BULLETIN OF ENGINEERING SCIENCE, TECHNOLOGY AND INDUSTRY

https://bestijournal.org | PT. Radja Intercontinental Publishing

E-ISSN: 3025-5821

IMPLEMENTATION OF THE VIGENERE CRYPTOGRAPHY ALGORITHM IN THE LHOKSEUMAWE STATE POLYTECHNIC CLOUD STORAGE SYSTEM

Dede Kurniawan[1], Indrawati[2], Hari Toha Hidayat[3], Martin Uribe[4]

Department of Information and Computer Technology Politeknik Negeri Lhokseumawe[1.2.3]

Columbia University[4]

*Correspondence Email:dedekurniawan.dk67@gmail.com

Abstract

Cloud storage is a technology used to store data online. However, this technology also poses problems in terms of security. Therefore, the author wants to build a cloud storage system by implementing cryptographic security to secure data. By implementing cryptographic techniques in cloud storage, users don't need to worry about data loss or theft. The cryptographic method applied is the Vigenere Cipher algorithm, which is a classic type of cryptography. Cloud storage is applied to public and private networks to test the comparison of data encryption times. Based on tests carried out, implementation on private networks is better with an average time of 3.84 seconds for encryption and 253.6 milliseconds for decryption. Meanwhile, on public networks, the average time is 45.3 seconds for encryption and 392 milliseconds for decryption. To measure whether cryptography is effective or not, the avalanche affect method is used which produces a value of 1.4% to 7% with an average of 3.92%.

Keywords: Cloud Storage, Vigenere Cipher, private, public, avalanche affect.

INTRODUCTION

In the current era of globalization, technological developments play a very important role in people's lives. Technology has made it easier and provides comfort that is useful in carrying out daily tasks that may not be able to be done at the same time. One example of this development is online digital data storage media. Limited data storage media is a problem that we often experience when storing important data, so special storage is needed to back up temporary data. Universities or colleges require programs or applications to process existing data, including the online KRS system, mail server and web portal for each unit within the University. The data processed and stored in the system will increase over time, requiring large storage space. Apart from the problem of the need for increasingly large storage space, a service is also needed that can guarantee data security, data recovery including easy access to the data anywhere and at any time [1]. Currently, students still store data on the hard disk of each computer or portable storage such as a flash disk or hard disk. Cloud storage is able to provide much better services than using regular digital storage. Cloud storage has the advantage of adapting to the needs of the user itself, and costs much less than replacing hardware in many places.

Data stored in cloud storage is very vulnerable to data theft, because cloud storage is stored online and is web-based. So, a good security system is really needed to protect data uploaded to cloud storage. Security in cloud storage systems must be maintained because there are many malicious users who want to manipulate or steal data. Therefore, a process is needed to secure the data by encrypting the uploaded files, by applying a method that exists in cryptography. Based on this background, researchers will analyze the security of data in Cloud Storage. Therefore, the author chose the final assignment (TA) with the title "Implementation of the Vigenere Cryptography Algorithm in the Lhokseumawe State Polytechnic Cloud Storage System". Based on the problems that have been described, the problem formulation that can be formulated includes security in the cloud storage system which is still vulnerable to theft, how to secure files uploaded to the cloud storage system using the vigenere cipher algorithm, how to compare the speed of the encryption process carried out in public networks and private on the cloud storage system. The aim of this research is to secure files uploaded by users by applying the Vigenere Cipher cryptographic algorithm so that files are safe from theft, to compare the security speed of cloud storage systems in public and private networks, to make it easy for service users to be able to share files with each other. other users from anywhere and at any time as long as they are connected to the internet network (online).

METHOD

System planning

System design is the next stage after system analysis, getting a clear picture of what is done in the system analysis, then continuing with thinking about how to form the system.

Flow chart

Encryption and decryption of data is depicted with a flowchart diagram using the Vigenere cipher algorithm. The Encryption and Decryption flowchart is shown in figures 1 and 2.

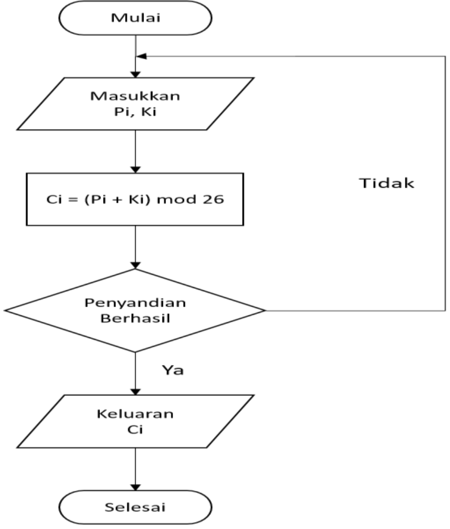


Figure 1. Vigenere Cipher Encryption Flowchart

The following is an explanation of the Vigenere Cipher algorithm encryption flowchart:

1. First declare the variable Pi as plaintext and also Ki as the key to carry out encryption.
2. Perform calculations using the encryption formula by adding the Pi and Ki values. Then the results are modified or the remainder is stored in the Ci variable.
3. Check whether the encryption value was successful or not. If the condition is correct then it will continue to the next stage.
4. Meanwhile, if the condition is not true, the condition will be returned when entering the Pi and Ki values.
5. Produces output with encrypted plaintext

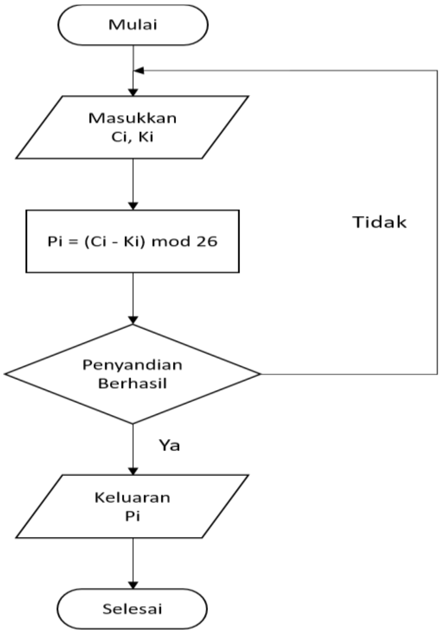


Figure 2. Vigenere Cipher Decryption Flowchart

The following is an explanation of the Vigenere Cipher algorithm decryption flowchart flow:

1. First declare the variable Ci as ciphertext and also Ki as the key to carry out encryption.
2. Perform calculations using the decryption formula by subtracting the Ci and Ki values. Then the results are modified or the remainder is stored in the variable Pi.
3. Check whether the value decryption was successful or not. If the condition is correct then it will continue to the next stage. Meanwhile, if the condition is not correct, the condition will be returned when entering the Ci and Ki values.
4. Produces output with ciphertext that has been previously converted into plaintext.

B. Use Cases

This section uses a Use Case to determine the behavior of actors who use the cloud storage system.

1. Use Case Admin

In the admin use case there are 6 use cases with the include symbol which leads to the data management use case. The use case that leads to the manage data use case can only be reached through the previous use case, as well as the manage data and login use case as shown in figure 3.

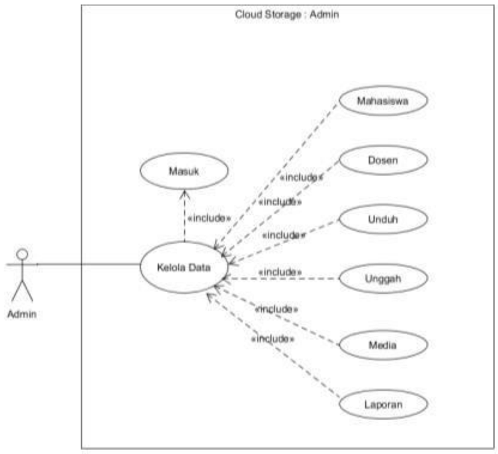


Figure 3. Admin Use Case

2. Use Case Lecturer

In the lecturer's use case there are 4 use cases with the include symbol which leads to the data management use case. The use case that leads to the manage data use case can only be reached through the previous use case, as well as the manage data and login use cases. And the list use case is an extension or alternative to the entry use case as shown in Figure 4.

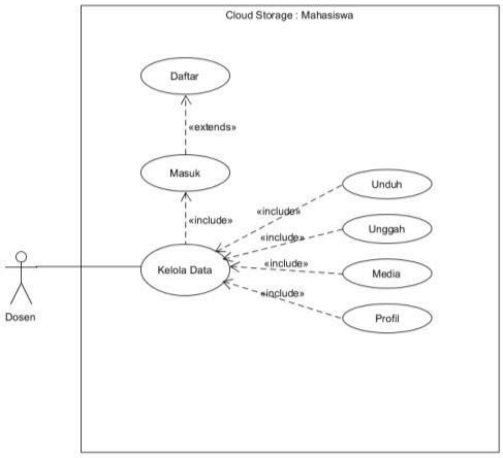


Figure 4. Lecturer Use Case

3. Student Use Case

In the student use case there are 5 use cases with the include symbol which leads to the data management use case. The use case that leads to the manage data use case can only be reached through the previous use case, as well as the manage data and login use cases. And the list use case is an extension or alternative to the entry use case as shown in Figure 5.

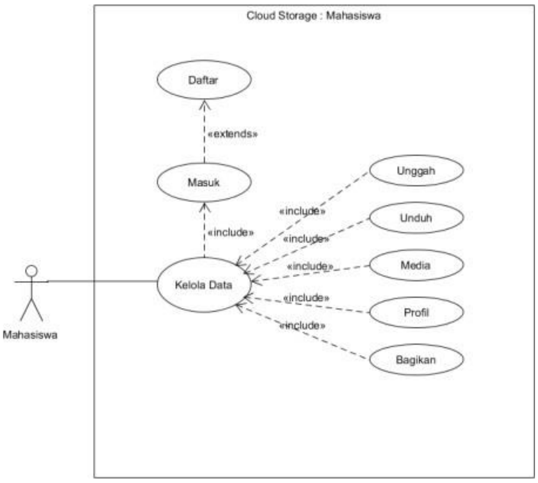


Figure 5. Student Use Case

RESULTS AND DISCUSSION

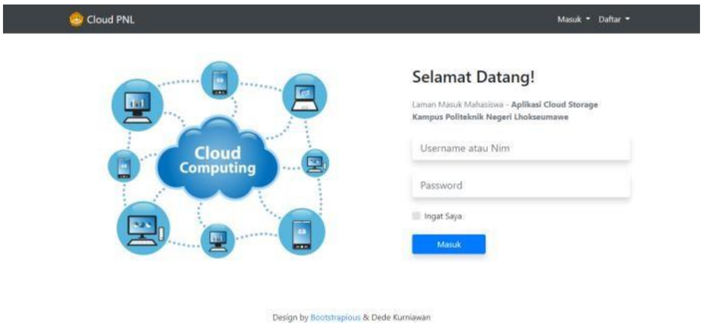
Encryption and decryption test results on value data in academic information systems using the Vigenere Cipher algorithm, value data is encrypted.

1. User Interface Page

The cloud storage system created has a user interface as a visual for the website. This application has several pages such as login page, register, home page, upload, share and other pages. An explanation of the use of each of these pages will be explained as follows.

a) Login Page Display

On this page the user carries out the login authentication process for the cloud storage application. To carry out the authentication process, users are asked to enter their username or ID and password to be able to enter the main cloud storage page. The Login Page display can be seen in Figure 6.



Selamat Datang!

Laman Masuk Mahasiswa - **Aplikasi Cloud Storage Kampus Politeknik Negeri Lhokseumawe**

Username atau Nim

Password

□ Ingat Saya

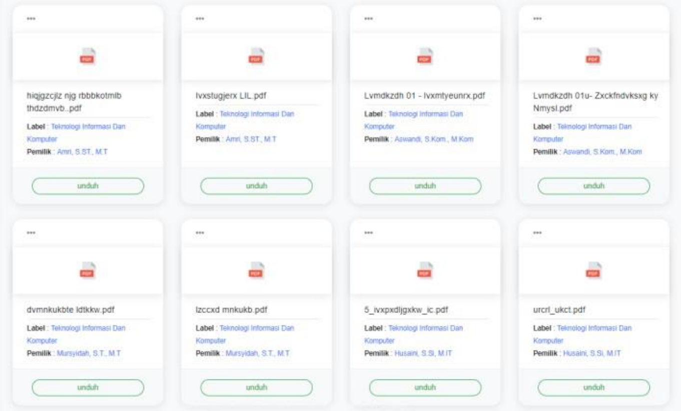
Masuk

Design by Bootstrapious & Dede Kurniawan

Figure 6 Login page display

b) Home Page View

On this page, files published by the user are displayed. Users can download as shown in figure 7.



hiqjgzcjlz njg rbbbkotmlb thdzdmvb..pdf
Label : Teknologi Informasi Dan Komputer
Pemilik : Amri, S.ST., M.T

Ivxstugjerx LIL.pdf
Label : Teknologi Informasi Dan Komputer
Pemilik : Amri, S.ST., M.T

Lvmdkzdh 01 - Ivxmtyeunrx.pdf
Label : Teknologi Informasi Dan Komputer
Pemilik : Aswandi, S.Kom., M.Kom

Lvmdkzdh 01u- Zxckfndvksxg ky Nmysl.pdf
Label : Teknologi Informasi Dan Komputer
Pemilik : Aswandi, S.Kom., M.Kom

dvmnkukbte ldtkkw.pdf
Label : Teknologi Informasi Dan Komputer
Pemilik : Mursyidah, S.T., M.T

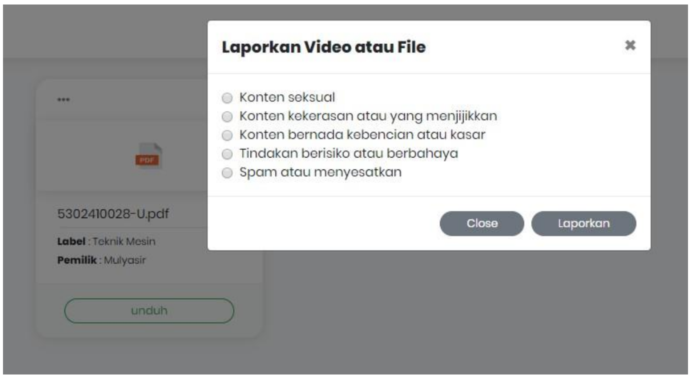
lzccxd mnkukb.pdf
Label : Teknologi Informasi Dan Komputer
Pemilik : Mursyidah, S.T., M.T

5_ivxpxdljgxkw_ic.pdf
Label : Teknologi Informasi Dan Komputer
Pemilik : Husaini, S.Si, M.IT

urcrl_ukct.pdf
Label : Teknologi Informasi Dan Komputer
Pemilik : Husaini, S.Si, M.IT

Figure 7. Home Page Display

Below is a pop-up form for reporting deviant content uploaded by other users as shown in Figure 8.



Laporkan Video atau File

○ Konten seksual
○ Konten kekerasan atau yang menjijikkan
○ Konten bernada kebencian atau kasar
○ Tindakan berisiko atau berbahaya
○ Spam atau menyesatkan

5302410028-U.pdf
Label : Teknik Mesin
Pemilik : Mulyasir

Figure 8. Reporting Pop-up Display

2. Cloud Storage Security Using Vigenere Cipher

The following is the manual calculation process in the encryption and decryption process in the Vigenere Cipher cryptographic algorithm.

The Vigenere cipher encryption formula is shown in equations (1) and (2) and the decryption formula is shown in equations (3) and (4):

Pi = (Ci-Ki) mod 26

or

Ci = (Pi + Ki) – 26, if the sum of Pi and Ki is more than 26

Pi = (Ci-Ki) mod 26

or

Pi = (Ci – Ki) + 26, if the result of subtracting Ci from Ki is minus

Information:

Ci = decimal value of the ith ciphertext character
Pi = decimal value of the ith plaintext character
Ki = decimal value of the ith key character
Character decimal value: A=0 B=1 C=2 ... Z=25

For example, if the plaintext is CLOUD STORAGE and the key is CRYPTOGRAPHY then the encryption process that occurs is as follows:

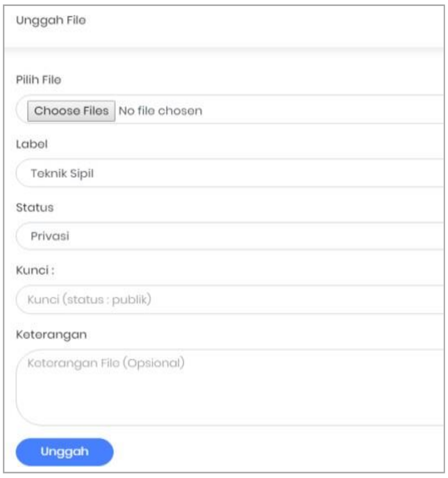
Plaintext :CLOUD STORAGE
KEY: CRYPTOGRAPHY
CIPERTEXT :MCWJW GZFRFOO

3. Vigenere Cipher Algorithm Testing Process

The tests carried out explain how the process of securing data in cloud storage uses the Vigenere Cipher method. The following is the process of testing the Vigenere Cipher algorithm on the system being created.

a) File Upload Page Display

On this page, to carry out the process of securing or encrypting files on the system, the user is required to enter a key with the public status option. This form consists of inputting a file in the form of a document that you want to publish and encrypt, input the type, namely the major category of the file content, input the status consisting of public and private, then input the key to encrypt with the name of the uploaded file and finally input the file description which is optional. The File Encryption Page Display can be seen in Figure 9



Unggah File

Pilih File
Choose Files No file chosen

Label
Teknik Sipil

Status
Privasi

Kunci :
Kunci (status : publik)

Keterangan
Keterangan File (Opsional)

Figure 9. File Upload Page Display

File Decryption View

When a user wants to download a file published by another user, a pop-up will appear asking the user to enter a keyword in order to download it.
decrypt the file you want to download. The description page display can be seen in Figure 10.

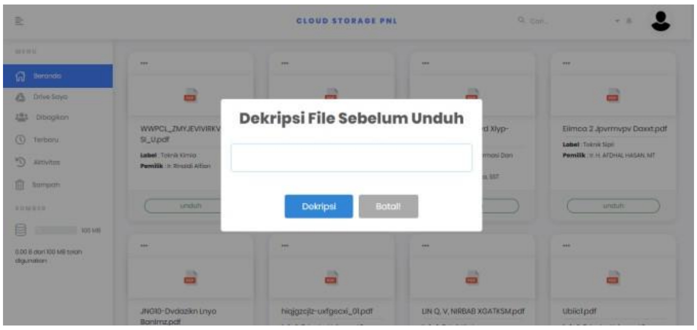


Figure 10. Decryption pop-up display

4. Comparative Testing of Cloud Storage Using Private and Public Networks

Testing of files and the time required for the encryption and decryption (upload) process when testing is carried out using private and public networks. Testing was carried out to compare cloud storage which was tested on private and public networks and carried out experiments on files including *.pdf. *.doc, *. ppt, *.avi, *. mp4, *. mkv. The test table is shown in tables 1 and 2.

TABLE 1 TESTING FILE SECURITY EXECUTION TIME (PRIVATE)

File Name	Size (kb)	Key	Encryption (s)	Decryption (ms)
database_data.pdf	767	cloud	1.71	266
organization-computer_00.pdf	178	cloud	1.33	235
Base Theory.docx	134	cloud	1.27	276
religious papers.doc	68 KB	cloud	1.25	266
bandwidth.ppt	661	cloud	1.51	238
Cryptography.ppt	60	cloud	1.20	256
Tutorials AutoCAD.avi	9,890	cloud	5.47	237
Tutorials Multimedia.avi	11,118	cloud	6.16	230
Programming C++.mp4	10,910	cloud	5.77	240
Grammar Questions.mp4	8,359	cloud	4.94	254
Arduino DIY.mkv	17,160	cloud	8.51	259
Install Arduino.mkv	15,189	cloud	6.97	287

In table 2, execution time testing on a private network is carried out. There are several parts such as file name, file size, key, encryption time and decryption time. Based on the tests carried out, results were obtained with an average encryption time of 45.3 seconds, an average decryption time of 392 milliseconds (private).

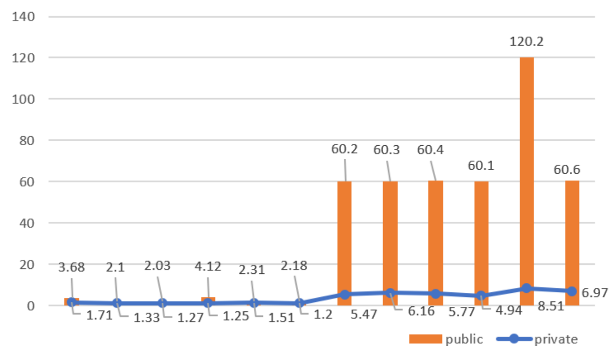


Figure 11. Encryption Time Chart

Figure 11 shows a chart with different shapes, namely bar and line charts. The blue line chart shows the encryption execution time on a private network. Meanwhile, the orange bar chart shows the encryption execution time on public networks according to the test data in tables 1 and 2.

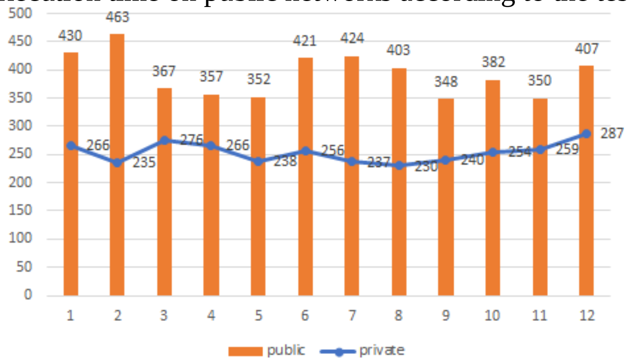
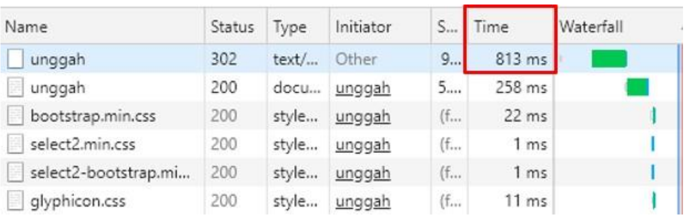


Figure 12. Decryption Time Chart

Figure 12 shows a chart with different shapes, namely bar and line charts. The blue line chart shows the decryption execution time on the private network. Meanwhile, the orange bar chart shows the decryption execution time on the public network according to the test data in tables 1 and 2.



Name	Status	Type	Initiator	S...	Time	Waterfall
unggah	302	text/...	Other	9...	813 ms	
unggah	200	docu...	unggah	5....	258 ms	
bootstrap.min.css	200	style...	unggah	(f...	22 ms	
select2.min.css	200	style...	unggah	(f...	1 ms	
select2-bootstrap.mi...	200	style...	unggah	(f...	1 ms	
glyphicon.css	200	style...	unggah	(f...	11 ms	

Figure 13. Database Schema View

In figure 13 is a display of the execution time of the encryption and decryption process taken via one of the features in the Google Chrome browser in the inspect element network section. If the value is in milliseconds, it is converted to seconds first before being entered in the test table.

TABLE 3 CLOUD STORAGE ENCRYPTION TESTING

File Name	**Size (kb)**	**Key**	**Encryption**	**Decryption (ms)**
database_data.pdf	767	cloud	dlgcv_flhu.pdf	succeed
organization-computer_00.pdf	178	cloud	qcuuqkdoml-mzajxvpf_00.pdf	succeed
Base Theory.docx	134	cloud	Nlbxdulb Nhqcw.docx	succeed
paper religion.doc	68	cloud	olyuocs oadol.doc	succeed
bandwidth.ppt	661	cloud	dlbxzkohb.ppt	succeed
Cryptography.ppt	60	cloud	Mcwjwqrfuik.ppt	succeed
Tutorials AutoCAD.avi	9,890	Study_	-	Fail
Tutorials Multimedia.avi	11,118	123qwerty	-	Fail
Programming C++.mp4	10,910	hello 123	-	Fail

In table 3, several files that can be encrypted and cannot be encrypted are tested. Files that cannot be encrypted are caused by the encryption key entered not matching the specified validation, namely alphabetic characters. Then the file cannot be successfully encrypted if the file size exceeds the maximum upload limit, namely 128 MB

5. **Testing the Effectiveness of Vigenere Cipher Cryptography on Cloud Storage Using the Avalanche Effect Method**

*Avalanche Effect*is a way to find out how much bit change has occurred in the ciphertext as a result of the encryption process. The greater the avalanche effect, the better the cryptographic algorithm.

The level of avalanche effect can be calculated using the formula in equation (5)

$$\text{AE} = \frac{\text{Jumlah bit yang tergeser pada cipherteks}}{\text{Jumlah bit cipherteks}} \text{ x } 100\%$$

The following are several samples of testing the Vigenere Cipher algorithm on cloud storage which are shown in tables 4 and 5:

TABLE 4 COMPARATIVE EARLY PLAINTEX

Plaintext Beginning	**Ciphertext Beginning**	**Early Binary Ciphertexts**
bandwidth	dlbxzkohb	01100100 01101100 01100010 01111000 01111010 01101011 01101111 01101000 01100010

TABLE 5 COMPARATIVE EARLY PLAINTEX

Plaintext Test	**Ciphertext Test**	**Bit Ciphertext**	**Total Different Bits**	**AE (%)**
bandwidth	dlbxzkohy	0110010001101100 01100010 01111000 01111010 01101011 01101111 01101000	5	7 %
bandwidthtr	dlbxzkohl	01100100 01101100 01100010 01111000 01111010 01101011 01101111 01101000	3	4.2 %
bandwidth	dlbxzkohz	01100100 01101100 01100010 01111000 01111010 01101011 01101111 01101000	2	2.8 %
bandwidth	dlbxzkohi	01100100 01101100 01100010 01111000 01111010 01101011 01101111 01101000	3	4.2 %

In table 4 is the initial process of converting the plaintext value into ciphertext using the vigenere cipher cryptographic method, then the ciphertext value is converted into a binary number. Then in table 5 the binary value is calculated and entered into the avalanche affect formula in equation 5 and the final result is obtained in the form of a percent from the binary value calculation of the avalanche affect formula.

CLOSING

Based on the discussion regarding the implementation of the Vigenere cryptographic algorithm in the Cloud Storage application, the following conclusions can be drawn:

1. The Vigenere Cipher cryptographic algorithm can be applied to secure files uploaded to cloud storage.
2. The cryptographic security process in cloud storage requires a plaintext that is taken from the file name and then encrypted with a key entered by the user.
3. Comparison of encryption – decryption times on private networks is better with an average time of 3.84 seconds and
4. 253.6 milliseconds. Meanwhile, on public networks the average time is 45.3 and 392 milliseconds.
5. The results of the effectiveness test on the avalanche effect were 1.4% to 7% with an average of 3.92%.

REFERENCES

SA Indrawata Wardhana, "Design and Implementation of Cloud Storage Architecture in Iain STS Jambi," Manaj. Sis. Inf., vol. 2, no. 1, pp. 244–259, 2017.

RH Dedi Kurniawan, Rita Afyenni, "Implementation of the AES Algorithm in Encrypting Files Integrated with Android-Based Cloud Storage Services," ISSN Media Elektron., vol. 3, no. September, pp. 4–5, 2018.

S. Mahfud, "Building a Search Engine Based Repository System Using the Knuth Morris Pratt Algorithm," vol. 1, no. 1, 2018.

TWP Bernard Raditio Parulian, Surya Michrandi Nasution, "Design and Implementation of Secure Cloud Using Diffie-Hellman Key Exchange and Triple Dec Algorithm (3Des) Design and Implementation of Secure Cloud By Using Diffie-Hellman Key Exchange and Triple Des Algorithm (3Des)," vol. 2, no. 2, pp. 3808–3815, 2015.

Andriani, "APPLICATION OF THE VIGENERE CIPHER ALGORITHM IN DATA SECURITY IN INFORMATION SYSTEMS," Teknol. Engineering Inf. and Comput., vol. 1, no. 17, pp. 1–4, 2018.

TWP Eka Cahya Pratama, Surya Michrandi Nasution, "DESIGN AND IMPLEMENTATION OF SECURE CLOUD USING DIFFIE-HELLMAN KEY EXCHANGE AND SERPENT CRYPTOGRAPHY ALGORITHM," vol. 2, no. 2, pp. 3808–3815, 2015.

AHB Ahmad Leo Yudanto, Herman Tolle, "Design and Construction of Biomedical Laboratory Management Information System Applications, Faculty of Medicine, Brawijaya University," J. Pengemb. Technol. Inf. and Computer Science., vol. 1, no. 8, pp. 628–634, 2017.

A. Hanani, "Design and Construction of an Online Academic Information System for the 66 State Islamic University of Malang," p. 140, 2008.

AH Muhbib, "Desktop Implementation of the Inventory System on Hudi Motor Karangrayung Grobogan," Udinus eprints, pp. 1–41, 2016.

YUSDIARDI, "SALES INFORMATION SYSTEM DESIGN (CASE STUDY: PT. I-CUBE CREATIVINDO) Thesis," 2014.

D. Kuswanto, SAA Tendean, and Mulaab, "Implementation of the Whitespace Steganography Algorithm and Rc6 Encryption for Text Security," Semin. Nas. Technol. and Engineering, pp. 1–8, 20