JAST : Journal of Applied Science and Technology
Volume. 1 Number. 2, July 2021
ISSN : 2775-4022
http://jurnal.unissula.ac.id/index.php/JAST

Web Based Security System Academic Exam Questions Using Advanced Encryption Standard

Bagus Satrio Waluyo Poetro[1], Sam Farisa Chaerul Haviana[2], Arief Budiman[3]
[1] Universitas Islam Sultan Agung/Lecturer/Informatics Department
[2] Universitas Islam Sultan Agung/Lecturer/Informatics Department
[3] Universitas Islam Sultan Agung/Alumni/Informatics Department

ABSTRACT

One way to measure the success of the academic process and achievement of student competence, is giving exams, from the smallest level namely daily tests, semester exams, to the highest level, namely the national exam. In an effort to maintain the security of exam question data, there is a data security method known as cryptography. In this research, a security system was designed that serves to protect exam questions so that data cannot be read by student before its time by using the Advanced Encryption Standard (AES) algorithm.

The AES algorithm is a type of symmetric algorithm where the encryption and decryption processes have the same key for the encryption and decryption processes. In the system that will be designed, the Caesar Cipher algorithm is used to form an additional key (seed) that is kept secret from the public. The results of this study indicate that AES encryption method can give results maximum so that the AES method can applied to virtual data storage system to protect the transmitted data.

Keywords: Exam***;*** AES***;*** Caesar Cipher***;*** Encryption; Decryption
corresponding email : *bagusswp@unissula.ac.id* .

1. INTRODUCTION

1.1. The Background of the Problem

National education functions to develop skills and form the character and civilization of a dignified nation in the context of educating the nation's life, aiming to develop the potential students to become human beings and become a democratic and responsible citizen. One way to measure the success of the academic process and achievement of student competence, is giving exams, from the smallest level namely daily tests, semester exams, to the highest level, namely the national exam [1].

Data security is very important in the process of sending or receiving data done through computer media. Security. This data is carried out in order to maintain confidentiality, integrity, validity and data availability [2].

In an effort to maintain the security of exam question data, there is a data security method known as cryptography. Cryptography itself is a method of securing data that can be used to maintain the confidentiality and authenticity of data. Cryptography is a science that is useful for scrambling data in such a way that the data cannot be read by outsiders who are not entitled to that basis, of course the data that has been scrambled must be able to be returned to its original form by the authorized party. Advanced Encryption Standard (AES) is a cryptographic algorithm as a standard symmetric key encryption algorithm that used in current time [3].

Therefore, in this research, a security system was designed that serves to protect exam questions so that data cannot be read by student before its time by using the Advanced Encryption Standard (AES) algorithm.

1.2. The Formulation of the Problem

In the implementation of this research, there are several problems that are the subject of discussion, namely:

1. How to apply the AES Method to the Exam Question Security System Application that was created?
2. How to design a document security application using the AES Method?

1.3. The Objectives

The aim of this research is:

1. Designing a software that can be used to secure data in the form of documents.
2. Measure the speed of encryption and decryption when the algorithm AES performs security on each file.

1.4. Benefits of the Research

From this research, the benefits obtained are as follows:

1. For Writers
   Can add a source of knowledge about cryptographic algorithms, especially in the encryption and decryption process in securing information.
2. For Readers
   Can add insight and knowledge about cryptography, especially in understanding the AES algorithm to secure information such as exam questions data.

2. LITERATURE REVIEW

2.1. Literature Review

In previous studies related to the topic of discussion, namely the application of cryptographic algorithms to certain applications and comparisons of cryptographic algorithms and methods have been carried out before.

Examples of several studies related to research entitled "Designing File Cryptography Applications using the Advanced Encryption Standard (AES) algorithm" resulted in the following tests:

a. Techniques in securing a file can be done by using a cryptographic algorithm.
b. To apply encryption and decryption techniques, the AES algorithm has transformations or stages for the algorithm process, namely Addroundkey, Subbytes, Shiftrows and Mixcolums.
c. In providing data security, it depends on the difficulty of the cryptographic algorithm itself, the more difficult the algorithm, the more difficult the security will be to solve [4].

Research entitled "Implementation of Cryptographic Data Security in Text Messages, Document File Content and Document Files using the Advanced Encryption Standard algorithm" resulted in the following tests:

a. The encrypted text message can still be opened but the text message becomes scrambled and disguised so that the information cannot be understood. The results of encrypted text messages are stored in a document file with the file extension type ".txt" format.

The decrypted text message with the matching key can be reverted to the original text message so that the information can be understood. The results of the decrypted text messages are stored in a document file with the file extension type ".txt" [5].

For further research entitled "Design of Data Security Applications with the Advanced Encryption Standard (AES) Algorithm" concluded that the creation of a data security system application for encryption and decryption of files and texts using Microsoft Visual Studio 2010 supports the development of an increasingly sophisticated era. The choice of the AES: Rijndael algorithm, because this algorithm is an algorithm that is quite difficult to solve at this time, before there is no attack capable of mathematical analysis effectively and efficiently because the pattern formed is quite random [6].

And in the study entitled "Implementation of the Advanced Encryption Standard (AES) and Message Digest (MD5) Methods on Document Encryption (LPSE INIB Case Study)" based on functional testing carried out to find out the system can run well based on the system design. The testing is done by means of the file generated by the encryption process can be doubled or even more than the size and number of characters from the original file because the encryption results are made in hexadecimal. For examples the character "U" in hexadecimal becomes "75" as well as characters, symbols and spaces also have hexadecimal. So the encrypted file and the processing time are affected by the size of the original file, but not by the type of file format. The larger the original file size, the larger the encrypted file size and the processing time required [7].

2.2. Basic Theory

2.2.1. Cryptography

Cryptography is the science and art of maintaining secrecy message by encoding it into a form that is not its meaning can be understood [8]. Usually cryptographic algorithms are not kept secret, even

encryption that keeps the algorithm secret is considered bad. The secret of the algorithm lies in the parameters used, so the key is determined by the parameters of the algorithm. It is the parameters that define the description key that must be kept secret [9].

Broadly speaking, the encryption process is the process of scrambling the "original script" so that it becomes a "random script" which makes it difficult for someone who does not have the description key to read it. What is meant by difficult to read is the possibility of getting back the original manuscript will take a long time. So this cryptographic technique has a very important aspect important in maintaining the confidentiality of the secured data, due to aspects of authentication, and data integrity is met use this method [10].

2.2.2. Advanced Encryption Standard (AES)

In January 1997, the National Institute of Standard and Technology or commonly abbreviated as NIST initiated a search to be used as a replacement for Standard Encryption Data (DES), the requirements for a new standard called the Advanced Encryption Standard (AES) must have:

1. 128bit block cipher with choice of three keys 128, 192, 256 bit,
2. Public and flexible design,
3. At least triple DES fellow three keys, and available royalty free worldwide.

The AES algorithm is a type of symmetric algorithm where the encryption and decryption processes have the same key for the encryption and decryption processes. The AES algorithm itself has three key types, namely 128, 192 and 256. Each of these types uses a different internal key, namely the Round key for each round. For the 128-bit AES encryption process, 10 rounds are carried out, as follows [4]:

1. AddRoundKey.
2. Rounds a>=9 times, the processes performed in each round are SubBytes, ShiftRows, MixColumns, AddRoundKey.
3. Final Round is the last round process which includes SubBytes, ShiftRows, AddRoundKey.

For the encryption process on the 128bit AES algorithm carried out by consists of 4 types of Bytes transformation, namely SubBytes, ShiftRows, MixColumns, and AddRoundKey, and for the decryption process also consists of 4 types of Bytes transformation, namely InvSubBytes, InvShiftRows, InvMixColumns, and AddRoundKey [11].

The AES algorithm encoding steps for the encryption and decryption process can be seen as follows:

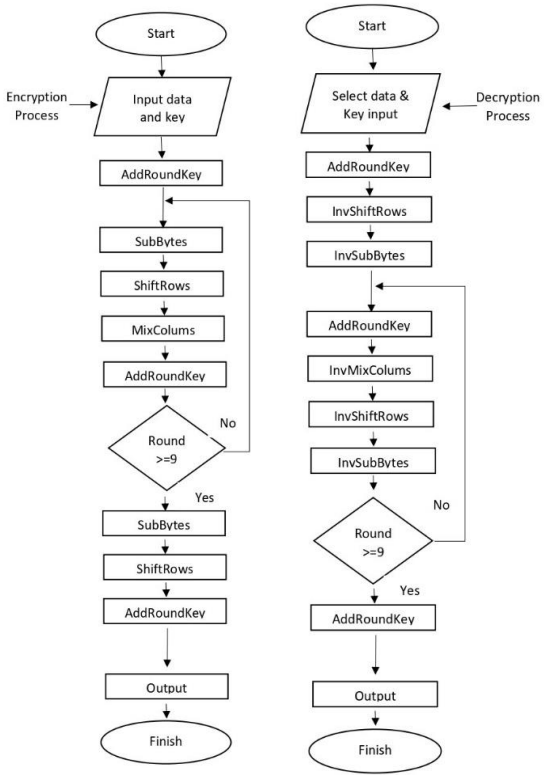


Figure 1. 10 Encryption Process Diagram and Decryption Process Diagram

3. RESEARCH METHOD

The method used to obtain the performance of the AES algorithm in performing encryption and decryption is applying the AES algorithm by creating applications that able to perform encryption and decryption by using AES [12].

3.1 Data Collection

The steps to obtain data for research purposes are as follows:

a. The data used in this study came from Unissula's informatics engineering studies such as lecturer data and exam questions.
b. The literature study was carried out in this research by searching for and studying cryptography from books, journals, internet and materials related to this research.

3.2 Prototyping

The method for building the system in this research is to use a prototyping software design process model. The prototyping method presents a complete picture of the system to be created. Making a Prototyping for system developers aims to collect information from users so that users can interact with the prototype model that was developed, because the prototype describe the initial version of the system for the continuation of the actual system the greater one [13]. For more details of the prototyping method can be seen in Figure 2.

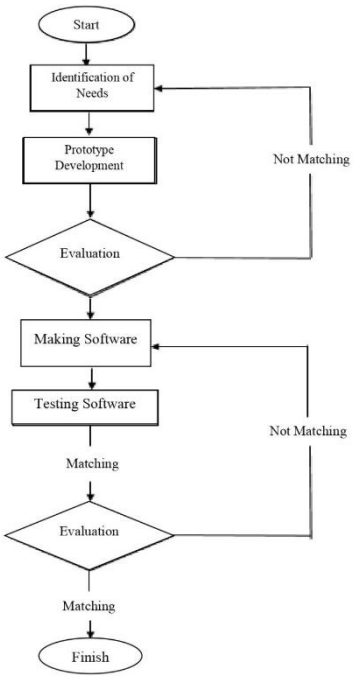


Figure 2. Flowchart Prototyping

3.3 File (document) Encryption and Decryption Process with Advanced Encryption Standard

In the system that will be designed the Caesar Cipher algorithm is used to form an additional key (seed) that is kept secret from the public. This algorithm including substitution ciphers where each letter in plaintext is shifed by other letters that have a certain position difference in the alphabet [14]. For example shifting with the key "4".

The workings of the system designed in this study consist of several processes such as the following:

A. Encryption Process

An explanation of the encryption process carried out in Figure 3 is as follows:

1. Enter file data and documents.
2. Then enter the password generation process, in this process the entered password will be combined with the seed key obtained from randomizing the password (Password + Seed)
3. After that, enter the document encryption process, in this process the document will be encrypted with the AES algorithm.
4. Then after the document encryption process is complete it will produce an encrypted document.
5. Done.

B. Decryption Process

The explanation of the decryption process carried out in Figure 3 is as follows:

1. Select File and enter a password.
2. Then go to the next process, namely the process of generating passwords and merging passwords and keys that have been scrambled (password + seed).
3. After generating the password is complete, enter the document decryption process, in this process the encrypted document will be returned to the original document (decryption).
4. After doing the description process, the document will return to the original document.
5. Done.

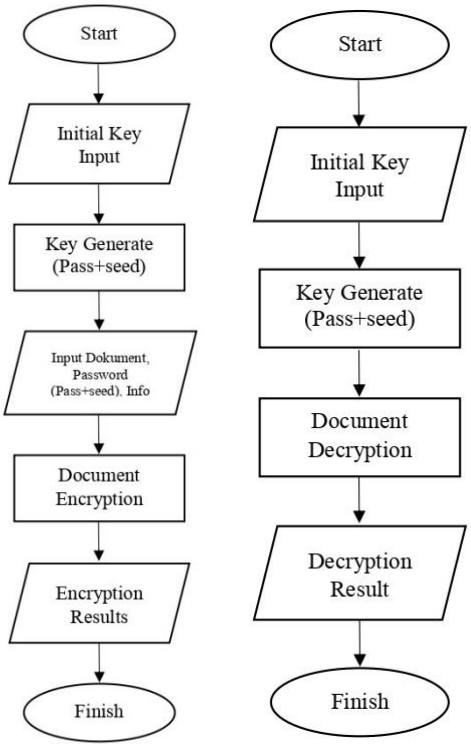


Figure 3. Flowchart of the Encryption and Decryption Process

3.4 Context Diagram

Context diagrams are level diagrams above, which is a global diagram of diagram an information system that describe the data flows into the and outward from within and outside the entity external [15]. The context diagram for security exam questions with the Advanced Encryption Standard algorithm can be seen in Figure 4.

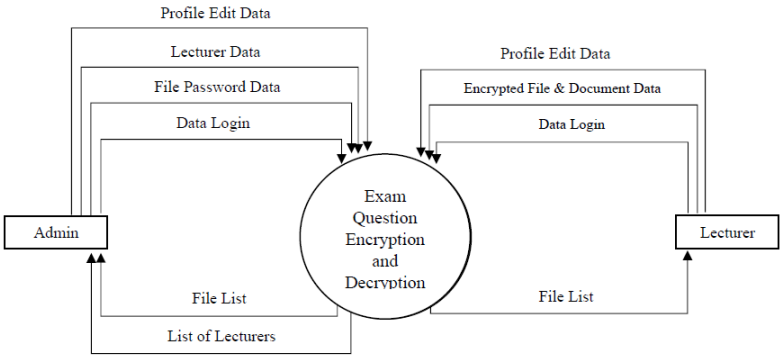


Figure 4. Context Diagram

Figure 4 is a context diagram that has two actors, namely admin and lecturer. The actor performs activities for the encryption and decryption system of exam documents. The admin actor performs activities such as logging into the system, after successfully logging in, the admin can manage data such as decrypting encrypted documents, downloading decrypted documents, then admins can also manage lecturer

data such as creating new accounts for lecturers, deleting lecturer accounts that have been used. has moved or for other reasons, the admin can logout from the system after use is complete.

Then for lecturer activities on the system, lecturers can log into the system, after successfully entering the system lecturers can send (upload) and encrypt documents, lecturers can also change profiles according to the needs of the lecturer, then lecturers can logout from the system.

4. RESULT AND ANALYSIST

4.1. Admin System Results and Tests

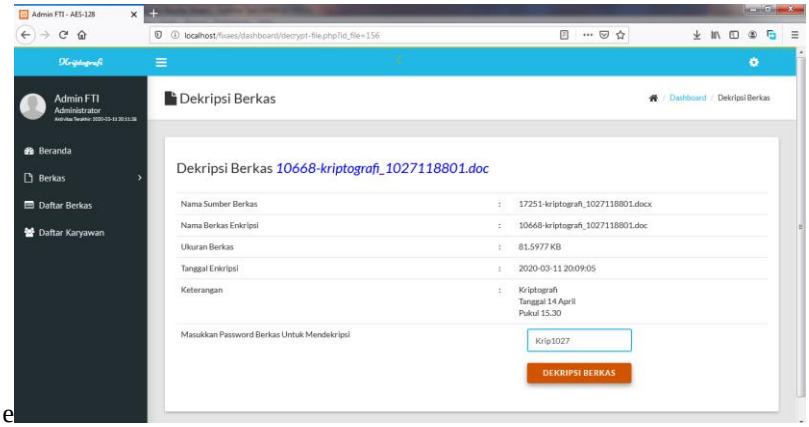
e 

Figure 5. File Decryption Page

Figure 5 shows what is needed in the file decryption process after selecting the files to be encrypted. For password decryption, it is done by taking letters from the name of the course as many as 4 words and the NIK of the lecturer as much as 4 numbers, then entering it into the input and pressing "Enkripsi Berkas".

Table 1. Document Decryption Successful

Identification	PDHUPL_3		
Test Item Name	Entering the correct password for the document to be encrypted		
Research Purposes	Checking the document can be decrypted again		
Initial Condition	1. Appropriate Document Password 2. Entered the document description page		
Scenario			
1. Enter password 2. Press the File Dekripsi Berkas			
Result			
Provided Data	**Which are expected**	**Observer**	**Conclusion**
Password = Citr1027	Documents can be decrypted again	Document successfully decrypted	Successful

Table 2. Document Decryption Failed

Identification	PDHUPL_4
Test Item Name	Entering the wrong password for the document to be encrypted
Research Purposes	Checking the document can't be decrypted anymore
Initial Condition	1. Wrong Document Password 2. Entered the document description page
Scenario	
1. 1. Enter password 2. 2. Press the File Dekripsi Berkas	
Result	

Provided Data	Which are expected	Observer	Conclusion
Password = Coba1234	The document cannot be decrypted again	System Response Document was not successfully decrypted and displayed “password yang anda masukan salah”	Successful

Table 3. Document Decryption Speed

Identification	PDHUPL_5		
Test Item Name	Decryption Speed		
Research Purposes	Check document description speed		
Initial Condition	Selecting a document of a different size		
Scenario			
Selecting the document and size to decrypt			
Result			
Provided Data	**Which are expected**	**Observer**	**Conclusion**
Password Decrypt	The document decryption process does not take too long for small documents.	Decryption results with a size of 81.59 KB in the process with a time of 7.05 seconds, for a size of 599.5 KB with a time of 50.65 seconds..	Successful

4.2. Lecturer System Results and Testing

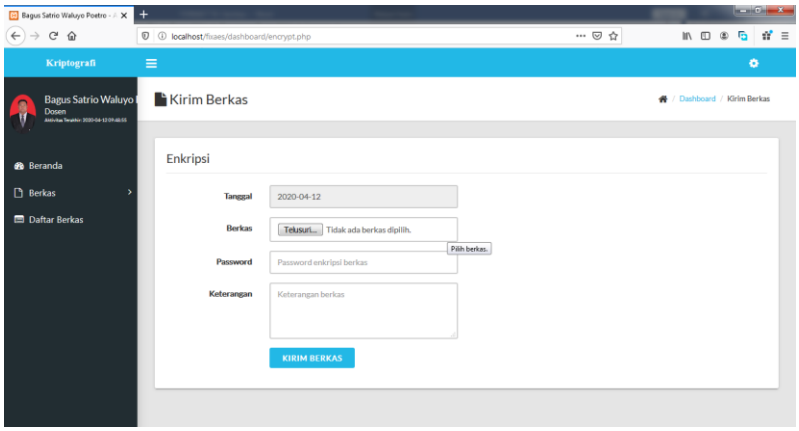


Figure 6. Page Send and Encrypt Files

Figure 6 shows how the procedure or rules for sending and encrypting files. For password encryption, it is done by taking letters from the name of the course as many as 4 words and the lecturer's NIK 4 as many as numbers, the specified file name (document) format is "name of course_NIK" then sending the file

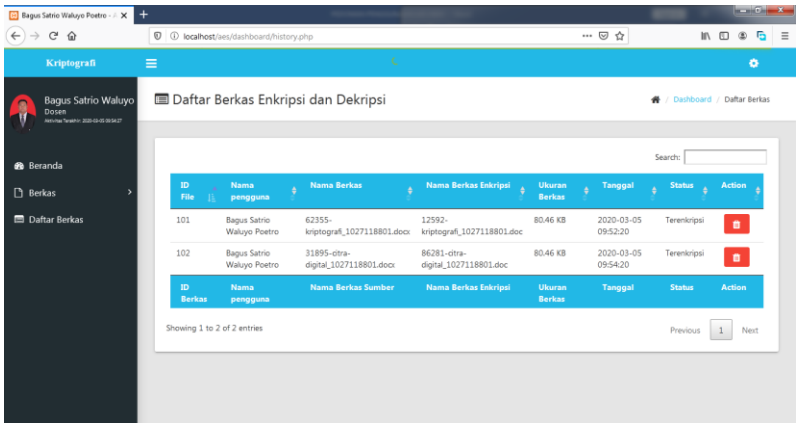


Figure 7. Pages of Lecturer File List

Figure 7 is the File List page, where the files that have been sent by the lecturer are displayed in this view.

Table 4. Encryption Process Successful

Identification	PDHUPL_3		
Test Item Name	Encrypt docx, doc and pdf formats.		
Research Purposes	Documents will be encrypted		
Initial Condition	1. The document is not encrypted 2. The lecturer is on the send file page		
Scenario			
1. 1. The lecturer inputs the initial key in the random password form then presses “Enter”. 2. 2. After that, the lecturer fills out the Delivery form 3. 3. Press the “Kirim Berkas” button.			
Result			
Provided Data	**Which are expected**	**Observer**	**Conclusion**
1. File : Citra Digital_1027118801.docx 2. Password : Citr1026Gmxv546: 3. Information : -Citra Digital - Exam Date	Documents can be encrypted	The system responds to the document successfully encrypted	Successful

Table 5. Encryption Process Failed

Identification	PDHUPL_4
Test Item Name	Encrypt jpg format.
Research Purposes	Encryption failed
Initial Condition	1. The image is in jpg format. 2. The lecturer is on the send file page
Scenario	
1. 1. The lecturer inputs the initial key in the form of a random password then presses “Enter”. 2. 2. The lecturer fills out the submission form 3. 3. Press the “Kirim Berkas” button.	
Result	

Provided Data	Which are expected	Observer	Conclusion
1. File: Gambar.jpg 2. Password : Citr1026Gmxv546: 3. Information : -Citra Digital -Exam Date	Encryption will fail	System responds "maaf, file yang bisa di enkripsi hanya docx, doc dan pdf"	Successful

Table 6. Checking the Encryption Process

Identification	PDHUPL_5		
Test Item Name	Check Document Encryption speed		
Research Purposes	Checking document encryption speed		
Initial Condition	Selecting a document of a different size		
Scenario			
Prepare documents to be encrypted			
Result			
Provided Data	**Which are expected**	**Observer**	**Conclusion**
1. File : Citra Digital_1027118801.docx (81.59KB) 2. Password : Citr1026Gmxv546: 3. Information : -Citra Digital -Exam Date	The document encryption process does not take too long for documents that are small in size.	Encryption results with a size of 81.59 KB are processed in 6.87 seconds, for a size of 599.5 KB, they are processed in 50.06 seconds.	Successful

5. CONCLUSION

From the test results for encryption and decryption of document files, it can be concluded that:

1. The original document with the encrypted and decrypted document has the same size (unchanged).
2. Encryption speed is faster than decryption. From the results, encryption with a size of 81.59 KB is processed in 6.87 seconds, for a size of 599.5 KB it is taken in 50.06 seconds, while for decryption with a size of 81.59 KB in 7.05 seconds, for a size of 599.5 KB it takes 50.65 seconds.

The results of this study indicate that AES encryption method can give results maximum so that the AES method can applied to virtual data storage system to protect the transmitted data.

REFERENCES

[1] L. Kusumastuti and S. Lestari, "Kejujuran Akademik Pada Siswa Sekolah Menengah Pertama Saat Menghadapi Ujian," Universitas Muhammadiyah Surakarta, 2015.

[2] Asriyanik, "Studi Terhadap Advanced Encryption Standard (AES) Dan Algoritma Knapsack Dalam Pengamanan Data," *J. Santika J. Ilm. Sains dan Teknol.*, vol. 7, pp. 553–561, 2017.

[3] A. R. Tulloh, Y. Permanasari, and E. Harahap, "Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen," *J. Mat. UNISBA*, vol. 2, no. 1, pp. 118–125, 2016.

[4] R. Tullah, M. I. Dzulhaq, and Y. Setiawan, "Perancangan Aplikasi Kriptografi File Dengan Metode Algoritma Advanced Encryption Standard (AES)," *J. Sisfotek Glob.*, vol. 6, no. 2, pp. 24–30, 2016.

[5] F. N. Pabokory, I. F. Astuti, and A. H. Kridalaksana, "Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard," *J. Inform. Mulawarman*, vol. 10, no. 1, p. 20, 2015.

[6] D. Nurnaningsih and A. A. Permana, "Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Encyption Standard (Aes)," *J. Tek. Inform.*, vol. 11, no. 2, pp. 177–186, 2018.

[7] G. Gumira, Ernawati, and A. Erlanshari, "Implementasi Metode Advanced Encryption Standard (AES) Dan Message Digest 5 (MD5) Pada Enkripsi Dokumen (Studi Kasus LPSE UNIB)," *J. Rekursif*, vol. 4, no. 3, pp. 277–287, 2016.

[8] A. Eka Putri, A. Kartikadewi, and L. A. Abdul Rosyid, "Implementasi Kriptografi dengan Algoritma Advanced Encryption Standard (AES) 128 Bit dan Steganografi menggunakan Metode End of File (EOF) Berbasis Java Desktop pada Dinas Pendidikan Kabupaten Tangerang," *Appl. Inf. Syst. Manag.*, vol. 3, no. 2, pp. 69–78, 2021.

[9] M. L. Wijaya, K. Yulianti, and H. S. Husain, "Caesar Cipher Dan Affine Cipher Untuk Mengubah Pesan Rahasia,"

J. EurekaMatika, vol. 5, no. 1, pp. 1–45, 2017.

[10] C. Saefudin, G. Abdillah, and A. Maspupah, "Pengamanan Source Code Program Menggunakan Algoritma Advanced Encryption Standard dan Algoritma Base64," *Pros. Semin. Nas. Apl. Teknol. Inf.*, pp. 9–18, 2019.

[11] B. S. W. Poetro, P. Studi, T. Informatika, and U. Diponegoro, "Kriptografi Citra Digital dengan Algoritma Rijndael dan Transformasi Wavelet Diskrit Haar," *Pros. Semin. Nas. Ilmu Komput. Univ. Diponegoro*, pp. 175–178, 2010.

[12] R. V. H. Chandra, A. Kusyanti, and M. Data, "Analisis Performa Proses Enkripsi dan Dekripsi Menggunakan Algoritme AES-128 Pada Berbagai Format File," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 3, no. 1, pp. 481–486, 2019.

[13] D. Purnomo, "Model Prototyping Pada Pengembangan Sistem Informasi," *J I M P - J. Inform. Merdeka Pasuruan*, vol. 2, no. 2, pp. 54–61, 2017.

[14] D. Seftyanto, M. Apriani, and T. Haryanto, "Peran Algoritma Caesar Cipher Dalam Membangun Karakter Akan Kesadaran Keamanan Informasi," in *Seminar Nasional Matematika dan Pendidikan Matematika FMIPA UNY*, 2012, no. ISBN : 978-979-16353-8-7, p. MP-883-MP-890.

[15] W. Nur Laila, "Sistem Informasi Pengolahan Data Inventory Pada Toko Buku Studi Kasus CV. Aneka Ilmu Semarang," *J. Tek. Elektro*, vol. 3, no. 1, pp. 40–55, 2011.