CRYPTOGRAPHY ON AUDIO FILES USING THE BLOWFISH ALGORITHM

[1]NUNIEK FAHRIANI, [2]ONNY KARTIKA WALUYA

[1,2]Faculty Of Informatics Engineering University Muhammadiyah Gresik Indonesia

Jl. Sumatera No.101, Gn. Malang, Randuagung, Kec. Gresik, Kabupaten Gresik

E-mail: [1]nuniekfahriani@umg.ac.id, [2]onnykawe07@gmail.com

ABSTRACT

Blowfish is a 64-bit block cipher with variable key length. The algorithm consists of two part: Key expansion and data encryption. Allowing its use in cryptography. In general, cryptography is about constructing and analyze communication protocols that can block an opponent. Various aspects of information security, Such as confidential data, Data integrity, Authentication and non repudance Is the center of modern cryptography. This case implementation with encryption and decryption techniques on audio files using java programming, aims to secure the audio data contained in it can be maintained and can only be read by user who have the cryptographic key.

Keywords: *encryption, decryption, blowfish, java.*

I. INTRODUCTION

Cryptography has become an important part in the world of information technology today. The use of cryptography increases with the increasing threat of cyber security. Cryptography is art or science to hide the contents of encoded / encrypted messages in such a way that it is not known what the content of the message is [1]. With the aim of securing the information contained therein. It is part of the computer security system. Because not all aspects of information security is handled by cryptography. Techniques used can be encryption and decryption. Encrypted data is also various, such as documents and other computer files.

According to John D. Howard in his book "An Analysis of security incidents on the internet" states that: "Computer security is a precautionary measure of computer users or irresponsible network users." [2] computer security can be physical, data, and applications. In the security of computer systems, especially for confidential data should, we need to do is make it difficult for irresponsible parties in accessing our data. In this research will focus on an encryption and decryption application of audio data that is in the form of audio files using blowfish algorithm.

II. PRINCIPLE OF SECURITY SYSTEM

Computer security is needed to avoid 'intruders' who can change data and run programs that can interfere with the system. In addition, it can also reduce the risk of threats from 'intruders' who just want to know, seek popularity or because of competition. Therefore, we need to understand the principle of security itself, namely: [3]

A. Confidentiality, where files are not distributed to users who should not be entitled to these files, or called unauthorized.
B. Integrity, that files remain original, undoubtedly authenticity, unmodified in its course from source to recipient.
C. Availability, where authorized users are granted access on time and are not constrained.

Basically, the most important and valuable component of a computer system is data. Protection of data can be done with encryption and decryption. The elements can be described as below:

DOI: https://doi.org/10.54732/jeecs.v3i1.139

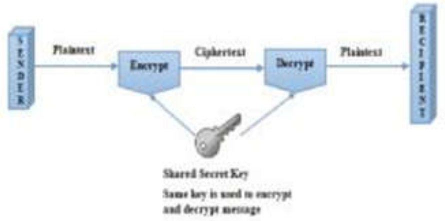


Figure 1. Encryption and decryption process

III. CRYPTOGRAPHY

Cryptography criteria consists of three basic functions, namely:

1. Encryption: is very important in cryptography, is the security of data transmitted in order to be kept confidential. The original message is called plaintext, which is converted into codes that are not understood. Encryption can be interpreted with a cipher or code.
2. Decryption: is the opposite of encryption. The encrypted message is returned to its original form (native text), called message decryption. The algorithm used for decryption is certainly different from the algorithm used for encryption.
3. Key, which is meant here is the key used to perform encryption and decryption. The key is divided into two parts, the secret key (private key) and the public key (public key) [5].

In pure science terms [6], Cryptography is the science of using mathematics for making plain text information (P) into an unreadable cipher text (C) format called encryption and reconverting that cipher text back to plain text called as decryption with the set of Cryptographic Algorithms (E) using encryption keys (k1 and k2) and the decryption algorithm (D) that reverses and produces the original plain text back from the cipher text. This can be interpreted as Cipher text C = E {P, Key} and Plain text C = D {C, Key} [4]

Characteristics of a good cryptosytem as follows:

1. System security lies in key secrecy and not on the secrecy of the algorithm used
2. A good cryptosystem has a large keyspace.
3. A good cryptosystem will generate randomly visible ciphertext in all statistical tests performed against it.
4. A good cryptosystem is able to withstand all previously known attacks.

IV. BLOWFISH ALGORITHM

An encryption method similar to DEC created by Bruce Schneier devoted to large microprocessors (32 bits up with large data cache). Blowfish is developed to meet the following design criteria [7]:

1. Fast, on the optimal implementation Blowfish can achieve speed of 26 clock cycles per byte.
2. Compact, Blowfish is able to run on less than 5KB memory.
3. Simple, Blowfish only use simple operations : addition, XOR, and table lookup on 32 bits operand. Its design is easy to analyze which make it resistant to implementation errors.
4. Variably security, length of Blowfish key can have variation and reach 448 bits (56 bytes).

Based on an article written by Suriski Sitinjak, et al.(2010). Blowfish was created by a cryptanalyst named Bruce Scheneir, President of Counterpane Internet Security, Inc (Consultant company on cryptography and computer security) and published in 1994.

Blowfish algorithm has 2 parts, namely key expansion and data encryption :

1. Key expansion, at this stage, it wil change the minimum key to sub key array by 4168 bytes.
2. Data encryption, this stage is done by 16 times loop and the input is X data consisting of 64 bits, which is in every loop use XOP operation. For each loop, first perform XOR left block with a subkey for round/loop.

Blowfish Workflow

A. Key Expansion Process

With the following steps:

1. Initialize first the P-array and then the four S-boxes, in order, with a fixed string. This string consists of the hexadecimal digits of pi. Example :
   P1= 0x243f6a88
   P2= 0x85a308d3
   P3= 0x13198a2e
   P4= 0x03707344
   and so on up to P18.
2. XOR P1 with the first 32 bits of the key, XOR P2 with the second 32-bits of the key, and so on for all bits of the key (possibly up to P14). Repeatedly cycle through the key bits until the entire P-array has been XORed with key bits.
3. Encrypt the all-zero string with the Blowfish algorithm, using the subkeys described in steps (1) and (2).
4. Replace P1 and P2 with the output of step (3)
5. Encrypt the output of step (3) using the Blowfish algorithm with the modified subkeys.
6. Replace P3 and P4 with the output of step (5).
7. Continue the process, replacing all entries of the P array, and then all four S-boxes in order, with the output of the continuously changing Blowfish algorithm.

B. Encryption Process

With the following steps:

1. Based on the method of blowfish encryption, for the initial step of the input file will be changed to binary. Encryption and decryption of blowfish is done by splitting the file into 64 bits. Which then 64 bit is initialized "x".
2. Input data "x" 64 bit is then split into two parts called XR (X Right) and XL (X Left) each 32 bits.
3. According to the book "Pengantar Ilmu Kriptografi" by Dony Ariyus [5], the process of encryption and decryption is done by simple function iteration 16 times. Here's the encryption formula:
   XL = XL XOR p[i]
   XR = F(XL) XOR XR Replace XL with XR
   Where is F formula is F(XL) = ((S[1,a] + S2[2,b] mod 232) XOR S[3,c]) + S[4,d]
4. After the 16th iteration, replace XL with XR again to cancel the last replacement.
5. Of all the steps above, the last step is to re-combine XR and XL to get ciphertext.

Encryption process with this blowfish algorithm can be seen in figure 2.

C. Decryption Process

For the Decryption Process, the steps exactly match the encryption process, it's just that the Pbox sequence is used in reverse order.

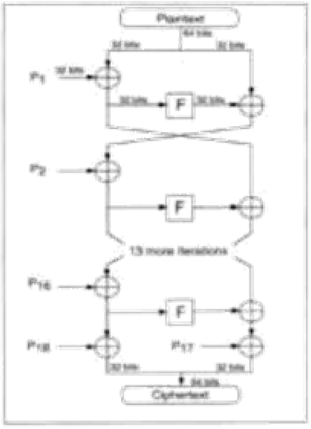


Figure 2. flow of blowfish algorithm encryption process

V. MUSIC FILE FORMAT

Music is a thing that is very liked by everyone, especially the people of Indonesia, Because Music is a soul language that is very entertaining anyone who heard it, listening to music can change the mood of the previously sad can be happy because of its beauty. If we are aware, in a lot of meaningful music contained that has its own meaning of the kind of music, it can be found in the lyrics and tones that are produced. From the definition of music described above is very unfortunate if all the amazing things that have a music in damaged by one of the things we really do not want. For example, there is a change, damage or recognize the work of the music.

Here are some types of music files:

1. **•wa**v is a sound file extension. The wav file is very good to use as a ringtone. The wav file is also found as an app system file.
2. **•mp3** is the most popular sound file extension. MP3 files on mobile can be opened with the application of ultramp3 or lcg jukebox or also TTPod. MP3 files usually contain songs. And often also found in the application system files.
3. **.aac** is the file extension of one of the sound file types.
4. **•xm** adalah is the usual sound file extension in the application system.
5. **•oog** is a sound file extension similar to wav.
6. **•wma** is a sound file extension from windows. Wma stands for Windows Media Audio.
7. **.rm** is a sound file extension that resembles amr.
8. **•rma** is a file extension almost equal to rm.
9. **•3**gp is a standard video file extension for mobile phones. This file is the result of video recording with mobile phone.
10. **•avi** is a normal video file extension can be opened in mobile using smartmovie or dvixplayer. In computer avi file can be opened with windows media player.
11. **•mp4** is a video file extension that is often found on mobile phones. Mobile apps that are suitable to open this type of file is a real one player, pvplayer, smartmovie equipped with mp4 codec.
12. **•mpg** mpg is a video file extension rarely found on mobile phones but is found in many computers.
13. **•flv** is a flv file extension file having similarity with video file with mpg format.
14. **•swf** is the extension of this video file can only be opened with flash player application. For example: macromedia flash player.
15. **.wmv** is a video file extension that is rarely found in mobile phones. On the computer The wmv file can be opened with windows media player. Wmv stands for windows media video.

Here is one of the picture of the music file extention :

Figure 3. Icon Extention File Audio

VI. IMPLEMENTATION

Interface Design

Interface design is an important part of the application because it is first seen when the application is run is the application interface. The design of the interface itself consists of designing the main menu interface, designing the encryption interface and decryption interface design. Here's a picture of interface design :

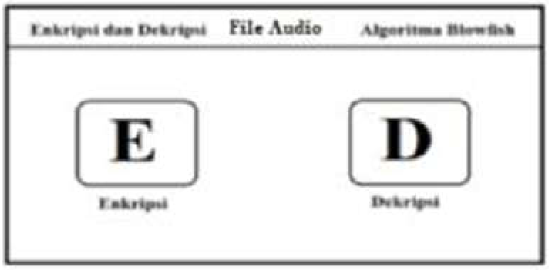


Figure 4. Main Page

Figure 4 Home page is the page that will appear the first time after the application is run. On this page there are two menus are encryption and decryption menu.

Build Encryption.java Class

This encryption class is a class that is used to perform the process of encryption and decryption of files. In making this program, used Netbeans 8.0.2 software by using Java language.

Encryption and Decryption Process

At this stage the program is designed to encrypt and decrypt files using the Blowfish algorithm.

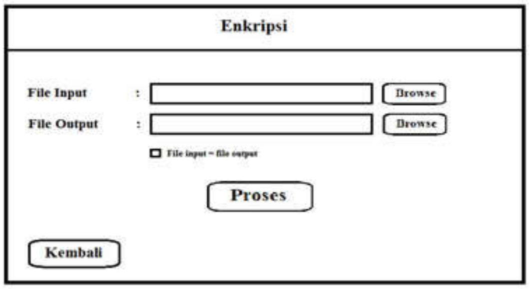


Figure 5. Encryption Page

Figure 5 is a page for encrypting audio files. This page contains a form to select an audio file from the computer directory to be encrypted.

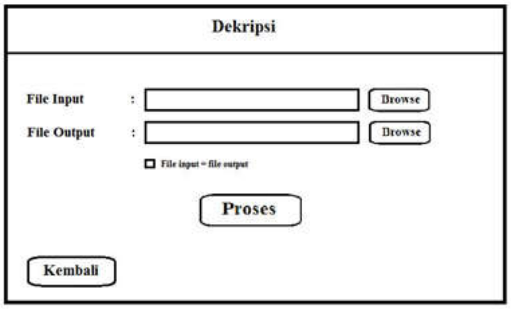


Figure 6. Decryption Page

Figure 6 is the Page for decrypting the audio file. This page contains a form to select an audio file from the computer directory to be decrypted.

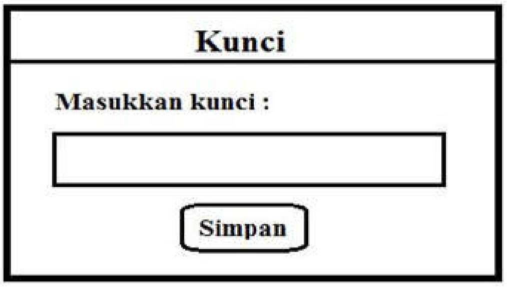


Figure 7. Key Page

Figure 7 is the Page to enter the key to be used in the encryption or decryption process.

System Implementation

The following is the implementation of the encryption and decryption application of audio files by using blowfish algorithm which is implemented with java netbeans 8.0.2 software performed with the steps below:

Step 1 Main Page

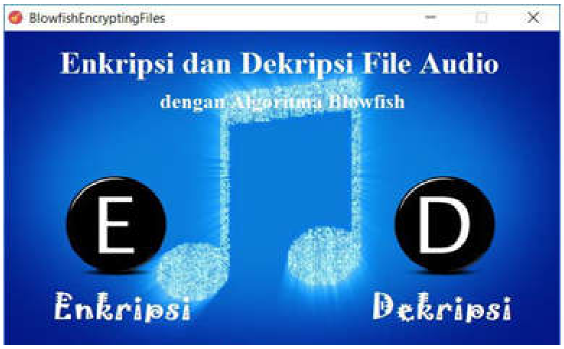
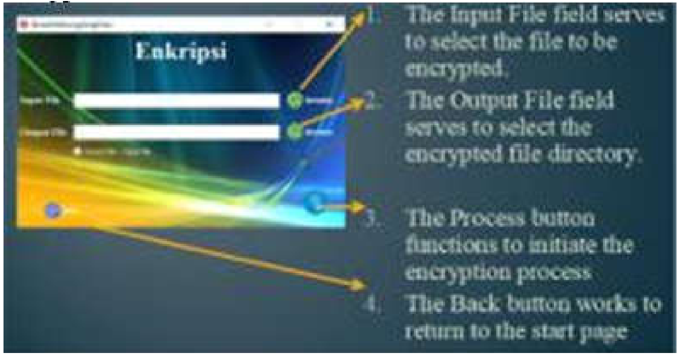


Figure 8. Main Page App View

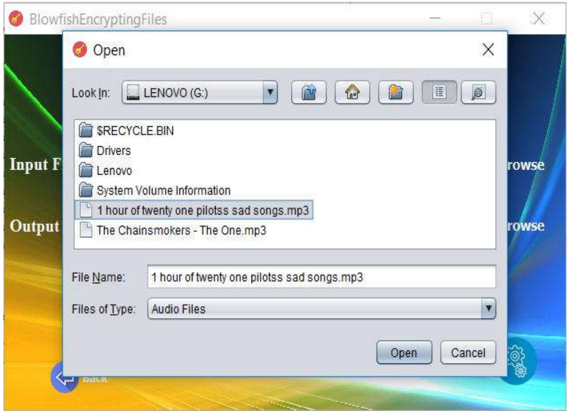
Step 2
Menu Encryption, retrieve files in the directory to be encrypted



1. The Input File field serves to select the file to be encrypted.
2. The Output File field serves to select the encrypted file directory.
3. The Process button functions to initiate the encryption process
4. The Back button works to return to the start page

Figure 9. Encryption Page View

Step 3
Before entering a key, that is selecting the file to be encrypted. Next enter the key to start encrypting.



Open

Look In: LENOVO (G:)

$RECYCLE.BIN
Drivers
Lenovo
System Volume Information
1 hour of twenty one pilotss sad songs.mp3
The Chainsmokers - The One.mp3

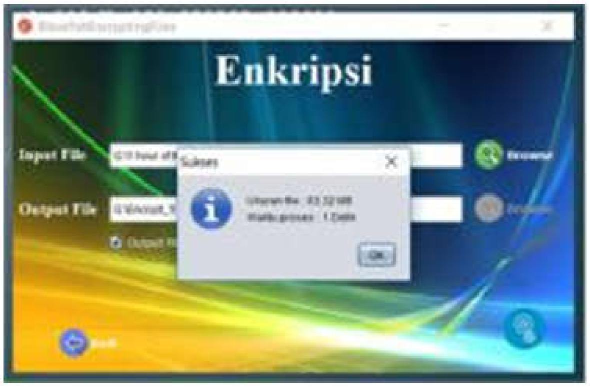
File Name: 1 hour of twenty one pilotss sad songs.mp3

Files of Type: Audio Files

Open Cancel

Figure 10. Memilih File Audio

Step 4
Successful display after the encryption process.



Ukuran file : 83.32 MB
Waktu proses : 1 Detik

Figure 12. Successful Encryption Process

Step 5
In the directory where the file will be saved, appear the file that has been encrypted.

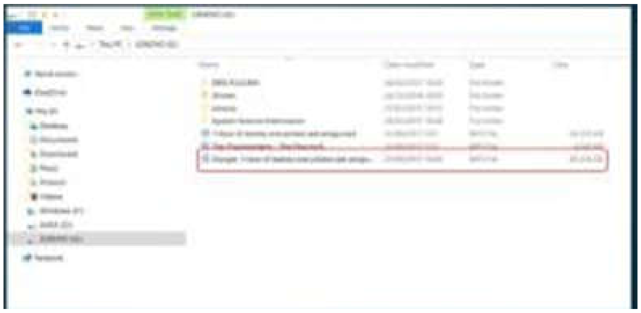
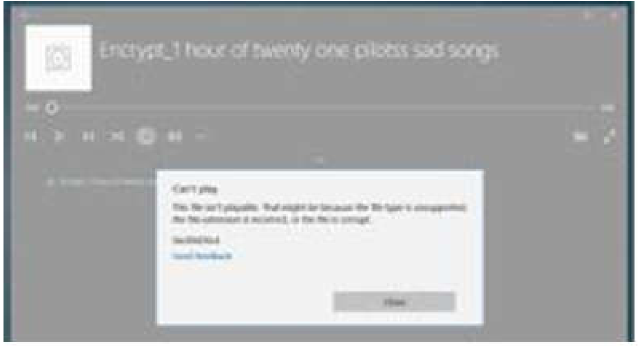


Figure 13. An encrypted file

Step 6
The encrypted file can not be played



Encrypt_1 hour of twenty one pilotss sad songs

Can't play

Figure 14. Encrypted Files Result

Step 7
Decryption is done in reverse from the encryption process. Retrieve the encrypted file from the directory then enter the same key at the time of encryption process, the process will be executed. And the file will return in the form of the original file.

VIII. DISCUSSION

Testing Application Program. At this stage, there will be tests on the application program made. The tests include encryption and decryption process test of ten *.mp3 format audio files. The result of the tests can be seen on table 1 and table 2 which contain plaintext/original file size and chipertext / encrypted file size.

Table 1. Results of Encryption Process

No	Plaintext File Name	Plaintext Size (Bytes)	Chipertext Size (Bytes)
1	Clean Bandit feat Zara Larsson - Symphony.mp3	3.541.718	3.541.720
2	Dido - Thank You.mp3	7.748.055	7.748.056
3	Michael Bublé - Nobody But Me.mp3	2.889.749	2.889.752
4	My Chemical Romance - Welcome To The Black Parade	5.034.350	5.034.352

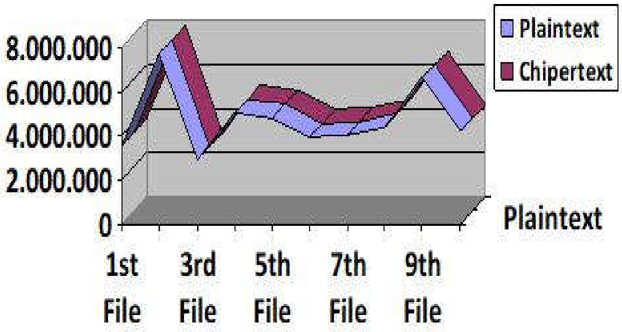
5	Snow Patrol - Chasing Cars.mp3	4.804.590	4.804.592
6	The Chainsmokers & Coldplay - Something Just Like This.mp3	3.956.139	3.956.144
7	twenty one pilots - Cancer.mp3	4.015.520	4.015.528
8	Twenty One Pilots - Guns For Hands.mp3	4.395.991	4.395.992
9	Twenty One Pilots - House Of Gold.mp3	6.617.709	6.617.712
10	Westlife - Fool Again.mp3	4.174.608	4.174.616

In Table 1 the chipertext size is slightly larger than the plaintext /original file. This is because there are several operations performed by the blowfish algorithm against files that are encrypted based on passwords or keys entered. The password used in this test has a length of 11 characters consisting of a combination of letters and numbers, namely blowfish123.

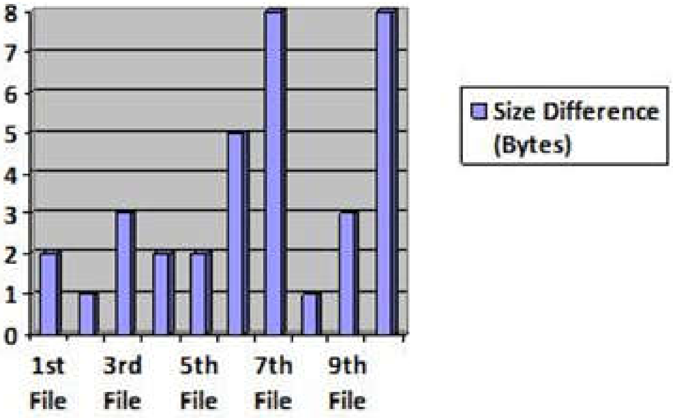
Table 2. Results of Decryption Process

No	Chipertext File Name	Chipertext Size (Bytes)	Plaintext Size (Bytes)
1	Encrypt_Clean Bandit feat Zara Larsson - Symphony.mp3	3.541.720	3.541.718
2	Encrypt_Dido - Thank You.mp3	7.748.056	7.748.055
3	Encrypt_Michael Bublé - Nobody But Me.mp3	2.889.752	2.889.749
4	Encrypt_My Chemical Romance - Welcome To The Black Parade	5.034.352	5.034.350
5	Encrypt_Snow Patrol - Chasing Cars.mp3	4.804.592	4.804.590
6	Encrypt_The Chainsmokers & Coldplay - Something Just Like This.mp3	3.956.144	3.956.139
7	Encrypt_twenty one pilots - Cancer.mp3	4.015.528	4.015.520
8	Encrypt_Twenty One Pilots - Guns For Hands.mp3	4.395.992	4.395.991
9	Encrypt_Twenty One Pilots - House Of Gold.mp3	6.617.712	6.617.709
10	Encrypt_Westlife - Fool Again.mp3	4.174.616	4.174.608

The difference between the original file size (plaintext) and the encrypted file (chipertext) in bytes size can be seen in the graph below.



Graph 1. Size of Plaintext and Chipertext File



Graph 2. Size Differences between Plaintext and Chipertext

From the tests conducted, obtained the difference in the size of plaintext and chipertext is less than 10 bytes. The difference in size obtained has an average of 3.5 bytes.

VIII. CONCLUSIONS AND SUGGESTIONS

Conclusions

1. The application made can be implemented well for encrypting and decrypting audio file because the file that already encrypted becomes unworkable and the content cannot be understood anymore.
2. The encryption process using blowfish algorithm will resize the file. The changed file size is insignificant, from the tests that have been done, the difference between plaintext and chipertext sizes have an average of 3.5 bytes.

Suggestions

There are still many lack in this encryption and decryption audio file application, hopefully this application system can be developed in the future. For example by adding some feature like adding choices in the algorithm and ability to encrypt folder.

VIII. REFERENCES

[1] A. Eko, and Smitdev Community, “Buku anti forensik uncensored mengatasi investigasi komputer forensik,” PT Elekmedia Komputindo, Jakarta, pp. 71, 2010.

[2] John D. Howard. 1997. “An Analysis Of Security Incidents On The Internet 1989 - 1995,” PhD thesis, Engineering and Public Policy, Carnegie Mellon University.

[3] S. Garfinkel.1995. “PGP: Pretty Good Privacy,” O’Reilly & Associates, Inc.,

[4] Bhardwaj Akashdeep, dkk. 2016 . “Security Algorithm For Cloud Computing”. International conference on computational modeling and security (CMS).

[5] A. Dony “Pengantar Ilmu Kriptografi : teori analisis & implementasi “, STMIK Amikom ,Penerbit Andi 2008

[6] Simarjeet Kaur “Cryptography and Encryption in Cloud Computing”, VSRD International Journal of CS and IT, 2012

[7] A. N Paskalis , "Penerapan Enkripsi ALgoritma Blowfish Pada Proses Steganografi EOF," Universitas Katolik Widya Mandira, Kupang,.

[8] Y. Aahmad. “Panduan Membangun Jaringan Komputer”. Kawan Pustaka 2009

[9] Rahardjo Budi. “ Keamanan Sistem Informasi Berbasis Internet, versi 5.4. PT Insan Infonesia - Bandung & PT INDOCISC. 2005

[10] CharlesS A., Sennewald and Curtis bailie. “Effective Security Management (Sixt Edition) “ ISBN: 978-0-12-802774-5. Elseiver Inc. 2016

[11] Mohan V. Pawar, Anuradha J.“Network Security and Types of Attacks in Network“, International Conference on Intelligent Computing, Communication & Convergence , 503-506 Odisha, India. 2015

[12] Todd Lamle. CompTIA Network + Study Guide 2nd Edition. Indianapolis: John Wiley & Sons. 2012