ALGEBRA : JURNAL PENDIDIKAN, SOSIAL DAN SAINS

ISSN : 2807-663X e-ISSN : 2807-629X
Journal Homepage : https://algebra.yana.or.id/index.php/ejournal/index
Volume 6 Number 2 (2026)

COMPARATIVE ANALYSIS OF TWOFISH AND BLOWFISH ALGORITHMS IN SECURING CSV (COMMA SEPARATED VALUES) DATA

Rizki Ali Akbar Pasaribu[1], Abdul Halim Hasugian[2], Aidil Halim Lubis[3]
[123]Program Studi Ilmu Komputer, Fakultas Sains dan Teknologi, Universitas Islam Negeri Sumatera Utara, Medan, Indonesia
Correspondence Email: innet71050500@gmail.com

ABSTRACT

Data security is a crucial aspect in the digital era, especially for the CSV (Comma Separated Values) data format, which is frequently used for data storage and exchange. This study aims to analyze and compare the performance of the Twofish and Blowfish cryptographic algorithms in securing CSV data. The analysis is based on three main parameters: encryption time, decryption time, algorithm security level, and changes to the encrypted or decrypted *file*s. The Twofish algorithm is known for its Feistel structure and its flexibility with key sizes up to 256 bits, while Blowfish uses a variable key size up to 448 bits with a simple Feistel structure. The results show that Blowfish has higher encryption and decryption speeds than Twofish, with an average speed of around 275.85 ms for Blowfish and 655.672 ms for Twofish. However, Twofish excels in security. This study is expected to serve as a reference in selecting the right algorithm for securing CSV data based on specific user needs, both in terms of speed and security.

Keywords: *Twofish* Algorithm; *Blowfish* Algorithm; data security; CSV; encryption.

INTRODUCTION

Text is a collection of symbols or characters that form words, sentences, paragraphs, or written documents (Nino, 2023). Text can be handwritten, printed, or electronic documents that can be read by humans, making it easier for someone to clearly understand the information conveyed. This is what makes text much better at conveying information compared to videos or recorded sounds, where the measure of clarity of the information conveyed is the clarity of a person's vocals (Manik & Juanfernando, 2023). Text is used to communicate ideas, information, and messages between people. In the context of computers, text also refers to data in the form of characters that can be processed by computer programs (Ramadhani et al., 2025).

Texts can have a wide variety of functions and styles. Their functions can vary, from providing information, entertaining, instructing, or conveying persuasive messages. Text styles can also vary, including formal, informal, scientific, narrative, or technical styles, depending on the purpose and context of their use (Rahayu et al., 2024). In the digital world, text is also often used in the form of short messages such as SMS, instant messages, or posts on social media. Furthermore, text is also used in the creation of web content, e-books, articles, reports, and much more (Suhelna, 2020).

In today's digital era, humans are highly dependent on technology. This is indicated by the fact that almost all human activities are inseparable from technology. For example, when someone wants to convey information, they can simply use an application, or when someone wants to find out the latest information, they can simply visit the many news sites they find. When we surf the internet, but with the ease of accessing information, people will also easily gain access to our personal data (Kurniawan et al., 2024). Of course, this is one of the negative impacts of today's technological age, so we need to maintain data security and privacy so that people cannot find out the information or sensitive data that we have (Asmawi, 2020).

To maintain the confidentiality and security of important information contained in a text, a technique is required, namely text encryption (Cryptography) (Soesanto Edy et al., 2024). Text encryption refers to the process of converting the original text into a form that cannot be understood by people who do not have the correct cipher key. In text encryption, the original text is changed using a specific algorithm to produce text that can only be decrypted by recipients who have the correct cipher key (Elvira Awal et al., 2022). used in various fields, including military security, finance, and information technology. Text encryption is also used in everyday applications such as email, text messaging, and online data transmission. Text encryption is a very important technique in maintaining the security and confidentiality of text data (Praptodiyono et al., 2021). By using this technique, text data can be kept secure and prevent unauthorized access from unauthorized parties. Text encryption also plays an important role in maintaining the security and integrity of information in the digital era (Sudrajat Puji Sutan et al., 2020).

Based on previous Twofish algorithm research by (Siswanto et al., 2023). With the title "Application of Twofish Cryptography Algorithm to Secure File Data" discusses the method of securing text in sensitive and important files because of frequent changes and manipulation of file contents, the author's goal in his research is to develop an application that uses Twofish cryptography techniques to encrypt file data, preventing careless people from knowing reports that will be sent from branches to the center. A total of 15 encrypted files were used in the trial, and the average size of the encrypted files was 0.11% larger. The encryption procedure took 9.5352 milliseconds, and the decryption process took 9.3294 milliseconds.

Based on previous Blowfish algorithm research by Ngarap Imanuel Manik and Hendrikus Juan Fernando with the title "Blowfish Algorithm Application Program on File Data Security System" Discusses How the Blowfish algorithm secures a data file which is obtained by applications that work with various data files, such as text, sound, video, and so on. The data can then be disguised and returned to its original state, and the larger the data file, the longer it takes to run the encryption and decryption process. This allows for the achievement of the expected results quite well and the smooth operation of the application program design.

Both the Twofish and Blowfish algorithms have been widely used for data security, particularly in cellular network communications, electronic banking procedures, and voice message encryption, among other fields. Both techniques utilize symmetric keys, block ciphers, Fiestel networks, and S-boxes, among other things (Ikhsan Rifki & Syamia, 2024). This leads to conflict between the Blowfish and Twofish algorithms in terms of how well the encryption and decryption processes assess time performance. Therefore, the authors conducted a study entitled "Comparative Analysis of the Twofish and Blowfish Algorithms in Securing CSV (Comma Separated Values) Data."

RESEARCH METHODS

The type of research used in this study is a system development method using the Waterfall model approach (Yulia Sari et al., 2020). This method is used to develop a specific product through sequential stages, including planning, literature study, system design, implementation, and testing, as well as to evaluate the effectiveness of the developed system (Ronaldo Praja Saputra et al., 2022). By digging up information obtained from data security, the researcher carried out a planning stage that identified a data security problem and in this final assignment the problem that will be identified is to conduct an analysis study of the Twofish and Blowfish algorithms to be implemented in text encoding. The text that will be encoded is data whose file format type is .csv.

This step involves conducting library research to obtain the necessary advanced theories. Before studying library materials related to the Twofish and Blowfish algorithms, CSV text, and the Typescript programming language, this study sought to gather basic knowledge that would be used in the research as well as information in the preparation stage of this study (Putra et al., 2022). At this stage, the system to be built was designed; the purpose of this system design was to obtain an overview of how the system would operate (Nasution & Tommy, 2026). The implementation stage is the stage where the system design that has been built is formed into a program. In creating the program, the researchers used the programming language Typescript (Rusli Mulyadi & Sany Ezrifal, 2021).

Next, a testing phase is carried out on the system that has been implemented to determine whether the encryption and decryption processes are running well or not with Black-box testing. Black-box testing itself is a test that focuses on the input (files to be encrypted) and output (results of files that have been encrypted) in the application and ensures that the results produced are as expected so that the program can be considered correct if it produces the correct output. If it is not appropriate, improvements are made until the program produces the correct output (Siswanto et al., 2021). The results obtained in this study are a comparison of the level of effectiveness between the two cryptographic algorithms, namely Twofish and Blowfish with the typescript programming language, while the level of effectiveness in question is the speed of the algorithm in terms of encrypting and describing CSV text.

RESULTS AND DISCUSSION

In the system design implementation phase, the researchers created a program based on their previous design, specifically the encryption and decryption processes for both the Twofish and Blowfish algorithms in a CSV file, where the values contained only strings and no other values.
For more details, see Figure 1.

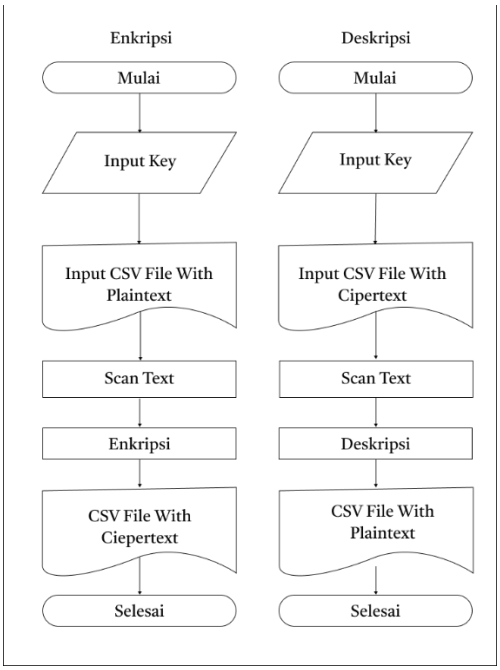


Figure 1. Rancangan Sistem

The application that has been built is then tested using the Black Box method which can be seen in Table 1.

Table 1. Aplication Test

No	Components	Tested Expected Result	Conclusion
1	Home Page	The application displays the main page on the web browser.	Success
2	Input *Key*	The application can accept key input from the user.	Success
3	Input *Algorithm*	The application displays the Blowfish and Twofish Algorithm options.	Success
4	Input *Type*	The application displays the Encrypt and Decrypt options.	Success
5	Input *File*	The application can specify which files to select.	Success

There are several differences between the Twofish algorithm and the Blowfish algorithm which can be seen in Table 2.

Table 2. Differences between the Twofish Algorithm and the Blowfish Algorithm

Components	Blowfish Algorithm	Twofish Algorithm
Year Created	1993	1997
Creator	Bruce Scheneier	
Comparison Algorithm	DES	AES
Block Length	64 bit	128 bit
Key Length	32 – 448 bit, kelipatan 8 bit	128, 192, 256 bit
Transformation Pseudo-Hadamard	No	Yes
Expansion and Filter	No	Yes
MDS Box	No	Yes
Iteration	16 Iteration	
License	Open	

Since the Blowfish and Twofish algorithms use Feistel networks and S-boxes in their implementation, the security level of these algorithms is also influenced by how the key is scheduled internally and how the S-boxes are created. The security level of cryptographic algorithms with symmetric keys or the same key during encryption and decryption can be measured by the level of algorithm complexity, the block length used, the key length used, and the level of randomness of the plaintext against the encrypted text (Rifaldy et al., 2026). can be clearly seen in Table 3.

Table 3. Security Level of Twofish Algorithm and Blowfish Algorithm

Components	Twofish Algorithm	Blowfish Algorithm
Algorithm	16 rounds; using Feistel network, S-box, MDS matrix, Pseudo Hadamard Transform (PHT) technique, and whitening technique; using addition, XOR, and combination operations of several algebraic complexes	16 rounds; using Feistel network and S-box; using addition, and XOR operations
Degree of Randomization	It is very complicated, because it uses a 16-round Feistel network, 4 key-dependent S-boxes, MDS matrix, PHT technique, whitening technique.	It's complicated, because it uses a 16-turn Feistel network and 4 key-dependent S-boxes.
Key Scheduling	Internal key scheduling depends on external key generation methods using XOR addition operations, vector algebra, polynomial algebra, and MDS matrices.	Internal key scheduling depends on external key generation method using addition and XOR operations.

To test the Twofish and Blowfish algorithms, the researcher used an application that had been created previously with the same key, namely "RIZKI", so the data obtained were as in Table 4 and Table 5.

Tabel 4. Encryption Process Speed of Twofish and Blowfish Algorithms

No	*File* Size (Bytes)	Twofish Encryption Time (ms)	Blowfish Encryption Time (ms)
1	910,480	47215	495
2	373,927	20311	155
3	568,959	31389	294
4	185,766	10803	116
5	546,145	28310	325
6	388,630	20311	166
7	678,208	37245	397
8	758,897	41701	395
9	683,360	37518	327
10	171,515	8924	71

Tabel 5. Twofish and Blowfish Decryption Process Speed

No	*File* Size (Bytes)	Twofish Decryption Time (ms)	Blowfish Decryption Time (ms)
1	1,368,789	58317	522
2	559,248	27686	153
3	853,531	36034	324
4	279,967	13064	75
5	823,230	37498	294
6	583,585	29104	229
7	1,012,684	41477	370
8	1,141,374	50599	364
9	1,036,260	37690	338
10	255,448	10676	107

Based on the data obtained in Table 4 and Table 5, it can be seen that the Blowfish algorithm is very fast in terms of encryption and decryption of CSV files, where during the encryption process for 10 different files, the average time obtained was 291ms and the average decryption time was 250ms, while the Twofish algorithm is very slow during the encryption process, namely requiring an average time of 29268ms and during the decryption process, requiring an average time of 32017ms.

In this section, researchers examine the differences in file sizes generated by the Twofish and Blowfish algorithms. This analysis is expected to provide an overview of the advantages and disadvantages of each algorithm in terms of data storage efficiency. As before, the authors used the same key for both algorithms, "RIZKI."

Tabel 6. File Size After Twofish and Blowfish Algorithm Encryption

No	*File* Size (Bytes)	Size Encryption *Towfish* (Bytes)	Size Encryption *Blowfish* (Bytes)
1	910,480	1,362,989	1,374,589
2	373,927	558,646	559,850
3	373,927	853,449	853,612
4	185,766	279,092	280,842
5	546,145	819,384	827,076
6	388,630	580,882	586,287
7	678,208	1,012,314	1,013,054
8	758,897	1,138,833	1,143,914
9	683,360	1,033,860	1,038,660
10	171,515	254,712	256,183

Tabel 7. File Size Against Key Length Encryption Process

No	*File* Size (Bytes)	Kunci	Size Enkripsi *Towfish* (Bytes)	Size Enkripsi *Blowfish* (Bytes)
1	373,927	R	557,625	561,139
2	373,927	Rizki	554,116	563,262
3	373,927	Rizki ali	563,236	565,936
4	373,927	Rizki ali akbar	561,621	564,838
5	373,927	Rizki Pasaribu ali	560,722	554,262
6	373,927	Pasaribu1234556771	566,051	564,930
7	373,927	@&!#@&#@(&(*!@#	563,548	559,053
8	373,927	12345678901234567890	558,317	564,043
9	373,927	###@@@@!!!!!!!!!!!!!!	558,346	560,601
10	373,927	12312@131Rizki123!@#	563,087	570,393

Based on the data obtained in Table 6, the results of the difference in file size in the encryption process using the Twofish and Blowfish algorithms with the key "RIZKI" are obtained, namely the average file size that changes is 561,756. Bytes and in Table 7 it is also obtained that the key length can also affect the file size during the encryption process in both algorithms Twofish and Blowfish where the longer the key, the time required for encryption and decryption will be longer and vice versa where the shorter the key, the time required will be faster but in terms of security, short keys will be easy to brute force

CONCLUSIONS

Based on the research results, a comparison between the Twofish and Blowfish algorithms shows that both cause a change in CSV file size of about 50% (Twofish 50.3% and Blowfish 50.7%), but both have contrasting advantages in other aspects. Twofish offers a higher level of security due to its more complicated and complex encryption process, while Blowfish is far superior in terms of time efficiency with an average speed of 275.85 ms, much faster than Twofish which takes 655.672 ms. In conclusion, Twofish is the best choice for security aspects, while Blowfish is the ideal solution for data processing speed.

BIBLIOGRAPHY

Asmawi. (2020). Aplikasi Penyandian Record Menggunakan Metode Twofish. *JUKI : Jurnal Komputer Dan Informatika*, *2*(2), 72–84.

Soesanto Edy, Rohmawatii Afifah, Anggraini Sherly Ninda, Hanifah Nur Saefani, & Handina Wardhani Vyandha Angelisa. (2023). Analisis Pengimplementasian Objek Vital Nasional, Pengamanan File, dan Cyber Security pada PT. Angkasa Pura. *Indonesian Journal Of Multidisciplinary*, *1*(1), 218–224.

Elvira Awal, E., Haodudin Nurkifli, E., & Nur Padilah, T. (2022). Analisis Perbandingan Hasil Enkripsi Dan Dekripsi Algoritma Kriptografi Rijndael dan Twofish Untuk Penyandian Data. *Jurnal Mahasiswa Ilmu Komputer (JMIK)*, *3*(1), 260–265.

Ikhsan Rifki, M., & Syamia, N. (2024). Message Security Application Using Mobile-Based AES Algorithm. *Journal of Computer Science, Information Technology and Telecommunication Engineering*, *5*(2), 595–606. https://doi.org/10.30596/jcositte.v5i2.20834

Kurniawan, C., Mochammad Fadhli MS, & Fauziah. (2024). ANALISIS PERBANDINGAN RUANG DAN WAKTU ALGORITMA ENKRIPSI BLOWFISH DAN TWOFISH PADA ENKRIPSI DAN DESKRIPSI BERKAS MENGGUNAKAN MODUL PYTHON. *Jurnal Teknik Elektro Dan Informatika*, *19*(1), 7–14.

Manik, N. I., & Juanfernando, H. (2023). Ciptaan disebarluaskan di bawah Lisensi Creative Commons Atribusi 4.0 Internasional. Program Aplikasi Algoritma Blowfish Pada Sistem Keamanan Data File Blowfish Algorithm Application Program For Data File Security Systems. *Journal of Information System, Applied, Management, Accounting and Research*, *7*(1), 10–21. https://doi.org/10.52362/jisamar.v7i1.984

Nasution, R. A., & Tommy. (2026). Analisis Performa Kecepatan Enkripsi File Video Menggunakan Algoritma DSA dan Twofish Berbasis Web. *Jurnal Komputer Teknologi Informasi Sistem Informasi (JUKTISI)*, *4*(3), 2068–2075. https://doi.org/10.62712/juktisi.v4i3.520

Nino, B. E. (2023). Perbandingan Performa Algoritma AES dan Twofish Menggunakan Metode Strict Avalanche Criterion pada Nomor Induk Kependudukan Indonesia. *Jurnal Teknologi Informasi*, *9*. https://ejournal.urindo.ac.id/index.php/TI

Siswanto, U., Dias Amsari, F., Prasetyo, B. H., Pramusinto, W., Utama, G. P., & Anif, M. (2021). *Pengamanan File Audio Menggunakan Algoritma Kriptografi Blowfish*. 262–269.

Praptodiyono, S., Muhammad, F., & Wiriyadinata, D. (2021). Analysis security system performance MIPv6 in signaling process using AES and Twofish algorithms. *Teknika: Jurnal Sains Dan Teknologi*, *17*(2), 158. https://doi.org/10.36055/tjst.v17i2.13069

Putra, Z., Abdullah, D., Dwika Putra, E., & Darmi, Y. (2022). Implementation of Blowfish Algorithm for Encryption and Decription on Android-Based QR Code Implementasi Algoritma Blowfish untuk Enkripsi dan Dekripsi pada QR Code Berbasis Android. *JURNAL KOMITEK*, *2*(2), 451–460. https://doi.org/10.53697/jkomitek.v2i2

Rahayu, A., Ardana, A. P., Pramudhita, C., Syafitri, D., & Sirega, R. Z. (2024). Perbandingan Algoritma RSA dengan Algoritma Blowfish Pada Perancangan Aplikasi Keamanan Data. *Jurnal Ilmu Komputer Dan Sistem Informasi (JIKOMSI*, *7*(1), 203–207.

Ramadhani, D. E., Nurul Sabrina, P., & Ashaury, H. (2025). Implementasi Algoritma Enkripsi Blowfish dan Rijndael dalam Pengamanan File Text. *JURNAL LOCUS: Penelitian & Pengabdian*, *4*(6), 7534–7544. https://locus.rivierapublishing.id/index.php/jl

Rifaldy, F., Limbong, H. P., Firjatullah, M., Gading, R. A., Prayoga, I., & Rusydi, I. (2026). PERBANDINGAN ALGORITMA DES, AES, IDEA, DAN BLOWFISH BERDASARKAN PANJANG KUNCI DAN CIPHERTEXT SEBAGAI INDIKATOR KEAMANAN DATA. *JORAPI : Journal of Research and Publication Innovation*, *4*(1).

Ronaldo Praja Saputra, Wahyudi, J., & Jumadi, J. (2022). Comparative Analysis of the Blowfish Algorithm and the Des Algorithm in the Document File Encryption and Decryption Process. *JURNAL KOMITEK*, *2*(2), 605–612. https://doi.org/10.53697/jkomitek.v2i2

Rusli Mulyadi, & Sany Ezrifal. (2021). *Algoritma Dan Pemograman I*. Pusat Pengembangan Pendidikan dan Penelitian Indonesia.

Siswanto, Muhammad Akbar, M. Anif, Ari Saputro, Subandi, & Basuki Hari Prasetyo. (2023). Implementasi Algoritme Twofish Untuk Melindungi Laporan Keuangan Bimba AIUEO. *SKANIKA: Sistem Komputer Dan Teknik Informatika*, *6*(6), 148–157.

Sudrajat Puji Sutan, R., Cahya Prihandoko, A., & Diksy Media Firmansyah, D. (2020). Analisis Perbandingan Kinerja Algoritma Kriptografi Serpent dan Twofish pada Dataset World Bank Projects and Operations. *BERKALA SAINSTEK 2020*, *8*(3), 65–74.

Suhelna, Y. (2020). Perancangan Aplikasi Penyandian Pesan Teks dengan Menggunakan Algoritma Digraph Cipher. *JUKI: Jurnal Komputer Dan Informatika*, *2*.

Yulia Sari, E., Ahmad Rifki Harir, & Dony Ariyus. (2020). MODIFIKASI HILL CIPHER MOD 36 KOMBINASI TRANSPOSISI DAN XOR KUNCI TABEL PERIODIK DENGAN LSB UNTUK PENYEMBUNYIAN PESAN. *CESS (Journal of Computer Engineering System and Science)*, *5*(5), 38–46.