JOSCEX
Journal of
Soft Computing
Exploration

Securing audio chat with cryptool-based twofish algorithm

Alya Aulia Nurdin[1], Djuniadi Djuniadi[2]
[1]Department of Computer Science, Universitas Negeri Semarang, Indonesia
[2]Department of Electrical Engineering, Universitas Negeri Semarang, Indonesia

Article Info

Article history:

Received Feb 15, 2022
Revised Feb 20, 2022
Accepted Mar 25, 2022

Keywords:

Securing audio chat
Twofish algorithm
Information security issue

ABSTRACT

Technology and the internet are growing very rapidly in society making it easy for people to share information and communicate with each other. However, the security of such data or information is something that should be highlighted. The utilization of technology and the internet has many security gaps that can make data or information vulnerable to being stolen and even misused. Valuable data or information is very likely to be accessed by unauthorized people. On the other hand, data and information are prone to be illegally altered and even duplicated. In connection with various possible data or information security issues, it is necessary to do a data security. The purpose of this study is to secure audio chat using a Cryptool-based Twofish algorithm. Based on research conducted, the security process with encryption and decryption simulations was successfully carried out on audio chat. Audio chat sent via IP Address can be encrypted into ciphertext and can be decrypted back into audio at a speed of 15.78 kB/s and the resulting size is also still the same, which is 160 packets. This Twofish algorithm proved to be well usable because the size and quality of chat audio generated from decryption is still the same as audio chat before it is encrypted.

Corresponding Author:

Alya Aulia Nurdin
Department of Computer Science,
Universitas Negeri Semarang.
Email: alyaaulianurdin@students.unnes.ac.id

1. INTRODUCTION

The development of technology and the internet is very rapid in society. This is certainly used by the community to facilitate and streamline their work and meet the needs of these communities. People can find information and share any information and communicate with each other by utilizing technology and the internet. Information that is well presented and presented has value and can be used in decision making [1].

However, over time, in communicating using technology and the internet, data and information security becomes a thing worth highlighting. Data and information security is an important and crucial problem to address. Data security is an extreme problem that touches many parts including PCs (personal computers) and correspondence [2]. There are many security loopholes that can make data or information vulnerable to theft and even misused when communicating over the internet. Crime in the internet world is very prone to occur. Cyber crime first occurred in the United States in the 1960s [3]. Some of the subsequent crimes ranging from manipulating student academic transcript data at New York's Brooklyn College, smuggling narcotics using computers, computer abuse committed by employees to unauthorized parties access to the Pacific National Bank Security Database, resulting in losses that reached $10.2 million in 1978 [4]. From the cases that have occurred and mentioned earlier shows that the valuable data or information is very likely to be accessed by unauthorized people. On the other hand, data and information are prone to be illegally altered and even duplicated. Hijacked data will have the possibility of being damaged and even lost which will cause large material losses [5].

This research was motivated by the anxiety of cyber attacks when conducting audio chat with internet networks. Audio chat or voice communication has become an important part of everyday human life. However, these voice communications are not necessarily fully usable securely due to security gaps and cyberattacks that may occur. Cyberattacks are something that can happen because of the connectivity provided to customers [6]. Data sharing systems and remote access pose security issues to be one of the weaknesses of data communication [1].

Data security can be done to overcome various possible data or information security problems. This can be encryption or cryptography. This encoding process is carried out so that the data transmitted cannot be read, understood, and used by other parties except those who have access to the data or information [7], [8]. In general, cryptography consists of two stages, namely encryption and decryption. Meanwhile, some algorithms that are widely used in cryptography, such as block algorithms, this algorithm will operate at any time with a size of 64 bits [9], [10]. The encryption and decryption can be seen in Figure 1.

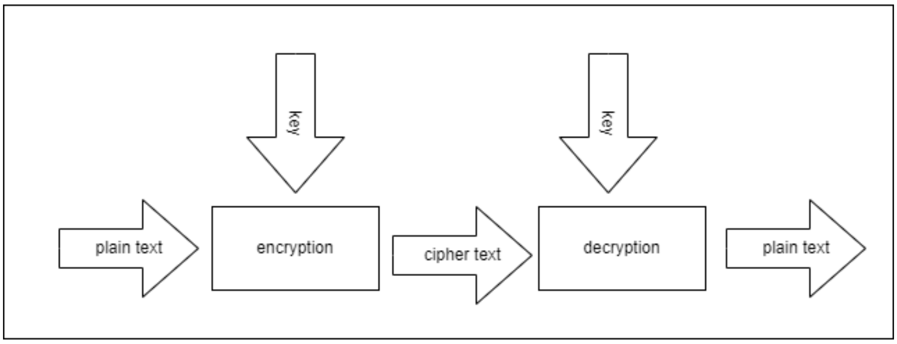


Figure 1. Encryption and decryption scheme [5]

Figure 1 shows encryption and decryption schemes. Encryption is the process of converting information or plaintext into other forms so that the actual content of the message cannot be understood or often called ciphertext [11]. This is done with the aim that the existing information is still protected from those who are not entitled to receive it. While decryption is the opposite process of encryption, which is transforming or converting certain data to data or information of the original form.

The study used a cryptographic algorithm to solve the security problem of audio chat data. The encryption and decryption algorithm used is the Twofish Algorithm. The Twofish algorithm is an algorithm created by Bruce Scheiner, while previously he also formulated the Blowfish Algorithm [12]. The design of the Twofish algorithm takes into account the criteria set by the National Institute of Standards and Technology (NIST) [13]. This algorithm is a 128-bit block algorithm and can receive keys with variable lengths of 128 bits to 256 bits. The key used at the time of encryption is the same as that used when decrypting with a length of 128 bits [14]. This Twofish algorithm uses a 16-round feistel network structure and also uses additional whitening on input (input) and output (output) [15]. In addition, the Twofish algorithm also uses key scheduling, hadamard pseudo-transformations or changes, and Maximum Distance Separable (MDS) [16]. The first process is to divide the plain text into four 32-bit words [17].

Previous research [1][18] Twofish algorithm is used and chosen for data security because it is quite efficient and there is no need to spend money because this algorithm is not patented. In addition, this algorithm also has a simple design and is easy to analyze and implement [13]. Twofish also runs very well on high-speed CPUs (Central Processing Unit), CPUs that have a small smart card as well as on hardware (hardware) [19].

Based on the description above, then by using the Twofish algorithm, cryptographic simulations will be carried out in the form of encryption and decryption of audio chat. The simulation aims to find out how voice communication data can be secured so that the data sent can only be understood and readable by parties who have access to the data. The simulation of data security in this study will be carried out using tools in the form of Cryptool 2 software. Cryptool is a program that can help analyze and perform cryptographic procedures in an integrated user interface [15].

2. METHOD

This research was conducted using several stages. The stages can be seen in the following image. Figure 2 shows the research stages.

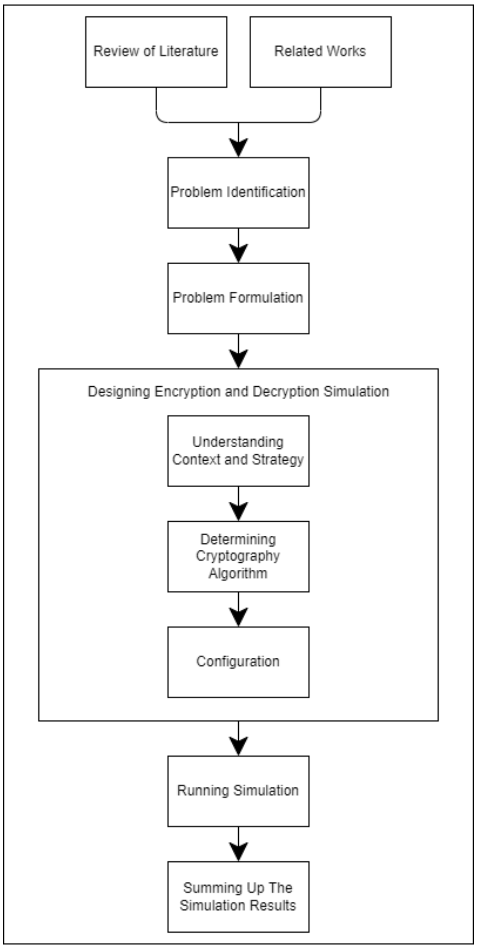

Review of Literature
Related Works
Problem Identification
Problem Formulation
Designing Encryption and Decryption Simulation
Understanding Context and Strategy
Determining Cryptography Algorithm
Configuration
Running Simulation
Summing Up The Simulation Results

Figure 2. Research stages

Figure 2 shows the stages of the study. These stages, namely literature studies, previous research, problem identification, problem formulation, designing encryption simulations & decryption, running simulations, and concluding simulation results.

2.1 Literature Study to Problem Formulation

Literature studies are conducted by studying the theories and practices of cryptographic algorithms for encryption and decryption of data. Then the discovery or identification of problems that currently occur in the community related to information security in audio chat.

2.2 Designing Encryption and Decryption Simulations

This stage aims to design how encryption and decryption will be carried out for the security of audio chat information data. The implementation of the design is carried out using the Cryptool 2 tool. The first stage, which is to understand the context and strategy, among others, is to understand how the components contained in Cryptool 2. The second stage is to determine the cryptographic algorithm to be used in the encryption and decryption of audio chat information, namely by using the Twofish algorithm. Figure 3 shows the structure of the Twofish algorithm that will be used in securing this audio chat. Based on Figure 3 the Twofish algorithm has a fiestel structure and has 16 rounds of encryption that can produce a 128-bit ciphertext.

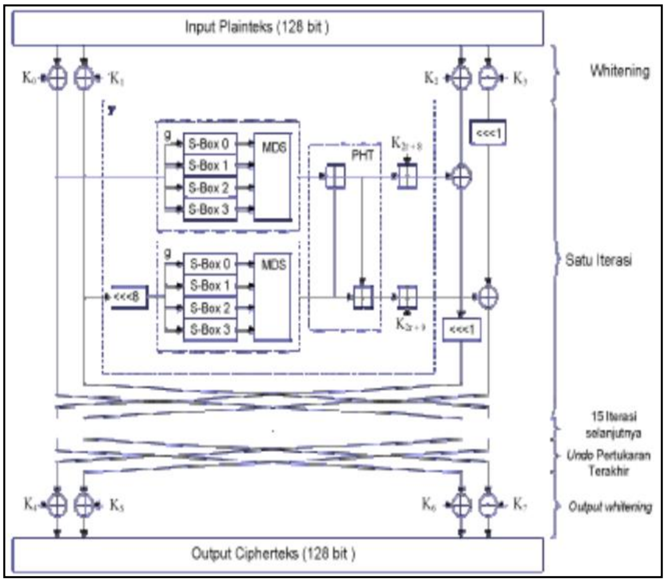


Figure 3. Twofish algorithm structure [18]

Furthermore, the third stage is to configure the algorithm used along with the components in Cryptool 2 to support the success of the encryption and decryption process.

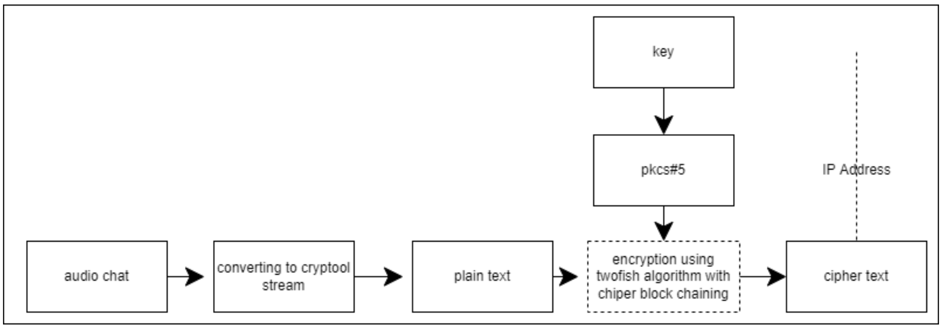

key
pkcs#5
IP Address
audio chat
converting to cryptool stream
plain text
encryption using twofish algorithm with chiper block chaining
cipher text

Figure 4. Encryption process design

Based on Figure 4, it can be seen that the encryption process begins with converting audio chat into cryptool stream and then goes through the encryption process with the Twofish algorithm to produce ciphertext. Meanwhile, in Figure 5 it can be seen that the ciphertext received from the IP Address will go through the decryption process with the Twofish algorithm to produce plaintext to then be converted into bytes until it turns into audio chat again.

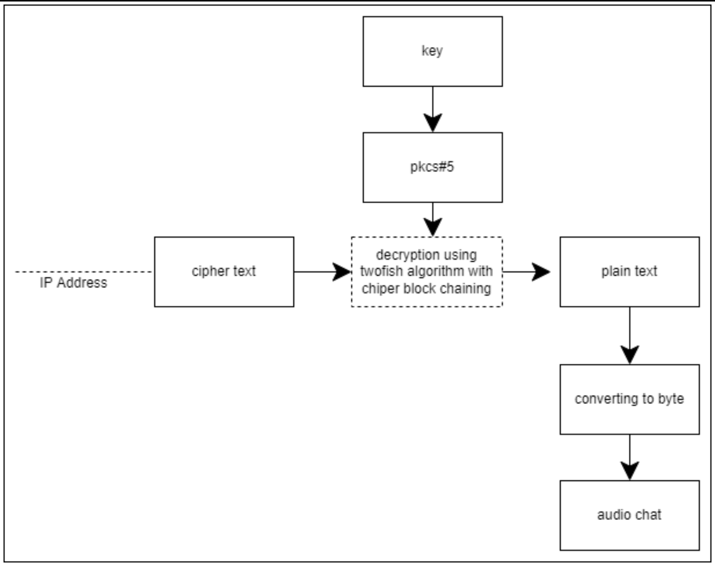


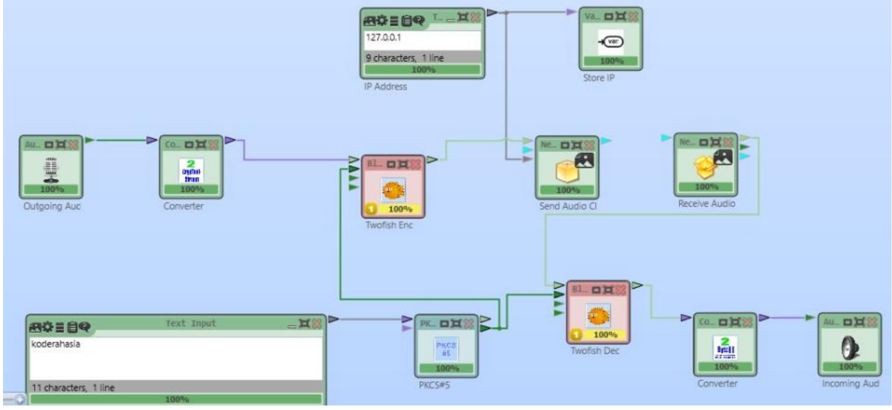
Figure 5. Decryption process design

2.3 Running Simulations and Summing Up Simulation Results

The process of simulating encryption and decryption of audio chat using the Twofish algorithm in Cryptool 2 is run at this stage. Then the analysis of simulation results is carried out.

3. RESULTS AND DISCUSSIONS

Based on the simulation design created, a model of the simulation circuit of the process of encryption and decryption of audio chat using the Twofish algorithm as in Figure 6 is produced. The encryption and decryption process starts from the Outgoing Audio component and ends at the Incoming Audio component in Cryptool. The encryption simulation series and decryption audio chat with cryptool 2-based twofish algorithm, shown in Figure 6.



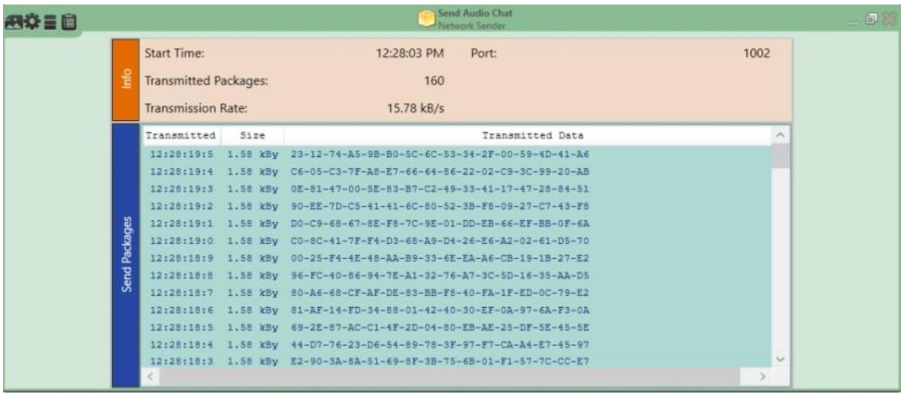
127.0.0.1
9 characters, 1 line

koderahasia
11 characters, 1 line

Figure 6. Encryption simulation series and Decryption Audio Chat with Cryptool 2-based Twofish Algorithm

As for before the encryption and decryption process will be done, first the configuration is carried out for each existing component. In the configuration of the encryption process, the first component, namely the component named "Outgoing Audio" is a component in Cryptool 2 that aims for audio input. This component uses the record feature on personal devices. Then the incoming audio chat will be converted first into a cryptool stream (so that packaged data can later be sent via audio send) using the help of the "Converter" component. This is done so that the audio becomes plaintext. The configuration used in the converter is: convert to cryptool stream, with endianness: big endian, and input encoding & output: UTF-8 (Universal Character Set (UCS) Tranformation Format).

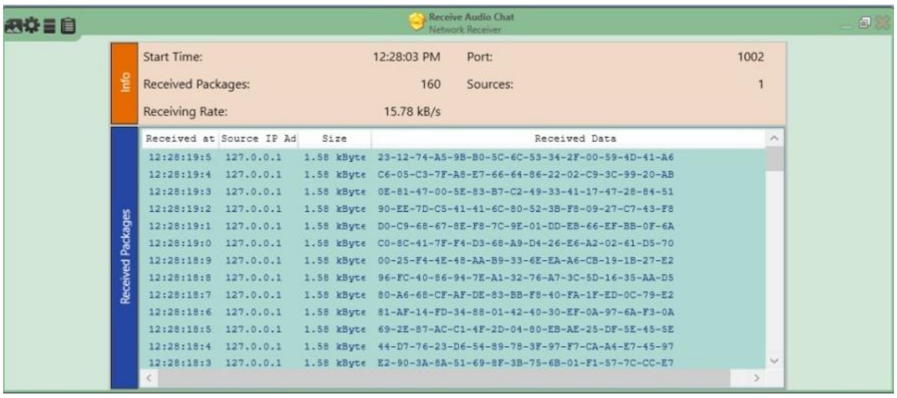
Once it becomes plaintext, it will then be encrypted using the Twofish algorithm with chaining mode configuration: chiper block chaining, and padding mode: PKCS7 (Public Key Cryptography Standard). Before encryption, of course, it is necessary to use a certain key (key) and the key is generated first into a safekey with PKCS #5. The configurations used are hash function: SHA256 (secure hash algorithm), iteration: 1000, string encoding: UTF-8, and output key length: 128 bits. The encryption process will produce a ciphertext that will be sent to the relevant IP address. This study used a local IP address, which is 127.0.0.1. Ip address will be stored in the "Variable Store IP" component first so that the components in the cryptool workspace do not have to be directly related to the next or previous process. The data transmitted to the relevant ip address via network sender, shwon in Figure 7.



Start Time:	12:28:03 PM	Port:	1002
Transmitted Packages:	160		
Transmission Rate:	15.78 kB/s		

Transmitted	Size	Transmitted Data
12:28:19:5	1.58 kBy	23-12-74-A5-9B-B0-5C-6C-53-34-2F-00-59-4D-41-A6
12:28:19:4	1.58 kBy	C6-05-C3-7F-A8-E7-66-64-86-22-02-C9-3C-99-20-AB
12:28:19:3	1.58 kBy	0E-81-47-00-5E-83-B7-C2-49-33-41-17-47-28-84-51
12:28:19:2	1.58 kBy	90-EE-7D-C5-41-41-6C-80-52-3B-F8-09-27-C7-43-F8
12:28:19:1	1.58 kBy	D0-C9-68-67-8E-F8-7C-9E-01-DD-EB-66-EF-BB-0F-6A
12:28:19:0	1.58 kBy	C0-8C-41-7F-F4-D3-68-A9-D4-26-E6-A2-02-61-D5-70
12:28:18:9	1.58 kBy	00-25-F4-4E-48-AA-B9-33-6E-EA-A6-CB-19-1B-27-E2
12:28:18:8	1.58 kBy	96-FC-40-86-94-7E-A1-32-76-A7-3C-5D-16-35-AA-D5
12:28:18:7	1.58 kBy	80-A6-68-CF-AF-DE-83-BB-F8-40-FA-1F-ED-0C-79-E2
12:28:18:6	1.58 kBy	81-AF-14-FD-34-88-01-42-40-30-EF-0A-97-6A-F3-0A
12:28:18:5	1.58 kBy	69-2E-87-AC-C1-4F-2D-04-80-EB-AE-25-DF-5E-45-5E
12:28:18:4	1.58 kBy	44-D7-76-23-D6-54-89-78-3F-97-F7-CA-A4-E7-45-97
12:28:18:3	1.58 kBy	E2-90-3A-8A-51-69-8F-3B-75-6B-01-F1-57-7C-CC-E7

Figure 7. Data transmitted to the relevant ip address via network sender



Start Time:	12:28:03 PM	Port:	1002
Received Packages:	160	Sources:	1
Receiving Rate:	15.78 kB/s		

Received at	Source IP Ad	Size	Received Data
12:28:19:5	127.0.0.1	1.58 kByte	23-12-74-A5-9B-B0-5C-6C-53-34-2F-00-59-4D-41-A6
12:28:19:4	127.0.0.1	1.58 kByte	C6-05-C3-7F-A8-E7-66-64-86-22-02-C9-3C-99-20-AB
12:28:19:3	127.0.0.1	1.58 kByte	0E-81-47-00-5E-83-B7-C2-49-33-41-17-47-28-84-51
12:28:19:2	127.0.0.1	1.58 kByte	90-EE-7D-C5-41-41-6C-80-52-3B-F8-09-27-C7-43-F8
12:28:19:1	127.0.0.1	1.58 kByte	D0-C9-68-67-8E-F8-7C-9E-01-DD-EB-66-EF-BB-0F-6A
12:28:19:0	127.0.0.1	1.58 kByte	C0-8C-41-7F-F4-D3-68-A9-D4-26-E6-A2-02-61-D5-70
12:28:18:9	127.0.0.1	1.58 kByte	00-25-F4-4E-48-AA-B9-33-6E-EA-A6-CB-19-1B-27-E2
12:28:18:8	127.0.0.1	1.58 kByte	96-FC-40-86-94-7E-A1-32-76-A7-3C-5D-16-35-AA-D5
12:28:18:7	127.0.0.1	1.58 kByte	80-A6-68-CF-AF-DE-83-BB-F8-40-FA-1F-ED-0C-79-E2
12:28:18:6	127.0.0.1	1.58 kByte	81-AF-14-FD-34-88-01-42-40-30-EF-0A-97-6A-F3-0A
12:28:18:5	127.0.0.1	1.58 kByte	69-2E-87-AC-C1-4F-2D-04-80-EB-AE-25-DF-5E-45-5E
12:28:18:4	127.0.0.1	1.58 kByte	44-D7-76-23-D6-54-89-78-3F-97-F7-CA-A4-E7-45-97
12:28:18:3	127.0.0.1	1.58 kByte	E2-90-3A-8A-51-69-8F-3B-75-6B-01-F1-57-7C-CC-E7

Figure 8. Data received by related ip addresses through network receiver

Based on Figure 7 and Figure 8 above, it can be seen that the audio chat that is encrypted into ciphertext and sent to the relevant IP address still has the same package size. It can also be seen in the orange column at the very top in the "info" section, namely on transmitted packages and received packages showing a number of 160. It shows and proves that the Twofish algorithm is a symmetrical algorithm with the same size of encryption message length as before it was encrypted. In addition, the size of packages that are still the same is also caused by the Twofish algorithm belonging to the chiper block that works by using data in the form of blocks or data groups of a certain length. From these results, it is also seen that this Twofish algortima has a good speed with a transmitting rate and receiving rate of 15.78 kB / s. This is because the Twofish algorithm that belongs to the symmetric algorithm has advantages, namely a higher operating speed when compared to asymmetric algorithms. With this, the Twofish algorithm in encryption and decryption of audio chat can be used well on real-time systems.

Furthermore, in order for the data to be received in the form of audio chat again, it is necessary to do a decryption process. Ciphertext obtained and received from the IP Address will be carried out the decryption process using the Twofish algorithm with the same configuration as in the encryption process. Before decryption, it is also necessary to use the same key as before. After the decryption process is complete, the ciphertext will change to plaintext. Furthermore, the plaintext will be converted into bytes with the help of the converter and the output that will appear is in the form of audio chat with the same size and quality.

4. CONCLUSION

Based on the results and analysis that has been done on the research, it can be concluded that the security of audio chat using the Twofish algorithm was successfully carried out with the Cryptool 2 tool. Audio chat which is a sound file can be encrypted into ciphertext with the Twofish algorithm so that it can be transmitted more securely to the relevant IP address and using a specific key. Audio chat can also be accepted and decrypted with the same package size. That is, the quality of the sound file is still the same.

REFERENCES

[1] J. H. P. Tambunan, H. A., & Sitorus, "Enkripsi dan dekripsi dalam proses pengiriman data dengan menggunakan algoritma twofish," *J. Bisantara Inform.*, vol. 1, no. 1, pp. 17–17, 2017.

[2] W. J. Shin, "Comparative analysis of aes, blowfish, twofish, and threefish encryption algorithms," *J. Anal. Appl. Math.*, vol. 10, 2017.

[3] M. C. B. Umanailo *et al.*, "Cybercrime case as impact development of communication technology that troubling society," *Int. J. Sci. Technol. Res.*, vol. 8, no. 9, pp. 1224–1228, 2019.

[4] D. J. Neufeld, "Understanding cybercrime," *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, pp. 1–10, 2010, doi: 10.1109/HICSS.2010.417.

[5] M. A. Twofish, "Aplikasi enkripsi dan dekripsi file menggunakan algoritma twofish," pp. 13–25.

[6] T. Poduval, A., Rai, N., Khan, P., Sane, A., Chaudhari, "A survey on different encryption techniques for image, Video, Audio And Docs," *Int. J. Eng. Appl. Sci. Technol.*, vol. 5, no. 11, pp. 284–288, 2021.

[7] N. Charibaldi and B. Yuwono, "Aplikasi enkripsi pengiriman file suara," vol. 2011, no. semnasIF, pp. 201–207, 2011.

[8] S. Sularno, D. P. Mulya, and R. Astri, "Determination of the shortest route based on bfs algorithm for purpose to disaster evacuation shelter," *Sci. J. Informatics*, vol. 8, no. 1, pp. 33–42, 2021.

[9] A. A. G. B. P. Ida Ayu Widyantari Arnawa, Putu Eka Widastra Hary C., "Perbandingan waktu enkripsi antara metode electronic codebook (ECB) dan chipher blick chaning (CBC) dalam algoritma blowfish," *J. Ilmu Komput. Indones.*, vol. 5, no. 1, pp. 50–54, 2020.

[10] D. A. A. Pertiwi and D. Djuniadi, "Simulations of text encryption and decryption by applying vertical bit rotation algorithm," *J. Soft Comput. Explor.*, vol. 2, no. 2, pp. 61–66, 2021.

[11] W. Haryono, "Comparison encryption of how to work caesar cipher, hill cipher, blowfish and twofish," *J. Comput. Appl. Informatics*, vol. 4, no. 2, pp. 100–110, 2020.

[12] F. Laylim and M. Q. Khairuzzaman, "Penerapan algoritma twofish dalam perancangan aplikasi chat berbasis android," *J. ENTERJ*, vol. Volume 2, pp. 76–87, 2019.

[13] F. Khusnul, "Implementasi keamanan pengiriman pesan suara dengan enkripsi dan dekripsi menggunakan algoritma twofish," vol. 1, no. 3, pp. 84–89, 2012.

[14] B. P. Siswanto, Saputro, A., Utama, G. P., Prasetyo, "Penerapan algoritma kriptografi twofish untuk mengamankan data file," *J. BIT Budi Luhur Inf. Technol.*, vol. 18, no. 1, pp. 9–18, 2021.

[15] I. Shulhan, "Analisis perbandingan antara algoritma rijndael dan algoritma twofish dalam penyandian teks," *J. Tek. Inform. Unika St. Thomas*, vol. Vol.03, no. no.02, pp. 90–98, 2018.

[16] I. P. G. H. Suweantara, E., Suputra, "Penggunaan metode kriptografi pada voice over internet protocolle," *J. SNATIA*, pp. 473–479.

[17] B. S. Setyawan, R. A., Sulistyo, S., Hantono, "Review: algoritma kriptografi untuk pengembangan aplikasi telepon anti sadap," *Proc. Conf. Inf. Technol. Electr. Eng.*, 2014.

[18] A. Hendra, "Analisis perbandingan kinerja algoritma twofish dan tea (tiny encryption algorithm) pada data suara," no. November, pp. 1–8, 1994.

[19] M. O. Gurning, "Aplikasi pesan dengan algoritma twofish pada platform android messaging application with twofish algorithm on android platform," vol. 3, no. 3, pp. 5022–5028, 2016.