILE DOKUMEN , AUDIO DAN GAMBAR DENGAN ALGORITMA DES," vol. VIII, no. 2, pp. 185–190, 2016.

[14] Y. Prayudi, "STUDI DAN ANALISIS ALGORITMA RIVEST CODE 6 (RC6) DALAM ENKRIPSI / DEKRIPSI DATA," vol. 6, no. D.

[15] P. Soepomo, "ELGAMAL UNTUK PROSES ENKRIPSI DAN DEKRIPSI GUNA," pp. 376–384, 2014.

[16] M. B. Aryanto, M. Tahir, S. I. Devita, and Z. N. Mustofa, "Implementasi Enkrip Dan Dekrip File Menggunakan Metode Advance Encryption Standard (AES-128)," vol. 3, no. 1, 2023.

[17] A. Manaor, H. Pardede, B. S. Ginting, and K. Lumbanbatu, "Aplikasi Pengamanan File Gambar Menggunakan Algoritma Elgamal," vol. 3, no. 2, 2018.

[18] K. Muttaqin, J. Rahmadoni, U. Samudra, and U. Andalas, "ANALYSIS AND DESIGN OF FILE SECURITY SYSTEM AES (ADVANCED ENCRYPTION STANDARD) CRYPTOGRAPHY BASED," vol. 1, no. 2, pp. 114–123, 2020.

[19] S. S. Tyagi, "Performance analysis of encryption and decryption algorithm," vol. 23, no. 2, pp. 1030–1038, 2021, doi: 10.11591/ijeecs.v23.i2.pp1030-1038.

[20] H. Wen, Y. Lin, and Z. Feng, "Engineering Science and Technology , an International Journal Cryptanalyzing a bit-level image encryption algorithm based on chaotic maps," *Eng. Sci. Technol. an Int. J.*, vol. 51, no. June 2023, p. 101634, 2024, doi: 10.1016/j.jestch.2024.101634.

[21] M. Vijayakumar and A. Ahilan, "An optimized chaotic S-box for real-time image encryption scheme based on 4-dimensional memristive hyperchaotic map," *Ain Shams Eng. J.*, no. December, p. 102620, 2023, doi: 10.1016/j.asej.2023.102620.