Application of Classical Cryptography in Text Communication

Wayan Darsana[1]
[1] Universitas Islam Negeri Sumatera Utara, Medan, Indonesia
[1]Sistem Informasi, Fakultas Sains dan Teknologi, Universitas Islam Negeri Sumatera Utara, Medan, Indonesia
[1]wayandsn@gmail.com

Article Info

Article history:

Received january 09, 2024
Revised january 27, 2024
Accepted february 05, 2024

Keywords:

classic cryptography
chat application

ABSTRACT

Advancements in data communications and computer networks have facilitated communication among numerous individuals using various hardware and software technologies. However, this progress also brings about a significant challenge: data and information security. Safeguarding data and information transmitted over communication networks necessitates the implementation of a data security system. One effective approach to achieve this is by utilizing cryptographic techniques. Cryptography involves encoding data transmitted through a network in a manner that only authorized parties can decipher. Data that remains unencrypted is referred to as plaintext, and once encrypted, it becomes ciphertext. Before the advent of computers, cryptography relied on character-based algorithms, often known as classical cryptographic algorithms. This research focuses on applying classical cryptography to encrypt and decrypt text data exchanged via chat applications. The test results demonstrate that the encryption and decryption processes effectively maintain data confidentiality.

Corresponding Author:

Wayan Darsana
Universitas Islam Negeri Sumatera Utara
Email: wayandsn@gmail.com

1. INTRODUCTION

Communication in the era of information technology no longer requires physical meetings. Technological advances make communication possible using a variety of hardware and software. One common way to communicate is through text messages. By sending text messages, information can be easily transmitted from the sender to the recipient. Sending text messages can be done via various platforms, including email, chat, SMS, and other forms of text communication.

The chat application is an example of text-based communication that is often used on social media. In addition, web services such as Facebook and Yahoo also provide chat features that allow users to send messages via the Internet.

Chat applications are often used because of their ease of use, even when someone is busy, they can still access this application. Using services such as Yahoo Messenger or Facebook Messenger requires a continuously active internet connection. However, not all computers, whether in the office or at home, have internet access. Most computers in offices are still connected to a Local Area Network (LAN). Therefore, a chat application is needed that can operate on a network like this.

Messages exchanged between chat application users need to be equipped with data security services to ensure that only people who have permission can access the contents of the messages. Even though communication is carried out offline via a LAN network, there is the potential that this communication path can be accessed by hackers who want to access the messages being transmitted. Therefore, a mechanism is needed to maintain the confidentiality of the messages sent.

Therefore, this research will raise two main problems, namely:

1. How do you develop a chat application that uses a Local Area Network (LAN) network?
2. How do you secure messages on chat applications to ensure the confidentiality of the contents of the messages sent?

2. METHOD

Cryptography comes from Greek and consists of two words, namely "crypto" which means to hide, and "graphia" which means writing. Cryptography is a scientific discipline that focuses on mathematical techniques related to aspects of information security, such as data encryption, data validity, data integrity, and data authentication. However, it is important to remember that cryptography cannot always solve all information security problems [1].

Cryptography can also be interpreted as the art or science of protecting message security. When messages are sent from one location to another, there is a possibility that the contents of the message can be accessed by unauthorized parties. To keep the message safe, the message can be changed into a code that cannot be understood by other parties [2].

Encryption is an encoding process that changes an understandable code or message (plaintext) into an incomprehensible code (ciphertext). Conversely, the process of changing ciphertext back into plaintext is called decryption. Both of these processes require special mechanisms and certain keys [1]. Cryptography is a science related to encryption techniques where data is encrypted using an encryption key so that it is difficult to read by parties who do not have the decryption key [1]. To return data to its original form, a decryption key is required. The encryption process is carried out using an algorithm with several parameters. Often, the algorithm itself is not kept confidential; instead, security lies in the use of certain parameters as keys.

Characteristics of classical cryptographic algorithms include being character-based and using symmetric keys. In classical cryptography, the encryption technique applied is symmetric encryption, where the decryption key is identical to the encryption key, as seen in Figure 1.

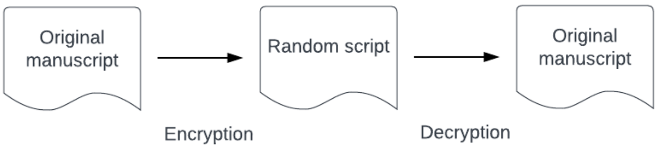
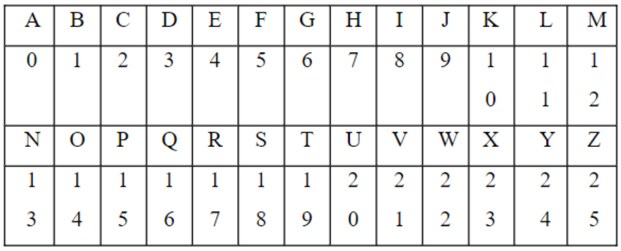


Figure 1. Encryption and Decryption Process

Caesar cipher is a classic algorithm. In classical cryptography, it is generally divided into two models, namely substitution and transposition techniques [3]. The substitution technique involves replacing characters in text with other characters. One example of a substitution technique is Caesar's cryptography. The method involves mapping A-Z characters into a series of numeric indices, as shown in Figure 2.



A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	1 0	1 1	1 2
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1 3	1 4	1 5	1 6	1 7	1 8	1 9	2 0	2 1	2 2	2 3	2 4	2 5

Figure 2. Character Mapping

The Caesar cipher algorithm involves shifting characters in text by using a key (k) which has a value range from 1 to 25. This can be explained mathematically as follows:

In the encryption process stage,

$$C = E\ (k, p) = (p + k)\ mod\ 26 \qquad (1)$$

To carry out the decryption process,

$$P = D(k, c) = (C - k) \bmod 26 \qquad (2)$$

From an application perspective, the connection between these computers occurs via a connection from one socket to another. This socket is a pair of values used to identify each end of an IP address and its associated port number [5]. To be able to communicate between two computers, the ports on each end must be open. The stages for initiating a connection between a client computer and a server can be described as follows.

1. The server starts by creating a socket that has unique characteristics (for example, by specifying an IP address and port number), so that it can be identified and found by the client. At this time, the server enters a "listening" state, which means the server is ready to accept service requests from clients.
2. The client also creates a socket, looks up the server's socket name or address, and then "connects" the socket to initiate communication.
3. After initiation is complete, the client and server can send and receive data to each other.

In developing the system to be built, we use the Basic programming language. This programming language is often chosen by beginners in the world of programming because of its ease of use and lack of strict rules when compared to procedural programming languages such as C or Pascal. In Visual Basic, the application design process begins with defining program objectives, designing views that will be used to communicate with users, and writing program code [4].

In programming using Visual Basic, the term often used is "object." These objects are used at the program layer to set the properties defined by that object. When the program is run, methods can also be applied to these objects according to the program's purpose. The process of creating an application with Visual Basic begins with creating a form first, followed by creating files and other modules. After these components have been combined and the program code has been written, the next step is to make the project into an executable file [4].

Research in the field of text-based communication (chat) has been carried out a lot. One of them is research conducted by Setiawan [5], who developed a chat application using a LAN network. This application can be used by several people simultaneously (multiuser) and also has facilities for sending files, which increases the effectiveness of communication between users. However, the weakness of this application is the absence of a history facility that records the contents of communications that have been made, so it cannot be accessed again in the next communication session. Research conducted by Zakaria [6] also developed chat communication technology using computers and cell phones via Bluetooth connections. In the developed system, there is a history facility that stores communication information that has occurred before.

Research on data encoding was carried out by Hasugian [7], who developed the Hill Cipher encoding technique for database storage. Information stored in the database is divided into several blocks, then an encryption process is carried out. This system was developed using the Visual Basic 6 programming language to carry out the encoding process in the database. The use of classical cryptography has also been researched by Fairuzabadi and Sasongko, who developed a data security system using the Delphi programming language and the C/C++ language. This research emphasizes the programming aspect by integrating mathematical formulas into programming languages.

In this research, what was done was to develop a chat application by applying classical cryptographic techniques. The main goal is that the information sent by users communicating in the system can be kept confidential.

3. RESULTS AND DISCUSSION

In the developed text-based communication process, messages are sent in the form of encrypted text (ciphertext). When the message arrives at the recipient's side, the message is converted back into plaintext, as can be seen in Figure 3. This entire process occurs through a Local Area Network (LAN) network. This system is a simple chat application that uses the Caesar cipher algorithm to encrypt the messages sent. This system allows two users to communicate via TCP/IP.

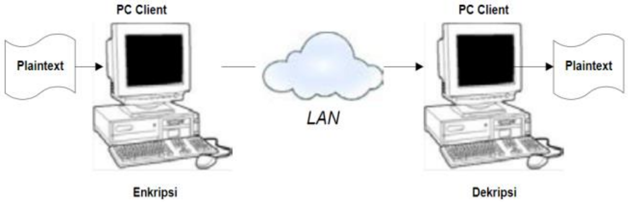


Figure 3. Design of the System Built

In general, the services available in the built application can be seen in Figure 4. This application provides facilities for filling in names and connecting to LAN networks. When carrying out the message-sending process, you are always involved in the encryption process, which involves the method/function for carrying out encryption. When reading a message, always use the decryption use case to return the encrypted message so that the message can be read by the system.

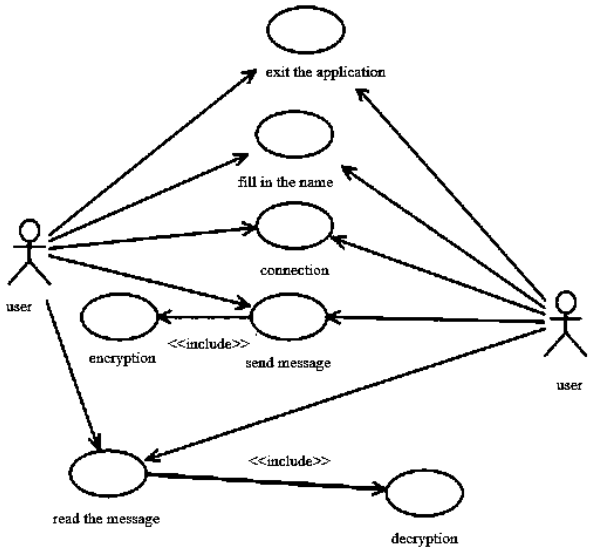
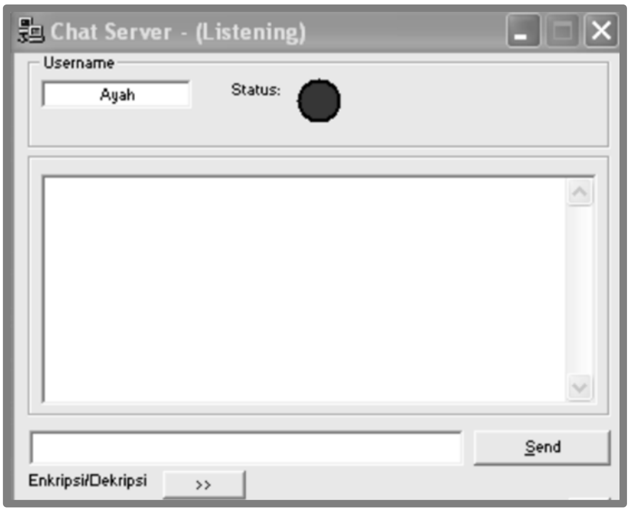


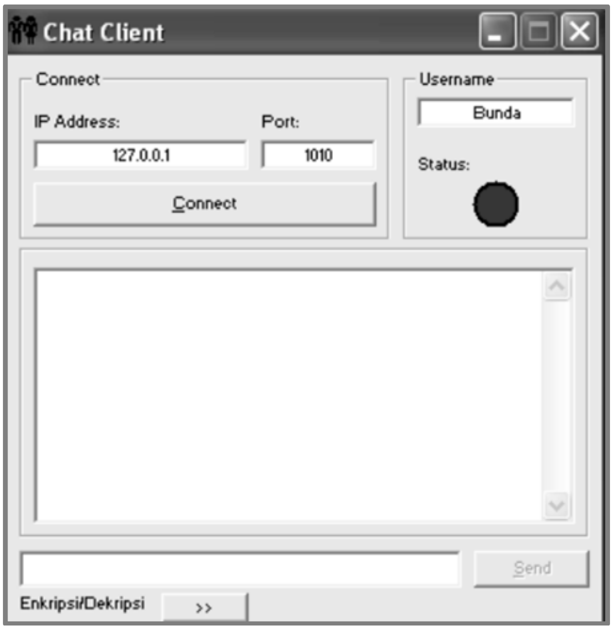
Figure 4. Use Case System Diagram

This research produces software that is developed in a client/server environment with a visual/desktop application model.

The application created includes two applications, one as a server and one as a client. The server application functions to wait for communication requests from the client, while the client must initiate communication. When both applications are activated, both will display a red light indicator, indicating that communication between the client and server has not been established, as seen in Figure 5.



(a) Server position waiting for requests



Chat Client

Connect

IP Address: 127.0.0.1

Port: 1010

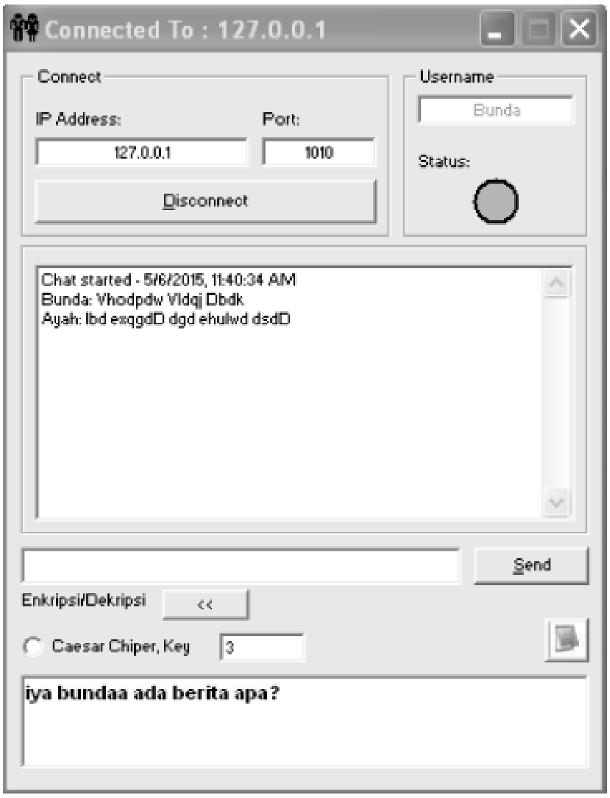
Username: Bunda

Status:

(b) The client position is active for the first time

Figure 5. Position of Client and Server Applications When Activated for the First Time.

Once communication is established, both indicator lights on both applications will turn green, indicating that communication has been successfully established. Text sent via the application will be encrypted using the Caesar Cipher algorithm with a shift of 3 characters, as seen in Figure 6. At the bottom of the application panel, there is text that can be read (plaintext), so that every time a message-sending session is carried out, the message will be automatically decrypted so it can be read by the recipient. During the real-time communication process, the key shift parameters of the Caesar Cipher algorithm can be changed, as seen in Figure 6, where the key shift is currently set to 3 characters.



Connected To : 127.0.0.1

Connect

IP Address: 127.0.0.1

Port: 1010

Username: Bunda

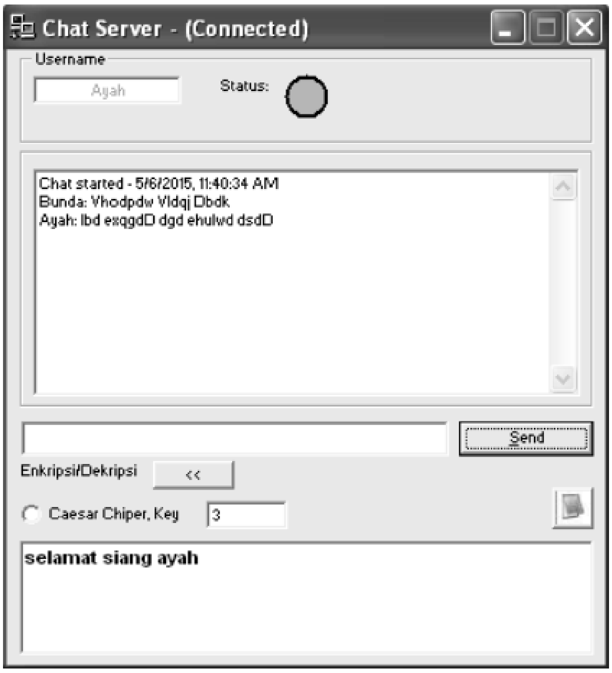
Status:

```
Chat started - 5/6/2015, 11:40:34 AM
Bunda: Vhodpdw Vldqj Dbdk
Ayah: lbd exqgdD dgd ehulwd dsdD
```

○ Caesar Chiper, Key 3

iya bundaa ada berita apa?

(a) Text on Client Application



Chat started - 5/6/2015, 11:40:34 AM
Bunda: Vhodpdw Vldqj Dbdk
Ayah: lbd exqgdD dgd ehulwd dsdD

selamat siang ayah

(b) Text on the Server Application

Figure 6. Text Delivery Pattern

At the bottom of the client and server applications, there is also a text file that contains the results of the process of sending messages in plaintext. So that after all text-based communication sessions have been completed, you can see the overall communication that has occurred. The results of the conversation session are saved in one text file so they can be opened easily using a text editor application such as Notepad.

Several tests carried out from the application side using the black box method can be described in Table 1. Black box testing is a software testing method that focuses on the functionality side, especially on the application input and output (whether it is what is expected or not). The testing or testing phase is one of the stages that must exist in a software development cycle (besides the design or design stage).

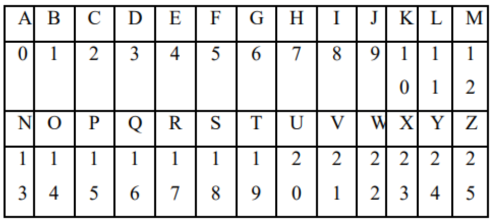
Table 1. Black Box Testing of Chatting Applications

No.	Test scenario	Test Case	Expected results	Test result	Conclusion
1	Fill in the name as the identity of the user who uses the application and makes the connection	Name: -	The system will respond that the connection process to start communication can be done after the user enters the name.	According to expectations.	Valid
2	Empty all message data fields, then press the Send button.	Message: -	The system will reject the message-sending process by displaying the information that "Message is Still Empty"	According to expectations.	Valid
3	Enter the message to be sent to the recipient. The message sent was a 'good afternoon' greeting. When the message arrives at the recipient's side it will be encrypted as 'shoddy vldqj'	Message: good afternoon	The system will encrypt messages using the Caesar cipher algorithm with a key shift of k=3.	According to expectations.	Valid

In terms of information content, the application that has been developed has also gone through a series of tests to measure the extent of the capabilities of the classical cryptography module integrated into the system. This test is carried out using input in the form of plaintext or ciphertext to observe the resulting output. The Caesar Cipher algorithm uses the modulus or remainder operation. The a/n division operation on integers produces two outputs, namely the quotient (q/quotient) and the remainder (r/remainder). The relationship between these four numbers is expressed in equation [1]:

$$a = q \times n + r \qquad (3)$$

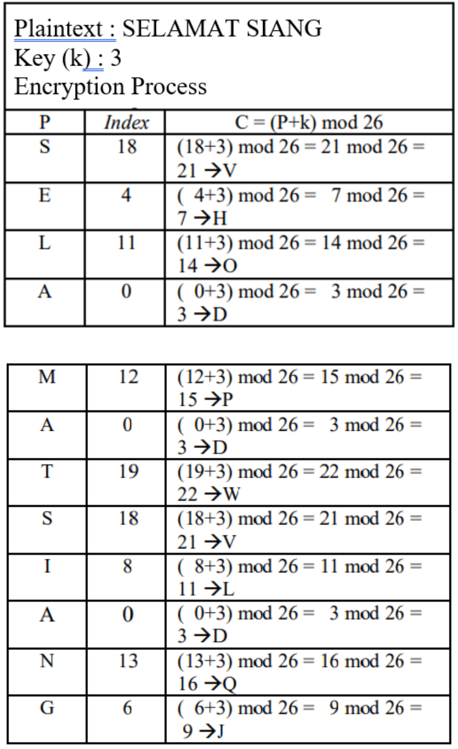
To understand how the Caesar Cipher algorithm works, we can use Formula 1) for the encryption process and Formula 2) for the decryption process. For example, if we have a plaintext "GOOD AFTERNOON," then the encryption and decryption process can be carried out with the steps shown in Table 2 and Table 3. In addition, the character mapping can be seen in Figure 7.



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

Figure 7 Character Mapping into Numerical Index

Table 2 Encryption Process

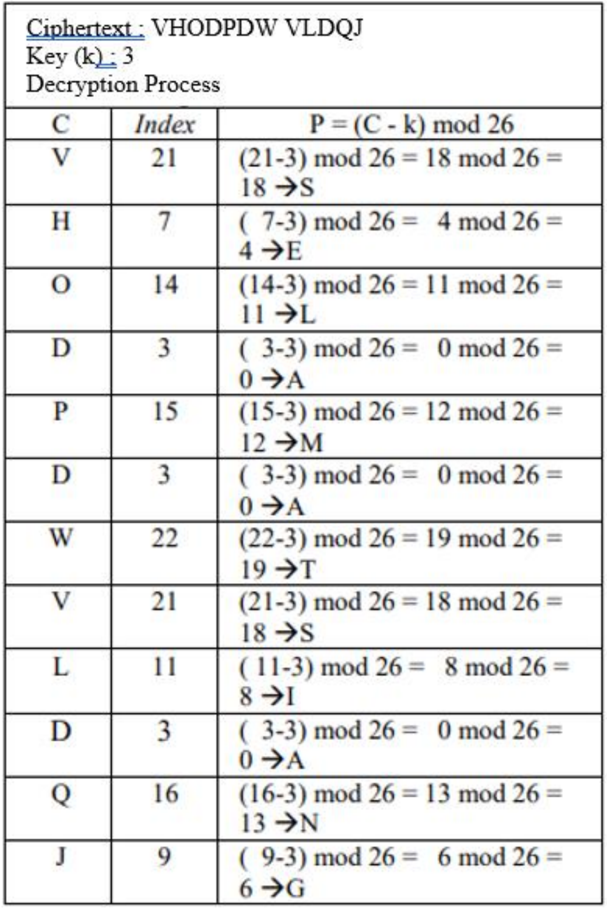


Plaintext : SELAMAT SIANG
Key (k) : 3
Encryption Process

P	*Index*	C = (P+k) mod 26
S	18	(18+3) mod 26 = 21 mod 26 = 21 → V
E	4	(4+3) mod 26 = 7 mod 26 = 7 → H
L	11	(11+3) mod 26 = 14 mod 26 = 14 → O
A	0	(0+3) mod 26 = 3 mod 26 = 3 → D
M	12	(12+3) mod 26 = 15 mod 26 = 15 → P
A	0	(0+3) mod 26 = 3 mod 26 = 3 → D
T	19	(19+3) mod 26 = 22 mod 26 = 22 → W
S	18	(18+3) mod 26 = 21 mod 26 = 21 → V
I	8	(8+3) mod 26 = 11 mod 26 = 11 → L
A	0	(0+3) mod 26 = 3 mod 26 = 3 → D
N	13	(13+3) mod 26 = 16 mod 26 = 16 → Q
G	6	(6+3) mod 26 = 9 mod 26 = 9 → J

So that the encryption process is obtained:
Plaintext: GOOD DAY
Ciphertext: VHOPDW VLDQJ

Table 3 Decryption Process



Ciphertext : VHODPDW VLDQJ
Key (k) : 3
Decryption Process

C	*Index*	P = (C - k) mod 26
V	21	(21-3) mod 26 = 18 mod 26 = 18 →S
H	7	(7-3) mod 26 = 4 mod 26 = 4 →E
O	14	(14-3) mod 26 = 11 mod 26 = 11 →L
D	3	(3-3) mod 26 = 0 mod 26 = 0 →A
P	15	(15-3) mod 26 = 12 mod 26 = 12 →M
D	3	(3-3) mod 26 = 0 mod 26 = 0 →A
W	22	(22-3) mod 26 = 19 mod 26 = 19 →T
V	21	(21-3) mod 26 = 18 mod 26 = 18 →S
L	11	(11-3) mod 26 = 8 mod 26 = 8 →I
D	3	(3-3) mod 26 = 0 mod 26 = 0 →A
Q	16	(16-3) mod 26 = 13 mod 26 = 13 →N
J	9	(9-3) mod 26 = 6 mod 26 = 6 →G

So the decryption process is obtained:
Ciphertext: VHODPDW VLDQJ
Plaintext: GOOD AFTERNOON

4. CONCLUSION

After this research is completed, it can be concluded that to build text-based communication applications, we can use socket programming with a client/server application architecture. The Caesar cipher algorithm can be used to encrypt and decrypt messages sent in chat applications.

For further research, you can develop chat applications in groups, so that many users can join the application to communicate. In terms of encryption methods, you can add several encryption technique options to increase data security in the application.

REFERENCES

[1] J. Rahmadoni, PERANCANGAN SIMULASI PEMBELAJARAN KRIPTOGRAFI KLASIK MENGGUNAKAN METODE WEB BASED LEARNING, vol. 1, Intecoms: Journal of Information Technology and Computer Science, 2018.

[2] P. Jaya, APLIKASI PENGAMANAN BASIS DATA DENGAN ALGORITMA RSA DAN WAKE BERBASIS DESKTOP, vol. 1, SKANIKA, 2018.

[3] A. Amrulloh, Kriptografi Simetris Menggunakan Algoritma Vigenere Cipher, vol. 5, CoreIT, 2019.

[4] M. A. Khan, M. A. Kalwar and A. K. Chaudhry, Optimization of material delivery time analysis by using Visual Basic for applications in Excel, vol. 2, Journal of Applied Research in Technology & Engineering, 2021.

[5] R. Junieles and S. F. Arindita, Karakteristik dan Fungsi Bahasa Iklan Bisnis Layanan Aplikasi Chatting di Youtube, vol. 7, Jurnal Konfiks, 2020.

[6] D. Iqbal, IMPLEMENTASI ALGORITMA LEVENSTEIN UNTUK KOMPRESI FILE VIDEO PADA APLIKASI CHATTING BERBASIS ANDROID, vol. 3, KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer), 2019.

[7] N. Farid, B. Nurhadiyono and Y. Rahayu, IMPLEMENTASI METODE STEGANOGRAFI LEAST SIGNIFICANT BIT DENGAN ALGORITMA HILL CIPHER PADA CITRA BITMAP, vol. 15, Techno.com.