`

COMBINATION OF AES ALGORITHM WITH BLOWFISH ALGORITHM FOR FILE ATTACHMENT AT E-MAIL SENDING

[1]Yongki Iswo, [2]Poltak Sihombing
Teknik Informatika Fasilkom –TI USU Jln. Universitas No.20A Kampus USU Medan 20155
[1]Yongki_iswo@students.usu.ac.id [2]poltakhombing@yahoo.com

Abstract

Data security in the delivery of online file becomes very important in the world of information itself. One way that can be done for the security of the data is to perform encryption before the data is sent. Cryptographic message encoding divided into two symmetric and asymmetric. Kriptogarfi AES (Advanced Encryption Standard) is a symmetric cryptographic algorithms means that the key used in the encryption process is the same as the key to the decryption process. The analysis concludes theory, AES encryption process is designed to make the process of encoding in secret with no security level of complexity linear with time as efficiently as possible through the use of processes of transformation of light in the implementation. Aside from the AES algorithm, Blowfish algorithm is also a symmetric cryptographic algorithm. Theory analysis shows that Blowfih a cryptographic algorithm that uses a key with variable length provided that no more than 448-bit. Blowfish also combine non-reverse function f, keydependent S-Box, dun Feistel network. The process of encryption and decryption using the ECB and CBC operation has the same worst case is *O* (n). In this study the authors combine these two algorithms in the security of a file attachment in an email that is expected to increase the security file.

Keywords -- *Chriptographi, AES, Blowfish*

1. **Introduction**

In line with the development of information and communication technologies, which formerly remote communication still use the conventional way, ie by sending each other letters, but now long-distance communication can be done easily and quickly, with the occurrence of technologies such as SMS (Short Messaging Service) and email . The Internet has made a more open communication and exchange of information is also growing rapidly past the boundaries of countries and cultures. But not all developments of communication technologies have a positive impact and benefit. One of the negative impact on the development of technology is the tapping or theft of data.

Cryptography is derived from the Greek cryptos which means "secret" (hidden) and graphein meaning "writing". Thus, cryptographic means "secret writing" which means hieroglyph [4] implementing the AES algorithm in increasing data security in cloud computing. As a result obtained faster computation time and increase data security from attack and leakage.

Other researchers [6] compare the performance of the AES algorithm with DES stated that the AES algorithm for deriving time comsumtion or use a smaller computational time compared with DES and AES algorithms produce a higher level of security than DES. AES assign Federal Information Processing Standards (FIPS) approved cryptographic algorithms used to protect electronic data [1].

Other algorithms are also frequently used in securing digital data is Blowfish algorithm. [5] examined the implementation of the Blowfish algorithm on comparison computing speed and power consumption for some kind of symmetric algorithms are DES algorithm. The results showed that the Blowfish algorithm is superior in terms of speed and power consumption, especially in the delivery of data over a network without cables or wireless. Other researchers [2] examined the security image data or image using the Blowfish algorithm. The results of the study revealed that the Blowfish algorithm has a very good level of security, but on the other hand increase data security depends on the number of rounds used. In other words, to obtain a high level of security is needed number of rounds that much anyway. Other researchers that [5] modify the Blowfish algorithm is to replace the XOR operation is a long process and spend a lot of energy.

Security is an important factor in the evaluation that includes resistance to all known passwords analysis and is expected to face the analysis of an unknown password. In addition, AES also should be used freely without having to pay royalties, as well as with Blowfish cryptographic algorithm and also cheap to be implemented on a smart card which has a small memory size. In this study will be combined with the AES algorithm Blowfish algorithm in order to avoid using too much round the Blowfish algorithm for the use of the round is too much to be directly proportional to the increase in memory usage or reduction of computational speed.

2. Basics Term

A. Symmetric Algorithm.

Symmetric algorithms or also called secret key algorithm is an algorithm which can be calculated from the encryption key encryption key and vice versa. Symmetric algorithm also called conventional algorithms, which can be determined decryption key from the encryption key, in other words the encryption key and decryption key together. Symmetric algorithms require an agreement between the sender and receiver of the message on a key before it can communicate securely. Symmetric algorithms can be classified into two types, namely stream ciphers and block ciphers. Stream ciphers operate bits per bit (or byte per byte) at a time. While block ciphers operate per group groups of bits called blocks (blocks) at a time.

People often use mathematical notation to simplify the writing and analysis, so that modern cryptography is always associated with mathematics. With original message M and the secret code C obtained from the encryption key K, we can be written as follows:

C = Ek (P)

In the decryption process, do the reverse operation, and can be written as follows:

P = Dk (P)

The process of encryption and decryption can be illustrated in the figure below

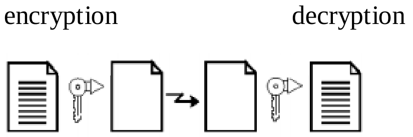


Figure 1. Encryption and decryption process of symmetric algorithm

Excess cryptography symmetry is:

a.Proses symmetric cryptographic encryption and decryption requires a short time.

b. Symmetric key size is relatively short.

c.Otentikasi sending a direct message from the ciphertext received unknown, because the key is known only to the recipient and the sender only.

Disadvantages cryptography symmetry is:

a. Symmetric key must be sent via a secure communication channel and both entities that communicate must maintain the confidentiality of the key.

b. Keys must be frequently changed, each time carrying out communication

B. Key of Symetry Algorithm

Cryptographic algorithm Advanced Encryption Standard (AES) 128 bit key length Nk use = 4 word (words) that each word consists of 32 bits for a total of 128-bit key, the original text block size of 128 bits and has 10 rounds. While round to lock consists of Ki = 4 words and the total round 128-bit key and an expanded key has size 44 words and 176 bytes. AES cipher algorithm took the key and perform key expansion routine (key expansion) to form the key schedule. Key expansion yielded a total of Nb (Nr + 1) word. This algorithm requires initial set consisting of Nb key word, and every round Nr need key data as Nb word. Results of the key schedule consists of a linear array of 4-byte word that denoted by [wi].

While Blowfish is a cryptographic algorithm that is designed to operate on 64-bit message block and use the key variable key length from 32 bits or 4 bytes to 448 bits or 56 bytes. Using as many as 16 rounds Feistel Cipher. Blowfish algorithm has a P-array of size 18 each of which contains a 32-bit subkey, and four S-Box with 256 entries. The algorithm consists of two main parts: the expansion key (key-expansion) and the encryption process. While the decryption process using the exact same process with the encryption process, differing only in the order subkey uses and use as many as 16 rounds Feistel Cipher. Blowfish algorithm has a P-array of size 18 each of which contains a 32-bit sub-keys, and four S-Box with 256 entries.

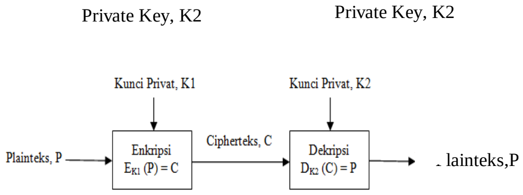


Figure 2. Symmetric key algorithm process

C. AES Algorithm

Cryptographic algorithm AES (Advanced Encryption Standard) is a symmetric cryptographic algorithm. Input and output of the AES algorithm consists of a sequence of 128 bits of data. The sequence data that has been formed in a group of 128 bits is referred to as a block of data or plaintext into ciphertext will be encrypted. Cipher key of AES consists of a key with a length of 128 bits, 192 bits, or 256 bits. Process round AES-128 encryption is done as much as 10 times (a = 10), as follows

1. Addroundkey
2. Round as a-1 times, the process undertaken in each round are: SubBytes, ShiftRows, MixColumns, and AddRoundKey.
3. Final round, is the process for the last round which includes SubBytes, ShiftRows, and AddRoundKey.

While the AES-128 decryption process, the process of rotation is also done as much as 10 times (a = 10), as follows:

1. Addroundkey
2.The round as a-1 times, where in each round is done the process: InverseShiftRows, Inverse SubBytes, AddRoundKey, and Inverse MixColumns.
3. Final round, is the process for the last round which includes InverseShiftRows, InverseSubBytes, and AddRoundKey.

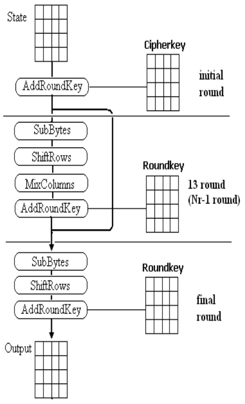


Figure 3. Encryption of process AES algorithm

In encryption and decryption of AES-192 round process done 12 times (a = 12), while for AES-256 round process done 14 times (a = 14).

D. Blowfish Algorithm

Blowfish is a symmetric key algorithm, Blowfish is also a block cipher, which means that during the process of encryption and decryption Blowfish will divide the message into blocks of equal size in length. The length of the block for the Blowfish algorithm is 64-bit.

[4] explains that the Blowfish was created by a cryptanalyst named Bruce Schneier, president of Counterpane Internet Security, Inc. (Company consultant on cryptography and computer security) and published in 1994. Created for use on computers that have a large microposesor (32- bits up with a large data cache). The size of a block algorithm Blowfish length is 64 bits or 8 bytes. Key lengths ranging from 32 bits or 4 bytes to 448 bits or 56 bytes. Using as many as 16 rounds Feistel Cipher. Blowfish algorithm has a P-array of size 18 each of which contains a 32-bit subkey, and four S-Box with 256 entries.

Blowfish encryption process consists of a simple function iteration (Feistel Network) as many as 16 rounds (iterations), is a 64-bit input data element X. Each round consists of a key-dependent permutation and substitution key- and data-dependent. All operations are addition (addition) and XOR on 32-bit variable. An additional operation is only four tables searches indexed array for each round. The steps are as follows.

1. For X into two parts, each of which consists of 32-bits: XL, XR.
2. For i = 1 to 16
   XL = XL XOR pi
   XR = F (XL) XOR XR
   Swap XL and XR

3.After iteration sixteen, exchange XL and XR again to perform Undo the last exchange.
4. Then do
XR = XR XOR P17
XL = XL XOR P1
5.Last , merge back XL and XR to get cipherteksnya

3. Encryption And Decryption Process

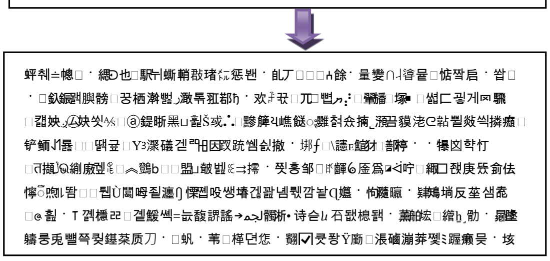
Stages of the process of data encryption is useful for securing messages in the form of writing symbols, which to secure the message author uses the AES algorithm and to reinforce the message author encrypt again by using the Blowfish algorithm. In the process of data encryption is done with the steps:

1. Insert the text file or the original message to be encrypted (plaintext) using the AES algorithm.
   Application examples: Suppose Andi send data to Alice. The data (plaintext) which will be sent by Alice are: Plaintex: 0 1 2 3 4 5 6 7 8 9 A B C D E F
2. In HEX : 30 31 32 33 34 35 36 37 38 3 41 42 43 44 45 46

Key : A B C D E F G H I J K L M N O P
In HEX : 41 42 43 44 45 46 47 48 49 4A
4B 4C 4D 4E 4F 50

1. Then the data is stored and for the next step the resulting ciphertext is saved in the specified directory and we encrypt the file again using the Blowfish algorithm.

```
CC1856582992B45CEE4D917B0B3D533695C96399EF747C267B93A8B5
73CEF988E6D83C28FED3A6B1AA10C57AA5C4322F1ADEDACF45670
8A828397E95D4E6EE96803B8D95F0B71585DFD7C3E7D57965691A337
B33C03A2A7F36289DF5E89D0AB27B33A9282A1CD563B1CA412E7637
2AC9930A3F09BF7CFA37F7ED36A63301BBAD7DF052233D25757F1D6
1B1436776D8E34A0DA60AA3743316334F60F77EAFDB64664093DAEC
54FF6D49E402F30AB5D512A0A346AFD5448642BB64F1338C91A7182
AD6FB28A15EFADA92BC5839D46852DB41F8CD53F145FDE316D5D5
FC1EDAA94D8E146D973D797C5797331A3206CF204B29EEC1D7CD64
B87CDB9C59C4D67F75B7DEEF12414F10C272E8E2C912F9AD80D3DA
F3AC20AB348A5B8BC59C4C824938929CC3B8E3F150615248FEF10106
35D893EE1AD05E202265CC9DAD96A60B98D6D5F58C16E703FA6CDE
```



. Figure 4. Encryption file with AES and Blowfish algorithm

3. to restore the files to forms the original message, then we decrypt prior to the blowfish algorithm then follow the aes algorithm in the key used to encrypt the file when the message.

4. Theory Analysis

In this study we will examine a file's that we have made in advance.

Table 1 .File Encryption with AES algorithm

File Name		A.htm	B.pas	C.bas	D.prg	E.txt
File Capacities		1 KB	15 KB	30 KB	7 KB	22 KB
T i m	**1**	4,4	12,2	17,5	6,88	9,38
	2	10	18,1	17,2	38,1	23,8
	3	17,5	2,5	1,57	34,4	25

e Spent	**4**	32,5	4,38	5,94	37,5	21,3
	5	13,8	10,6	7,19	21,3	0,16
	6	38,1	4,69	16,6	35,6	26,2
	7	5	19,4	15,9	15	26,25
	8	30	10,63	10,31	15,63	19,38
Average		18,91	10,31	11,52	25,55	16,97

results from table 1. The above can be displayed in graphical form, as shown in figure 5 below.

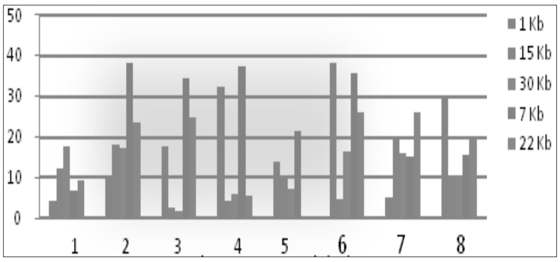


Figure 5. Process execution time file encryption with AES cryptographic

AES encryption algorithm is implemented by using the mode Electronic codebook (ECB). AES encryption process flow diagram with the ECB. Steps to perform the encryption process on AES ECB mode is:

a. *Padding plaintext.*
b. Ekspansi kunci.
c. Enkripsi blok *plaintext* 128 bit.
d. *Output.*

Execution time in step a, b, and d is constant (eg α) because it is not influenced by the size of the input. While step c (eg execution time = ε) influenced the number of input plaintext block 128 bits, so for input size n block takes εn. Overall, the execution time AES encryption with ECB mode is εn + α, with ε and α is a constant and n is the number of input block. So notation-*O* for worst case process AES encryption with ECB mode is:

$$E(AES) = \varepsilon n + \alpha$$

Obtained complexity E (AES) is within the scope *O* (n).

If the research message encryption using AES algorithm produces the output with time varying time consumption as well as file encryption using the Blowfish cryptographic algorithm that generates a second ciphertext file shown in the table below.

Table 2. Encryption File with Blowfish algorithm

File Name		A.enc	B. enc	C. enc	D. enc	E. enc
File Capacities		1 KB	15 KB	30 KB	7 KB	22 KB
Time Spent	**1**	2,39	0,20	0,25	0,15	0,34
	2	0,13	0,50	0,19	0,15	0,60
	3	0,11	0,20	0,20	0,16	0,36
	4	0,11	0,20	0,19	2,43	0,36
	5	0,10	0,19	0,20	0,12	0,59
	6	0,13	2,41	0,19	0,16	0,36
	7	0,10	1,20	0,19	0,13	0,60
	8	0,10	0,17	0,20	0,25	0,36
Average		0,39	0,51	0,20	0,44	0,45

in table 2 above displayed some executable files or encrypted using Blowfish algorithm. In the data encryption using the Blowfish algorithm is implemented in two operating modes, namely the ECB and CBC.

1. Step to ECB mode encryption is:
   a. key expantion
   b. *padding*
   c. encryption 64-bit plaintext block
   d. *output*

   Execution time in step a, b, and d is constant because it is not influenced by the size of the input, eg α_l. While the step c is influenced by the number of blocks of input plaintext 64-bit, so for input size n block the execution time required for ε_ln. Overall execution time encryption with the ECB operating mode is ε_1n + α_l, with ε_ln and αl is a constant and n is the number of input block. So notation-*O* for the worst case the ECB mode encryption process are:

$$E(ECB) = \varepsilon_l n + \alpha_l \in O(n)$$

2. Steps to perform l [d.2] to register feedback
   e. *output*

Execution time of a, b, c and e are constant because not influenced by the size of the input, eg a2. While the step d is affected by the number of blocks of input plaintext 64-bit, so for input size n block the execution time required by the EP. Overall execution time encryption with the ECB operating mode is ε_2n + α_2, with ε_2n and α_2 is a constant and n is the number of input block. So notation-*O* for the worst case CBC mode encryption process are:

$$E(CBC)\ \varepsilon_2 n + \alpha 2 \in O(n)$$

5. Results Description of Data

By using the Blowfish algorithm is happening several processes and test results of this study produced data ciphertext with varying time consumption, namely:

Table 3. Decryption File with Blowfish algorithm

File Name		A.dec	B. dec	C. dec	D. dec	E. dec
File Capacities		1 KB	15 KB	30 KB	7 KB	22 KB
Time Spent	**1**	0,10	0,24	0,22	0,17	0,33
	2	0,12	0,31	0,23	0,16	0,33
	3	0,11	0,20	0,23	0,17	0,36
	4	1,10	0,35	0,27	0,14	0,34
	5	0,09	0,17	0,17	0,12	0,59
	6	0,07	0,42	0,19	0,17	0,33
	7	0,09	0,17	0,43	0,13	0,33
	8	0,09	0,17	0,19	11,88	10
Average		0,10	0,25	0,24	1,62	1,58

In table 3 above displayed some executable files or decryption using the Blowfish algorithm and this file does not yet have meaning. With the conversion of different time and with different file but the decryption process is the capacity of the file remains the same as before in the decrypted file. Just as the process of encryption algorithm, Blowfish decryption algorithm is also implemented in the ECB and CBC operation mode.

1. Steps to perform decryption ECB mode is:
   a. key exspansion
   b. decrytption blok *ciphertext* 64 bit
   c. *unpadding*
   d. *output*

Execution time in step a, c, and d is constant because it is not influenced by the size of the input, say β1. While the step b is influenced by the amount of input ciphertext block 64-bit, so for input size n blocks required execution time of δ1 and β1 a constant and n is the number of input block. So notation-*O* for the worst case decryption process ECB mode is:

$$D_{(ECB)} = \delta_1 n + \beta_1 \in O(n)$$

2. Steps to perform decryption CBC mode is:
   a. initialization value for the initialization vector (IV), and in the store registers forward
   b. key expansion.
   c. decryption process
      c1. copy 64-bit ciphertext block to the register value
      c2. decrypt ciphertext block 64-bit
      c3. XOR plaintext block a 64-bit result of step [c.2] with a 64-bit block of ciphertext to register forward
      c4. copy 64-bit ciphertext blocks on the register value (step [c.1]) to register forward.
   d. unpadding
   e. *output*

Execution time of a, b, d and e are constant because not influenced by the size of the input, eg β2 while step c is influenced by the number of blocks of ciphertext input 64-bit, so for input size n block the execution time required for δ2n. Overall execution time decryption operation mode of the ECB is δ2n with δ2 + β2 and β2 is a constant and n is the number of input block. So notation-*O* for the worst case CBC mode decryption process is:

$$D_{(CBC)} = \delta_2 n + \beta_2 \in O(n)$$

If the message decryption research using the Blowfish algorithm produces the output with time varying time consumption as well as the process of decryption of ciphertext file-1 into ciphertext-2 are shown in Table below.

Table 4. decryption file with AES algorithm

Nama File		A.dec	B. dec	C. dec	D. dec	E. dec
File Capacities		1 KB	15 KB	30 KB	7 KB	22 KB
Time	1	5	3,75	7,81	29,38	37,5
	2	14,38	17,88	1,88	1,25	37,5
	3	16,25	5,94	6,88	22,5	38,75
	4	16,25	0,31	14,69	38,75	11,86
	5	6,25	15,63	7,19	6,25	32,5
Spent	6	30	3,75	5,63	13,16	9,36
	7	38,75	0,63	15	11,87	33,75
	8	18,75	13,75	14,06	11,88	10
Average		18,20	7,70	9,14	16,87	24,53

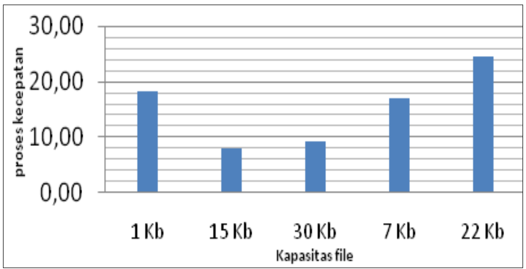


Figure 6. Graph decryption file with AES algorithms.

Once we look at the graph of the second file decryption algorithm above, the authors also make the graph change time spent or time encryption and decryption process is completed by combining the two agoritma.

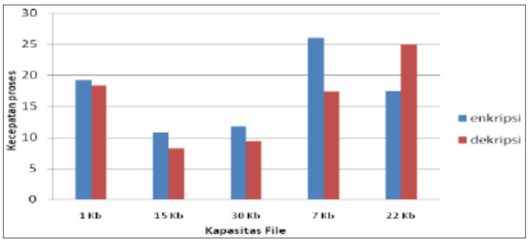


Figure 7. Graph encryption and decryption file with both algorithms.

From Figure 7. The above authors to conclude bahwas file decryption process faster computation time compared with the process of encrypting the files of the two algorithms. On the file size of 22 Kb encryption process is faster than the decryption process, but if we look at the type of the file is a text file (* .txt) file while the other is a file from the programming language under dos (* .pas, *. Bas, * .PRG) and under windows is HTML (Hyper Text Markup Language) which is used to design the website.

6. Conclusion

From the results of research conducted by the authors of the combination of the AES algorithm with Blowfish algorithm.

1. The process of encryption with AES cryptographic algorithm will change the size of the file twice the size of the original, while the use of cryptographic algorithms blowfish file size will remain as the size of the original file.
2. With Blowfish cryptographic algorithm has time encryption and decryption are more cepatdi compare with AES.
3. By using the Blowfish algorithm has a time encryption and decryption faster and will have better security by adding the number roundnya but requires more memory space.

The time required to perform encryption and decryption with AES and Blowfish algorithm combines in one such process is not fast, but sipengguna can include 2 keys on the cryptographic process. To the authors conducted 2 times the process of encryption and decryption

7. References

[1] Adib, S.E. & Raissauni.. AES Encryption Algorithm Hardware Implementation Architecture: Resource and Execution Time Optimization. International Journal of Information & Network Security (IJINS). Tetuan. Vol. **1,** pp. 110-118, 2012.

[2] Landge, I., Contractor, B., Patel, A. & Choudhary, R.. *Image Encryption and Decryption USING Blowfish Algorithm.*World Journal of Science and Technology(WJST),India. vol, 2, pp. 151-156, 2012

[3] Sachdev, A. & Bhansali, M, Enhancing Cloud Computing Security using AES Algorithm, International Journal of Computer Application (0975-8887) vol, 67**,**pp. 19-23, 2013

[4] Sitinjak, S., Fauziah, Y. & Juwairiah, *Aplikasi Kriptografi File Menggunakan Algoritma Blowfish*, Seminar Nasional Informatika, UPN Veteran Yogyakarta. pp. 78-86**,** 2010

[5] Singh, G., Singla A.K. & Sandha, Superiority of Blowfish Algorithm, International Journal of Computer Applications (0975-8887), vol. 44 pp, 23-26, 2012

[6] Sumitra, Comparative Analysis of AES and DES security Algorithms International Journal of Scientific and Research Publications, vol. **3,** pp. 1-5, 2013