Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 6, Number 1, January 2022
DOI : https://doi.org/10.33395/sinkron.v7i1.11236
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Implementation Combination Cryptographic Algorithm Triangle Chain Cipher And Vigenere Cipher In Securing Data In Database

Ahmad Arif[1)], Adidtya Perdana[2)], Arief Budiman[3)]
[1)2)3)] Universitas Harapan Medan, Indonesia
[1)]ahmadarif1307@gmail.com, [2)]adid.dana@gmail.com, [3)]ariefdiman13@gmail.com,

Submitted : Dec 24, 2021 | **Accepted** : Jan 1, 2022 | **Published** : Jan 7, 2022

Abstract: Data security is most important today, because the rampant data theft resulting in a lot of misuse of data by irresponsible parties so that it makes us anxious as data owners, for data storage it is usually stored in the database. From these problems the idea emerged to create a cryptographic system where the system can secure data by encrypting and decrypting also make data fully save and then the data owned by the user. This study aims to secure the data in the database by encrypting the original data without destroying the original data when later after decrypted. To perform this security, a cryptographic methodology is used with both of method that is Vigenere Cipher and Triangle Chain Cipher algorithms which are implemented in the application because both of methodology have same root that is classical cryptographic. This application will later be used as a medium for users to secure their data in the database so that later data theft will not to be easy. After doing fully research that produces applications that can implement combination of Vigenere Cipher and Triangle Chain Cipher algorithms,data in the encrypted database field is safe because encryption has been done to the data.

Keywords: Kriptografi,Vigenere Cipher, Triangle Chain Cipher, Database

INTRODUCTION

Data security is very important today, due to rampant data theft result in a lot of misuse of data so that it causes anxiety for us as data owners, for data storage it is usually stored in database. Database is an organized collection of data that is accessed and stored electronically from a computer system (Alasi et al., 2020).One of the data security techniques is cryptography.

Cryptography is a data security method that has two processes, namely encryption and decryption. There are several types of cryptographic methods, one of which is the Triangle Chain Cipher (TCC).(Irawan, 2020). In addition, there is also the vigenere cipher method, which is one of the standard cryptographic algorithms that prevents attacks during transmission (Alasi et al., 2020)

In a study conducted by (Ismail et al., 2021) with the research title "Email message security system using classical cryptographic algorithms" which in this study discusses the security of email messages using classical cryptography where by securing email messages the contents of the email become more secure. and it is not easy for unauthorized persons to know.

In research conducted by (Nurdin, 2017) with the research title "Analysis and implementation of cryptography on secret messages using the transposition cipher algorithm" in this study discusses the use of the Transposition Cipher cryptographic algorithm in securing messages which is the purpose of security. This algorithm is an old algorithm but can still be used as an alternative in securing data.

In research conducted by (Yusfrizal, 2019)with the research title "Design of cryptographic applications on text using the reverse cipher and android based rsa method" in this study discusses the combination of reverse cipher and rsa methods so as to produce better security.

Purpose of this research is to secure the data in the database by encrypting the data and then decrypting it if you want to restore the original data.

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 6, Number 1, January 2022 e-ISSN : 2541-2019
DOI : https://doi.org/10.33395/sinkron.v7i1.11236 p-ISSN : 2541-044X

LITERATURE REVIEW

Cryptography

Cryptography is a branch of mathematics that explores mathematical approaches linked to data secrecy and other elements of information security. but not every issues of information security will be mark in cryptography. However, in cryptography, not all subject of information security will be handled(Tarigan & Maha, 2018). Process to convert plaintext into ciphertext is called encryption, while the process to convert ciphertext back to plaintext is called decryption or. Cryptography need parameters for the conversion process that are controlled by the single key or several keys.

Cryptography can be interpreted as a science produce a secret message. the original message is referred to as plaintext encoded into encrypted message which is that's mean similar with ciphertext via the encryption process and the ciphertext is change back into plaintext back through the process called description.(Yusfrizal, 2019)

Cryptographic algorithms are logical steps how hide messages from people who are not entitled to the message.(Setyawati et al., 2021)

Cryptography is a knowledge and art to protect confidentiality of messages (data or information) with secret technique in the form of a code that has no meaning(Dakhi et al., 2020).

Cryptography Classic

Classical cryptography is a character-based algorithm, that is, encryption and decryption are performed on each character of the message. Cryptography has a long history, ranging from Caesar cryptography which developed in BC to modern cryptography used in communication between computers in the 20th century. There are 2 most basic techniques, namely substitution techniques and transposition techniques (Ismail et al., 2021)

Classical cryptography is character-based of cryptography (encryption and decryption are performed on each character) and Modern cryptography is cryptography that works by using bit mode (expressed in 0 and 1)(Juliadi et al., 2013).

Triangle Chain Cipher

The encryption algorithm, commonly known as Triangle Chain Cryptography or Triangle Chain, is an encrypted one-time pad algorithm, the original idea from the length of randomly generated keys and encrypted plaintext keys. Is the code that was born. However, for cryptographic algorithms that use triangular chains, these keys are automatically generated using the chaining technique.

This triangular chain algorithm has a replacement rule based on the Caesar cipher, that is, by shifting characters. The power of this cipher lies in the key, which is an integer value that indicates the character shift according to the operation of the Caesar cipher. The second strength lies in the sequence of numbers that acts as a multiplier with the keys. The series of numbers can be in the form of specific numbers, such as: B. Odd series, even series, Fibonacci series, prime number series, number series that you can create yourself.

In fact, the triangular substitution cipher is not simplified, but with double encryption (double encryption), plaintext is encrypted with triangular encryption I, and the first encryption result is re-encrypted with triangular encryption II. Will be done. The one from Triangle II is the opposite of Triangle I (Irawan, 2020). The formula for the triangle chain crypto algorithm is:

The first triangular encryption matrix for the 1st row:
M1j = A[G] + (D * E[1]) mod 256
For the 2nd row and so on for the value of G ≥ i:
CFG = C(F-1)G +(D * E [F]) mod 256
So the ciphertext value obtained is:
CFG at the value of G = (B+F)-B.
Second triangle encryption matrix
The A value is obtained from the CFG value at F = G For the 1st row:
C1G = A[G] + (D*E[1])) mod 256
For the 2nd row and so on for the value of G ≤ (B+1) – F:
CFG = C(F-1)j+(D*E[F])) mod 256
So the ciphertext value obtained is:
CFG at the value of F = (B+1)-F.
Information:
A = plaintext
B = Number of plaintext characters
C = Encoded container matrix
D = Key
E = Row (multiplier row by key)

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 6, Number 1, January 2022 e-ISSN : 2541-2019
DOI : https://doi.org/10.33395/sinkron.v7i1.11236 p-ISSN : 2541-044X

F = Multiplier index
G = Index of plaintext characters

The decryption process is the opposite of the encryption process. The next matrix operation in the decoding process.

1) Since the operation of the first triangular decryption matrix is opposite to that of the encryption matrix, this operation is the opposite of that of the second triangular encryption matrix. The value of H is a ciphertext table of length B, that is H[B]. Apply the following formula to the first line(Irawan, 2020).

G≤(B+1)–F
C1G = H [G] - (D * E[1])) mod 256
As for the second and subsequent rows where the value of j i, the formula applies :
Mij = (C(i-1) j - D * (E[F])) mod 256.
So the plaintext value obtained is:
Mij at the value of j = (N+i)-i.
The second triangular decryption matrix for the first row applies the formula:
Decryption matrix
C1G = H [Gj] – (D * E[1])) mod256
As for the second row and so on, the value of G ≥ F, apply formula Cij = H[F-1]F – (D * E[F])) mod 256. The plaintext value obtained is :
Mij at the value of G = (B+1)-F.
So the plaintext value obtained is:
CFG at the value of G = (B+F)-B.
Information:
H = *Cipherteks.*
B = Number of characters *cipherteks*.
C = The container matrix for the cipher results is used as plain text.
D = Key .
E = Row.
F = multiplier index.
G = ciphertext character index (Irawan, 2020)

Vigenere Cipher

The Vigenère cipher is a traditional cryptographic technique that employs a compound alphabetic substitution mechanism. Unlike the Caesar cipher, which uses the single-alphabet substitution technique, which encrypts all letters in a message with the same key, compound-alphabet substitution encrypts each letter with a distinct key. (Alhogbi, 2017)

If the key in the Caesar cipher is merely one value, the key in the Vigenère cipher is a row of letters. Each plaintext letter will be encrypted with a distinct key thanks to the key in the form of a series of phrases. If the length of the key used is less than the plaintext length, the key will be repeated until the plaintext length equals the key length. If just one plaintext letter is known, this approach will reduce the chances of solving the ciphertext.

Here is the formula for the Vigenere Cipher

Enkripsi =
$Cx = (Px + Kx) \bmod 26$
Dekripsi =
$Px = (Cx - Kx)\ Mod\ (26)$

Where :
Cx = decimal value of the x-th ciphertext character
Px = x-th plaintext character decimal value
Kx = x-th key character decimal value

(Alasi et al., 2020)

Database

Database is a large storage area where there is a collection of data that contains not only operational data but also descriptive data. As stated by Connolly and Begg (2015: 63), that the database is a collection of logically connected data and a description of the data, designed to find information needed by an organization. In designing a database, one of the things that needs to be considered is efficiency (Pahlevi et al., 2018).

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 6, Number 1, January 2022 e-ISSN : 2541-2019
DOI : https://doi.org/10.33395/sinkron.v7i1.11236 p-ISSN : 2541-044X

MySQL

Mysql is a well-known open source database server that is commonly used for servers and the Internet. MySQL is commonly used in combination with PHP to construct dynamic and sophisticated server applications. MySQL has its own function thats called SQL (Structured Query Language) and already been enhanced by MySQL(Istiono et al., 2016).

MongoDB

The C++ language was used to create MongoDB, a document-oriented database. MongoDB grew in popularity as a result of its capacity to store data quickly. MongoDB also offers strong scalability, meaning it can handle massive volumes of data at a cheap cost. When compared to traditional relational databases, which consist of tables, SQL, and schemas that must be established upfront, MongoDB's schema is less difficult, allowing users to employ dynamic schemas comparable to JSON. MongoDB is a NoSQL database server, to put it another way.(Eka Putra, 2021)

ExpressJS

ExpressJS is a NodeJS framework that is useful for making it easier to create NodeJS-based applications using a highly flexible and customizable design pattern. In addition, ExpressJS is also a very lightweight framework and is suitable for creating web applications and API(FAJRIN, 2017)

FlowChart

Flowchart is a symbolic representation of an algorithm or procedure to solve a problem, using a flowchart will make it easier for users to check the forgotten parts in problem analysis, besides that flowcharts are also useful as a facility to communicate between programmers who work in a project team. Flowcharts help understand complex and lengthy logical sequences. Flowcharts help communicate the course of the program to other people (not programmers) it will be easier(Roni, 2019).

RESEARCH METHOD

The research methods used are:

1) Literature study by collecting various data from sources such as reference books, journals, internet and other sources.
2) Analyzing the problem and solving it with the method used.
3) Preparation of reports.

RESULT

System Analyst

In this system analysis, it explains how the system works.

Figure 1. System Analyst Block Diagram

EnkripsiVigenere Cipher

Table 1. Vigenere Cipher Character Table

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Table 1 describes the decimal code of the letters of the alphabet from A-Z.

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 6, Number 1, January 2022
DOI : https://doi.org/10.33395/sinkron.v7i1.11236
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Encryption Formula :
$C_i = E_k(M_i) = (M_i + K_i)\ mod\ 26$

Formula Description :
$M_i = D_k(C_i) = (C_i - K_i)\ mod\ 26$
$M_i = D_k(C_i) = (C_i - K_i) + 26$ (If the result $(C_i - K_i)$ is minus)

Description :
C = *Ciphertext* E = *encrypt*
K = Key D = d*ecrypt*
M = *Plaintext*

To prove it requires a calculation with the following:
Message : HARAPAN
Key : UNHAR
Because there are more plaintext letters than keys, then
Message : HARAPAN
Key : UNHARUN
Encryption Process:
$C_0 = 1$ (B)
$C_1 = 13$ (N)
$C_2 = 24$ (Y)
$C_3 = 0$ (A)
$C_4 = 6$ (G)
$C_5 = 20$ (U)
$C_6 = 0$ (A)

$C_0 = (7+20)\ mod\ 26$
$C_1 = (0+13)\ mod\ 26$
$C_2 = (17+7)\ mod\ 26$
$C_3 = (0+0)\ mod\ 26$
$C_4 = (15+17)\ mod\ 26$
$C_5 = (0+20)\ mod\ 26$
$C_6 = (13+13)\ mod\ 26$
Hasil *Cipher* = BNYAGUA

Decryption Process:
$P_0 = 7$(H)
$P_1 = 0$(A)
$P_2 = 7$(R)
$P_3 = 0$(A)
$P_4 = 15$(P)
$P_5 = 0$(A)
$P_6 = 13$(N)
Plaintext Results = HARAPAN

$P_0 = (1 - 20) + 26$
$P_1 = (13 - 13)\ mod\ 26$
$P_2 = (24 - 7)\ mod\ 26$
$P_3 = (0 - 0)\ mod\ 26$
$P_4 = (6 - 17) + 26$
$P_5 = (20 - 20)\ mod\ 26$
$P_6 = (0 - 13) + 26$

Triangle Chain Cipher Encryption

The calculation process with the Triangle Chain Cipher method can be done by performing the encryption and decryption process, for example in the following cases:

Encryption:
Triangle Chain Cipher Algorithm Encryption
Information:
P = plaintext.
N = Number of plaintext characters.
M = Encoded container matrix K = Key.
R = Row (row multiplier by key).
i = Multiplier index.
j = Plaintext character index.

Plainteks:
Table 2 is the result of the calculation of vigenerecipher
Table 2. Table of Cipher Vigenere Results

B	N	Y	A	G	U	A
66	78	89	65	71	85	65

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 6, Number 1, January 2022
DOI : https://doi.org/10.33395/sinkron.v7i1.11236
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Nb : key = 3 ; R = N, i = R ; J =N

First Triangle Encryption Triangle Chain Cipher Algorithm

First Triangle Encryption Triangle Chain Cipher Algorithm
Line one (i = 1)
j >= i : { 1,2,3,4,5,6,7 }

M11 = [M01 + (K * R1)] mod 256
= [B + (3 * 1)] mod 256
= (66 + 3) mod 256
= 69 mod 256
= 69
= E

M12 = [M02 + (K * R1)] mod 256
= [N + (3 * 1)] mod 256
= (78 + 3) mod 256
= 81 mod 256
= 81
= Q

M13 = [M03 + (K * R1)] mod 256
= [Y + (3 * 1)] mod 256
= (89 + 3) mod 256
= 92 mod 256
= 92
= \

M14 = [M04 + (K * R1)] mod 256
= [A + (3 * 1)] mod 256
= (65 + 3) mod 256
= 68 mod 256
= 68
= D

M_{15} = [M_{05} + (K * R_1)] *mod* 256
= [G + (3 * 1)] *mod* 256
= (71 + 3) *mod* 256
= 74 *mod* 256
= 74
= J

M_{16} = [M_{06} + (K * R_1)] *mod*256
= [U + (3 * 1)] *mod* 256
= (85 + 3) *mod* 256
= 88 *mod* 256
= 88
= X

M_{17} = [M_{07} + (K * R_1)] *mod* 256
= [A + (3 * 1)] *mod* 256
= (65 + 3) *mod* 256
= 68 *mod* 256
= D

Row two (i = 2)
j >= i : { 2,3,4,5,6,7}

M_{22} = [M_{12} + (K * R_2)] *mod*256
= [Q + (3 * 2)] *mod* 256
= (81 + 6) *mod* 256
= 87 *mod* 256
= 87
= W

M_{23} = [M_{13} + (K * R_2)] *mod* 256
= [\ + (3 * 2)] *mod* 256
= (92 + 6) *mod* 256
= 98 *mod* 256
= 98
= b

M_{24} = [M_{14} + (K * R_2)] *mod*256
= [D + (3 * 2)] *mod* 256
= (68 + 6) *mod* 256
= 74 *mod* 256
= 74
= J

M_{25} = [M_{15} + (K * R_2)] *mod* 256
= [J + (3 * 2)] *mod* 256
= (74 + 6) *mod* 256
= 80 *mod* 256
= 80
= P

M_{26} = [M_{16} + (K * R_2)] *mod*256
= [X + (3 * 2)] *mod* 256
= (88 + 6) *mod* 256
= 94 *mod* 256
= 94
= ^

M_{27} = [M_{17} + (K * R_2)] *mod* 256
= [D + (3 * 2)] *mod* 256
= (68 + 6) *mod* 256
= 74 *mod* 256
= 74
= J

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 6, Number 1, January 2022
DOI : https://doi.org/10.33395/sinkron.v7i1.11236
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Row three (i = 3)	j >= i : { 3,4,5,6,7}
Row four (i = 4)	j >= i : { 4,5,6,7}
Row five (i = 5)	j >= i : { 5,6,7}
Row six (i = 6)	j >= i : {6,7}
Row seven (i = 7)	j >= i : { 7}

E	W	k	_	~	”	•
H	Z	n	b	**ü**	**ù**	**ÿ**
N	`	t	h	P	**Ø**	
W	I	}	Q	**å**		
c	u	**‰**	}			
r	„	**ÿ**				
”	–					
TM						

First triangle encryption result = EWk_~”•

Triangle Chain Cipher . Second Triangle Encryption Algorithm

Line one (i =1)	j >= i : { 1,2,3, 4, 5, 6, 7 }
Row two (i =2)	j >= i : { 1,2,3, 4, 5, 6}
Row three (i =3)	j >= i : { 1,2,3, 4, 5}
Row four (i = 4)	j >= i : { 1,2,3, 4}
Row five (i =5)	j >= i : { 1,2,3}
Row six (i =6)	j >= i : { 1,2}
Row seven (i =7)	j >= i : {1}

E	W	k	_	~	”	•
H	Z	n	b	**ü**	**ù**	**ÿ**
N	`	t	h	P	**Ø**	
W	I	}	Q	**å**		
c	u	**‰**	}			
r	„	**ÿ**				
”	–					
TM						

Second Triangle Encryption Result = TM–,**ÿ**{(DCS)(OSC) **ÿ**

Description of the first triangle:
Cipher = TM–**ÿ**{(DCS)(OSC) **ÿ**

Line one (i =1)	j >= i : { 1,2,3,4,5,6,7 }
Row two (i =2)	j >= i : { 2,3,4,5,6,7}
Row three (i =3)	j >= i : { 3,4,5,6,7}
Row four (i =4)	j >= i : { 4,5,6,7}
Row five (i =5)	j >= i : { 5,6,7}
Row six (i =6)	j >= i : { 6,7}
Row seven (i =7)	j >= i : {7}

TM	–	**Ÿ**	}	DCS	OSC	**ÿ**
-	“	•	z	~	”	•
	ì	**É**	t	x	**Ä**	**Å**
		å	k	o	**ï**	**å**
			_	c	del	z
				Y	|	k
					^	Y
						D

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 6, Number 1, January 2022 e-ISSN : 2541-2019
DOI : https://doi.org/10.33395/sinkron.v7i1.11236 p-ISSN : 2541-044X

The result of the first triangle decryption = **-ìå**_Y^D
Description of the second triangle:
Cipher = **-ìå**_Y^D

Line one (i =1)	j >= i : { 1,2,3,4,5,6,7 }
Row two (i =2)	j >= i : { 1,2,3,4,5,6 }
Row three (i =3)	j >= i : { 1,2,3,4,5 }
Row four (i =4)	j >= i : { 1,2,3,4}
Row five (i =5)	j >= i : { 1,2,3 }
Row six (i =6)	j >= i : { 1,2}
Row seven (i =7)	j >= i : {1}

-	**ì**	**å**	_	Y	^	D
“	**è**	**â**	\	v	[	A
ì	**ä**	}	V	P	U	
ä	{	t	M	G		
x	o	h	A			
i	`	Y				
W	N					
B						

The result of the first triangle decryption = BNYAGUA

Database Design

Database design is the design of the database owned by the system, from table relations to database relations.

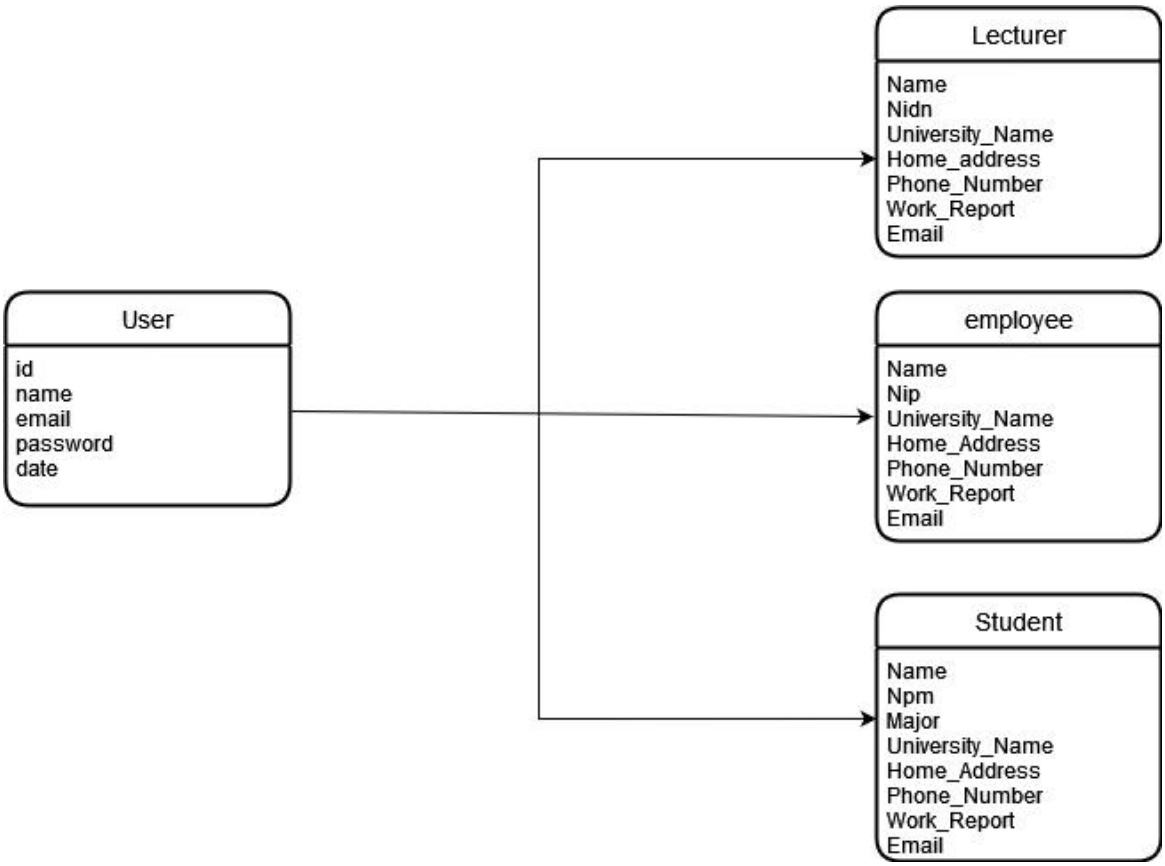

Figure 2. Relationships Between Tables

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 6, Number 1, January 2022
DOI : https://doi.org/10.33395/sinkron.v7i1.11236
e-ISSN : 2541-2019
p-ISSN : 2541-044X

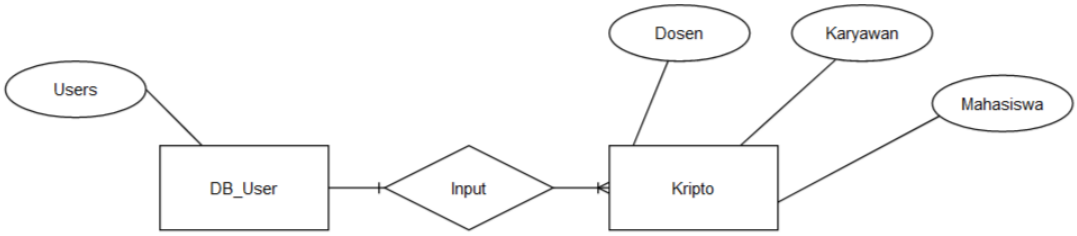

Figure 3. Database Relations

System Test

In this system test, encryption is carried out on the Performance Report Field in the lecturer table, the Performance Report in the employee table and progress reports in the student table. This time, the encryption uses the key set by the system, namely UNHAR for Vigenere Cipher and 3 for Triangle Chain Cipher.

Nama Dosen	NIDN	Nama Kampus	Alamat Rumah	Nomor Telepon	Laporan Kinerja
Adidtya Perdana	2147483647	Universitas Harapan	Jalan Amaliun no.5	2147483647	Melaksanakan Tugas sebagai Dosen dengan baik

Figure 4. Plaintext display result

In the first test there is a plaintext in the form of: Carrying out tasks as a Lecturer well

Figure 5. cipher display result

DISCUSSIONS

The use of a combination of 2 cryptographic methods is one way to strengthen the security of the data security program in the database, this is because an irresponsible party must find the algorithm and the key used in this method twice, which causes the cryptanalysis process to be long. The selection of the Vigenere cipher and Triangle chain cipher methods is based on the fact that both are classical cryptographic techniques that can be combined.

CONCLUSION

The following are the conclusions from the implementation of the combination of the Triangle Chain Cipher and Vigenere Cipher cryptographic algorithms in securing data in the database, namely:

In this study, the data security application used to keep messages secret in the database using a combination of the Triangle Chain Cipher and Vigenere Cipher algorithms was successfully applied.

The level of data security using this combination of algorithms is strong because to be able to find the contents of the initial message, you must search for methods from both algorithms.

ACKNOWLEDGMENT

in the accomplishment of this research, this time i am want to thank all the people who have help with this research. Primarily i would thank Allah for give me healthy and being able to complete this research with success. then i would like to thank my parents and all of my friend whose valuable support has been very helpful to completion this research.

*name of corresponding author

REFERENCES

Alasi, T. S., Al, A. T., & Siahaan, A. (2020). Algoritma Vigenere Cipher Untuk Penyandian Record Informasi Pada Database. *Jurnal Informasi Komputer Logika*, *1*(4). http://ojs.logika.ac.id/index.php/jikl

Alhogbi, B. G. (2017). Bab Ii Tinjauan Pustaka Dan Landasan Teori. *Journal of Chemical Information and Modeling*, *53*(9), 21–25. http://www.elsevier.com/locate/scp

Dakhi, O., Masril, M., Novalinda, R., Jufrinaldi, J., & Ambiyar, A. (2020). Analisis Sistem Kriptografi dalam Mengamankan Data Pesan Dengan Metode One Time Pad Cipher. *INVOTEK: Jurnal Inovasi Vokasional Dan Teknologi*, *20*(1), 27–36. https://doi.org/10.24036/invotek.v20i1.647

Eka Putra, A. (2021). (2021). *Perancangan dan Pengembangan Basis Data Tidak Terstruktur untuk Aplikasi Sentiment Analysis Twitter dan Instagram Bahasa Indonesia*. 6–30.

FAJRIN, R. (2017). Pengembangan Sistem Informasi Geografis Berbasis Node.JS untuk Pemetaan Mesin dan Tracking Engineer dengan Pemanfaatan Geolocation pada PT IBM Indonesia. *Jurnal Informatika*, *11*(2), 33–40. https://doi.org/10.26555/jifo.v11i2.a6090

Irawan, Y. (2020). Implementasi algoritma triangle chain cipher dalam penyandian pesan. *KAKIFIKOM : Kumpulan Artikel Karya Ilmiah Fakultas Ilmu Komputer*, *02*(02), 83–92.

Ismail, T., Informatika, U. I., Email, P., & Klasik, A. K. (2021). *Sistem keamanan pesan email menggunakan algoritma kriptografi klasik*. *4*(April), 47–57.

Istiono, W., Hijrah, & Sutarya. (2016). Pengembangan Sistem Aplikasi Penilaian dengan Pendekatan MVC dan Menggunakan Bahasa PHP dengan Framework Codeigniter dan Database MYSQL pada Pahoa College Indonesia. *Jurnal TICOM (Online)*, *5*(1), 53–59. https://media.neliti.com/media/publications/93757-ID-pengembangan-sistem-aplikasi-penilaian-d.pdf

Juliadi, Prihandono, B., & Kusumastuti, N. (2013). Kriptografi Klasik Dengan Metode Modifikasi Affine Cipher Yang Diperkuatdenganvigenere Cipher. *Buletin Ilmiah Mat. Stat. Dan Terapannya (Bimaster)*, *02*(2), 87–92.

Nurdin, A. P. N. (2017). Analisa Dan Implementasi Kriptografi Pada Pesan Rahasia. *Jesik*, *3*(1), 1–11. nnurdin69@gmail.com

Pahlevi, O., Mulyani, A., & Khoir, M. (2018). Sistem Informasi Inventori Barang Menggunakan Metode Object Oriented Di Pt. Livaza Teknologi Indonesia Jakarta. *Jurnal PROSISKO*, *5*(1). https://livaza.com/.

Roni, M. R. A. (2019). SISTEM INFORMASI E-COMMERCE PEMESANAN INTERIOR RUMAH DI ALFARUQ INTERIOR DENGAN MENGGUNAKAN METODE RAPID APPLICATION DEVELOPMENT (RAD). *Angewandte Chemie International Edition*, *6(11)*, *951–952.*, *2015*, 7–24.

Setyawati, E., Widjayanti, C. E., Siraiz, R. R., & Wijoyo, H. (2021). Pengujian keamanan komputer kriptografi pada surat elektronik berbasis website dengan enkripsi metode MD5. *Jurnal Manajamen Informatika Jayakarta*, *1*(1), 56. https://doi.org/10.52362/jmijayakarta.v1i1.367

Tarigan, E., & Maha, D. H. S. (2018). Kombinasi Vigenere Cipher Dan Polyalphabetic Cipher Pada Pengamanan File Text. *Publikasi Ilmiah …*, 71–77. http://jurnalnya.stmikneumann.ac.id/index.php/pitin/article/view/41

Yusfrizal, Y. (2019). Rancang Bangun Aplikasi Kriptografi Pada Teks Menggunakan Metode Reverse Chiper Dan Rsa Berbasis Android. *Jurnal Teknik Informatika Kaputama (JTIK)*, *3*(2), 29–37.

*name of corresponding author