Jurnal Komputer, Informasi dan Teknologi Vol: 4, No 1, 2024, Page: 1-10

Implementation Of A Combination Of Stream Cipher Algorithm And Rotate 13 For Data Security

Ikhsan Tri Mukrozi [1)*]; Sapri [2)]; Abdussalam Al Akbar [3)]

[1,2,3)] Universitas Dehasen Bengkulu

DOI: https://doi.org/10.53697/jkomitek.v4i1.1727

*Correspondence: Ikhsan Tri Mukrozi
Email: ikhsan@jurnalunived.com

Received: 04-04-2024
Accepted: 15-05-2024
Published: 29-06-2024

Abstract: The issue of data security and confidentiality is one of the important aspects of data, messages and information. Stream Cipher is often referred to as a stream cipher. The advantage of this method is that it is relatively faster in the encryption-decryption process and is also not limited by the length of the plaintext. ROT13 is a substitution cipher encryption by shifting characters forward 13 times, counting 1 character in front of it, and shifting characters based on the order of characters in the ASCII table. By combining the Stream Cipher and ROT13 algorithms, it produces a method that can provide a better level of security compared to the application of each of these methods separately. The results of the analysis and testing carried out using different decryption keys resulted in the ciphertext cannot be returned which shows normal things because the method used is symmetrical cryptography so that the decryption process can only be done using the same key as the key during decryption.

Keywords: *Security, Stream Cipher, ROT13*

Introduction

Current developments in the world of technology and information have had a major impact on data security and confidentiality. Data is an important aspect that contains facts or details of events that have not been or have been processed to become a reliable source. Data can be in the form of numbers, characters, symbols or other signs that can be used as information media. Data security and integration is an important aspect that must be considered and is an important issue and continues to develop along with the progress of the times. These security problems make users have their own needs for data security(Pudi et al., 2017). The need for better data security has given rise to various types of methods and techniques that can be used in data security activities(Noura et al., 2023). There are many ways to protect data from threats from parties who do not have the right to process the document data, and there are quite a few people who have their data read which they do not have the right to. So we need a way to increase the security of the data

on these documents, namely with cryptography. Cryptography is a technique that can be used to secure information. Cryptography has two stages that are commonly carried out, namely the encryption and decryption stages. Encryption is a process carried out to change the original message into cipher text, while decryption is a process carried out to change the encrypted message into a message that can be read and understood.(Ridho et al., 2022).Several cryptographic methods include the Stream Cipher method and the Rotate 13 (ROT 13) method. Stream Cipher operates bit by bit, so in the encryption process there are only two possibilities, namely changing or not changing (Hidayatuloh, Yustantina, & Kusmadi), it is possible that the message to be encrypted can still be known by other people. This can be minimized by combining Stream Cipher encryption results with ROT 13. In the ROT13 coding system, a letter is replaced by a letter in 13 positions. The rot13 method is an encryption method that changes letters into letters that are 13 places away from the original letters (Kurniawan, Mayasari, & Fitriani, 2023; Ding et al., 2019). The combination of these two methods in cryptography is called super encryption which is expected to have good performance in protecting data.

Methodology

Figure 1. Research Stages

Information :

- Identification of problems, At this stage the problem is formulated which will be the object of research. The problem formulation is carried out to determine what problems exist in the research object and provide boundaries for the problems to be researched which focus on document security using Stream Cipher and ROT 13.
- Application of the Method*Stream Cipher,*At this stage, the Stream Cipher and ROT 13 methods are applied to data which is done manually where the process of generating keys, encryption and decryption on documents is calculated in stages to analyze the computing process of the Stream Cipher and ROT 13 methods so that they can help in building applications or systems that will be used to secure data.
- System planning, At this stage, the document security system designed using the Stream Cipher and ROT 13 methods will be built. The process of generating keys, encryption and decryption and the stages are designed using auxiliary diagrams such as flowcharts and interface design.

- Implementation and Testing, Implementation includes installation and development of applications that will be used to secure documents using the Stream Cipher and ROT 13 methods. After the application is built and installed, testing is then carried out by carrying out encryption and decryption experiments on several test data to obtain validation of the functional and output from the application.
- Analysis of output results. This stage is carried out by analyzing and observing the output results of the application being built. The output observed in this activity is the output from the encryption and decryption process of the application being built. The encryption results will be observed to see whether the encrypted data can no longer be recognized or is no longer the same as the original data, while the decryption data is observed to ensure that the decrypted data must match the original data before being encrypted.
- Conclusion: At this stage, conclusions are drawn up from research activities on the implementation of the Stream Cipher and ROT 13 methods on the data. The application output results and other conditions found in the application will be explained in this conclusion section.

Result and Discussion

The application for implementing a combination of the Stream Cipher and Rotate 13 algorithms for file security was built in accordance with the analysis and design as described in the previous chapter, namely the research methodology chapter, so in this section the results of the application built using the design carried out in the previous chapter will be presented(Jiao et al., 2020). In this chapter, discussion will be carried out on the results of the system built, system functionality and analysis of system performance based on the output results produced by the system. The application of a combination of the Stream Cipher and Rotate 13 (ROT13) algorithms successfully encrypted the contents of the document file(Milian & Sulistyo, 2023). The combination of this algorithm is difficult to solve because it uses two keys. The process of securing the contents of a document file by combining the Stream Cipher and ROT13 methods, by encrypting the message in the document file and with a key that has been created as a form of message encoding step. In the first stage, using the Stream Cipher method the message is encrypted, then using the ROT13 method the message is encrypted in one process. In this chapter, discussion will be carried out on the results of the system built, system functionality and analysis of system performance based on the output results produced by the system.In the implementation application of the combination of Stream Cipher and Rotate 13 algorithms for file security, there are several interfaces or interfaces designed to make it easier for users to use or run this application(Risman, 2021). The interface or interfaces are as follows:

Main course

In the main menu display there are three main menus, namely the encryption, decryption and exit menus. The appearance of the main menu can be seen in Figure 2 below:

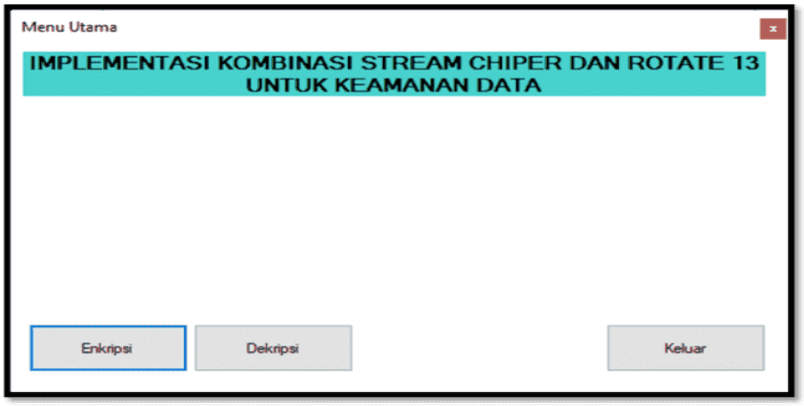

Figure 2 Application Main Menu

Form Encryption

*Form*This is used to encrypt document files entered by the user. The user first opens the plaintext file to be encrypted or directly types the plaintext message to be encrypted in the plaintext column. The appearance of the encryption form can be seen in Figure 3

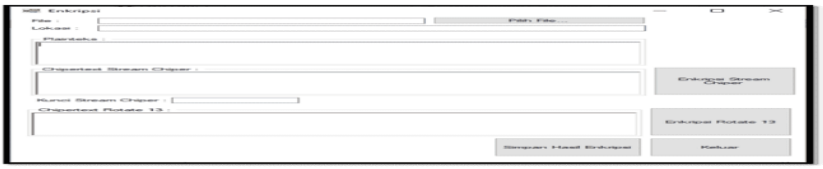

Figure 3 Encryption Form

*Form*Decryption

*Form*This is used to decrypt the ciphertext message entered by the user. The user first opens the ciphertext file that will be decrypted. The appearance of the decryption form can be seen in Figure 4

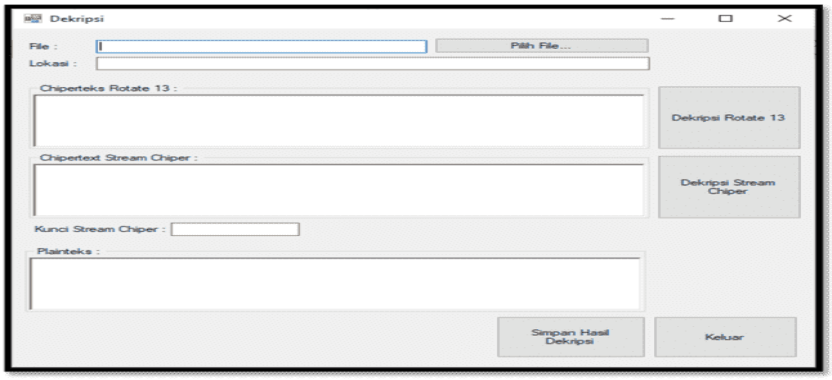

Figure 4 Description Form

Testing Encryption and Decryption of *.docx and Pdf files with the same key

The same key encryption and decryption test is a test where the encryption and decryption processes use the same key. The test uses a file with the docx extension "power of attorney" and the Stream Cipher key "19010160".

Figure 5 Results of the Stream Cipher File Encryption Process *.Docx

The testing process carried out in this research aims to analyze the cryptographic method used to encrypt *.docx and *.pdf files using the Stream Cipher and ROT13 methods. In the first test, where encryption and decryption were carried out with the same key, it could be seen that the encryption and decryption process went very well, where the encrypted ciphertext could be perfectly returned to plaintext. The second test discusses testing encryption and decryption using different keys to see the function of the application if different keys are given during the encryption and decryption process. From the tests carried out by cipherteks, it cannot be returned, which shows that it is normal because the method used in this research is symmetric cryptography so that the decryption process can only be carried out using the same key as the key at the time of decryption.

Black Box Testing

The testing carried out on this application is by using a black box technique. This black box technique is a testing technique that focuses on the output of the response, or simply to find out whether there are errors or functions that do not work as expected. The purpose of this testing is to guarantee that the software built has reliable quality, namely being able to present the main studies of the analysis, design and coding specifications of the software itself. The following is a black box testing table.

Table 1 Black Box Testing

Test Type	Test Description	Test Type

Open	Search for .txt and .docx files	*Black Box*
Encryption	Encryption Process	*Black Box*
Decryption	Dection Process	*Black Box*

Table 2 Test Case Files

File Test Cases			
Input Data	**Which are expected**	**Observation**	**Conclusion**
Enter files	Files can be processed	The file was processed successfully	[x] accepted [ ] rejected
Encryption	The file has been successfully encrypted	The file is successfully changed according to the key used	[x] accepted [ ] rejected
Decryption	The file has been successfully decrypted	The file is successfully returned to plaintext using the same key during encryption	[x] accepted [ ] rejected

Table 4.3 File Test Results

File Test Results			
Input Data	**Which are expected**	**Observation**	**Conclusion**
Enter file.docx	Files can be processed	The file was processed successfully	[x] accepted [ ] rejected
Encryption	The file has been successfully encrypted	the file is successfully changed according to the key used	[x] accepted [ ] rejected
Decryption	The file has been successfully decrypted	The file is successfully returned to plaintext using the same key during encryption	[x] accepted [ ] rejected

Conclusion

Securing document files with the extension *.doc and *.pdf by applying the Stream Cipher and Rotate 13 cryptographic algorithms in document security can be combined well. The encryption process begins first using the Stream Cipher method, then the encryption results are encrypted again using the Rotate13 method so that it becomes safer because it cannot be opened directly through other applications. Implementation of a combination of these methods produces a method that can provide a better level of security compared to implementing each method separately. Encryption and decryption testing uses different keys to see how the application functions if it is given a different key during the encryption and decryption process. From the tests carried out by cipherteks, it cannot be returned, which shows that it is normal because the method used is symmetric cryptography so that the decryption process can only be carried out using the same key as the key at the time of decryption.

References

Alfina, O., & Harahap, F. (2019). Pemodelan Uml Sistempendukung Keputusan Dalam Penentuan Kelas Siswa Siswa Tunagrahita. *METHOMIKA: Jurnal Manajemen Informatika & Komputerisasi Akuntansi*, 143-150.

Dewi, E. (2018). Implementasi Kebijakan Tentang Pengelolaan Perpustakaan Oleh Pegawai Perpustakaan Dalam Upaya Meningkatkan Minat Baca Masyarakat (Studi Analisis di Kecamatan Cijulang Kabupaten Pangandaran). *Jurnal MODERAT*, 60-68.

Ding, L., Liu, C., Zhang, Y., & Ding, Q. (2019). A new lightweight stream cipher based on chaos. *Symmetry*. https://www.mdpi.com/2073-8994/11/7/853

Ekta , N., Christian, A., & Wijaya, K. (2021). Implementasi Metode (User Centered Design) PadaRancang Bangun Sistem Informasi Perpustakaan : Studi Kasus : SMK Negeri 1 Gelumbang. *Jurnal Pengembangan Sistem Informasi dan Informatika*, 69-77.

Gunawan, & Kirman. (2019). Implementasi Algoritma Turbo Boyer Moore Untuk Pencarian Data Pada Transaksi Keuangan Duta Phonecell Sawah Lebar. *Jurnal Media Infotama*, 9-15.

Hidayatuloh, K., Yustantina, & Kusmadi. (2021). Perbandingan Metode Stream Cipher Dan Hill Cipher Dalam Keamanan Data. *Jurnal Infotronik* , 27-31.

Hidayatuloh, K., Yustantina, & Kusmadi. (2021). Perbandingan Metode Stream Cipher Dan Hill Cipher Dalam Keamanan Data. *Jurnal Infotronik*, 27-31.

Jiao, L., Hao, Y., & Feng, D. (2020). Stream cipher designs: a review. *Science China Information Sciences*. https://doi.org/10.1007/s11432-018-9929-x

Kurniawan, D., Mayasari, N., & Fitriani, W. (2023). Perbandingan Algoritma Cipher Dengan Algoritma ROT13 pada proses pengamanan data. *Jurnal darma agung*, 534-541.

Milian, Y. C., & Sulistyo, W. (2023). Model Pengembangan Keamanan Data dengan Algoritma ROT 13 Extended Vernam Cipher dan Stream Cipher. *Jurnal JTIK*. https://www.journal.lembagakita.org/jtik/article/view/716

Mubarak, A. (2019). Rancang Bangun Aplikasi Web Sekolah Menggunakan UML (Unified Modeling Language) Dan Bahasa Pemrograman PHP (Hypertext Preprocessor) Berorientasi Objek. *JIKO (Jurnal Informatika dan Komputer)*, 19-25.

Munandar, A., Rosnelly, R., & Sianturi, C. J. (2020). Rancang Bangun Aplikasi Keamanan Data Teks Menggunakan Algoritma Stream Cipher. *Jurnal FTIK (Fakultas Teknik dan Informatika Komputer)*, 407-416.

Noura, H., Salman, O., Couturier, R., & Chehab, A. (2023). Lesca: Lightweight stream cipher algorithm for emerging systems. *Ad Hoc Networks*. https://www.sciencedirect.com/science/article/pii/S1570870522001718

Pardede, A., Manurung, H., & Filina, D. (2017). Algoritma Vigenere Cipher Dan Hill Cipher Dalam Aplikasi Keamanan Data Pada File Dokumen. *Jurnal Teknik Informatika Kaputama (JTIK)*, 26-33.

Pramudya, E., Hatmi, M., Susanto, A., Mulyono, I., & Muslih. (2020). Kombinasi Algoritma Rot13 Dan Vigenere Cipher Pada Alamat Directory File Untuk Keamanan Dokumen. *Seminar Nasional (SEMNAS) LPPM UNiversitas Muhammadiyah Purwokerto*, 548-555.

Pudi, V., Chattopadhyay, A., & ... (2017). Secure and lightweight compressive sensing using stream cipher. *IEEE*. https://ieeexplore.ieee.org/abstract/document/7948801/

Ridho, A., Mutia, C., & Sinaga, A. P. (2022). Analisis Enkripsi dan Dekripsi Cipher Teks Menggunakan Kombinasi Gronsfeld Cipher Dengan Reverse Cipher. *Jurnal Teknik Informatika Kaputama (JTIK)*, *6*(1).

Risman, R. (2021). Comparison of Performance Rot13 and Caesar Cipher Method for Registration Database of Vessels Berthed at PT Samudera Indonesia. *International Journal of Basic and Applied Science*. https://ijobas.pelnus.ac.id/index.php/ijobas/article/view/61

Sari, D. P., & Saragih, N. E. (2023). Implementasi Algoritma Vigenere Cipher Dan Rot13 Untuk Keamanan Pesan Pada Aplikasi Chatting. *Journal of Informatics and Computers*, 1-8.

Sikumbang, A., Haryanto, E., & Saleh, A. (2020). Kombinasi Metode Stream Cipher Dan Caesar Cipher Dalam Pengamanan Data Kredit Customer. *Jurnal FTIK*, 693-703.

Silalah, L., & Sindar, A. (2020). Penerapan Kriptografi Keamanan Data Administrasi Kependudukan Desa Pagar Jati Menggunakan SHA-1. *Jurnal Nasional Komputasi dan Teknologi Informasi*, 182-186.

Suendri. (2018). Implementasi Diagram UML (Unified Modelling Language) Pada Perancangan Sistem Informasi Remunerasi Dosen Dengan Database Oracle (Studi Kasus: UIN Sumatera Utara Medan). *ALGORITMA: Jurnal Ilmu Komputer dan Informatika*, 1-9.

Ummah, H., Sodikin, I., & Susetyo, J. (2019). Perancangan Sistem Informasi Rental & Inventaris Alat Multimedia Berbasis Web Menggunakan Metode Customer

Relationship ManagemenT. *JURNAL REKAVASI (Rekayasa dan Inovasi Teknik Industri)*, 15-24

W
a
h
y
u
n
i
,

R
.
,

&

I
r
a
w
a
n
,

Y
.

(
2
0
2
0
)
.

A