Combining Advanced Encryption Standard (AES) and One Time Pad (OTP) Encryption for Data Security

Indrastanti R. Widiasari
Satya Wacana Christian University
Salatiga, Indonesia

ABSTRACT

The development of telecommunications technology and data storage using the computer has become a necessity because there are many jobs that can be completed quickly, accurately, and efficiently. In addition it allows data transmission distance is relatively fast and cheap, but on the other hand long-distance data transmission is possible others can tap into and alter transmitted data as the number of users that many in a computer network. Therefore, the system of data security and confidentiality of data is one important aspect in the development of the world of telecommunications, especially communications and using computers connected to the network. This research used a cryptographic algorithm Advanced Encryption Standard (AES) and One Time Pad (OTP) to encrypt the file. The merger is intended to cryptographic algorithms with low complexity is more than just using the existing cryptographic algorithms.

Keywords

Advanced Encryption Standard, AES, One Time Pad, OTP, encryption, decryption.

1. INTRODUCTION

Cryptography is one of the methods used to maintain security in data transmission. Along with the increase in importance, many methods are found and extended use. Among these methods are methods that only requires a simple mathematical operation, but there is also a method that involves the theory of complex and difficult implementation. Cryptographic methods are used to secure confidential data so that the data is not known to others who are not interested. One method that is very simple in cryptography is by shifting the characters in the alphabet. If the encryption is done by shifting three letters to the right, the letter A is encoded with the letter D, the letter B is replaced encoded with E, and so on. Decryption is done by reversing the encryption rules, namely by shifting three letters to the left. This method is very simple, so easily predictable because there is a one-one correspondence between the original letter and the letter password. If a letter predictable password, then all the letters the same password will be predictable as well. To avoid this, do not text encryption each letter, but a word consisting of several letters at once.

DES including the type of block cipher, because the algorithm processes the bit plaintext blocks consisting of 64 bits per block using 56-bit keys for encryption and one-time process that produces ciphertext consists of 64 bits per block. However, in 2000, precisely in October Rijndael algorithm was selected as a standard algorithm for encryption. Rijndael algorithm is then known as the Advanced Encryption Standard (AES). After experiencing some of the standardization process by NITS, then adopted a standard Rijndael algorithm officially on May 22, 2002.

There are also other methods of cryptography, the One Time Pad (OTP). One Time Pad is also known as the Vernam cipher or cipher-perfect an algorithm where the plaintext is combined with a random key. It is the only known method for mathematical encryption unresolved. Used by a team of special operations and insurgent groups during World War II. One Time Pad encryption system earned a reputation as a solid but simple in the world with absolute security that is unmatched by modern cryptographic algorithms. The development of telecommunications technology and data storage using the computer has become a necessity because there are many jobs that can be completed quickly, accurately, and efficiently. In addition it allows data transmission distance is relatively fast and cheap, but on the other hand long-distance data transmission is possible others can tap into and alter transmitted data as the number of users that many in a computer network. Therefore, the system of data security and confidentiality of data is one important aspect in the development of the world of telecommunications, especially communications and using computers connected to the network.

This research used a cryptographic algorithm Advanced Encryption Standard (AES) and One Time Pad (OTP) to encrypt the file. The merger is intended to cryptographic algorithms with low complexity is more than just using the existing cryptographic algorithms.

2. DATA SECURITY

Data security is the way to ensure that data is kept secure from theft and that access to it can be controlled. Thus data security helps in protecting personal data. Data security has several aspects, among others: [1]

• Privacy/Confidentiality

Privacy/Confidentiality can be said to act to keep the information from unauthorized access. Privacy tend more towards data private, while dealing with the confidentiality of data provided to other parties for a specific purpose and is only allowed for certain uses them. Form of attack is usually a wiretapping effort. Efforts can be made to improve the privacy and confidentiality is to use cryptographic technology.

• Integrity

Integrity is the information that should not be altered without the permission of the owner of the information. Common form of attack is the presence of viruses, Trojan horses, or other users change the information without permission, "the man in the middle attack" in which one puts oneself in the middle of the conversation and posing as someone else.

• Authentication

Authentication is defined as a method to certify that truly original, or people who access or disclosure is really the question.

• Availability

Availability relates to the availability of information when needed. Some of the barriers are found, such as "denial of service attack" (DOS attack), where the server sent requests (usually false) barrage or unexpected demand and therefore cannot serve other requests or even down, hangs, crashes. It also found mail bomb, where a user sent an e-mail barrage (thousands of e-mail) with a large size so that the user can not open e-mails or difficulty accessing e-mail. Information systems are being attacked or hacked to inhibit or eliminate access to information.

• Access Control

Access Control is a way to control access to information which is dealing with the problem of authentication and privacy. The method used is to use a combination of user id or password or using other mechanisms.

• Non-repudiation

Non-repudiation is an aspect that keeps a person cannot be denied having a deal which support for electronic commerce.

3. CRYPTOGRAPHY

Cryptography is derived from the Greek "cryptos" means "secret" (secret) and "graphein" meaning "writing" (writing). Thus, cryptography means "secret writing" (hieroglyph). During the war, cryptography is used to change the message from the language that is understood to be difficult to understand even have no meaning. But at the present time, cryptography is not only related to one's privacy, but it also has other functions as data integrity, authentication and non-repudiation [2].

Cryptography is the art and science of maintaining the security of the message. A word contained in the definition of art is actually derived from the facts of previous early cryptography, where each person has a way to write secret messages. This led to writing secret messages has its own aesthetic. In its development, cryptography can also be viewed as one of the disciplines, because the techniques that are used in the process of cryptography can be mathematically formulated so that it becomes an official method [3].

Cryptography consists of two main processes. Ie encrypt the plaintext (original message understood its contents or meaning) into ciphertext (the message is not understood, which is the result of the transformation of the plaintext) is called encryption (encryption) or enchipering (according to ISO 7498-2 standard name) and returns the ciphertext into plaintext called decryption (decryption) or deciphering (according to ISO 7498-2 standard name) [2]. Plaintext to be encrypted and decrypted using a special algorithm that is also called the cipher and a key. Cipher itself actually is a mathematical function. While the key is a series of bits that are used to encrypt and decrypt data. The key can be any value from a number of points. Thus the level of security of the algorithm using a key based privacy is key, not by the details of the algorithm itself.

The purpose of cryptography from the beginning until today is the emergence of that information remains protected from unauthorized parties know. Encryption and decryption scheme using the key is shown in Figure 1.

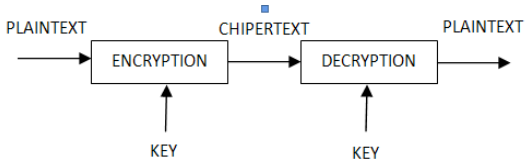

Fig 1: General Process Using Encryption-Decryption Key [2]

Message (plaintext) which will be kept confidential will experience the process of encryption, which is the process of changing plaintext into ciphertext as a result. This process will involve the secret key to be used to disguise the content of the message. To be able to read back the message decryption process is done. The process of changing ciphertext into plaintext decrypted again, using a secret key. Secret key can be the same secret key used in the encryption process (identical) or can also use different secret keys. Cryptographic concept has actually been used, although it is still very simple. There are some underlying cryptographic principles, namely:

• Confidentiality (confidentiality) is a service that sent the message is secret and unknown to the other party (unless the sender, the recipient or the parties have permission). Normally this is done by creating a mathematical algorithm that is able to transform the data to be difficult to read and understand.
• Data integrity (the integrity of the data) that the service is able to recognize or detect any manipulation (deletion, addition, or alteration) unauthorized data (performed by others).

• Authentication (authenticate) the services related to identification. Neither authenticate the parties involved in the delivery of data and authentication of the authenticity of data or information.

• Non-repudiation (anti-denial) is a service that can prevent a party to deny the actions taken previously (denying that the message originated from him).

Assuming the key K, the encryption process E, the decryption process D, P plaintext, ciphertext C, the encryption and decryption functions can be written as shown in Equation 1 [2].

$$EK (P) = C \text{ and } DK (C) = P \qquad (1)$$

and both of these functions satisfy Equation 2 [2].

$$DK (EK (P)) = P \qquad (2)$$

Cryptographic system (cryptosystem) is a 5-tuple (P, C, K, E, D) which meets the following conditions: [4]

• P is the set of plaintext,

• C is the set of ciphertext,

• K or keyspace, is the set of keys,

• E is the set of encryption function ek: P → C,

• D is the set of decryption function dk: C → P,

• For each k Є K there is ε_k Є ***E*** and d_k Є ***D***. P is a function such that dk (εk (x)) = x, for every plaintext x Є P.

A cryptographic system consists of an algorithm, all possible plaintext, ciphertext and keys. Cryptographic system is a

facility of converting plaintext into ciphertext, and vice versa. Cryptographic algorithms can be divided into two based on the key, namely:

• Symmetric Algorithms

Where the key is used for encryption and decryption keys are the same. They are often referred to as secret key algorithms, singular key algorithm or algorithms of the keys. This algorithm requires the sender and receiver agree on a certain key before they are communicating. Safety depends on the symmetric key algorithm, so that communication remains secure, the key must remain secret.

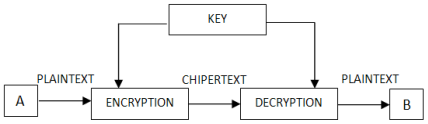

Fig 2: The process of Symmetric Algorithm [2]

Key properties such as these make the sender should always ensure that the path used in the distribution key is the safe or ensure that the person appointed to bring the key to the exchange is one who can really be trusted. The problem will be complicated if the communication is done jointly by the user n and any two parties to exchange a key, there will be as many as (n-1) / 2 secret keys must be exchanged securely. The advantages of symmetric cryptographic algorithms are the time for encryption and decryption process which is relatively fast. This is due to the efficiencies that occur at power key. Because the process is relatively fast, the algorithm is appropriate for use in digital communication systems such as GSM in real time.

• Asymmetric Algorithm

This algorithm is an algorithm where the encryption key used is not the same as the decryption key. This algorithm uses two keys, ie public key and private key. The public key is public, generally distributed while the private key is kept secret by the user. Although public key is known but it will be very difficult to know the private key is used. In general, the public key will be used as the encryption key while the private key is used as a decryption key.

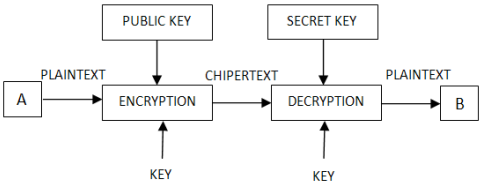

Fig 3: Process Asymmetric Algorithm [2]

The advantages of asymmetric algorithms are to provide security to anyone who exchanges information between them even though there are no agreement on the security message each other beforehand and did not know each other. Besides the problem of key management is also better because of the number of keywords used is much less.

While the weakness of this asymmetric algorithm is for the same security level, the key used is longer than symmetric algorithms. Of speed is also lower than symmetric algorithms.

4. ADVANCED ENCRYPTION STANDARD (AES)

The algorithm is the most widely used in the world Encryption Data Standard (DES) adopted from NIST (National Institute of Standards and Technology). DES includes the type of block cipher, because the algorithm processes the bit plaintext blocks consisting of 64 bits per block using 56-bit keys for encryption and one-time process that produces ciphertext consists of 64 bits per block [2].

In 1997 the National Institute of Standards and Technology (NIST) held a program to define algorithms for data encryption standard known as Advanced Encryption Standard (AES) as a replacement for the Data Encryption Standard (DES) algorithm previously used as a standard for data encryption. This is done because the key used on the DES algorithm is too short (56-bit) and so it cannot guarantee a high level of data security needed today. Triple-DES emerged as an alternative solution to the problems that require a high level of data security such as banks, but it is too slow in some uses.
NITS duty to assess the algorithms that have been entered as a candidate for the AES with the key criteria used should be long, the block size used to be bigger, faster, and flexible. In 1999 elected as five algorithms for AES final candidates are MARS, RC6, Rijndael, Serpent, and Twofish. In 2000, precisely in October Rijndael algorithm was selected as a standard algorithm for encryption. Rijndael algorithm is then known as the Advanced Encryption Standard (AES). After experiencing some of the standardization process by NITS, then adopted a standard Rijndael algorithm officially on May 22, 2002 [2].

AES is a block cipher algorithm that utilizes permutation and substitution system (P-box and S-box), this is different from that used in the Feistel network block cipher algorithms in general. AES is divided into three [2], namely:
• AES-128

• AES-192

• AES-256

4.1. Encryption Process

AES encryption operation begins with changes in the input data (plaintext) and data (key) to form a data matrix of size 4x4. Later in the series of transformation functions of encryption, such as the scheme shown in Figure 4. In the AES encryption process performed following four transformations nine times, namely SubBytes, ShiftRows, MixColumns, and AddRoundKey. In the tenth round of the process which have done three transformations, namely SubBytes, ShiftRows, and AddRoundKey.

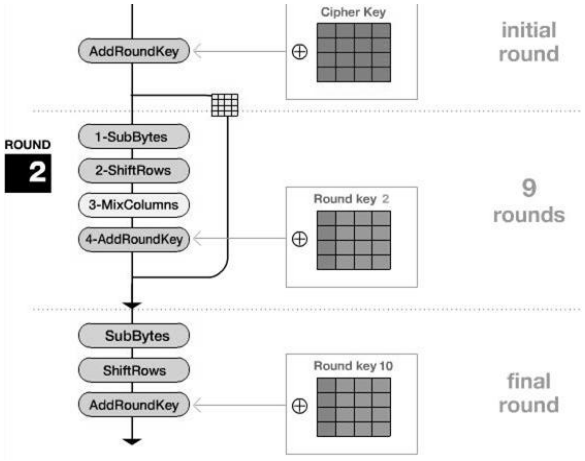

Fig 4: AES Encryption Process [5]

Operation transformation in the AES is technically described as follows:

a. Tansformation SubBytes

SubBytes transformation is a transformation that substituting one state with a single cell in the corresponding cells in the S-Box. The elements of the S-Box itself has been defined previously and are permanent. Figure 5 shows the transformation of SubBytes. SubBytes examples can be seen that happen, for example, will be the replacement of the element 19 on the state, then the corresponding element in the S-Box located on the row and column of the ninth. The process is performed on each element in the state. Examples of calculations performed by the SubBytes with input A and a key character after the first character is a decimal value AddRoundKey converted into hexadecimal, then matched with sbox, results from sbox converted into decimal form. To sbox can be seen in Figure 6, while the results of the sbox who have converted to decimal can be seen in Figure 7.

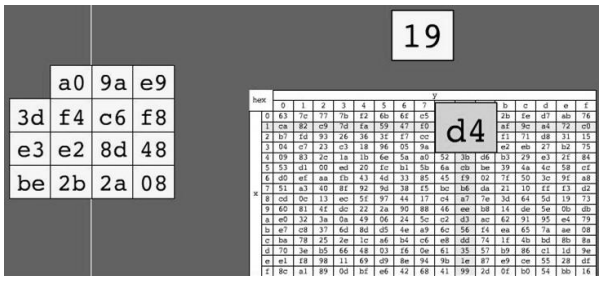

Figure 5 Transformation SubBytes [5]

hex	y															
x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Fig 6: sbox

$$\text{SubBytes} = \begin{bmatrix} 81 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Fig 7: The results of the Amended sbox to Decimal

b. Transformation ShiftRows

In ShiftRows transformation, byte on the last line is a line of one, two and three of the state, is shifted in a circle with a number of different shifts. The operation can be seen in Figure 8.

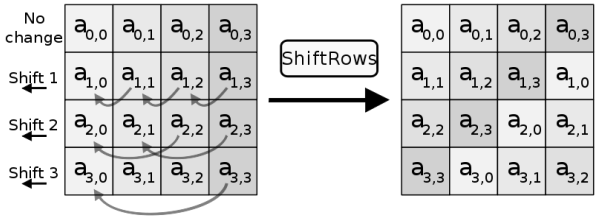

Fig 8: Transformation ShiftRows [5]

Transformation ShiftRows in Figure 8 is done by shifting the matrix element byte. The shift occurred in the series A03, a13, a23 and A33. This shift is done per line to be shifted one step forward, except for a row of index 0 is the shift amount is 0, so it does not shift. For example ShiftRows calculations with input characters A and one key character does not change, because the first row is not shifted. The results of the calculations ShiftRows can be seen in Figure 9.

$$\text{ShiftRows} = \begin{bmatrix} 81 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Fig 9: Example of Calculation ShiftRows

c. MixColumns Transformation

MixColumns transformation operates on the state column by column. The MixColumns scheme is shown in Figure 10

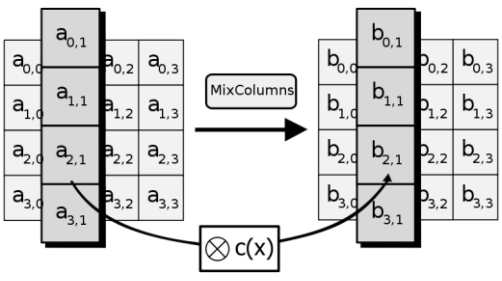

Fig 10: MixColumns Transformation [5]

MixColumns transformation can be determined based on the column. In the transformation matrix, it multiplies one column by matrix c (x), which is shown in Figure 11.

Based on Figure 10 and Figure 11 MixColumns transformation that occurs as a column a01, a11, a21, and A31. Column multiplied by the matrix in Figure 11 and produces column b01, b11, b21 and b3, 1. Calculation of MixColumns the decimal value is converted into a binary, then do check if it is 8 bits of the binary number. Then it makes a shift to the left (ShiftLeft) three times, then the results of each shift at the XOR. The last XOR result is converted to decimal. The result of the XOR then converted to decimal shown in Figure 12.

02	01	01	03
03	02	01	01
01	03	02	01
01	01	02	03

Fig 11: The matrix c (x) transformation MixColumns [5]

$$MixColumns = \begin{bmatrix} 205 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Fig 12: The MixColumns Transformation

d. Transformation AddRoundKey

In AddRoundKey transformation, round round key is added to the state with the XOR operation. Each key consists of a number of Nb word. AddRoundKey operation is shown in Figure 13. Suppose a2, 2 is a given operating point AddRoundKey with key k2, 2, then the output is b2, 2.

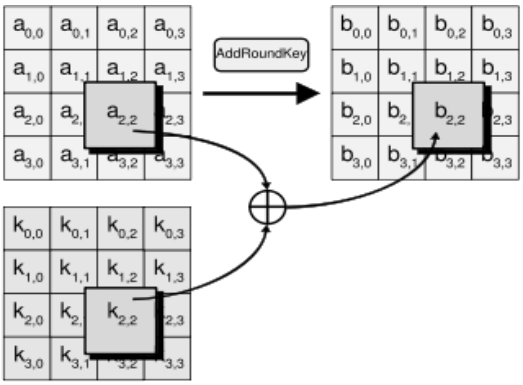

Fig 13: Transformation AddRoundKey [5]

For an example of the calculations used in the form of character input A and use the key character 1 then input and key inserted into the matrix four times. Matrix of key inputs and results can be seen in Figure 14. Then the input in the form of character A and a character key first converted into a binary number. Further binary XOR mentioned it. The result of the XOR is the change to decimal. XOR the results can be seen in Figure 15.

$$Input = \begin{bmatrix} A & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad Kunci = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Figure 14 Matrix Input and Key Results

$$AddRoundKey = \begin{bmatrix} 112 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Figure 15 Results and Key Input XOR

4.2. Decryption Process

AES decryption process has a set of processes that use the matrix inversion function (inverse) of the matrix transformation results in the encryption process. Figure 16 is a pseudocode AES decryption process[8].

Based on Figure 16, it can be seen on the operating pseudocode AES decryption performed the following four transformations nine times, ie InvShiftRows, InvSubBytes, AddRoundKey, and InvMixColumns. In the tenth round of the process, it does three transformations, namely InvShiftRows, InvSubBytes, and AddRoundKey.

```
InvCipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
begin
byte state[4,Nb]
state = in
AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1]) // See Sec. 5.1.4
for round = Nr-1 step Nr-1 downto 1
InvShiftRows(state)
InvSubBytes(state)
AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])
InvMixColumns(state)
end for
InvShiftRows(state)
InvSubBytes(state)
AddRoundKey(state, w[0, Nb-1])
out = state
end
```

Fig 16: AES Decryption Process Pseudocode

5. ONE TIME PAD (OTP)

Cryptography One Time Pad (OTP) was created in 1917 by Gilbert Vernam. Vernam's OTP or password is a password that combines the key message. OTP algorithm is a symmetric key algorithm type, which means that the key used to encrypt and descriptions are the same. In the encryption process, these algorithms use the stream cipher in which the cipher derived from the exlusive-or between the bits of plaintext and key bits [7].

5.1 Formation Process Key

OTP method is an improvement of cryptographic Caesar. One Time Pad using a key whose length is equal to its plaintext. One way to decrypt the encrypted message is to know the keywords used. Encryption is done by the One Time Pad encryption is actually the same as Caesar, but because the key length equal to the plaintext, then each letter in the plaintext will have different shifts.

5.2 System Work One Time Pad

System One Time Pad encryption work is actually very simple, because it only uses the logic of exlusive-or the simple and not too complicated to understand. Although not as complex cryptographic algorithms are others, but for the security level of cryptographic One Time Pad can match it [5].

Here is an example of a simple concept built by the One Time Pad: [6]

For the encryption process is C = P XOR K While the description is P = C XOR K The explanation is C = chippertext, P = plaintext, and K = the secret key used.

Working system of this method also requires knowledge in the fields of mathematical logic, in particular the Meng-XOR operand with each other operand. Meaning of Exclusive OR (Exlusive disjunction) is that if both inputs are the same then the output value is F (false), but when the two different inputs will generate value T (true)[9].

Besides XOR logic is also necessary to understand the conversion of ASCII to binary. This is because, every character entered will see its ASCII form is then converted to binary, it also applies to the key used. Then after getting a binary value, new data will be the XOR. Table 1 is a simple example of the use of binary and XOR the characters.

Table 1 Example of Using Binary and XOR on Character.

	Letters	Binary
Input	A	100 0001
Key	L	110 1100
Results (XOR)		010 1101

XOR the results of Table 1 is 010 1101 which when converted to the form of the character will be a symbol minus (-). Results of this value are not necessarily always be a symbol less, as this can be of varying XOR results obtained. It can be used per character says, One Time Pad can also be used on a word or phrase.

Table 2 XOR operation

A	B	A ⊕ B
0	0	0
0	1	1
1	0	1
1	1	0

From Table 2 it can be seen the properties for the XOR operation,

• A A = 0

• A 0 = A

• A 1 = A ', where A' is the complement of A

XOR operator is often used as one component in the formation of more complex ciphers. However, repeated use of a key that is constantly causing a cipher can be easily solved using frequency analysis (as discussed in the letter that appears most frequently in a language). The virtue of this technique is easy to implement and not XOR operation is computationally expensive. Therefore, XOR cipher is often used to hide information in the case and then fitted with an additional safety mechanism. However, if the key is made along the message (the message), non-recurring and bit-bitnya random, it will present the effect of one-time-pad (also known as the Vernam cipher) which cannot be solved, even though in theory.

6. METHOD

The design of the system is an overview of the design and manufacture of sketches, so it can be a unity. At this stage, the tools used are flowchart diagrams.

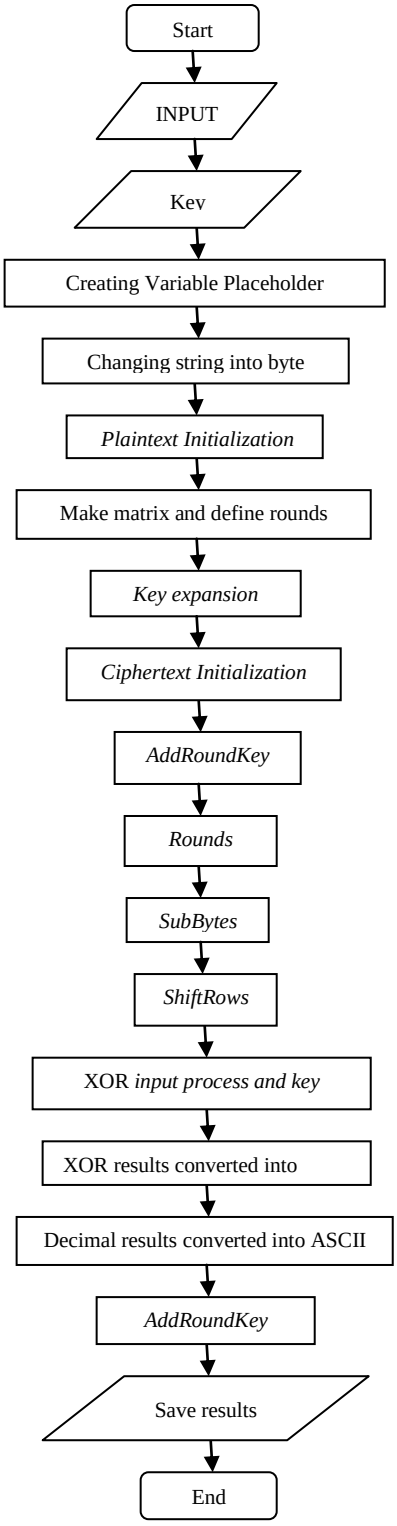

Fig 17: File Decryption Process Flowchart

The design is made to a data security system security system that was developed to run in accordance with established procedures. This section describes the process of file encryption and decryption process files.

The system runs when the system starts the application, the user then provide input along with the key, the system creates a variable based on bits of plaintext, ciphertext, and the key is stored in an array with a capacity of 16 bytes. Once the process is completed, the string of the key and the plaintext is converted into bytes, then the system initializes plaintext which then produces a matrix Nb, Nk, and Nr where Nb is the number bits, Nk is the number keys, and Nr is the round number. After the resulting matrix then the system determines many rounds of Nb, Nk, and Nr. The next step taken by the system is the key expansion and cipher initialization as variable placeholders. Then began the initial velocity AddRoundKey then performed Rounds. Rounds are repeated nine times.

The next step taken by the system is the key expansion and cipher initialization as variable placeholders. Then it begins AddRoundKey as early turnover. After that the results of the encryption key is converted into a binary string. Then the system performs the shifting matrix InvShiftRows state in play. Further InvSubBytes to substitute one cell in one cell state corresponding to the S-Box (matrix state), then do InvRounds. InvRounds own repeated nine times, in InvRounds performed four transformations, namely, AddRoundKey, InvMixColoumns, InvShiftRows, and InvSubBytes. The last is AddRoundKey as the final round and the file decryption has been completed. Figure 17 describes how the structure of the data on the decryption system which data security system designed

7. TESTING

The results of user testing conducted on the application shown in Table 3. Based on the test results in Table 3, the AES cryptographic applications and the user OTP is valid because there is no error in the application of cryptography AES and OTP.

Table 3 User Testing Table

Activity	*Valid Testing*	*Invalid Testing*
Selecting *file input*	✓	-
Select where to save the output files	✓	-
Provide keywords	✓	-
Encrypt *file*	✓	-
Decrypt *file*	✓	-
Viewing the Help menu	✓	-

In this analysis some tests based on file size and file type for a process, the file size before and after the encryption, and the key length of the processing time. This is done to determine whether the size and type influence the processing time, the file size before and after encryption if there is a change, and if you use a key length of whether it will take longer than using a shorter key.

Table 4 Key Length Testing Results

Key (Character)	Size (KB)	Encryption Time (ms)	Decryption Time (ms)
1	99	84	13
2	99	82	12
3	99	120	13
4	99	69	16
5	99	837	12
6	99	81	31
7	99	85	13
8	99	83	13

The longest key that will be used a maximum of eight characters in length, because the system is limited to a maximum length of eight characters. As for the key to be used the shortest one character, because the system is also limited by the minimum one character. Tests based on the key length can be seen in Table 4. Based on the testing that has been done, the key length does not affect the processing time, processing time is affected by the performance of the computer used. In the analysis used Word Document, test using a computer with a core 2 duo processor and memory of the GB (Gigabyte).

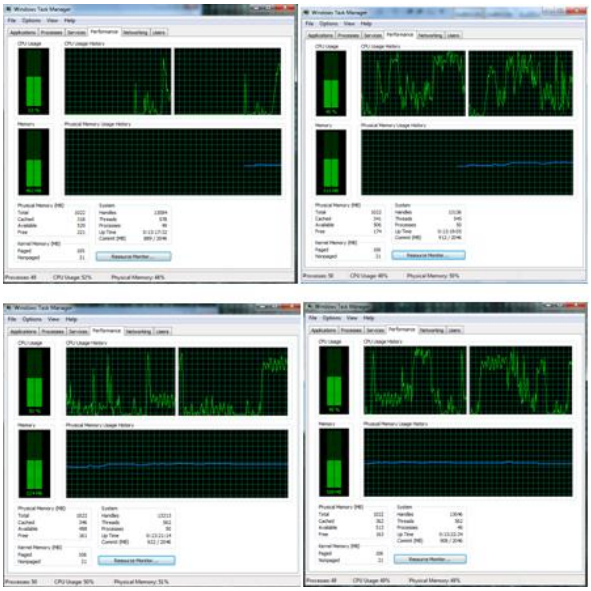

Fig 20: Process Performance Computers

Test results based on file size and file type of the processing time and the file size before and after encryption in Word Document file types shown in Table 5. Based on the testing time has been made to the size of the file it is known that the decryption time tends to be faster than the time of encryption. Based on computer performance are shown in Figure 20, shows that the process at the time of encryption and decryption are performed by the CPU is not stable. Speed encryption and decryption process is not only dependent on the size of the file, but also influenced by the performance of the computer used. Besides the file size is equal to the size of the source file, which means that AES cryptographic algorithm and OTP does not change the size of the file. Figure 21 shows the graph of the speed of processing time to the size of the file.

Table 5 Test Results on Time File Type Word Document

No.	Initial Size (KB)	Encryption Time (ms)	End Size (KB)	Decryption Time (ms)
1	14.918	2211	14.918	467
2	6.449	2119	6.449	314
3	5.101	1054	5.101	1022
4	4.451	1798	4.451	664
5	4.242	2084	4.242	211
6	2.938	124	2.938	2648
7	2.314	245	2.314	24
8	2.025	1694	2.025	699
9	1.947	183	1.947	217
10	1.095	956	1.095	730
11	781	124	781	848
12	701	5571	701	50
13	630	80	630	12
14	612	98	612	18
15	298	95	298	14
16	260	79	260	11
17	252	217	252	66
18	190	135	190	12
19	154	476	154	14
20	103	100	103	12
21	99	75	99	17
22	68	79	68	9
23	59	48	59	19
24	52	149	52	15
25	50	72	50	19
26	49	99	49	66
27	46	59	46	21
28	42	116	42	10
29	33	64	33	16
30	28	64	28	11

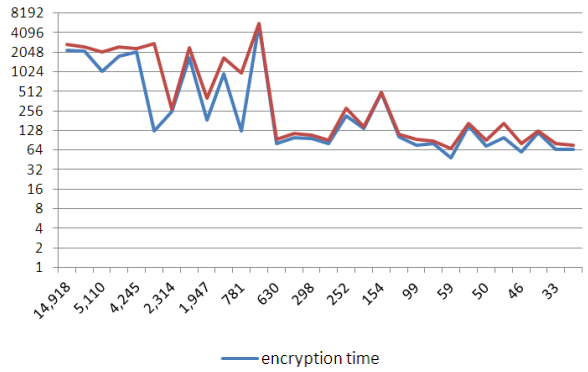

Fig 21: Graph Testing Against Time Encryption and Decryption File Size

8. CONCLUSION

Based on the research and testing that has been done on the system and OTP AES cryptographic applications, then some conclusions can be drawn as follows:

1. Cryptography algorithm Advanced Encryption Standard (AES) can be merged or combined with cryptographic algorithms One Time Pad (OTP).

2. By inserting algorithm One Time Pad (OTP) to the algorithm Advanced Encryption Standard (AES), the resulting application and OTP AES cryptography.

3. Key length does not affect the processing time.

4. File size after encryption is the same size as the original file.

5. Computer performance affects length of processing time.

9. REFERENCES

[1] Garfinkel, Simson, 1995, *PGP: Pretty Good Privacy*, O'Reilly & Associates, Inc.

[2] Munir, R., 2006, Kriptografi, Penerbit Informatika, Bandung.

[3] Schneier, Bruce, 1996, Applied Cryptography, John Wiley & Sons.

[4] Stinson, Dough, 1995, Criptography, CRC Press, Inc.

[5] Munir, R., 2004, *Chipher* yang tidak dapat dipecahkan,http://www.informatika.org/~rinaldi/Kriptografi/Unbreakable%20chiper.pdf (Diakses tanggal 19 Maret 2011).

[6] Saragih, F.R., 2008, Penggunaan Kriptografi *One Time Pad* (Algoritma Vernam) dalam Pengamanan Informasi.

[7] Astutik, Duwi., 2007, Algoritma Enkripsi *One Time Pad* untuk Sistem Pengamanan *Access Database Server* Menggunakan Bahasa Pemrograman *Visual Basic*,http://diglib.unnes.ac.id/gsdl/collect/skripsi/index/assoc/HASH04a4/d9c8b5eb.dir/doc.pdf (Diakses tanggal 2 Mei 2011).

[8] Kurniawan, Y., 2004, Kriptografi, Keamanan Internet dan Jaringan Komunikasi, Penerbit Informatika, Bandung

[9] Manongga, Danny., 2007, Matematika Diskrit, Salatiga : Fakultas Teknologi Informasi Universitas Kristen Satya Wacana.

[10] Bhattacharya, Palaka & Karyar, Morteza., 2004, *Translucent Databases: A Precursor to Privacy Sensitive Databases, CSCI E170- Security, Privacy, and Usability, Fall*.pdf. (Diakses tanggal 12 Mei 2011).

[11] McLeod, Raymond, Jr. dan George Schell, 2001, *Management Information System*, Pretince Hall: New Jersey.

[12] Munir, R., 2005, Matematika Diskrit, Penerbit Informatika, Bandung.

[13] Primanio., 2007, Pemanfaatan Kembali Kriptografi Klasik dengan melakukan Modifikasi Metode-Metode Kriptografi yang Ada.

[14] Wayner, Peter., 2002, *Translucent Database*, Baltimore MD.