International Journal of Pure and Applied Mathematics
Volume 117 No. 15 2017, 893-904
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

Implementation of Blowfish Cryptography Algorithm, The Data Encryption Standard And Base64 In Secure Web-Based Data On Pt. Lumintech Solusindo

Ady Widjaja[1],Mujito[2], Singgih Hadi Saputra[3]

UNIVERSITAS BUDI LUHUR

ady_w168@yahoo.co.id, jitosalemba@gmail.com, gundulg25@gmail.com

ABSTRACT - One way with the use of cryptographic methods for the Sphinx or disguise the data file of these, so it can't be seen by the parties are not responsible for maintaining the security of your data or the information stored in the file. The method used is the algorithm Blowfish, DES and Base64. Use of the cryptographic system intended to double the data is not easily exploited because the process data security is exercised twice so that the data has safety that double as well. This data security application created with the PHP programming language or web-based. application has two users access. The admin user in specializing to set the system and user members for public users Use this application when it was verified. The result of the encryption will be stored into the server storage. To see who else is equipped with features to access the application system log that can be to record the activity of each user login.

Keywords: Cryptography, Blowfish, Data encryption standard (DES), Base64

1. Introduction

Data delivery via electronic media has been be daily necessities. Delivery of data through the Internet is a communications network the method is relatively quick and inexpensive, but not ensure the security of data sent. PT. Lumintech Solusindo is a service company in the field of telecommunications technology. Where each employees use the internet for conduct communication and sending of files. File that question is the financial transaction reports employee attendance and reports. For now on PT. Lumintech Solusindo yet there are applications therefore data security. Where it is in question so that the important data that became a secret the company can be secured, so that the other party Unable to find out any information contained on such important data. According to Sitinjak et.al., (2011) that is one of the Blowfish algorithm algorithms are not patentable and strong enough because it has a huge key spaces and its length can vary, so it's not easy attacked on the part of the key. While according to Munir in Kusumawati and Anisa (2014) DES have the security level because external DES key length. Method security data used is Cryptography [15] Blowfish and DES for a safer and results resistant to attack.

2. The Cornerstone Of The Theory

2.1. Cryptographic

The word Cryptography is derived from Greece Kryptos Wednesday (hidden) and Graphien (writing). Cryptography is the art and science to keep the news. In Cryptography we will see some important terms such as plaintext, ciphertext, encryption, decryption, cryptanalysis, and cryptology. The plaintext is data that can be read, While the techniques for making data cannot be read is called encryption. Data that has been encrypted called ciphertext, and techniques for restoring ciphertext into plaintext is called decryption. Cipher is a cryptographic algorithms, i.e. mathematical function that plays a role in encryption and decryption of the data. Perpetrators who are experts in the field Cryptography is called a cryptographer. Cryptanalysis is the science to decipher ciphertext becomes the plaintext with no proper way, While those who mastered this science called Cryptanalyst [11]. In a good kriptosistem must have the following characteristics [16]:

a. security systems lies in confidentiality key and not on a confidentiality algorithm used.
b. have the space key (keyspace) is great.
c. Generate ciphertexts that look random in all statistical tests conducted against him.

d. able to withstand the attack of the whole known before.

Cryptographic algorithm consists of three basic functions, IE:

a. Encrypt

It is very important in Cryptography, is the safeguarding of data submitted in order to be maintained in strict confidence. A message original called the plaintext, which is converted into code that is not understandable. Can encrypt interpreted with a cipher or code. Is the same as with if not understand a Word then do is to see it in a dictionary or glossary. Different from the case with encrypt, to change the original text to the text-code used algorithm can encode the desired data.

b. Decrypt

Is the opposite of encrypt. A message the disencrypt has returned to the form origin (original text), called the decrypt the message. The algorithm used to decrypt certainly different or opposite with algorithms that used to encrypt.

c. Key

The key question here is the key used to encrypt and decrypt. The key is divided into two parts, the key the secret (the private key) and public (public key key).

If the encryption process was described, and decrypt such scientific Picture 1:

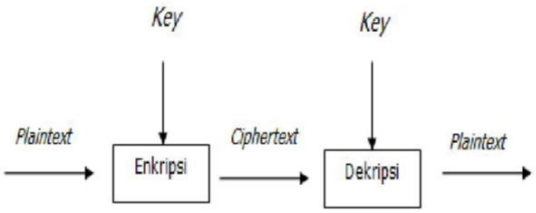

Figure 1: the process of encryption and decrypt scientific

2.2. Blowfish

In cryptography, Blowfish is created by a Cryptanalyst named Bruce Schneier, President of Counterpane Internet company Security, Inc. (company consultant about Cryptography and computer security) and published in 1994. Made for used on a computer that has micro possesor large (32-bit and above with cache large data). Blowfish algorithm is which are not patentable and license free, so everyone can use this algorithm to secure the data. The length of the block from blowfish Algorithm use 64 bits or 8 bytes. Key length varies between 32 bit or 4 bytes to 448 56 bit or byte. Using feister cipher as many as 16 rounds. Each iteration consists of permutations with input is key, and substitution of data. All operations performed by leveraging the operation XOR and the addition of. Additional other operating is merely four search tables (lookup table) an array of indexed for each round. Algorithm Blowfish has the P-array-size 18 each contains 32 bit subkey written in hexadecimal form. And has four S-boxes every SBox have a size of 256 entries of data reading in hexadecimal form. Blowfish uses a subkey. This key must be computed before encryption or decryption of the data. Blowfish is also related to the format ASCII (American Standard Code for Information Interchange) because all strings will the encrypt be changed being the ASCII code. In doing the calculation algorithm Blowfish, there are 3 part calculation, namely:

a) Key-Expansion

Function key change (minimum 32-bit, the maximum 448-bit) into multiple arrays subkey (is) with a total of 4,168 bytes. Blowfish uses a subkey large. These keys must be calculated before the encryption or decryption of data.

b) Data encryption

Consists of a simple function (Feistel iteration Network) 16 times round. Each rounds consist of a permutation lock dependent and substitution of key and data dependent. All operations are additions (addition) and XOR on 32-bit variables. Other additional operations is just four tables (table search lookup array indexed) for each round. Blowfish is a Feistel network consisting of 16 rounds. Input is 64 bit data elements.

c) Decryption of Data

How to do the same with decryption How to do the encryption as above, However, in the process of decryption sequence P0, P1, ..., P17 used in reverse order. For easy-to-understand illustrations can be seen Blowfish algorithm in Figure 2.

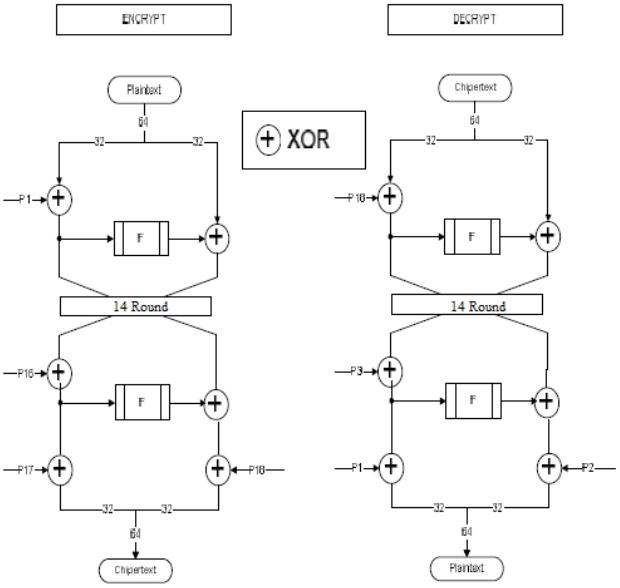

Figure 2: Blowfish encryption Algorithm and scientific decrypt

As for the function F to Blowfish-like Pictures 3.

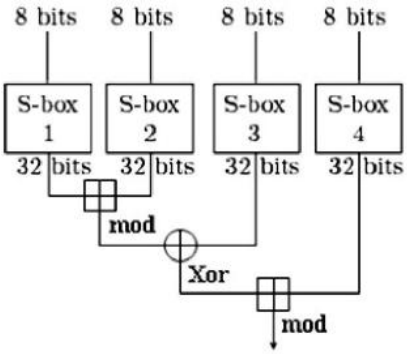

Figure 3: function F Blowfish

F-function for blowfish has 4 S-Box each receive 8-bit input and will generate 32 bits. Mathematically the F-function can be written as, the following:
F (xL) = ((S1, S2, a + b mod 232) XOR S3, c) + S4, d MOD 232

2.3. The Data Encryption Standard (DES)

The DES algorithm developed at IBM under the the leadership of w. l. Tuchman in 1972. This algorithm is based on the Lucifer algorithm created by Horst Feistel. DES is block cipher cryptographic symmetry that operates on 64 bit block size. DES encrypt 64 bit plaintext into 64 bit ciphertext with using 56 bit internal key or subkey. Internal key raised from external key length 64 bit. more details can be seen on Figure 4:

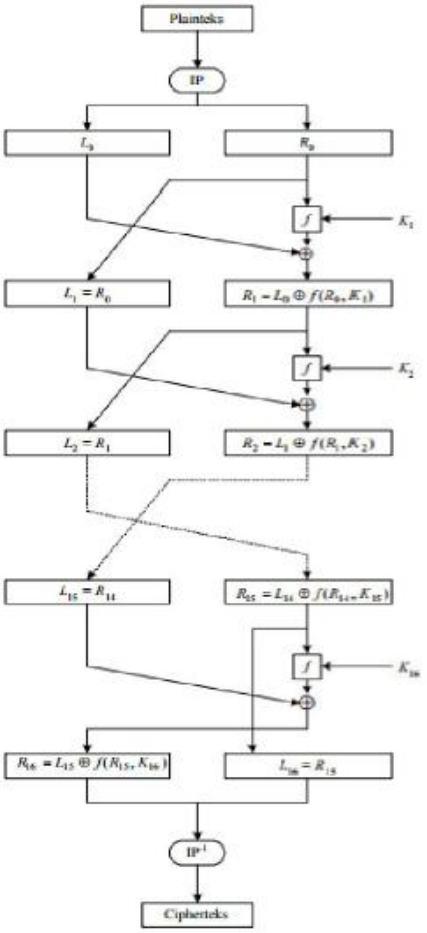

Figure 4: the Data Encryption Standard Algorithm (DES)

In the encryption process, the block is divided plaintext into two parts, the left (L) and right (R), each length is 32 bits. The second part of this enter into 16 rounds of DES. At each round I, R is block inputs to functions the transformation is called f. f function, block R combined with internal key Ki. Ex. of the function f on the Xor-kan with block L for get a new block of R. While the block L the new block is directly taken from the R before. This is one round of DES. Mathematically, one round of DES stated as:
Li = Ri-1
RI = Li-1 $\oplus$ f (Ri-1, Ki)
One round of DES is a Feistel network model. Feistel network image for one round of DES could seen in Figure 5.

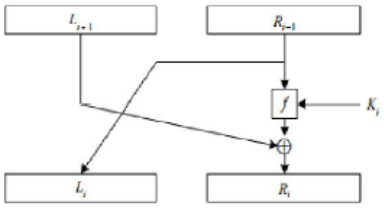

Figure 5: the algorithm one round of DES

Each of the first round against the block plaintext initial permutation (initialization done permutation or IP). The purpose of the initial permutation is randomize plaintext so that the sequence of bits-bits in it change. Since there are 16 rounds then it takes key internal as much as 16 pieces, namely K1, K2, ..., K16. This internal keys can be raised before the encryption process or in conjunction with the encryption process. Internal key raised from external key provided by the user. Key external length is 64 bits or 8 characters. Suppose an external key is composed of 64 bit is this external Key k. be the input for the permutation by using matrix permutation PC-1 compression. In permutations, each bit to the eight (parity bit) from eight byte key is ignored. The results of the permutation is 56 bits, so that it can It is said that the length of DES keys are 56 bits. Furthermore, 56 bit is divided into 2 parts-right and the left, each of which 28 bits in length. Furthermore, the second section slid left (left shift) along one or two bits depending on each round. The operation of the shift are wrapping or round shift. Suppose (Ci, on) stated the merger of the Ci and Di. (Ci + 1, + 1) retrieved by shifting the Ci and In one or two bits. After shifting the bits, (Ci, on) experiencing permutations compression by using matrix PC-2. With this, the internal key permutation Ki lowered from (Ci, Di) which in this case is the Ki the merger of bit-bit Ci and Di. So, any key internal Ki has a length of 48 bits. Process encryption block against plaintext after initial permutation. Each block plaintext experience 16 rounds of encryption. Each round of encryption is that Feistel network mathematically expressed as

Li = Ri-1

RI = Li-1 $\oplus$ f (Ri-1, Ki)

Diagram of computing the function F can be viewed from Figure 6:

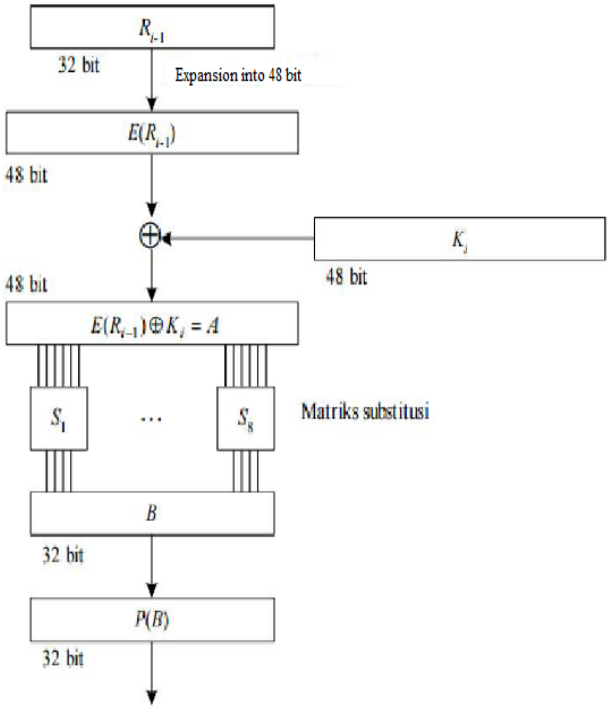

Figure 6: function F the Data Encryption Standard (DES).

E is a function of expansion which expands the block Ri-1 length 32-bit into a block of 48 bits. Function the expansion was realized using a matrix expansion permutation. Furthermore, the result of the expansion, i.e. E (Ri-1) 48 bit long in-Xor-to with a length of 48 bit Ki produce A vector length is 48 bits:

E (Ri-1) $\oplus$ Ki = A (4)

Vector A are grouped into 8 groups, each of the 6 bits, and be input in process substitution. Process substitution is done with using the eight S-boxes. Each box-S receive input and produce output bit 6 4 bit. The output vector is the substitution process B its length is 48 bits. The vector B becomes the input for the permutation process. The purpose of this permutation is the process to randomize the results of S-box substitution. Permutation performed using a matrix permutation P (Pbox). Bit-bit P (B) is the output of the function f. Finally, bit-bit P (B)-Xor-kan Li-1to get Ri.

RI = Li-1 $\oplus$ P (B)

Thus, the output of the round to-i was

(Li, Ri) = (Ri-1, Li-1 $\oplus$ P (B))

The last permutation performed after 16 laps against the combined block left and right blocks. Process initial permutation matrices using the permutation inverse (inverse of the initial permutation IP-1). Process decryption is the reverse of the ciphertext against of the encryption process. DES algorithm the same for the encryption and decryption. If it is on the process of encryption key sequence is used internally is the K1, K2, ..., then in the process of decryption K16 is the reverse

2.4. Base64 Encoding-Decoding

Base64 is a general term for a number of schemes similar encoding encode binary data and translate it into a base 64 representation. The term Base64 MIME encoding content comes from (Multipurpose Internet Mail Extension). Base64 encoding schemes are commonly used when There is a need to encode binary data which need to be stored and transferred over media that designed to handle textual data. This to ensure that the data remains intact without changes during the delivery. Base64 is used common in some applications including email through MIME, and data storage complex in XML (Extensible Markup Language). A widely used Base64 transformation in the world of the Internet as a data format for the media transmit data. Due to the results of the transformation of the Base64 form of the plaintext, then this value is would be much more easily sent, compared to formats the data in the form of binary. Base64 transformation is one of the algorithms for Encoding and Decoding the data into a ASCII format, based on the number of basic 64 or could be said to be one of the methods used to perform encoding (encoding) against the data extension. The characters are generated in Base64 transformation is composed of A.. Z, a.. z and 0 .. 9, and coupled with the two the last character i.e. symbol + and / and one of the characters is equal to (=) used for adjustments and to fulfill the data extension or the term is referred to as the charger pad. Characters the symbol will be generated depending on the the algorithm processes running.

3. The Design Of The System And Application

The design is a process that is done to design the application. The design of the system made in General is to encrypt and decrypt uses Blowfish and DES-based method the Web, as for some stages in the design the applications are as follows:

3.1 Use Case Diagram

The first stage in the design of the system is Create Use Case diagrams. The design of the the functionality of the system can be seen in Figure 7.

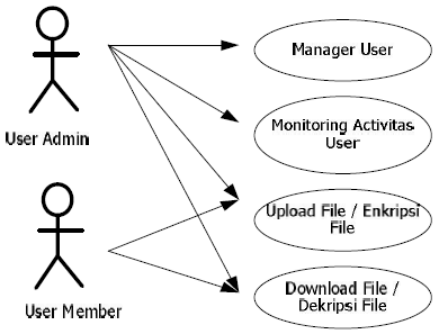

Figure 7. Use Case Diagram Data Security System

3.2 The draft Menu

After the design of the application flowchart Encrypt with DES and the Blowfish method has been designed, then the next will do the design of the program menu. Draft menu the programs are categorized into two parts, namely:

a. the Admin User Menu

The admin user menu is a menu where spesial for admin access only.

1. Home page: user after login interface.
2. Log system: interface for featuring a list of activates systems such as failed logins, recordings of visitors.
3. User File: displays the list of files that have been uploaded to the server.
4. User Manager: the user can manage all users who have been there in the database and view user activity.
5. Logout: Exit the system.

b. Members User Menu

The menu display is user member to access the user member. The menu has been in provide among other things: the home page, and user Files.

1. Home page: user after login interface.
2. User File: displays the list of files that have been uploaded to the server.
3. Logout: exit the system.

3.3 The Design Of The Algorithm Of The Program

For the design of process application can encrypt seen in Figure 8.

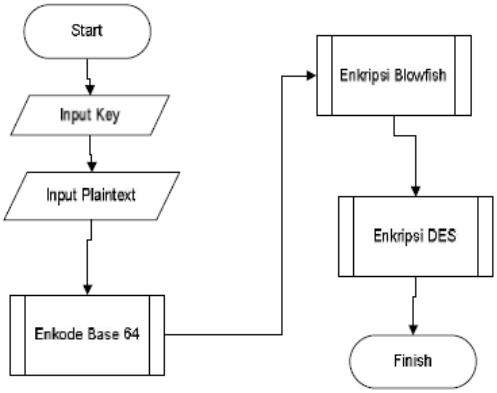

Figure 8. process Encryp

For design application can decrypt process seen in Figure 9.

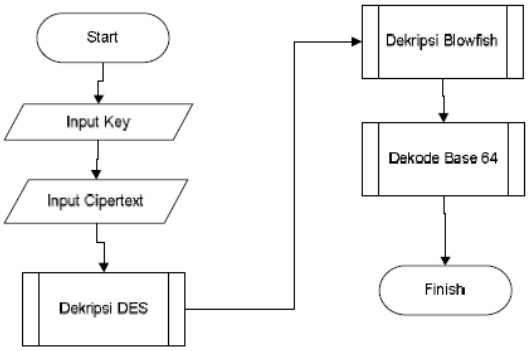

Figure 9. process Decrypt

4. RESULTS and DISCUSSION

In general each program has an input and in this application, the output has the input form files from a local directory to be uploaded via the encryption process so that the files will be stored in the a storage server with files that are already encrypted. Before the uploading user is required Enter the key to securing the files. To display the form of encryption can be seen on Figure 10:

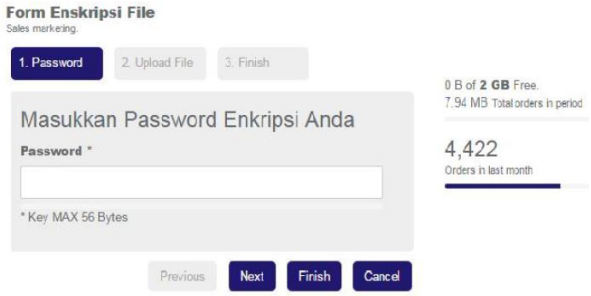

Figure 10 : display the upload form or encryption

To view files which have been uploaded can be Select user file menu. Every user can have own storage directory. Every item there is download menu on the select a user to Download the tar files which have been uploaded in addition files can be deleted if the file is no longer important or user storage capacity is up. Display the list of files the user can be seen in Figure 11.

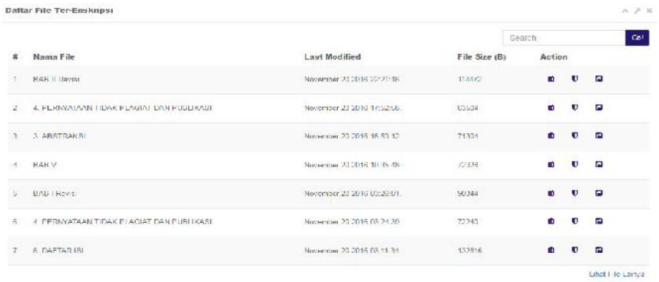

Figure 11: file list view ter-encryption

In addition the user can download the file again will be in need of a storage server in terms of before the download process should include secret key encrypt key so that the appropriate file back meaningful. For the download page can be seen in Figure 12.

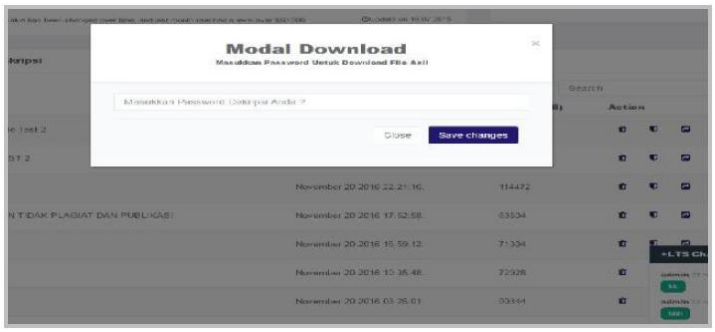

Figure 12: display download form or decryption

The following is an example of the file before the trial results and after doing encryption.

Table 1: File before and after Encryption

File Types	Before	After
Text		
Image		
Audio		
Video		

On the results of the test conducted as many as 17 times with different file types the average file size original 957166.4444 B for average results encryption 1203242.556 b. the encryption process makes the size of the file gets larger 25.70881089% of size the original. In terms of the average time the encryption process and decryption from the results of testing 280.913 s for the process of encrypt and to the process of decryption 278.862 s.

Table 2: the results of the testing algorithm

i	File Name	Type File	Original Size (B)	Enkripsi (B)	Combine 2 chiper		Change from original size (%)
					Time for execute Encrypt (s)	Time for execute Decrypt (s)	
1	Doc_01. Invoice MAC.docx	Docx file	945094	1257474	220.373	210.352	33,05279686
2	Doc_02. Invoice NW.docx	Docx file	276160	3482689	588.704	581.753	26,10853617
3	Doc_03. Invoice Tara Telko.docx	Docx file	943428	1255267	212.702	208.722	33,05382075
4	Img_01. Nota Petty Cash_2.png	Image file	3254091	4271820	721.111	721.751	31,27536999
5	Img_02. Nota Petty Cash_1.png	Image file	239654	309641	52.023	51.533	29,2033515
6	Img_03. Nota Petty Cash_3.png	Image file	653972	866885	148.579	149.658	32,55689846
7	Nota Jabar Agustus.pdf	Pdf file	1366181	1791434	302.257	302.057	31,12713469
8	Nota Tara September 2016.pdf	Pdf file	3577793	4717085	798.866	791.885	31,84342973
9	SEPTEMBER 2016.pdf	Pdf file	101041	133536	22.441	22.811	32,16021219
10	Timesheet Imam suryadi November 2016.xlsx	xlsx File	14614	18189	0.313	0.317	24,46284385
11	Timesheet Nur Kholis_Agustus 2016.xlsx	xlsx File	81689	104220	17.071	17.981	27,58143691
12	Timesheet Nur Kholis_September 2016.xlsx	xlsx File	138354	177706	29.772	29.472	28,4429796
13	text_01. about_Arithmetic_Operators.help.txt	txt file	13898	14327	0.252	0.297	3,086775076
14	text_02. TableTextServiceSimplifiedQuanPin.txt	txt file	1635484	1707810	290.157	288.166	4,422299454
15	text_03. status.txt	txt file	1444165	1478728	247.814	255.065	2,393286086
16	wav_01. Windows Balloon.wav	Audio File	17549	22648	0.39	0.379	29,05578665
17	wav_02. Windows Battery Low.wav	Audio File	24803	30192	0.493	0.558	21,72721042

5. CONCLUSION

From the test results and previous discussion then it can be inferred, the application can run appropriate functions. The application can secure data with the results of unknown meaning. File size affects the timing of the process the program. In order for the test results better to suggest that it may use the higher hardware specification

BIBLIOGRAPHY

1. Hendrayanto, Rudy, Nilawati, A. Ramadona. “Program Aplikasi Enkripsi Dan Dekripsi Sms Pada Ponsel Berbasis Android Dengan Algoritma Des”. Prosiding Seminar Ilmiah Nasional Jenis File Sebelum Sesudah Text Gambar Audio Video Komputer dan Sistem Intelijen (2012). Vol.7 : 631-633
2. Marcel , Jonathan. “Studi Perbandingan Cipher Blok Algoritma Blowfish Dan Algoritma Camellia” . (2010)
3. Kusumawati, Tri Ika Jaya, Anisah, Devi. “Analisa dan implementasi steganografi untuk pelaporan internal perusahaan menggunakan algoritma Data Encryption Standard (DES) dan metode End Of File (EOF)” Berbasis java programing”. Jurnal Telematika MKOM (2015). Vol. 7. No. 2. 117-186
4. Muslim, Amrullah Imaduddin, Isnanto, R. Rizal, Widianto, Eko Didik. “Perancangan dan Implementasi Algoritma DES untuk Microprosesor Enkripsi dan dekripsi pada FPGA”. Jurnal Teknologi dan Sistem komputer
5. (2015). Vol. 3, No. 2 : 259-266
6. Prasetiyo, Budi, Gernowo, Rahmat, Noranita, Beta. “Kombinasi Steganografi Berbasis Bit Matching dan Kriptografi DES untuk Pengamanan Data”. Scientific Journal of Informatics (2014). Vol.1, No.1 : 79- 94
7. Primartha, Rifkie. “Penerapan Enkripsi Dan Dekripsi File Menggunakan Algoritma Data Encryption Standard (DES)”. Jurnal Sistem Informasi (2011) : 371-387
8. Putro, Sigit Susanto. “Peranan Kriptografi Dalam Keamanan Data Pada Jaringan Komputer”. Jurnal Ilmiah Kursor (2007), Vol.3, No. 2 : 20-30
9. Rizal, Ansar, Suharto. "Implementasi Algoritma RC4 untuk Keamanan Login Pada Sistem Pembayaran Uang Sekolah." Dielektrika (2011).
10. Sadikin, Rifki. “Kriptografi Untuk Keamanan Jaringan”. Yogyakarta: Andi, 2012.
11. Sitinjak, Suriski, Fauziah, Yuli, Juwairiah “Aplikasi Kriptografi File Menggunakan Algoritma Blowfish”. Seminar Nasional Informatika (2010), Hal . 78-86

12. Sulaiman, Oris Krianto, Ihwani, Mohamad, Rizki, Salman Fajar. “Model Keamanan Informasi Berbasis Tanda Tangan Digital Dengan Data Encrytion Standar (DES) Algorithm” Jurnal Nasional Informatika dan Teknologi Jaringan (2016).Vol.1 No.2 : 14-19
13. Udayana, Putu Agus Eka Darma, Sastra, Nyoman Putra. “Perbandingan Performansi Pengamanan File Backup Lpse Menggunakan Algoritma Des Dan Aes”. Jurnal Teknologi Elektro (2016). Vol.15, No.01 : 111-117
14. Utami, Ema, Tambunan, Shanty Erikawaty Aryani. “Penerapan Algoritma Blowfish Untuk Membuat Sebuah Model Kriptosistem Algoritma Dan Menganalisis Kinerja Algoritma Blowfish Dengan Simulasi Data Terbatas.” JURNAL DASI (2010): 33-44.
15. Chellaprabha.B, “Improving The Security Of Computer Networking Using Steganography Technique”, International Journal of Innovations in Scientific and Engineering Research (IJISER), ISSN: 2347-971X (online), ISSN: 2347-9728(print), Vol.3.no.4, pp.33-37, 2016, http://www.ijiser.com/.
16. Rajesh, M., and J. M. Gnanasekar. "Annoyed Realm Outlook Taxonomy Using Twin Transfer Learning." International Journal of Pure and Applied Mathematics 116 (2017): 547-558.
17. Rajesh, M. & Gnanasekar, J.M. Wireless Pers Commun (2017),https://doi.org/10.1007/s11277-017-4565-9
18. Rajesh, M., and J. M. Gnanasekar. "GCCover Heterogeneous Wireless Adhoc Networks." Journal of Chemical and Pharmaceutical Sciences (2015): 195-200.
19. Rajesh, M., and J. M. Gnanasekar. "CONGESTION CONTROL IN HETEROGENEOUS WANET USING FRCC." Journal of Chemical and Pharmaceutical Sciences ISSN 974: 2115.
20. Rajesh, M., and J. M. Gnanasekar. "GCCover Heterogeneous Wireless Ad hoc Networks." Journal of Chemical and Pharmaceutical Sciences (2015): 195-200.
21. Rajesh, M., and J. M. Gnanasekar. "CONGESTION CONTROL USING AODV PROTOCOL SCHEME FOR WIRELESS AD-HOC NETWORK." Advances in Computer Science and Engineering 16.1/2 (2016): 19.
22. RAJESH, M. "TRADITIONAL COURSES INTO ONLINE MOVING STRATEGY." The Online Journal of Distance Education and e-Learning 4.4 (2016).
23. Rajesh, M. "Object-Oriented Programming and Parallelism."
24. Rajesh, M., K. Balasubramaniaswamy, and S. Aravindh. "MEBCK from Web using NLP Techniques." Computer Engineering and Intelligent Systems 6.8: 24-26.