Journal of Computer Networks, Architecture and High Performance Computing
Volume 6, Number 1, January 2024
https://doi.org/10.47709/cnahpc.v6i1.3298

Submitted : Dec 6, 2023
Accepted : Dec 22,2023
Published : Jan 1, 2024

Electronic Archive Design With Rivest Cipher 4 Cryptographic Based File Security

Sulistiyanto [1)*], Indra Satriadi [2)], Arif Rahman [3)]
[1,2,3)] Informatics Management, Sriwijaya State Polytechnic, Srijaya Street Bukit Besar, Palembang, South Sumatera
[1)] sulistiyanto@polsri.ac.id*, [2)] abididit72@gmail.com, [3)] arif.rahman@polsri.ac.id

ABSTRACT

The transformation of archival document storage systems is starting to shift from physical formats that require a lot of space and storage equipment to the electronic or digital realm (often called electronic archives). This is considered to reduce the costs of procuring equipment and storage space. In line with changes in paperless storage patterns, the issue of data security and confidentiality becomes important, so that information from documents to be archived can be maintained and cannot be used by irresponsible people. One technique for securing documents digitally is to use cryptography and the algorithm chosen is Rivest cipher 4. The RC4 (Rivest Chiper 4) algorithm was chosen because the execution speed in file encryption is faster than other algorithms. This article aims to implement the RC4 algorithm into an electronic archive (e-Archieve) application. The application development method uses the waterfall method with 5 stages. The application was built using the PHP programming language and MySQL database, as well as the Rivest Cipher 4 cryptographic algorithm. The result of the application development is an electronic archive website. Every file uploaded to the server can be encrypted by the admin. Encrypted files will change to random characters like a virus. The application was tested using black box testing techniques, where all features worked as expected.

Keywords: Application**,** Cryptography, E-Archive, Rivest Cipher 4, Security

INTRODUCTION

Archives are records of information that are stored so that they can be retrieved if needed (Nyfantoro et al., 2020). The availability of information can support the achievement of decision-making goals. Another benefit of archives is for learning based on events and mistakes in the past (Dominy, 2017) and as evaluation material for future improvements. Archives that have original and authentic value are stored permanently for long-term preservation to facilitate access to these archives (Balogun, 2018). Technological developments have influenced the archives sector, resulting in changes in perceptions regarding efficiency in the use of archival information as well as changes in managing archives (Nyfantoro et al., 2020). This change in perception has an impact on archive management activities that previously processed printed archive formats into electronic archive formats, which are often called Electronic Filling Systems (EFS).Archiving in print format, in the process, creates limitations and weaknesses. This limitation is the use of physical space to store documents. As documents increase, the need for storage cabinets and physical space is absolutely necessary, making it difficult to save on equipment and supplies (Ngadiyah & Arohman, 2020). Another weakness is that it is time- and space-bound, meaning that archive services are only allowed in the archive room during working hours (Setyawan, 2021). To save equipment and supplies in the long term, it is necessary to transform physical filing into an electronic system. The presence of electronic archives offers a number of conveniences and opportunities for managing them, such as saving storage space and providing wide and free access. Electronic archives also provide significant changes in the ease and speed of sending and sharing compared to physical archives (Yusuf & Zulaikha, 2019).Because

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 6, Number 1, January 2024
https://doi.org/10.47709/cnahpc.v6i1.3298

Submitted : Dec 6, 2023
Accepted : Dec 22,2023
Published : Jan 1, 2024

archives are important documents that are useful and involve a lot of sensitive information, the existence of electronic archives must fulfill three aspects of information security, namely aspects of confidentiality, data integrity, and availability, as well as aspects of authentication of information recipients and aspects of non-repudiation (Febriyani & Arfriandi, 2021; Nadeak, Devani, et al., 2023). Apart from that, electronic archival documents must also meet data security criteria in terms of data integrity, meaning that the documents must maintain the integrity of their data contents from changes made by unauthorized parties. Authentication means that electronic documents must be verifiable and ensure their authenticity, and non-repudiation means that electronic documents must be accountable and their authenticity must be acknowledged without denial (Nadeak, Malahayati, et al., 2023). The increasing issue of document theft (BBC Indonesia, 2022) makes it necessary to provide security for documents that will be uploaded or saved to online storage. To maintain the confidentiality of archival documents, it is necessary to secure electronic archival documents. One way is to carry out the coding (encryption) process of the data contents of archival documents using cryptographic techniques. Cryptography is the science of converting or changing original messages or text called plaintext into scrambled messages or text called cipher text using encryption and decryption processes (Sumarno, 2018). Various cryptography-based file security methods have been widely used, including securing files with AES 192 cryptography (Azhari et al., 2022; Pramusinto et al., 2019); the RSA algorithm (Ihwani, 2016); and the RC4 method (Saragi et al., 2020). Of the many existing encoding algorithms, the RC4 algorithm is considered faster in encryption and decryption processing time than other algorithms (Nugrahani, 2023) because of its simplicity (Watrianthos, 2019).The aim of this research is to build an electronic archive application with the RC4 algorithm as an algorithm for encoding archival documents, so that archival documents that will be entered or uploaded into this application will maintain the authenticity of the data and cannot be changed by illegal parties.

LITERATURE REVIEW

Cryptography

Cryptography comes from the Greek words kryptos and gráphō, which mean "writing hidden". Cryptography is the science that studies how to create a message sent by the sender can be delivered to the recipient safely. Cryptography can fulfill general requirements for a transaction, namely: (1) Confidentiality is guaranteed by encryption (encoding); (2) The integrity of the data is carried out with a one-way hash function; (3) Guarantee of the identity and authenticity of the parties carrying out transactions is carried out using passwords or digital certificates. Meanwhile, transaction data authenticity can be done with a digital signature; (4) Transactions can be used as evidence that cannot be denied (non-repudiation) with utilize digital signatures and digital certificates.

Algoritma Rivest Cipher 4 (RC4)

RC4 is a type of code flow which means the encryption operation is carried out per 1 byte character for one operation. The Rivest Code 4 (RC4) cryptographic algorithm is one of the key algorithms symmetrical made by RSA Data Security Inc (RSADSI) in the form of a stream chipper. This algorithm discovered in 1987 by Ronald Rivest and became a symbol of RSA security (Rivest Shamir Adleman). RC4 uses key lengths from 1 to 256 bytes which are used for initializes a 256 byte long table. This table is used for the next generation of pseudo random which uses XOR with plaintext to produce ciphertext. Each elements in the table are interchanged at least once. RC4 is one of them type of stream cipher, which processes units or input data at one time. In this way encryption or decryption can be carried out at variable length. This algorithm does not have to wait a certain amount input certain data before processing. The RC4 encryption method is very fast, approximately 10 times morefast from DES.

RC4 Stream Cipher algorithm for encryption-decryption:

1. S-Box (Array S) initialization process

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 6, Number 1, January 2024
https://doi.org/10.47709/cnahpc.v6i1.3298

Submitted : Dec 6, 2023
Accepted : Dec 22,2023
Published : Jan 1, 2024

For i = 0 to 255, S[i] = i
2. S-Box (Array K) initialization process
For i = 0 to 255, S[i] = i
3. Then carry out the S-Box randomization step. i=0; j=0
For i= 0 to 255{ j = (j+S [i] + [k] mod 256
Swap S[i] and S[j]}
4. Create pseudorandom bytes, i= (i+1) mod 256
J = (j+S[i]) mod 256
Swap S[i] and S[j]
T=(S[i] + S[j]) mod 256
K=S[t]

State of The Art Method

Cryptography-based digital document security systems have been widely used by researchers, as in research (Febriyani & Arfriandi, 2021) which uses the RC4 algorithm to secure exam documents schools with the extension *.doc. Documents will be encrypted when they are saved into the database, so that if there is illegal activity that accesses files from the database, the files will not be available read, because the file is encrypted. In an attempt to use CrackStation to try to carry out illegal activities by taking the file illegally, the result is that the file cannot be read, because the file not yet decrypted using the public key. In research (Fahmi, 2021) also used the RC4 (Rivest Chiper 4) algorithm to secure documents that already exist in the digital archive system. The algorithm is used, because according to him processing time is faster than other similar algorithms. Apart from the RC4 method, there is also the RSA (Reves Shamir Adleman) method used by (Agustina et al., 2017) in creating a digital document security system. In the process, data is sent first encrypted by the sender and produces encrypted data, which is then encrypted data The data will be sent to the recipient for a decryption process which produces data which are actually. From this research it can be concluded that the level of security with using the RSA method is included in the category of methods that are safe to use for the process document security

METHOD

Research framework.

Figure 1 is a diagram of the thinking framework used, starting from modeling to system construction, and then implementation.

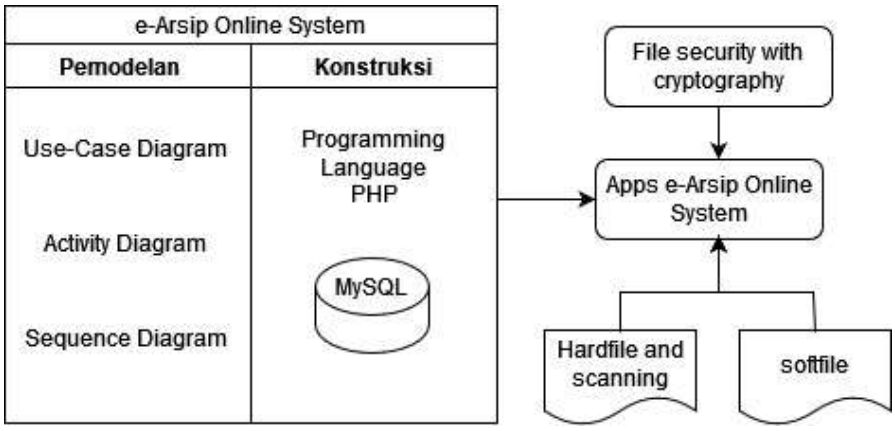


Fig. 1 Research framework

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 6, Number 1, January 2024
https://doi.org/10.47709/cnahpc.v6i1.3298

Submitted : Dec 6, 2023
Accepted : Dec 22,2023
Published : Jan 1, 2024

System development method

The design or research method used in this research is the waterfall model. According to Pressman (2003) in (Febriyani & Arfriandi, 2021) the waterfall model is a classic model that is systematic, sequential in building software. There are five stages in the waterfall research method, including communication, planning, modeling, construction and deployment as in the Fig.2

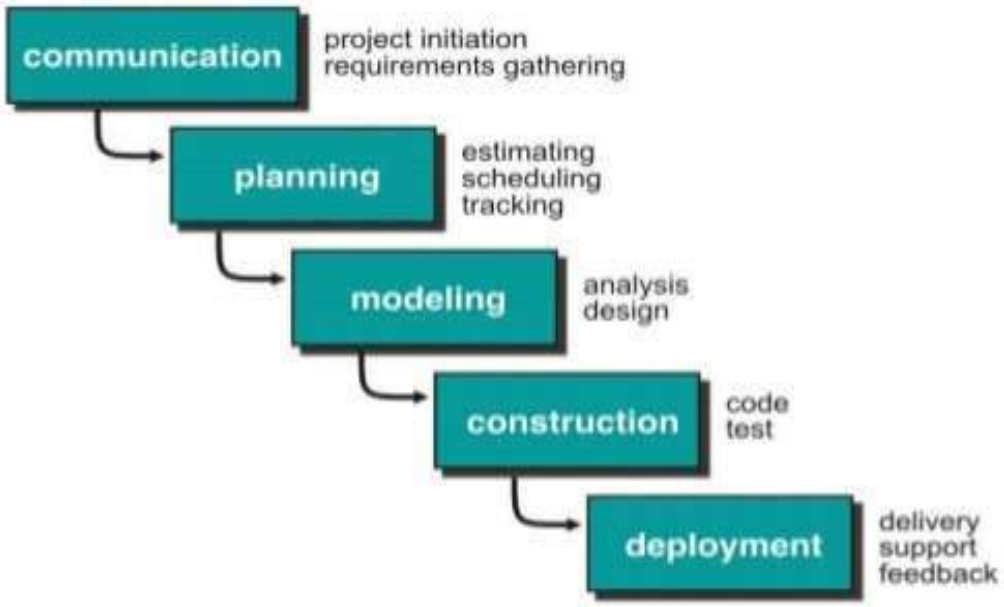


Fig. 2 Waterfall model

1) Communication

The first step in building a system is analyzing and communicating system requirements based on the results of data collection. From the communication stage, it was concluded that there was a need for an online digital-based document archiving system with cryptography as document security.

2) Planning

The planning stage describes the technical tasks that must be carried out starting from data collection to system testing, the risks that may occur when carrying out these tasks, and the results to be obtained, namely the creation of a document archiving system.

3) Modelling

The modeling stage focuses on designing a digital document archiving system scheme using an object approach, namely Use-Case Diagrams, then designing a database using MySQL as a data storage system, then designing an interface using Balsamiq Mockup. The flow of the application can be seen in the Fig.3.

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 6, Number 1, January 2024
https://doi.org/10.47709/cnahpc.v6i1.3298

Submitted : Dec 6, 2023
Accepted : Dec 22,2023
Published : Jan 1, 2024

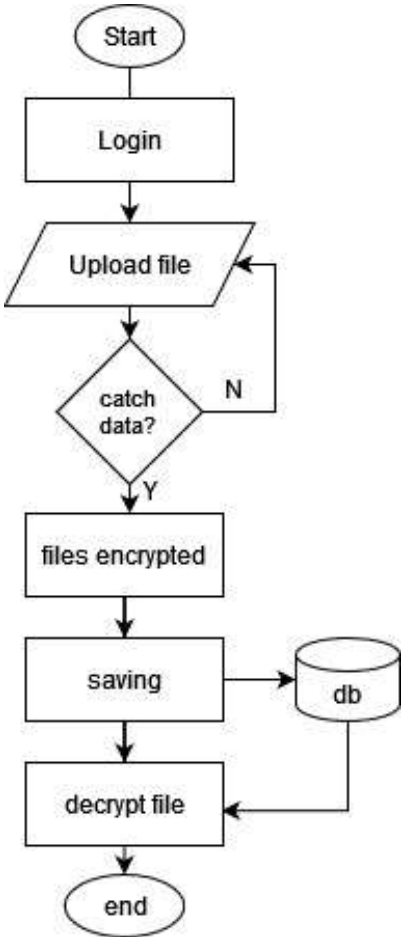


Fig. 3 System Flowchart

4) Construction

Construction is the code creation stage, resulting in a system that has been previously designed. The programming language used to build the system is PHP and uses a MySQL database as data storage. The RC4 algorithm is used to secure documents uploaded to the system.

After the coding process is complete, testing will be carried out on the system that has been created. System testing is carried out using black box testing. Black box testing is carried out to find out whether the functions in the program can run well starting from receiving input, processing and providing output.

5) Deployment

The deployment stage is the stage where the system is ready to be used by users. Then, to keep the system running well, maintenance needs to be carried out periodically according to needs

RESULT

Communication

This stage is carried out by conducting observations at partner locations and interviews with school principals. The results obtained were that many archives were scattered on various officers desks. Apart from that, many internal archives still use paper, so they are prone to being slipped. From the results of observations and interviews, it is recommended to create an online electronic archive application. This proposal is intended to handle the large amount of paper used for internal records.

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 6, Number 1, January 2024
https://doi.org/10.47709/cnahpc.v6i1.3298

Submitted : Dec 6, 2023
Accepted : Dec 22,2023
Published : Jan 1, 2024

Planning

The planning stage involves analyzing needs based on the results of observations and interviews. The results of the analysis were carried out by considering the application creation method approach. The application creation method chosen was an object approach. The object approach focuses on the structure and behavior of information systems that include data and processes. With the object approach, there are several diagrams that need to be created to describe the structure and behavior of a system. This diagram can also be useful as a communication tool and explain to users the system that will be created. The diagrams that will be created include use-cases, activity diagrams, sequences and data modeling.

Use-case is a depiction of how users interact with the system. Use-cases are used to identify and communicate to programmers what needs to be in the system.

Activity diagrams can be used to describe the behavior or business process activities of a system, and can also model everything from processes at the highest level to detailed activities below.

A sequence diagram is a dynamic model that shows explicitly the messages that flow between objects. It can also be understood that a sequence is a scenario of how the application or system runs from the back-end side.

1) Modelling

At the modeling stage, the diagrams created include use-case and activity diagrams.

a) Use-case Diagram

There are several use-cases or objects in the design of this e-archive application based cryptography, including users being able to upload files and being able to download files. Meanwhile, admins can see files that have been uploaded by users and can encrypt or decrypt file that has been uploaded by the user. Application use-case can seen Fig.4

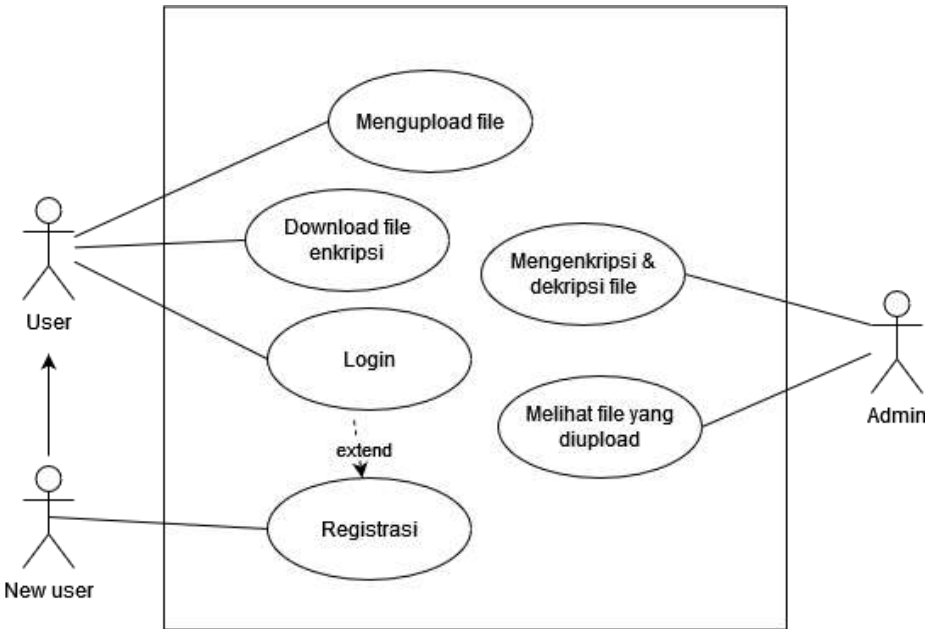


Fig. 4 Application use-case diagram

b) Activity diagram encrypt/decrypt file

The process or activity that occurs when a user performs the decrypt or encrypt file function is as follows Fig 5. The encryption or decryption process can only be carried out by the admin because it reduces multiple access by users and centralized processes

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 6, Number 1, January 2024
https://doi.org/10.47709/cnahpc.v6i1.3298

Submitted : Dec 6, 2023
Accepted : Dec 22,2023
Published : Jan 1, 2024

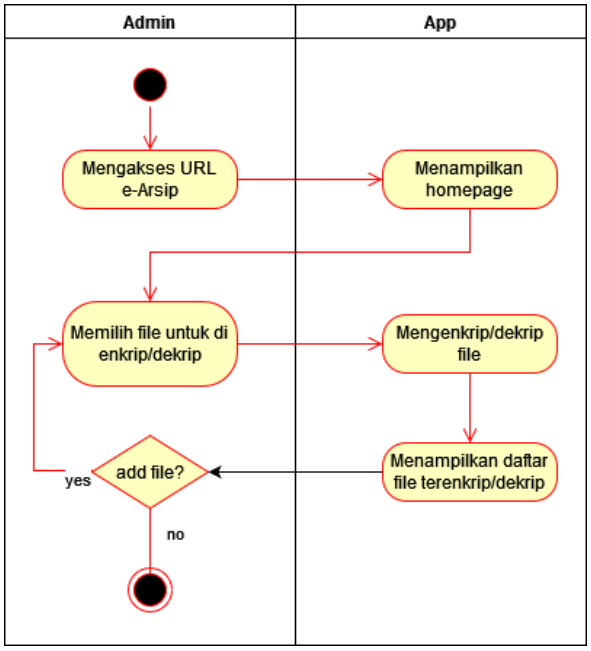


Fig. 5 Activity diagram for encrypt or decrypt file

c) Sequence

The sequence diagram in Fig.6 illustrates the encryption and decryption process that runs behind the application. This diagram is intended for programmers in creating program code

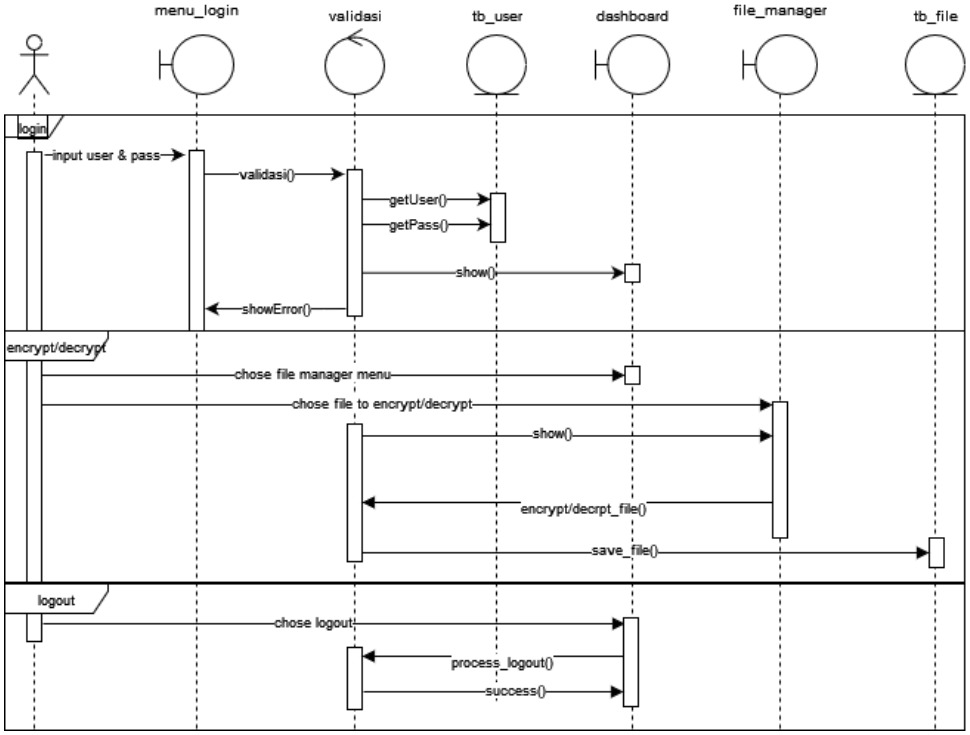


Fig. 6 Sequence diagram for encrypt or decrypt file

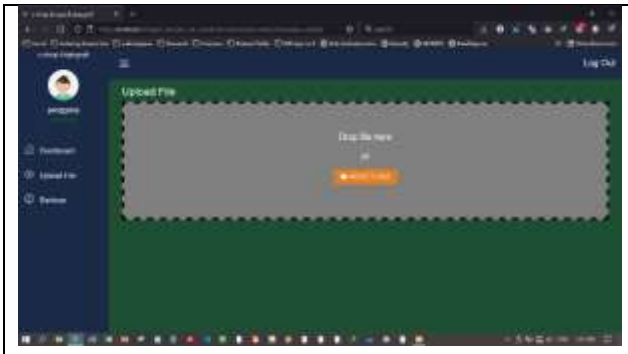
* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 6, Number 1, January 2024
https://doi.org/10.47709/cnahpc.v6i1.3298

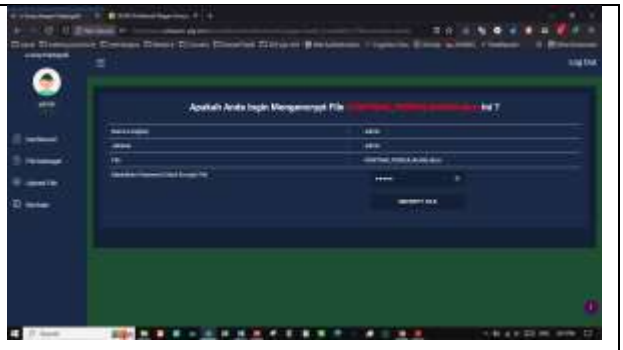
Submitted : Dec 6, 2023
Accepted : Dec 22,2023
Published : Jan 1, 2024

DISCUSSION

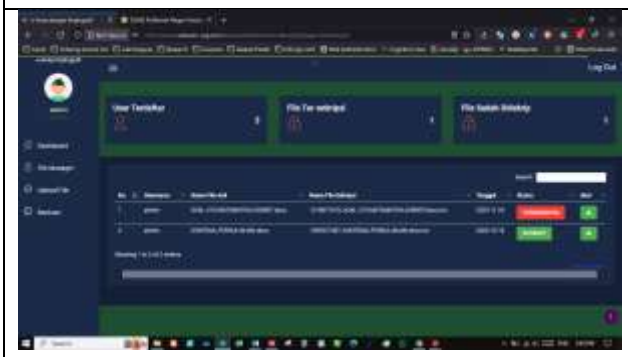
Files that have been uploaded on the upload page (a), will be visible on the admin page dashboard. Files that can be uploaded here are files with the extension .doc, .docx, .xls, .txt, .pdf. Here the admin has the authority to encrypt and/or decrypt files that have been uploaded. To decrypt a file, you need to enter a password which is the public key (b), and this public key can be given to a trusted party. The status of whether the file has been encrypted or not will look like in image (c). The contents of the document file resulting from encryption will change to random characters whose meaning cannot be understood, as in image (d). The application can encrypt uploaded files and change the contents of the document file into random characters. These results are the same as research (Febriyani & Arfriandi, 2021) (Maulana & Simanjorang, 2021).



(a)



(b)



(c)

(d)

Application testing is carried out using the black box testing method, which aims to find out whether the functionality of each feature is in accordance with user needs. The way to test the black box testing method is to create a test scenario by entering various data inputs according to the form page on the application.

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 6, Number 1, January 2024
https://doi.org/10.47709/cnahpc.v6i1.3298

Submitted : Dec 6, 2023
Accepted : Dec 22,2023
Published : Jan 1, 2024

Tabel 1 Testing the functionality of uploading files

No	Feature tested	Expected result	Actual result	Description
1	User uploads file with extension.docx,.doc,.txt	Application displays message: *File successfully uploaded to server*	Application displays message: *File successfully uploaded to server*	Aims to validate files that are allowed to be uploaded into the application
2	Users upload files other than.docx,.doc,.txt extensions	Application displays message: *File failed to upload, extension not allowed*	Application displays message: *File failed to upload, extension not allowed*	Validates files that are not allowed to be uploaded into the application

Tabel 2 Examination of file encryption and decryption functionality

No	Feature tested	Expected result	Actual result	Description
1	Administrator encrypts files	The application displays the message: *The file has been successfully encrypted*	The application displays the message: *The file has been successfully encrypted*	Randomizes file characters and changes them to random characters with the extension .txt
2	The administrator decrypts the file	The application displays the message: *The file has been successfully decrypted*	The application displays the message: *The file has been successfully decrypted*	Converts random file contents to original file contents and returns from .txt form to .docx extension

Test results using CrackStation to test the encryption results of the application as in the Ffig.7 shows that from the sample tested, the encryption results could not be cracked

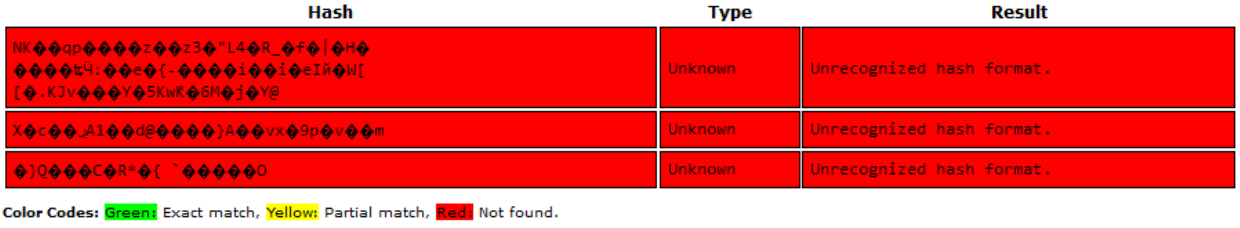


Fig. 7 CrackStation Testing

Cryptography with the RC4 algorithm belongs to the Stream Cipher group that encrypts ordinary text combinations using XOR bit-wise (exclusive-or). RC4 uses key lengths from 1 to 256 bytes to initialize tables with a length of 256 bytes. This table is used for subsequent pseudo-random generations that use XOR with plaintext to generate ciphertext. Each element in the table is exchanged at least once. The working stages of this algorithm are as follows (Fahmi, 2021):

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 6, Number 1, January 2024
https://doi.org/10.47709/cnahpc.v6i1.3298

Submitted : Dec 6, 2023
Accepted : Dec 22,2023
Published : Jan 1, 2024

1. S-Box (Array S) initialization process
   for i = 0 to 255, S[i] = i
2. Initialization process of S-Box (Array K)
   for i = 0 to 255, S[i] = i
3. Then do the S-Box shuffle step
   i=0; j = 0
   for i= 0 to 255{
   j=(j+S[i]+[k] mod 256
   Swap S[i] and S[j]}
4. Making pseudorandom bytes
   i= (i+1) mode 256
   j= (j + S[i]) mod 256
   Swap S[i] and S[j]
   t=(S[i] + S[j]) mod 256
   K=S[t]

Byte K is XORed with plaintext to produce ciphertext (encryption process) or XORed with ciphertext to produce plaintext (decryption process).
The disadvantage of this application is that the files uploaded to be encrypted are still limited to document files (.doc,.docx,.xls,.txt,.pdf); it cannot encrypt audio and video files. Apart from that, the encryption process is not automatically carried out during the file upload process, so it is vulnerable to negligence by users who forget to encrypt their files.

CONCLUSION

The document file uploaded to the e-archive application using the Rivest Cipher 4 cryptographic technique was successfully encrypted, and the contents of the file were changed to random characters. The execution time when encrypting or decrypting a file is relatively dependent on the size of the file being uploaded. Overall, the time required is fast. From the CrackStation test results, it was also obtained that the encryption results could not be broken, so this algorithm was used to encode file documents in electronic archives.

REFERENCES

Agustina, A. N., Aryanti, & Nasron. (2017). Pengamanan Dokumen Menggunakan Metode Rsa (Rivest Shamir Adleman) Berbasis Web. *Proceeding SENDI_U*, *3*(3), 14–19.

Azhari, M., Mulyana, D. I., Perwitosari, F. J., & Ali, F. (2022). Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES). *Jurnal Pendidikan Sains Dan Komputer*, *2*(01), 163–171. https://doi.org/10.47709/jpsk.v2i01.1390

Balogun, T. (2018). *The nexus between digitization, preservation and access in the context of selection of materials for archives*.

BBC Indonesia. (2022). *Bjorka klaim retas dokumen Presiden Jokowi, pemerintah bentuk satgas dan ungkap motif*. https://www.bbc.com/indonesia/indonesia-62870532

Dominy, G. (2017). The effects of an administrative and policy vacuum on access to archives in South Africa. *Archival Science*, *17*, 393–408.

Fahmi, K. (2021). Pengamanan Data Arsip Pada Balai Desa Sidodadi Menggunakan Kriptografi Modern RC4. *Resolusi: Rekayasa Teknik Informatika Dan Informasi*, *2*(2), 58–66. http://www.djournals.com/resolusi/article/view/241

Febriyani, F. S., & Arfriandi, A. (2021). *Implementasi Algoritma RC4 pada Sistem Pengamanan Dokumen*

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 6, Number 1, January 2024
https://doi.org/10.47709/cnahpc.v6i1.3298

Submitted : Dec 6, 2023
Accepted : Dec 22,2023
Published : Jan 1, 2024

Digital Soal Ujian. *6*(3), 171–177.

Ihwani, M. (2016). Model Keamanan Informasi Berbasis Digital Signature Dengan Algoritma Rsa. *CESSJournal Of Computer Engineering System And Science*, *1*(1), 15–20.

Maulana, R., & Simanjorang, R. M. (2021). Implementasi Kriptografi Pengamanan Data Pribadi Siswa SMA Swasta Jaya Krama Beringin Dengan Algoritma RC4. *Jurnal Nasional Komputasi Dan Teknologi Informasi (JNKTI)*, *4*(6), 377–383. https://doi.org/10.32672/jnkti.v4i6.3533

Nadeak, E., Devani, F. T., Malahayati, & Sulistiyanto. (2023). Perception of Privacy Concerns in Using Instagram Among Students (Case Study: Sriwijaya State Polytechnic). *2023 10th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, 273–277. https://doi.org/10.1109/EECSI59885.2023.10295759

Nadeak, E., Malahayati, M., & Sulistiyanto, S. (2023). Intention to Disclose Privasi Informasi di Antara Pengguna Tiktok: Studi Pada Remaja. *Innovative: Journal Of Social Science Research*, *3*(1), 456–467. https://doi.org/https://doi.org/10.31004/innovative.v3i1.3365

Ngadiyah, N., & Arohman, A. (2020). ANALISIS PENGELOLAAN ARSIP DINAMIS DAN STATIS DI MTs NEGERI 2 PRINGSEWU LAMPUNG. *Jurnal Ilmiah Ekonomi Manajemen: Jurnal Ilmiah Multi Science*, *11*(01), 77–88. https://doi.org/10.52657/jiem.v11i01.1195

Nugrahani, S. S. (2023). *Perbandingan Kinerja Algoritma AES, Grain V1, dan RC4 pada Protokol MQTT*. Universitas Sebelas Maret.

Nyfantoro, F., Salim, T. A., & Mirmani, A. (2020). Perkembangan Pengelolaan Arsip Elektronik Di Indonesia: Tinjauan Pustaka Sistematis. *Diplomatika: Jurnal Kearsipan Terapan*, *3*(1), 1. https://doi.org/10.22146/diplomatika.48495

Pramusinto, W., Wizaksono, N., & Saputro, A. (2019). Aplikasi Pengamanan File Dengan Metode Kriptografi AES 192, RC4 Dan Metode Kompresi Huffman. *Jurnal BIT (Budi Luhur Information Technology)*, *16*(2), 47–53.

Saragi, D. R., Gultom, J. M., Tampubolon, J. A., & Gunawan, I. (2020). Pengamanan Data File Teks (Word) Menggunakan Algoritma RC4. *Jurnal Sistem Komputer Dan Informatika (JSON)*, *1*(2), 114. https://doi.org/10.30865/json.v1i2.1745

Setyawan, H. (2021). Digitisasi Arsip Dalam Rangka Layanan Arsip Statis dalam Jaringan pada Masa Pandemik Covid19. *Khazanah: Jurnal Pengembangan Kearsipan*, *14*(2), 116. https://doi.org/10.22146/khazanah.63408

Sumarno. (2018). Analisis Kinerja Kombinasi Algoritma Message-Digest Algortihm 5 (MD5), Rivest Shamir Adleman (RSA) dan Rivest Cipher 4 (RC4) Pada Keamanan E-Dokumen. In *Tesis* (Vol. 2, Issue 1, pp. 1–71). http://jurnal.unprimdn.ac.id/index.php/JUSIKOM/article/view/140

Watrianthos, R. (2019). Perbandingan Teknik Kriptografi Metode Sapphire Ii Dan Rc4. *Jurnal Informatika*, *3*(2), 17–40. https://doi.org/10.36987/informatika.v3i2.213

Yusuf, M. R., & Zulaikha, S. R. (2019). Perkembangan pengelolaan arsip di era teknologi. *Acarya Pustaka: Jurnal Ilmiah Perpustakaan Dan Informasi*, *6*(2), 96–103. https://ejournal.undiksha.ac.id/index.php/AP/article/view/22253

* Corresponding author