ICRSH
INTERNATIONAL CONFERENCE ON RESEARCH IN SOCIAL SCIENCES AND HUMANITIES
International Conference on Research in SOCIAL SCIENCES & HUMANITIES
FRANKFURT, GERMANY
24-26 OCTOBER, 2019

Enhancing Database Transmission Security by Implementing Triangle Chain Cipher Algorithm

Windarto1), Ajat Sudrajat2)

1,2) Informatics Engineering, Faculty of Information Technology, Universitas Budi Luhur,
1,2) Jl. Ciledug Raya, Petukangan Utara, Jakarta 12260

ABSTRACT

Budi Luhur Salemba is a branch campus of Universitas Budi Luhur. To facilitate the management of students data, Budi Luhur Salemba use a database that would be sent later to Universitas Budi Luhur. Currently, the information contained in the Oracle database is taken by the application and converted into a JSON file form then transmitted to Universitas Budi Luhur by uploading through the Universitas Budi Luhur's website. The form of the uploaded information is still exactly the same as the raw data displayed as the final information, so it can still be seen by unauthorized parties. In order to keep the information accessed by unauthorized parties, a method of securing information is required so that the information transmitted is not easily seen or accessed by unauthorized parties. The method intended is the encryption method using Triangle Chain Cipher algorithm. Before the information being encrypted and uploaded on to Universitas Budi Luhur's website, student's data must be extracted from the Oracle database and then converted into an Access database. Once the information had been encrypted, then the encrypted information would be sent over the website or email. When the information had been received, the must be decrypted before being processed. This symmetric algorithm works twice, so that each characters is substitute with a key and a factor that is used as a multiplier as in the algorithm formula. The encrypted Database will be transformed into an ASCII code as cipher text. The result is by implementing Triangle Chain Cipher algorithm in the application, student's information and data student's information and data that would be sent to the central campus is expected to be more protected from unauthorized parties' access.

Keywords: communication; cryptography; database; information; security; triangle chain cipher.

1. INTRODUCTION

The rapid development of information technology and accompanied by the increasing needs to accessing information, has been impact on changes of the mindset of the society, institutions or companies in obtaining information. For example, information that was once easily obtained from printed media, now easily obtained on the internet. As the importance of the accurate and reliable value information, makes computer experts to think about how to secure confidential information that should not be known by anyone. This is should be done, so that the information is safely keep, which will makes tranquility to its users.

Budi Luhur Salemba is a branch campus of Universitas Budi Luhur. To manage its student's data, it's use an academic information system where its data is stored in the oracle database. The information in the database will periodically be retrieved and converted in to the JSON file format to be sent to the central campus. Currently, the information which sent to the central campus is exactly still the same as the final displayed information, so that it can still be seen by unauthorized parties. The impact is the vulnerability of the data to alteration, addition, even manipulation by unauthorized parties.

To minimize any misuse of information, the branch campus needs to secure its students data before being sent to the central campus. Therefore, an information security technique is needed. Cryptography is one of the information security techniques. By using cryptography, information will be changed in to an encoded form of its original information so it is unreadable by unauthorized parties. Furthermore, if the information is being stolen, it is not easy to read because it does not formed as its original information. One of the cryptographic methods that can be used to encode information is Triangle Chain Cipher algorithm. This algorithm performs the encoding of the characters twice and reverted in the results of the previous process, each character is substituted with the key and the factor used as a multiplier that generates the encoding based on the 256 ASCII code.

By encrypting the student's academic information which will be sent to the central campus, it is expected that the information will be more protected from a misuse of unauthorized parties. Looking at the above background, it can be formulated that the problem in this research is that the academic information of students which sent from the branch campus to the central campus is still in its original form so it is vulnerable to be abused if there is an information theft.

After analyzing the problem, the research question is how to secure the student's academic information so that the information sent from the branch campus to the central campus is not easily known by unauthorized parties?

In order to make this research be more directed and not to come out from the topic, the authors give some boundaries as follows:

a. The algorithm that will be implemented to encrypt and decrypt data is a traingle chain cipher.
b. The data that will be encrypted is the student's academic data on the table of MSTUDENTWACABANG.
c. The encrypted data will be stored in Ms. Access format.
d. The encryption results will be displayed based on 256 ASCII code.
e. The key that will be used to the encryption and decryption process is numbers between 1 to 20.

2. THEORY

2.1 DATABASE

Databases are a collection of data or digital information that is systematically generated and can be modified by its creators and accessible at all times. The Database consists of rows and columns (tables) and can be interconnected with other tables. By implementing the database, data and information management will be more efficient [5].

2.2 CRYPTOGRAPHY

According to Smart [3], an encryption algorithm, or cipher, is a means of transforming plaintext into ciphertext underthe control of a secret key. This process is called encryption or encipherment Cryptography is present to minimize any form of theft crimes, data manipulation by unauthorized parties.

The cryptographic algorithm consists of three functions [1] that is:

a. Encryption: is the security of data or information kept confidential. Encryption can also be interpreted as the process of manipulating a data or information so it is difficult and not even easy to understand.

b. Decryption: Is the process of returning data or information that has been previously secured to the original without any damage.
c. Key: The key used for the encryption and decryption process consists of two keys namely the secret key and the general key.

Figure 2:1 Cryptographic Mechanism

The cryptographic process is essentially very simple. PlainText will be passed on the encryption process so it will generates ciphertext. Then, to regain the plaintext, the ciphertext decryption process will generates back the plaintext.

In addition of utilizing an algorithm, modern cryptography also use keys to encrypts and decrypts the plaintext.

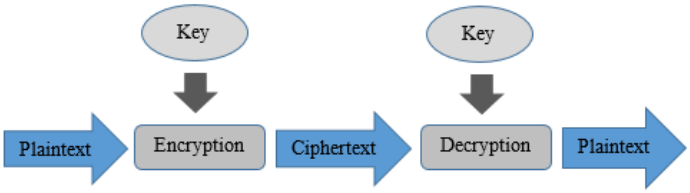


Figure 2.2: Key-based Cryptography

The cryptographic mechanisms in figure 2.2 are called key-based cryptography. The cryptosystem will consists of algorithm and key along with all its plaintext and ciphertext.

In its evolution there are two types of cryptosystem algorithm, namely the symmetric key encryption algorithm and the asymmetric key encryption algorithm.

a. Symmetric Cryptosystem

Symmetric cryptosystem uses a key that is principally identical to the encryption and decryption process, but a piece of key can also be derived from other keys. The symmetric cryptosystem is sometimes called secret-key cryptography which is more traditional form of cryptography, where a single key can be used to encrypt and to decrypt messages.

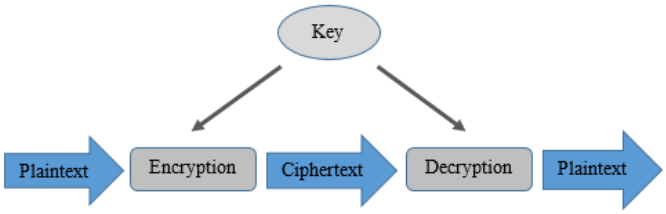


Figure 2.3: Symmetric Cryptosystem

By using a symmetrical cryptosystem, the sender and the recipient of the information must approve the used key where both of parties are not afraid of messages being stolen. Despite its weakness, the symmetrical crypto-system also has advantages such as faster in processing the encryption process compared to the asymmetric crypto-system.

b. Asymmetric Cryptosystem

Asymmetric crypto-system uses two piece of keys. One key can be published know as a public key, while the other key must be keep confidential also known as secret key, figure 2.4 below illustrates the asymmetric cryptography:

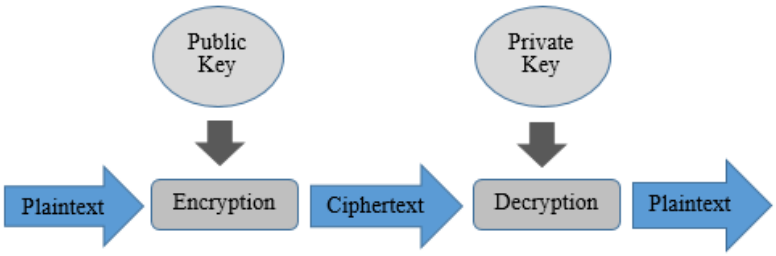


Figure 2.4: Asymmetric Cryptosystem

(1) Public key: is a key that anyone can know.

(2) Private key: is a key that is strictly confidential (should not be published).

Using the public key, user can only encrypt the data or message but unable to decrypt it and only the user who has the secret key who's able to decrypt it back. Asymmetric cryptosystem is able to send data more secure than symmetrical cryptosystem.

2.3 TRIANGLE CHAIN CIPHER (TCC) ALGORITHM

According to Hondro and Nurcahyo [2]. a cryptographic algorithm of the Triangle Chain cipher is the development of the One Time PAD algorithm where the keys are used

automatically and the large number of keys plaintext. This algorithm has similar rule to Caesar Cipher algorithm where each of its characters will be slides using a key. To slide the characters, the key that is used in this algorithm must be in an integer value. The characters will be encrypted twice and the next result will depend on the previous encryption result that's why it is called a chain triangle algorithm. This algorithm also improve the single-alphabet substitution encryption technique that is susceptible to a frequency analysis.

a. TCC Encryption Algorithm

The following are the encryption formulas for the triangle chain cipher:

1) First triangle encryption matrix formula

First row formula:

$$M_{[1j]} = P_{[j]} + (K * R_{[1]}) \, mod \, 26$$

Second row formula and so on for $j \geq i$

$$M_{[ij]} = M_{[i-1]j} + K * R_{[i]}) \, mod \, 26$$

Thus obtained ciphertext value as follows:

$M_{[ij]}$ by the value of $j = (N + i) - N$

2) Second triangle encryption matrix formula. Value of P obtained from M_{ij} at $i = j$

First row formula:

$$M_{[1j]} = P_{[j]} + (K * R_{[1]}) \, mod \, 26$$

Second row formula and so on for

$j \leq (N + 1) - i$

$$M_{[1\ j]} = M_{[i-1]} + (K * R_{[i]}) \, mod \, 26$$

Thus will be obtained ciphertext value as follows:

$M_{[ij]}$ by the value of $j = (N + 1) - i$

Details:

P = Plaintext or character

N = number of characters or plaintext

M = Matrix that holds the encryption result

K = Encryption Key

R = Row (is the multiplier factor that will be multiplied by the key)

i = is the index factor as multiplier

j = Character index or plaintext on the row

b. TCC Decryption Algorithm

The following are the encryption formulas for the triangle chain cipher:

1) First triangle decryption matrix formula

First row formula:

$$M_{1j} = C_{[j]} - \left(K * \left(R_{[1]}\right)\right) mod\ 26$$

Second row formula

$$j \leq (N+1) - i$$

$$M_{[ij]} = M_{[i-1]j} - \left(K * \left(R_{[i]}\right)\right) mod\ 26$$

After the plaintext obtained from the first triangle process, then it will take each rows with the following formula:

$M_{[ij]}$ by the value of $i = n$ and $j \leq (N+1) - i$

2) Second triangle decryption matrix formula.

First row formula:

$$M_{1j} = C_{[j]} - \left(K * \left(R_{[1]}\right)\right) mod\ 26$$

Second row formula for $j \geq i$

$$M_{[ij]} = C_{[i-1]j} - \left(K * \left(R_{[i]}\right)\right) mod\ 26$$

Thus will be obtained the plaintext value as follows:

$M_{[ij]}$ by the value of $j = (N+i) - N$

Details:

N = number of characters or plaintext

M = Matrix that holds the encryption result

K = Encryption Key

R = Row (is the multiplier factor that will be multiplied by the key)

i = is the index factor as multiplier

j = Character index or plaintext on the row

3. DESIGN

3.1 System Architecture

The design phase is a process that should be done before built the application. In general, the application to be built is a desktop-based database security application which implements a symmetric key cryptographic algorithm that is the Triangle Chain Cipher algorithm. [6]

Figure 3.1 illustrates the system architecture design.

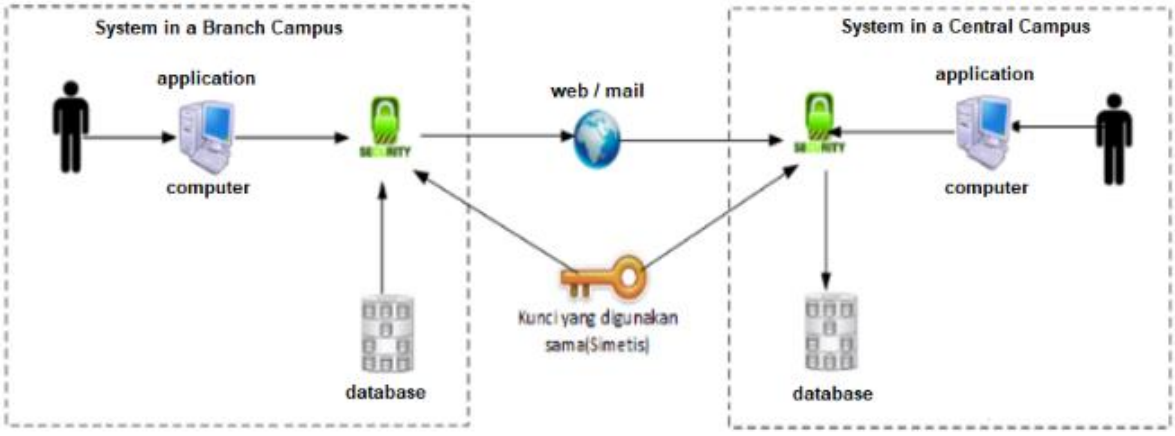
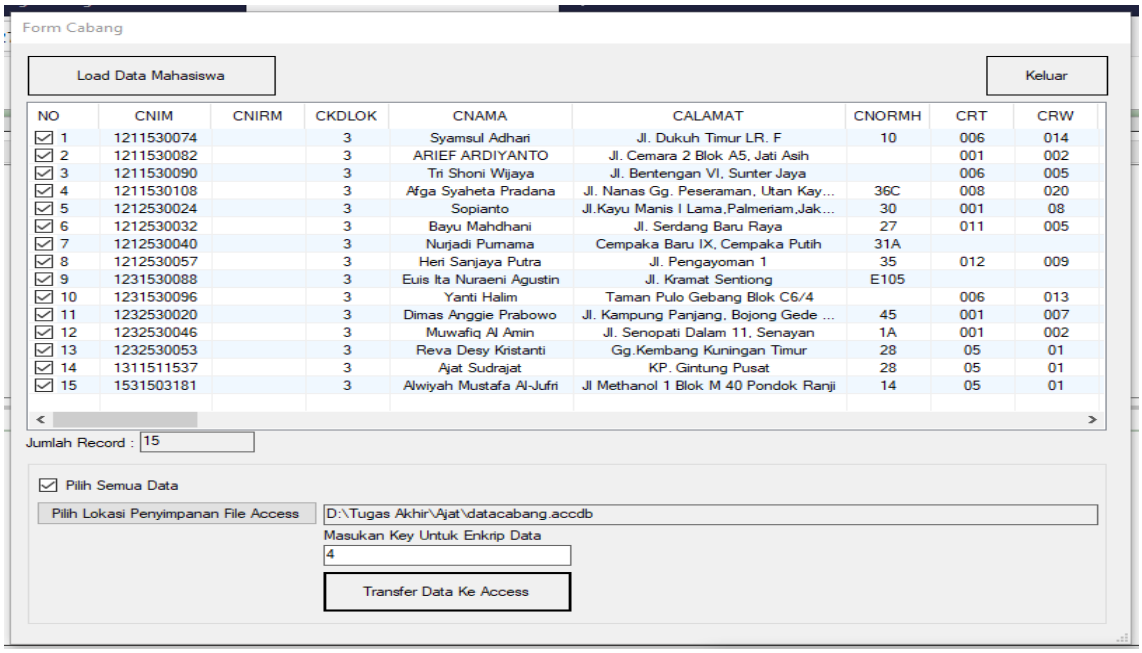


Figure 3.1: System Architecture

4. DISCUSSION

4.1 Encryption Testing Process

The encryption testing process is done by retrieving the students data from the table of MBLOWWACABANG in the database. After the data has been encrypted, it will be saved to Ms. Access file format. The following image is a testing result after encrypting fifteen records.



NO	CNIM	CNIRM	CKDLOK	CNAMA	CALAMAT	CNORMH	CRT	CRW
1	1211530074		3	Syamsul Adhari	Jl. Dukuh Timur LR. F	10	006	014
2	1211530082		3	ARIEF ARDIYANTO	Jl. Cemara 2 Blok A5, Jati Asih		001	002
3	1211530090		3	Tri Shoni Wijaya	Jl. Bentengan VI, Sunter Jaya		006	005
4	1211530108		3	Afga Syaheta Pradana	Jl. Nanas Gg. Peseraman, Utan Kay...	36C	008	020
5	1212530024		3	Sopianto	Jl.Kayu Manis I Lama,Palmeriam,Jak...	30	001	08
6	1212530032		3	Bayu Mahdhani	Jl. Serdang Baru Raya	27	011	005
7	1212530040		3	Nurjadi Purnama	Cempaka Baru IX, Cempaka Putih	31A		
8	1212530057		3	Heri Sanjaya Putra	Jl. Pengayoman 1	35	012	009
9	1231530088		3	Euis Ita Nuraeni Agustin	Jl. Kramat Sentiong	E105		
10	1231530096		3	Yanti Halim	Taman Pulo Gebang Blok C6/4		006	013
11	1232530020		3	Dimas Anggie Prabowo	Jl. Kampung Panjang, Bojong Gede ...	45	001	007
12	1232530046		3	Muwafiq Al Amin	Jl. Senopati Dalam 11, Senayan	1A	001	002
13	1232530053		3	Reva Desy Kristanti	Gg.Kembang Kuningan Timur	28	05	01
14	1311511537		3	Ajat Sudrajat	KP. Gintung Pusat	28	05	01
15	1531503181		3	Alwiyah Mustafa Al-Jufri	Jl Methanol 1 Blok M 40 Pondok Ranji	14	05	01

Figure 4.1 Original Data Before Encryption

After the encryption process succeeded, the data will be saved into the Ms. Access file format.

MMAHASISWACABANG

CNIM	CNIRM	CKDLOK	CNAMA	CALAMAT	CNORMH	CRT	CRW	CNOTELP	CKDPOS	CTEMPLHR
1211530074		{	[qÑÝÉ½~‰¼Ø‹Ùq	Š¾tdi;}è"ÄÝ¡Bôl¦¾ô†	¡	ÌÈÒ	ÌÉÐ	üÚ½¥ œœ¯Ãü:		Þáß‹Ñæôõ
1211530082		{	¥,M%ê°ÅÒÈÙý!R„³	®\' Ç•Qá¶qàÒ¤²ÐÏÅÕßõŽâX™¤AxYÌ		ÌÈÍ	ÌÈÎ	üÚ½¥¤š«ÁØ$	QKDFS	š-«¡»Á
1211530090		{	8þÅTgd[RMíS)ž½%E	ZðNÀ'i,Ø•rG%þ¤ÓÍ¼Ä3yŽØ%vpíÿq		ÌÈÒ	ÌÈÑ		QHCIP	;N;&33=b
1211530108		{	íÊ‹M¼Ç¡"‰™\tæ›ÿP...Ò-	¾HZ¤RÍjÕ‡¼"kÒŒŒygA>%1-J 4'à%rÍçuíqŒYøNÕ	ÍÍß	ÌÈÒ	ÌÉÎ	IF%éåŸÝßi&Et	QGAFP	Þáß‹Ñæôõ
1212530024		{	GK<-%:Pc	fÀÂG-=™¬iÕ¢EßD-¬¯•]ø4EXiy¦ÅíQP¶=ŸõŽ ...Ä e!ÉŽ	£	ÌÈÍ	¨	IL+óåÚÔãï&DI	QGAHP	Þáß‹Ñæôõ
1212530032		{	ÒÅ¹™0QaltŒ¡Òù	Š¾tsYBøáâx"ÂõBi@¦,ñm¡	¢§	ÌÉÍ	ÌÈÑ	üÚ½¥ š©½Ù$		Þáß‹Ñæôõ
1212530040		{	²¥vJ%ôí Ô%6NeÅ	ë=ÀY6¡ êÙÂ¥8QX,([•½è}ki¨HÅDj0	ÏÉÝ			üÚ½¥ šœ-ÂÞ#		Þáß‹Ñæôõ
1212530057		{	øÕ³qàóéæÚÑñéÀ0}¬â1	.øŠTdaZKEek•Ê¬õ	£¥	ÌÉÎ	ÌÈÕ		QGAFP	¬©¬¡¶¿
1231530088		{	9ñ•Wπ•UÔê!öàñ*=ô]³ùW åb	†dÊ^‡Š]U=LÜ;a†°Ñ+f£	1Ôô!					š°¥¢-Ë
1231530096		{	E}úlÕ^`Ù¤1Y	©YÙšèÜÍ˜`wïÿ1*-FS(nÄûSL»"wà		ÌÈÒ	ÌÉÏ		QGIEP	Þáß‹Ñæôõ
1232530020		{	ðÍ'M/"•ª",‹'\tæ›ýN"Û;	¾HZ¤Oíïã‰ª³Şôíª~UJ3ÐÄïK^f³ÓÄK± ÿ"?Ôxå¥=á	¤¥	ÌÈÍ	ÌÈÓ	,óåÜÛbï&		Þáß‹Ñæôõ
1232530046		{	±¥{A*üð ÅüÄ!q™Ò	òπÞpKí®o8ÙÄ™8Lali...P©Ô "if±!™6	¡±	ÌÈÍ	ÌÈÎ	üÚ½¥¡šC¯ÅÚü	QFAMP	Þáß‹Ñæôõ
1232530053		{	Ž]2É\\a[UØ'Ze‹°É°!¥	¿fÔ§}lê½¦ƒ{Gmjqš'Ý½öÜÍÅ5'ê	¢¯	¥	¡			<EXU
1311511537		{	Ñîı˜0Wuh,„.ª Å$	ª\æ¬˜µ¦ šŸl,!Km¼	¢¯	¥	¡			<EXU
1531503181		{	5è£Mý-„ô!1ÿøàòýÔ5˜ýÎY'Ï]	vß$'aè¦ý¤s0Œm46H;/ÃùÜ{D\¼3r°+‼"Nírí•	¡¤	¥	¡			<EXU

Figure 4.2: Encrypted Data

4.2 Decryption Testing Process

The decryption testing process is done by reversing the encrypted Ms. Acess file to its original form. The following image describes the decryption process.

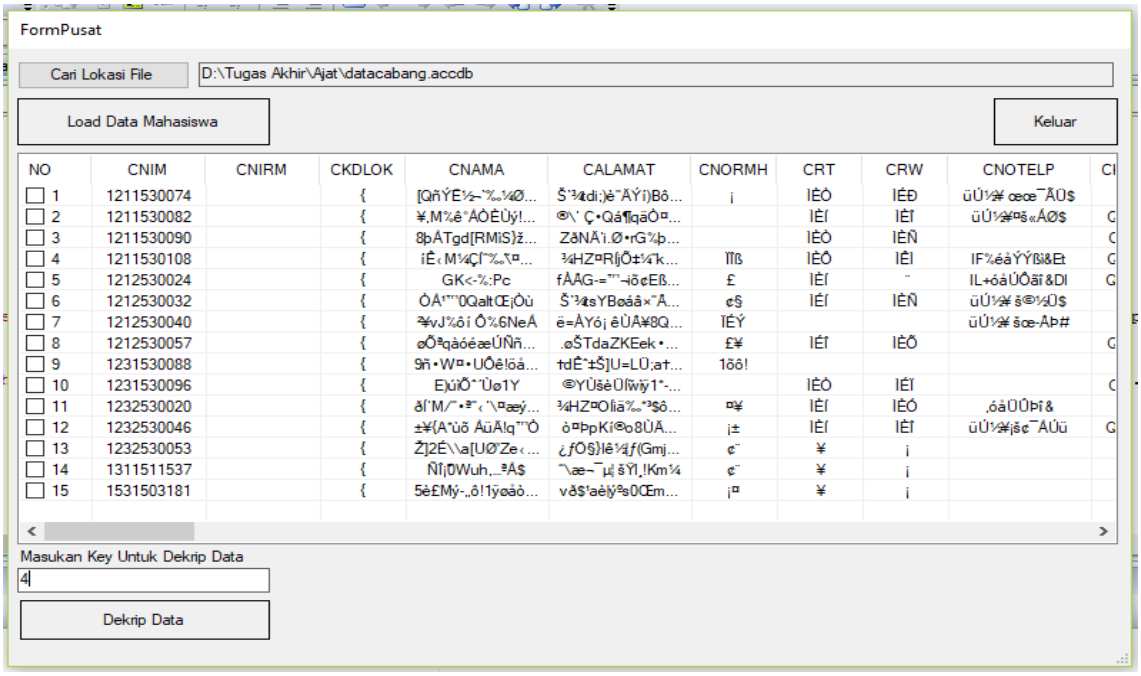


Figure 4.3: Decrypted Data

Once the data is successfully restored to its original form, the data will be transfered to the database

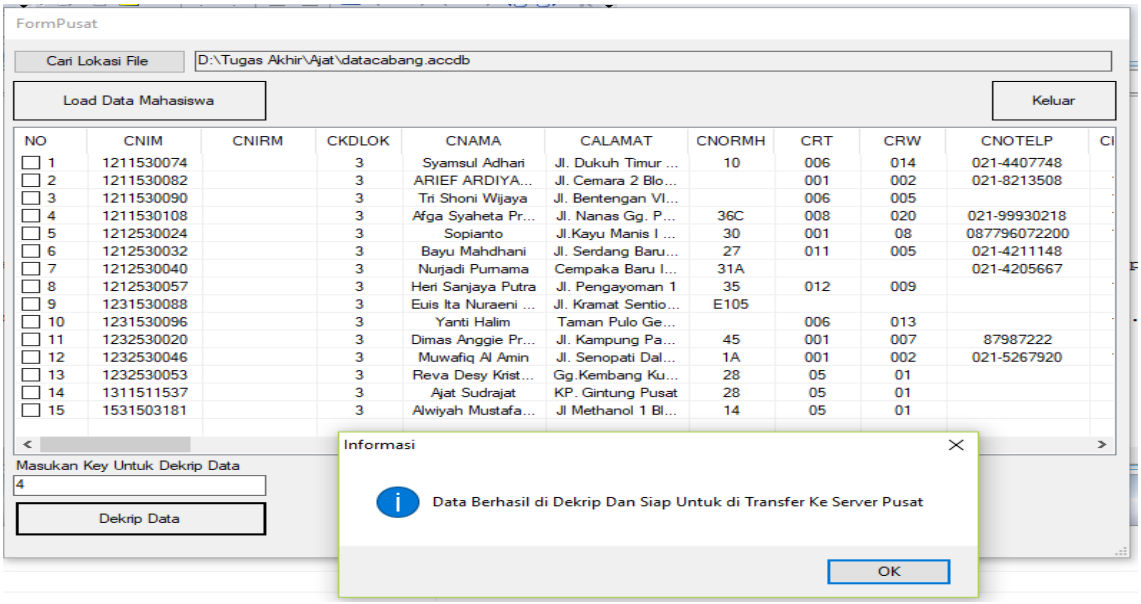


Figure 4.4: Original Data After Decryption

4.3 Encryption and Decryption Testing Results

In the following table 4.1 and 4.2, it discusses the comparison between the encryption and the decryption process of the records in the table of MSTUDENTWACABANG.

Tabel 4.2: Encryption Testing Results

Testing	No. of Records	Previous Size (bytes)	Following Size (bytes)	Processing Time (seconds)
1 st Testing	1 Record	283	283	07.20
2 nd Testing	2 Records	560	560	11.40
3 th Testing	15 Records	4,502	4,502	01:19.31

Tabel 4.2: Decryption Testing Results

Testing	No. of Records	Previous Size (bytes)	Following Size (bytes)	Processing Time (seconds)
1 st Testing	1 Record	283	283	05.34
2 nd Testing	2 Records	560	560	09.62
3 th Testing	15 Records	4,502	4,502	01:15.54

4.4 Result Analysis

Based on testing results, it can be analyzed that there are several advantages and disadvantage of the application that has been built, as follows:

(1) Advantages

(a) The decryption process is faster than the encryption process.

(b) The decrypted data is not damage and the users are able to read it.

(2) Disadvantage

(c) The application only able to encrypt text.

5. RESULTS

5.1 CONCLUSION

Based on the testing result which has been discussed in various data set, it can be conclude that:

a. By implementing the Triangle Chain Cipher algorithm in an application, it can secure the student's academic information before being sent via internet from unauthorized parties.
b. The application can perform the encryption and decryption process to the table of mstudentwacabang and its records.
c. Application can restore the encoded data to original data without any damages and changes.

5.2 SUGGESTIONS

Although this application has been able to function as expected, yet it has some shortages. Therefore, development to improve the capabilities of the application is still necessary. Some feedback and suggestions to improve and develop the next application are as follows:

a. The application is to be expected to have a capability to encrypt another data format other than text.
b. The application is to be expected to have a capability to compress data, thereby it could save the storage space.

DAFTAR PUSTAKA

[1] Barakat, Mohamed, Christian Eder, Timo Hanke. 2018. *An Introduction to Cryptography*. Kaiserslautern: The University of Kaiserslautern.

[2] Hondro, R.K., dan Gunadi, W.N., 2014. Analisis dan Perancangan Sistem yang Menerapkan Algoritma Triangle Chain Cipher (TCC) Untuk Enkripsi Record Tabel Database. *Jurnal Teknologi Informasi & Komputer*, 3(2), hal. 118-127.

[3] Smart, Nigel, Cryptography: An Introduction, 3rd ed. NY: McGraw Hill.

[4] Singh, S., 2016. Implementasi Pengamanan File Text dengan Metode Triangle Chain Cipher dan RC4. Available: http://repository.potensi-utama.ac.id/jspui/handle/123456789/1290

[5] Situmorang, H., 2016. Keamanan Basis Data Dengan Teknik Enkripsi. *Jurnal Mahajana Informasi*, vol. 1(1), pp. 22-27.

[6] Sommerville, I., 2009. *Software Engineering*. 9th ed. Scotland: Pearson