Jurnal E-Komtek
Vol. 9, No. 2. (2025) pp. 340-350
https://jurnal.politeknik-kebumen.ac.id/index.php/E-KOMTEK
p-ISSN : 2580-3719 e-ISSN : 2622-3066

Comparison of DES, AES, IDEA RC4 and Blowfish Aglorithms in Data Encryption and Decryption

Stefanus Eko Prasetyo[1], Gautama Wijaya[2], Felix[3]

[1-3]Department of Information Technology, Universitas Internasional Batam, Indonesia, 29426

2132037.felix@uib.edu

https://doi.org/10.37339/e-komtek.v9i1.2259

Published by Politeknik Piksi Ganesha Indonesia

Artikel Info
Submitted:
05-06-2025
Revised:
09-06-2025
Accepted:
16-06-2025
Online first :
30-06-2025

Abstract

The advancement of information technology has had a significant impact, one of which is as a medium for transmitting information from one place to another, making information access easier for many people. However, the ease of access to communication media also poses challenges for information security, as information becomes more vulnerable to being accessed, stolen, or manipulated by irresponsible parties. To protect the confidentiality of information, specific methods are needed, one of which is cryptography. In cryptography, there are various algorithms, including DES, AES, IDEA, Blowfish, Twofish, and RC4. This research aims to compare the performance of several cryptographic algorithms in the data encryption and decryption processes, focusing on processing speed and the size of the encrypted file. The results of the research show differences in processing time and file size of encrypted and decrypted data for each algorithm.

Keywords: *Aglorithms, Decryption, Encryption.*

Abstrak

Kemajuan teknologi informasi telah membawa pengaruh besar, salah satunya dengan menjadi sarana untuk mengirimkan informasi dari satu lokasi ke lokasi lain, yang memudahkan akses informasi bagi banyak orang. Namun, kemudahan akses pada media komunikasi ini juga menimbulkan tantangan terhadap keamanan informasi yang disampaikan, karena informasi menjadi lebih rentan untuk diakses, dicuri, atau dimanipulasi oleh pihak-pihak yang tidak bertanggung jawab. Untuk menjaga kerahasiaan informasi, dibutuhkan metode khusus, salah satunya adalah kriptografi. Dalam kriptografi, terdapat berbagai algoritma seperti DES, AES, IDEA, Blowfish, Twofish, dan RC4. Penelitian ini bertujuan untuk membandingkan kinerja sejumlah algoritma kriptografi dalam proses enkripsi dan dekripsi data, dengan melihat kecepatan proses dan ukuran file hasil enkripsi. Hasil penelitian menunjukkan adanya perbedaan pada waktu proses dan ukuran file enkripsi serta dekripsi dari masing-masing algoritma.

***Kata-kata kunci**: Agloritma, Dekripsi, Enkripsi,*

1. Introduction

The rapid advancement of information technology has driven the development of communication media as a means of delivering information across locations, thus facilitating access to various communication media **[1] [2] [3].** However, this ease of access also brings risks to the security of the transmitted information, as data becomes more vulnerable to access, theft, or manipulation by unauthorized parties **[4] [5].** To address this issue, special methods are required to protect the confidentiality of information, one of which is cryptography **[6] [7].**

Cryptography consists of two main types of algorithms: symmetric and asymmetric **[8].** Symmetric algorithms use a single key for both encryption and decryption processes. This algorithm is further divided into two categories, namely stream ciphers and block ciphers **[9] [10].** Stream ciphers operate at the single-bit level, while block ciphers process data in specific bit blocks. To date, various symmetric cryptographic algorithms have been developed for both categories **[11] [12].**

Some algorithms that fall under the symmetric algorithm category include DES, AES, Blowfish, IDEA, RC4, Twofish, Saphent, and Skipjack. Each of these algorithms has its strengths and weaknesses, both in terms of processing speed and the level of data security (ciphertext) produced.

Considering the differing characteristics of these algorithms, the author is interested in implementing and comparing the performance of DES, AES, Blowfish, IDEA, RC4, and Twofish algorithms in an application for data encryption and decryption **[14] [15].** The performance of the algorithms is measured based on the encryption and decryption speed of files and the size of the files produced after encryption.

2. Method

a. Type of Research

This research adopts a comparative method, which is a method that compares the similarities and differences between two or more facts or characteristics of the objects being studied within a specific framework of thought. In this research, the variables used are independent, but involve more than one sample or testing at different times. The comparative method can also be considered a type of descriptive research aimed at analyzing cause-and-effect relationships by examining the factors that influence the emergence of certain phenomena.

Therefore, the main objective of this comparative research is to compare two or more groups related to a specific variable.

This research model is designed to provide an overview of the comparison between cipher algorithms such as DES, AES, IDEA, Blowfish, RC4, and Twofish in the encryption and decryption processes, particularly in terms of processing speed. The developed application has several main menus, including a file/text menu that allows users to perform encryption and decryption on selected text or files, as well as a comparison menu that displays a form to compare the results of the available algorithms.

b. Software Interface

In this research, the specifications of the software used are as follows: visual Studio as the main programming language, and starUML as a tool for designing the system. This software is used to build and design the interface as well as the system flow of the developed application.

c. System Design and Construction

The stages in the development of this software consist of several main parts is **Figure 1.**

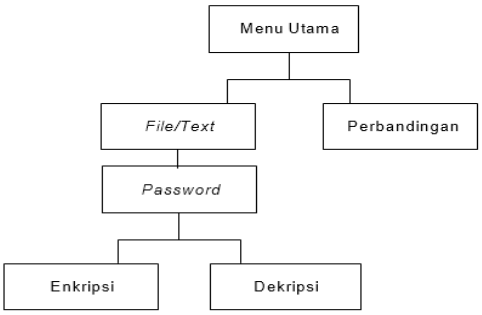

Figure 1. Process Hierarchy

1) Usecase Diagram

A use case illustrates the interactions that occur within the system, providing an overview of the user or actor that is associated with the system and the aspects related to the user within the system.

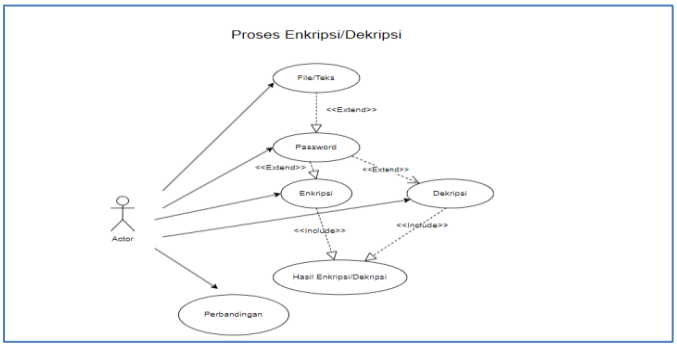

Figure 2. Usecase Diagram

2) Encryption Activity Diagram

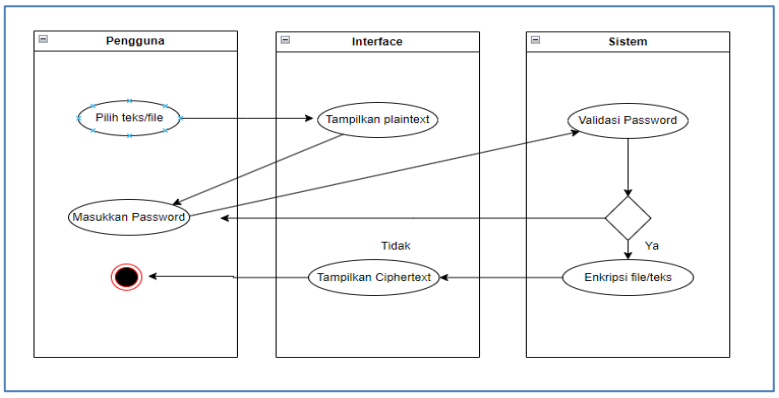

Figure 3. Encryption Activity Diagram

3) Decryption Activity Diagram

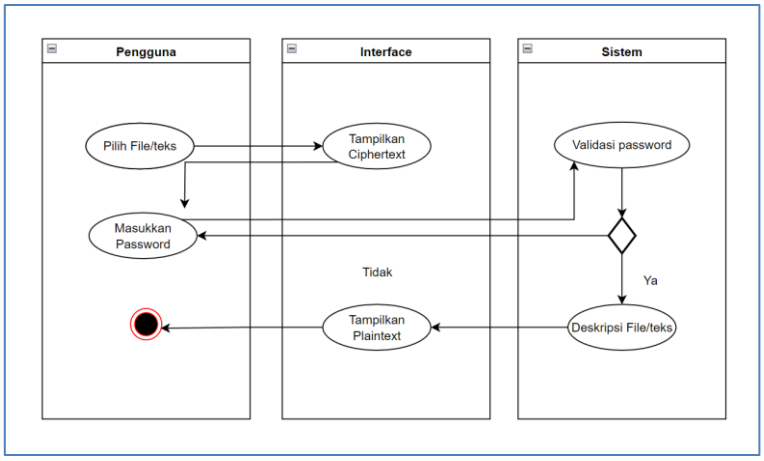

Figure 4. Decryption Activity Diagram

4) Comparison Activity Diagram

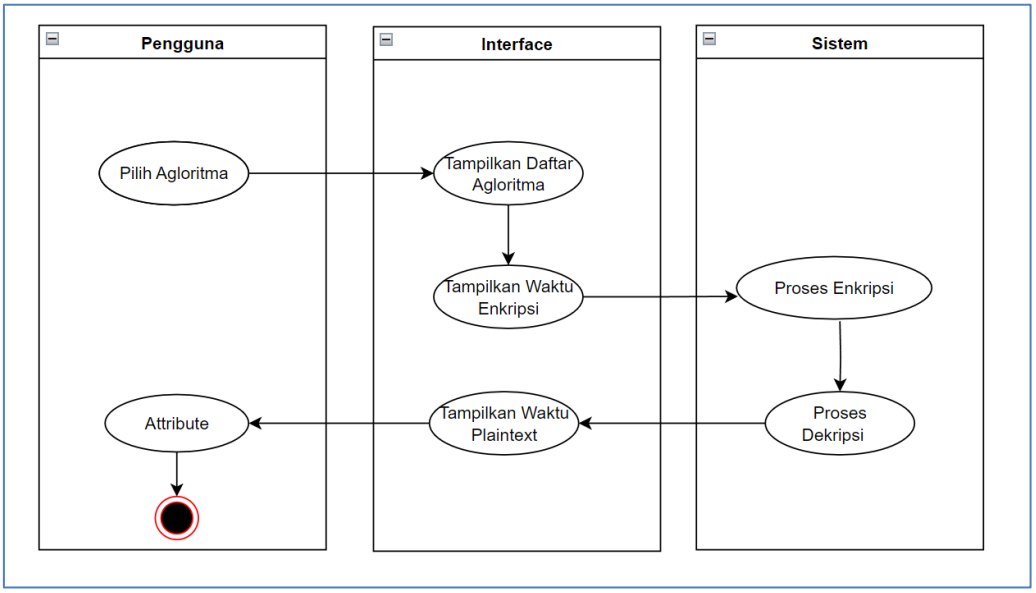

Figure 5. Comparison Activity Diagram

5) Interface Design

This section will represent the implementation or construction of the user interface of the program to be developed.

6) Design of the file and Text Encryption/Decryption Form

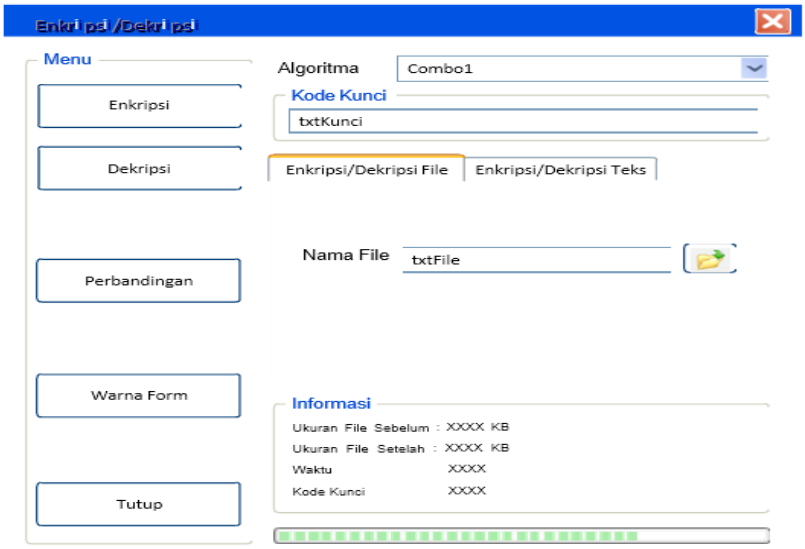

Figure 6. Design of the File and Text Encryption/Decryption Form

7) Design of the Algorithm Comparison Form

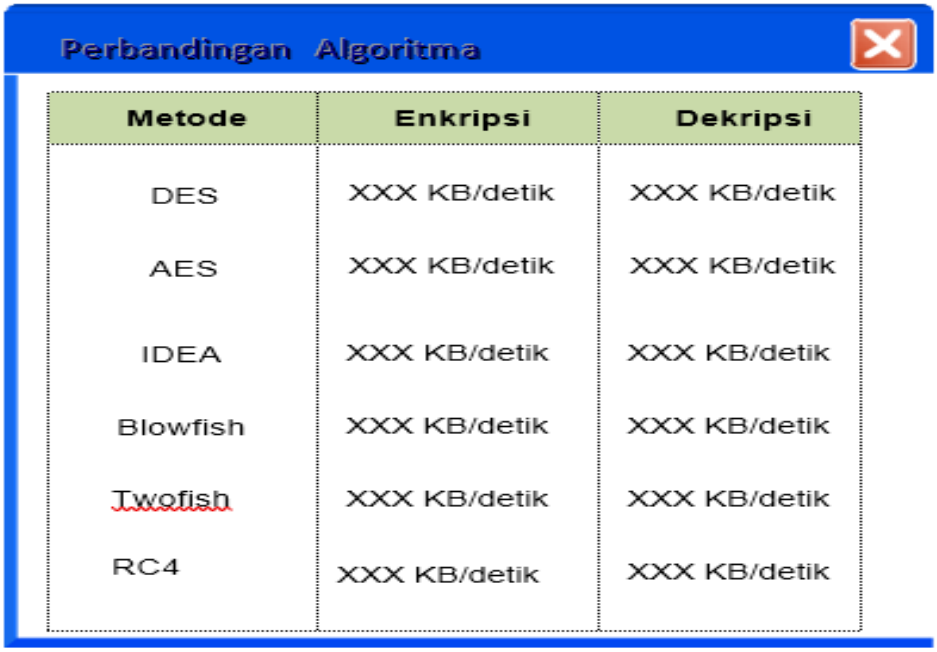

Figure 7. Design of the Algorithm Comparison Form

3. Results And Discussion

a. System Implementation

In order for the application to function optimally, a number of supporting files are required to facilitate the processes to be carried out. Below are some of the files that support the implementation of this program.

Table 1. List of Supporting Files for Program Implementation

No	Nama Folder	Nama / Tipe File	Deskripsi
1	Enkripsi-Dekripsi	Enkripsi-Dekripsi.exe	File executable untuk menjalankan aplikasi Enkripsi-Dekripsi
2	\Classes	*.cls	Berisi file-file class untuk keempat algoritma
3	\Skins	*.skn	Berisi file-file skin/kulit form
4	\Forms	*.frm dan *.frx	Berisi file-file form aplikasi
5	\Modules	*.bas	Berisi file-file modul untuk mendukung desain aplikasi dimana didiklarasikan berbagai fungsi pendukung program
6	\Package	*.*	Berisi file-file setup untuk menginstalkan komponen-komponen pendukung seperti file-file *.dll, file *.ocx dan file-file komponen pendukung lainnya

b. System Interface

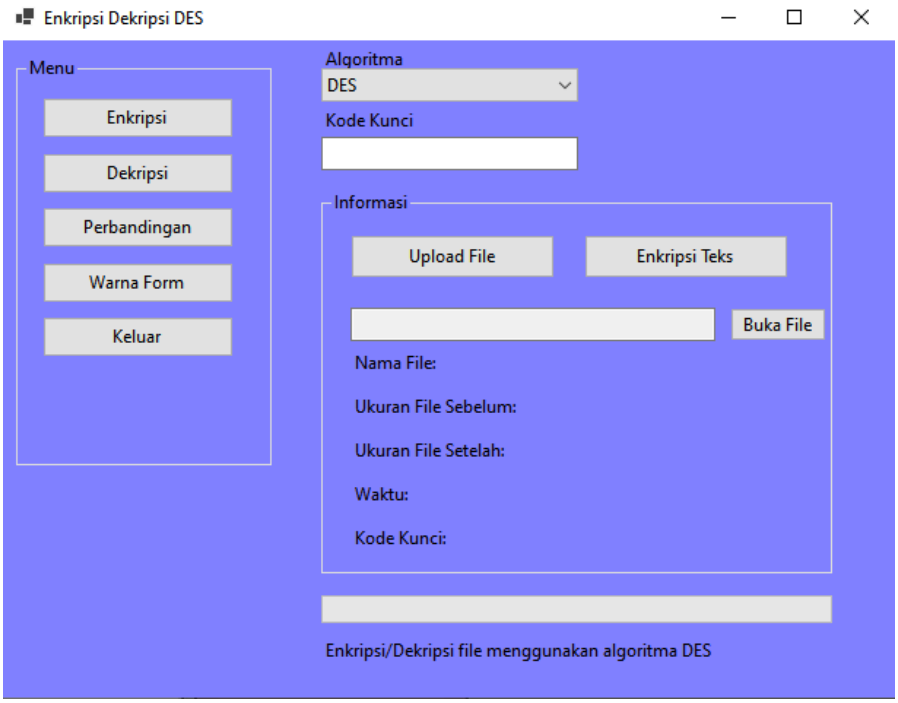

Figure 10. Main Form Display

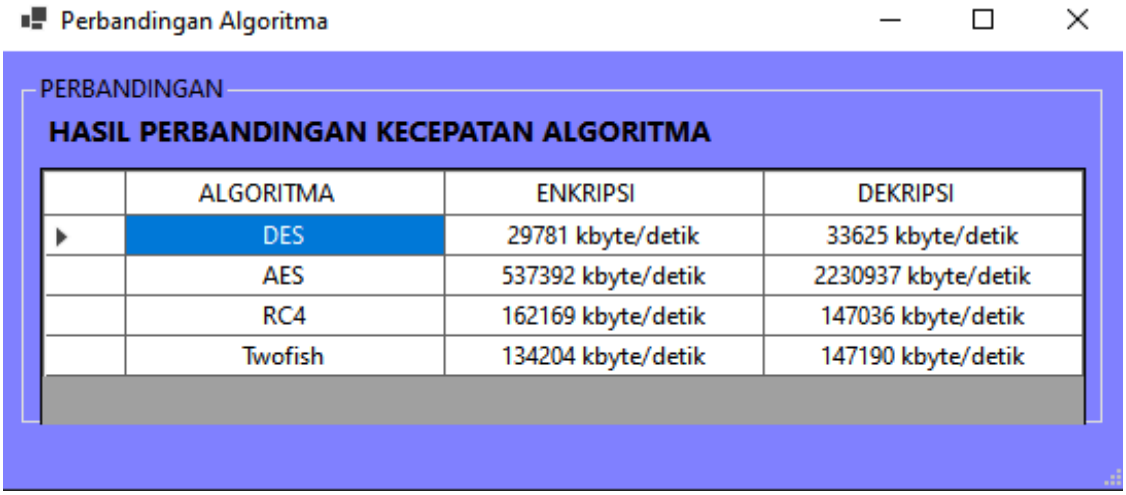

Figure 11. Display of the Type of Motif Form

c. Validity Testing

This validity testing aims to ensure that the developed application functions properly and also to validate the proposed hypothesis. The author used two methods to test the validity of this application: by measuring the speed of the encryption and decryption processes, as well as the size of the file generated after the process is completed.

The testing was carried out using various types of files with different sizes. The details of the test files can be seen in **Table 1.**

Table 1. List of Application Test Files

No	Nama File	Tipe File	Ukuran (byte)
1	BAB I.doc	Microsoft Office Word Document (.doc)	110.592
2	BAB I.pdf	PDF Document (.pdf)	77.824
3	BAB I.txt	Text Document (.txt)	8.192
4	Enkripsi-Dekripsi.exe	Application (.exe)	405.504
5	Enkripsi-Dekripsi.rar	WinRAR archive (.rar)	86.016
6	Enkripsi-Dekripsi.zip	WinRAR ZIP archive (.zip)	114.688
7	logo.bmp	BMP File (.bmp)	69.632
8	logo.gif	GIF File (.gif)	12.288
9	logo.jpg	JPG File (.jpg)	24.576
10	logo.png	PNG File (.png)	45.056
11	olah data.xls	Microsoft Office Excel Worksheet (.xls)	69.632
12	Pororo.mp4	MPEG-4 File Format (.mp4)	13.885.440
13	Tom and Jerry.flv	Flash Video File (.flv)	21.344.256

Using the various types of files above, the encryption and decryption testing process was carried out using the DES, AES, IDEA, Blowfish, RC4 and Twofish algorithms. The results of these tests can be seen in **Table 2.**

Table 2. Results of Program Implementation Testing

RC4	Doc	110.592	1.269	110.592	1.206
	Pdf	77.824	1.269	77.824	1.206
	Txt	8.192	1.269	8.192	1.206
	Exe	409.600	1.269	405.004	1.206
	Rar	409.600	1.269	409.600	1.206
	Zip	409.600	1.269	114.688	1.206
	Bmp	69.632	1.269	69.632	1.206
	Gif	69.632	1.269	12.288	1.206
	Jpg	24.576	1.269	24.576	1.206
	Png	69.632	1.269	45.056	1.206
	Xls	69.632	1.269	69.632	1.206
	Mp4	13.885.440	1.269	13.885.440	1.206
	Flv	21.344.256	1.269	21.344.256	1.206
Rata-rata		2.804.066	1.269	2.804.066	1.206
Twofish	Doc	110.592	1.364	110.592	1.333
	Pdf	77.824	1.364	77.824	1.333
	Txt	8.192	1.364	8.192	1.333
	Exe	409.600	1.364	405.004	1.333
	Rar	409.600	1.364	409.600	1.333
	Zip	409.600	1.364	114.688	1.333
	Bmp	69.632	1.364	69.632	1.333
	Gif	69.632	1.364	12.288	1.333
	Jpg	24.576	1.364	24.576	1.333
	Png	69.632	1.364	45.056	1.333
	Xls	69.632	1.364	69.632	1.333
	Mp4	13.885.440	1.364	13.885.440	1.333
	Flv	21.344.256	1.364	21.344.256	1.333
Rata-rata		3.440.737	1.364	3.440.737	1.333

Algoritma	Tipe File	Ukuran (byte)	Enkripsi	Ukuran (byte)	Dekripsi
			Kecepatan		Kecepatan
DES	Doc	110.592	531	110.592	515
	Pdf	77.824	484	77.824	430
	Txt	8.192	764	8.192	2.215
	Exe	409.600	492	405.004	1.945
	Rar	86.016	484	86.016	1.996
	Zip	114.688	484	114.688	1.622
	Bmp	69.632	437	69.632	421
	Jpg	24.576	436	24.576	1.159
	Png	69.632	482	69.632	1.248
	Xls	69.632	469	69.632	1.468
	Mp4	13.885.440	1.819	13.885.440	159.563
	Flv	21.344.256	2.776	21.344.256	291.465
Rata-rata		2.789.061	3.979	2.788.746	2.804
AES	Doc	110.592	390	110.592	515
	Pdf	77.824	490	77.824	490
	Txt	8.192	893	8.192	2.215
	Exe	409.600	539	405.004	624
	Rar	409.600	539	409.600	469
	Zip	409.600	539	114.688	395
	Bmp	69.632	372	69.632	372
	Gif	69.632	372	12.288	390
	Jpg	24.576	405	24.576	406
	Png	69.632	405	45.056	400
	Xls	69.632	372	69.632	392
	Mp4	13.885.440	5.876	13.885.440	6.834
	Flv	21.344.256	8.273	21.344.256	8.456
Rata-rata		3.440.737	1.465	3.440.737	1.506

The speed of data encryption and decryption can not only be measured manually, but also using benchmarking techniques. This technique is a built-in feature in the application designed to measure the encryption and decryption speed of each algorithm in kilobytes per second.

In this benchmarking technique, the data is first buffered into memory with a size of 1,000,000 bytes (approximately 1 GB). The results of this test provide more detailed information, as shown in the following illustation:

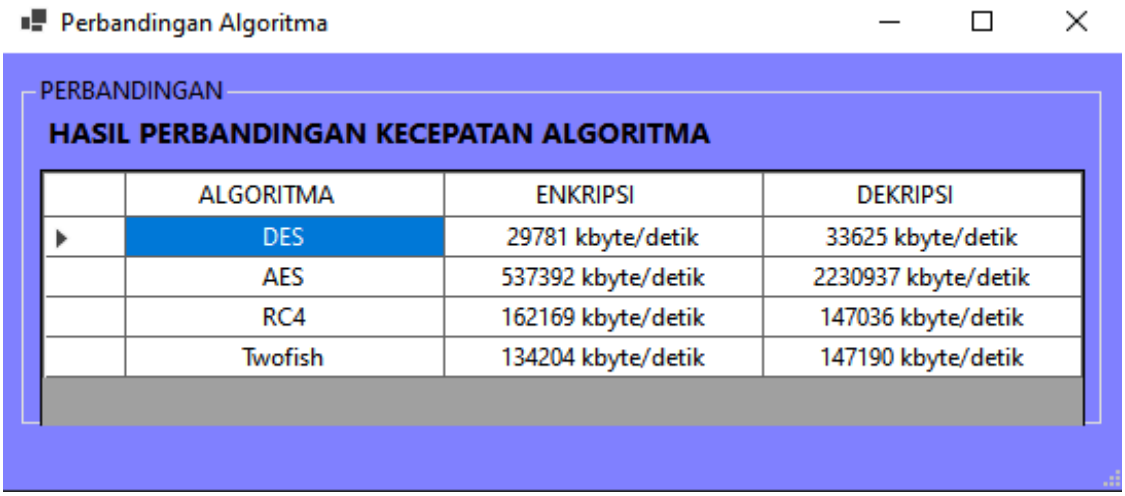

Figure 14. Benchmarking Results of Data Encryption and Decryption Speed Comparison

Based on the testing results using the algorithm comparison form, the encryption and decryption process speeds of the two algorithms can be summarized as presented in **Table 3.**

Table 3. Results of Algorithm Speed Comparison Analysis

Agloritma	Enkripsi (Kbyte/detik)	Dekripsi (Kbyte/detik)
Des	402	608
AES	1.508	1.443
IDEA	173	57
Blowfish	1.063	1.075
RC4	1269	1206
Twofish	1364	1333

Based on the results of the decryption speed comparison analysis of the four algorithms, it can be observed that the AES algorithm has the highest speed percentage at 45%, followed by Blowfish at 34%, DES at 19%, and finally the IDEA algorithm, which only reaches 2%. Therefore, it can be concluded that the AES algorithm is the fastest in the encryption and decryption processes compared to the other three algorithms. The speed ranking is as follows: AES first, followed by Blowfish, DES, and lastly, IDEA.

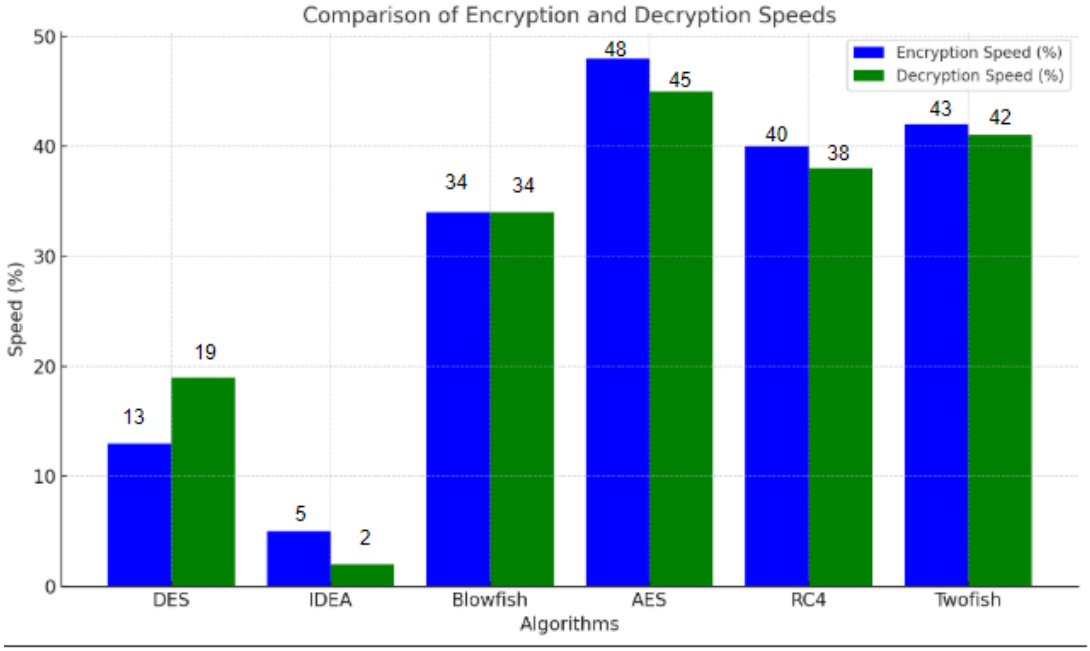

Table 4. Comparison of Encryption and Decryption Speeds of Cryptographic Algorithms

4. Conclusion

The DES algorithm is faster than IDEA, with an encryption speed of **13%** and decryption speed of **19%**, compared to IDEA's encryption speed of **5%** and decryption speed of **2%**.Blowfish outperforms DES, achieving **34%** for both encryption and decryption speeds, while DES achieves an encryption speed of **13%** and decryption speed of **19%**. AES shows better performance than Blowfish, with an encryption speed of **48%** and decryption speed of **45%**, compared to Blowfish's **34%** for both processes. AES significantly outperforms IDEA, with AES reaching **48%** encryption speed and **45%** decryption speed, while IDEA achieves only **5%** encryption speed and **2%** decryption speed. RC4 has an encryption speed of 40% and a decryption speed of 38%, while Twofish has an encryption speed of 43% and a decryption speed of 42%.

Twofish outperforms RC4. AES achieves an encryption speed of 48% and a decryption speed of 45%, compared to RC4's 40% encryption and 38% decryption speeds. AES is superior in encryption and decryption speed. Blowfish achieves 34% for both encryption and decryption speeds, whereas RC4 achieves 40% for encryption and 38% for decryption. RC4 outperforms Blowfish in both encryption and decryption speeds.RC4 shows better performance compared to DES, with an encryption speed of 40% and decryption speed of 38%, while DES achieves 13% for encryption and 19% for decryption. RC4 outperforms IDEA with an encryption speed of 40% and a decryption speed of 38%, compared to IDEA's 5% encryption speed and 2% decryption speed. AES shows better perfomarnce compared to Twofish with an encryption speed of 48% compared to 45%, and a decryption speed of 45% compared to 42%.

Twofish outperforms Blowfish, achieving an encryption speed of 43% compared to 34% and a speed of decryption 42% compared to 34%. Twofish outperforms DES, with an encryption speed of 43% compared to 13% and a decryption speed of 42% compared to 19%. Twofish demonstrates a significant advantage over IDEA, with an encryption speed of 43% compared to 5% and a decryption speed of 42% compared to 2%. This comparison highlights that both RC4 and Twofish have notable advantages in performance over other algorithms in specific areas.

Refrences

[1] Widyawan, D., & Imelda, I. (2021). Pengamanan File Menggunakan Kriptografi Dengan Metode Aes-128 Berbasis Web Di Komite Nasional Keselamatan Transportasi. *Skanika*, *4*(1), 15–22. https://doi.org/10.36080/skanika.v4i1.2216

[2] Rediansyah, S., Shita, R. T., & ... (2023). Pengamanan File Berbasis Web Dengan Menerapkan Algoritme Aes-128 Pada Pt. Samudra Katulistiwa Nusantara. *Prosiding Seminar …*, *2*(April), 166–174.

[3] Siswanto, S., Saputro, A., Utama, G. P., & Prasetyo, B. H. (2021). Penerapan Algoritma Kriptografi Twofish Untuk Mengamankan Data File. *Bit (Fakultas Teknologi Informasi Universitas Budi Luhur)*, *18*(1), 9–18. https://doi.org/10.36080/bit.v18i1.1446

[4] Firdaus, R., & Santika, R. R. (2022). Penerapan Algoritma AES-128 Untuk Enkripsi Dokumen Di PT Caveo Biometric Security. *Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI) Universitas Budi Luhur*, *September*, 111–120.

[5] Simbolon, I. A. R., Gunawan, I., Kirana, I. O., Dewi, R., & Solikhun, S. (2020). Penerapan Algoritma AES 128-Bit dalam Pengamanan Data Kependudukan pada Dinas Dukcapil Kota Pematangsiantar. *Journal of Computer System and Informatics (JoSYC)*, *1*(2), 54–60.

[6] Ignasius, A., & Shaka Yudha Sakti, D. V. (2022). Penerapan Algoritma Aes (Advance Encryption Standart) 128 Untuk Enkripsi Dokumen Di Pt. Gunung Geulis Elok Abadi. *Skanika*, *5*(1), 1–10. https://doi.org/10.36080/skanika.v5i1.2118

[7] Nugroho, A. P., & Suseno, H. B. (2020). Keamanan Data Transaksi Nasabah Pada Aplikasi Bank Sampah Berbasis Web Menggunakan Algoritma AES. *"QUERY: Jurnal Sistem Informasi Keamanan Data Transaksi Nasabah Pada Aplikasi Bank Sampah Berbasis Web Menggunakan Algoritma AES.," 04*(April), 9–17.

[8] Cristy, N., & Riandari, F. (2021). Implementasi Metode Advanced Encryption Standard (AES 128 Bit) Untuk Mengamankan Data Keuangan. *Jurnal Ilmu Komputer Dan Sistem Informasi (JIKOMSI)*, *4*(2), 75–85.

[9] Setiawan, A., & Fatimah, T. (2021). Implementasi Algoritma Kriptografi Rc4 Untuk Keamanan Database Aplikasi Penggajian Karyawan Berbasis Web Pada Pt. Trans Intra Asia. *Skanika*, *4*(1), 66–71. https://doi.org/10.36080/skanika.v4i1.2044

[10] Tambunan, H. S., Gunawan, I., Novica Aswita, R. S., Nasution, Z. M., & Sumarno, S. (2021). Implementasi Algoritma Aes & Rc4 Terhadap Keamanan Data Produk Benih Sayuran di PT. Ewindo. *Jurnal Sosial Sains*, *1*(6), 461–468. https://doi.org/10.59188/jurnalsosains.v1i6.126

[11] Setti, S., Gunawan, I., Damanik, B. E., Sumarno, S., & Kirana, I. O. (2020). Implementasi Algoritma Advanced Encryption Standard dalam Pengamanan Data Penjualan Ramayana Department Store. *JURIKOM (Jurnal Riset Komputer)*, *7*(1), 182. https://doi.org/10.30865/jurikom.v7i1.1960

[12] Pseudocode, J., Efendi, R., & Susilo, B. (2016). *Vigenere Cipher Dalam Aplikasi*. *III*, 69–82.

[13] Rahman, A. U., Miah, S. U., & Azad, S. (2014). Advanced encryption standard. *Practical Cryptography: Algorithms and* Arif, Z., & Nurokhman, A. (2023). Analisis Perbandingan Algoritma Kriptografi Simetris Dan Asimetris Dalam Meningkatkan Keamanan Sistem Informasi. *Jurnal Teknologi Sistem Informasi*, *4*(2), 394–405. https://doi.org/10.35957/jtsi.v4i2.6077

[14] Fitriana, R. N., & Djuniadi, D. (2022). Analisis Perbandingan Algoritma AES Dan RC4 Pada Enkripsi dan Dekripsi Data Teks Berbasis CrypTool 2. *Systemic: Information System and Informatics Journal*, *7*(2), 1–7. https://doi.org/10.29080/systemic.v7i2.1263

[15] Schneier, B., Kelsey, J., Whiting, D., Wagner, D., & Hall, C. (1998). Twofish : A 128-Bit Block Cipher. *NIST AES Proposal*, *15*(1), 1–27.