CRYPTOGRAPHY APPLICATIONS FOR SECURITY DATA TO USE OF KEY EXCHANGE DIFFIE-HELLMAN AND THE ALGORITHMS RIJNDAEL

Ridwan[1,] Ir. Taryana Suryana, M.Kom[2]

Indonesian Computer university
Jl. Dipatiukur No. 112-116, Coblong, Lebakgede, Bandung, Bandung City, West java 40132
E-mail : Ridwan.10109502@yahoo.com[1], taryanarx@gmail.com[2]

ABSTRACT

Cryptography is a science that deals with a transformation of the data to the data more difficult to understand in by means of mengenkripsi , to prevent it from the alteration of without permission , or prevent it from the use of no chill . Cryptography also can be defined as the process of turning back the data encrypted into a form easily understood .Cryptography so that also can be defined as a process to protect the data .

Cryptography applications for security data by using the method exchange key diffie-hellman and algorithms rijndael (a case study in national civil service agency regional iii) is to secure a file when will make deliveries , first the sender same recipients make the exchange a lock or generate the key to a file will be on encryption that is by using algorithms exchange key diffie -hellman , after getting the key file will be by the use of encryption algorithms rinjndael to the encryption and dekripsi file , the sender will

Keywords:Cryptography, Diffie-hellman , Algorithms rijndael, Client server

INTRODUCTION

The state human resources agency (bkn) regional iii located in jln .Surapati no.10 bandung 40124 government institutions are formed to undertake the task of government in management state human resources in accordance with the provisions laws and regulations .Bkn have some part of them the finance division , of employment , the field of mutation , the field of information , and technical field human resources . So with a number of a document that must be process at bkn regional iii need to security document must be managed well that there should be no abuse data by a third party .On the other hand exchange documents as computer-based it develops to one of the media most commonly used , so By the documents sent via computer network . At current time in bkn regional iii has had problems security documents , documents free accessed by various parties and no security in the document documents among others financial document , human resources , mutation , and removal of and the can read and change because there has been no an application for encrypt file , therefore necessary a security good that document that is on a computer is safer .Of all of the data that must be processed need to security the data must be managed well that there should be no abuse as nip employees to fake , human resources documents that occurredin use , and some bkn must be made system to secure documents when send the document to recipients not to can be opened documents . So to secure documents that is important and address things above need a way to secure a data or information by using a technique cryptography.

2.1 Data security

Security menrupakan one of the most important in a system information , maslh security lot less in see , information determine almost every element of every human life .Information is very important for life it without information so almost all cannot be done well .For example if we bought tike chariots and paid by credit card usage , information about ourselves will be saved and in gather and used by the bank and flight .Only less of the stuff that bias done in the modern world without involving collection , exchange , of making or pengaksesan information .Now informasisudah be commodities very important .Even it is said that we have been / based on an information society .

The ability to access and provide information quickly and accurately be very esiensial for an organization , both commercial organization company , college , government agencies , social and organization .

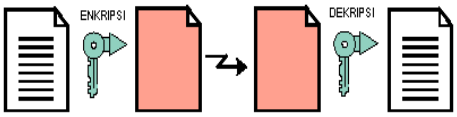
2.1.1 Cryptography

In etymology said cryptography (cryptography) comes from the greek, namely kryptos which means that is graphein which means writing (prayudi,) 2005.The beginning cryptography understood as the science of hide the message (council, 2012), but over time progress

until now understanding cryptography develop into the science Mathematical about the techniques used to complete a security issues in the form of privacy and authentication (diffie , 1976) .The history of writing oldest secret can be found about a society ancient egypt , namely 3000 bc .The egyptians using secret engraving which is called by hieroglyphics to convey a message to those who are entitled to.

Said cryptography derived of alliance of two words in greek namely kriptos and graphia.Said kriptos used to described something hidden, secret or mysterious.As a graphia means writing.Cryptography is defined as science and a lesson in hieroglyph with a consideration that communication and data can be coded to prevent it from spies or one else wants to knowing the contents, by using codes and certain rules and other method so that only a person who is entitled that can be know the message actually.In another sense, cryptography is the arts and sciences in securing message.

In world of cryptography, a message called plaintext or cleartext.the process of disguise of messages with such as manner as well as to hide the original called encryption.a message has encrypted called ciphertext.the process return a ciphertext to plaintext called decryption.



Picture 1.1 The concept of the basis of encryption and decryption

2.2.1 DIFFIE HELMAN

Diffie-hellman key exchange is the method where subject exchange secret keys through a medium that unsafe without expose key .This method shown by dr .W .Diffie and dr .M .E .Hellman in 1976 in papernya new directions in cryptography .This method permits two users to exchange secret keys through a medium that unsafe without a key additional .This method having two parameter system , p and g.

Both of the parameters of the public and can be used by all users of the system .The parameters of p is a prime number , and paramater g (often called generator) is an integer that is smaller than its p having the property of the following: for every n numbers between 1 and inclusive p-1 , there is square grid k g so that at last = n mod p the use of algorithms diffie-hellman in exchange the key which can be done safely and effectively in processing compared to algorithms rsa who tend to be more old in processing the algorithm .The process of a key exchange it can be carried out more than 2 people were identified as meet 2 principle has been discussed earlier .

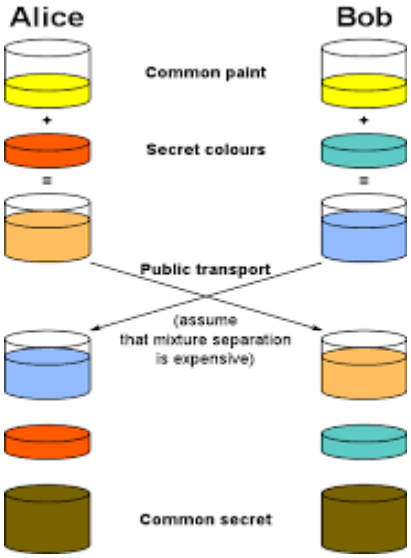
Algorithm diffie-hellman focus in the change of key value and the mathematical process in the determination of key the same end .

2.2.1.1 The Workings Of The Diffie Hellman Key Exchange Protocols

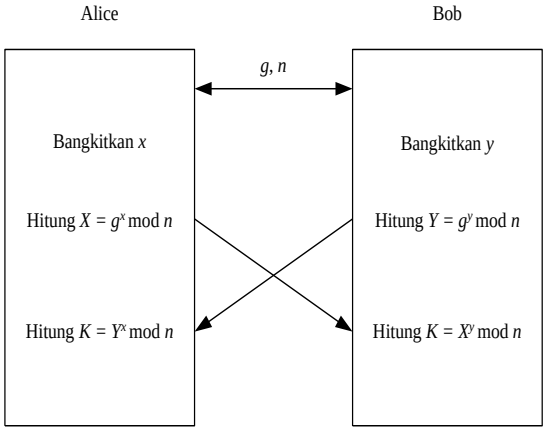
Key protocol agreement diffie-hellman (diffie-hellman key agreement) build a key session without the use of shared key earlier .Messages that swap between alice and bob could be read by anyone who can tap / eavesdrop (eavesdrop) and si tappers would not get the key sessions knowing that finally used by alice and bob .On the other side , diffie-hellman not doing authentication on parties involved .One of the main use of diffie-hellman protocol is in the internet key exchange (ike / exchange key internet) , a central part of ip security architecture (ipsec diffie-hellman) protocol has two parameters , p and g , which both public nature and probably will be used by all users in a particular system P must parameters in the form of a prime number .Rounded mod bilangan-bilangan p (an abbreviation of modulo p) have range from 0 to p-1 , because x mod p are stills from x divided p , and forming what mathematicians call as group under multiplication .Parameter g (usually called a generator) should be in the form of a primitive roots (primitive root) of p: for every n numbers from 1 to p -1 there must be so value k g n = ^ k mod p. as example if p is a prime number 5 (on a system that actually will be used a figure much greater) , then we will choose 2 as a generator because:

1 = 2^0 mod p
2 = 2^1 mod p
3 = 2^3 mod p
4 = 2^2 mod p

Suppose alice and bob want to agreed in a key unsymmetrical divided.Alice and bob and other people have know value p and g. alice meng-generate a value private random a and bob meng-generate a random value private b. both a and b taken from scratch integer { 1,….. , p-1 }.Alice and bob sent down pair of values public they, value will they send each other without encrypted, as follows.Public value from alice is: g ^ a mod p and value public bob adalahg ^ b mod p then they sell value pubik they.Finally, alice counting g ^ ab mod p = (g ^ b mod p) ^ a mod p and bob counting g ^ ba mod p = (g ^ a mod p) ^ b mod p alice and bob now have joint in a pipe. mod p = g ^ ba mod p as the key symmetrical those who are dealt one same lain.sebuah variant of diffie-hellman sometimes called diffie-hellman that already repaired (fixed) allowing it authentication of one or both parties.



picture 1.2 exchange kunci Diffie- Hellman



Picture 1.3 Process Diffie-Helman

example 1 :

Alice and Bob agreed $n = 97$ and $g = 5$ ($g < n$)

1. Alice Select $x = 36$ and calculate $X = g^x \bmod n = 5^{36} \bmod 97 = 50$
   Alice send X kepada Bob.
2. Bob memilih y = 58 and v
   $Y = g^y \bmod n = 5^{58} \bmod 97 = 44$
   Bob send Y kepada Alice.
3. Alice calculate key simetri K,
   $K = Y^x \bmod n = 44^{36} \bmod 97 = 75$
4. Bob calculate key simetri K,
   $K = X^y \bmod n = 50^{58} \bmod 97 = 75$

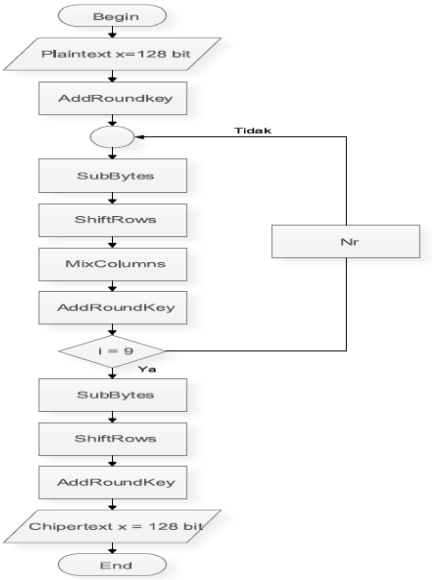
So, alice and bob now have a encryption keys symmetry the same, namely $K = 75$.

2.2.2 Algorithm Rijndael

Rijndael including in type cryptography algorithm which are symmetry and ciphers block .Thus this algorithm have the same lock when encryption and decryption and input and its output of block with the number of bit certain .Rijndael support a variety block size and locks will be used .But rijndael have block size and the key Which remains of 128 , 192 , 256 bit .Election block size data and the keystone would be determining the amount of a process must go through to the process of encryption and decryption .The following are the comparison of a process must go through for each input .Rijndael including in type cryptography algorithm which are symmetry and ciphers block .Thus this algorithm have the same lock when encryption and decryption and input and its output of block with the number of bit certain .Rijndael support a variety block size and locks will be used .But rijndael have block size and locks fixed amount 128 , 192 , 256 bit .Election block size data and the keystone would be determining the amount of a process must go through to the process of encryption and decryption .The following are the comparison of a process must go through for each input .

Blocks input data and the key operated in shape array .Any member of array before produce output ciphertext come to state .Every state will experience process as a broad outline consisting of four stages, namely , addroundkey , subbytes , shiftrows , and mixcolumns .Except stage mixcolumns , third stage others will be repeated at any process besides, phase mixcolumns will not do in the final stages of .The process decryption is kebalikkan of decryption .Since they occur some stage in the process encryption , then required subkeysubkey which will be used in each phase .

Development the number of keys to use needed because the needs of subkeysubkey which will be used can thousands of bit , while key provided by default only 128-256 bit .Jumla total key required as subkey is as many as nb (nr + 1) , where nb been the large block data in a unit word .While nr is the sum stage to go in a unit word .For example , when used 128 bit (4 word) block data and 128 bit (4 word) key it will be done 10 times process (see table 1) .Thus of the formula obtained 4 (10 plus or minus one = 44 word = 1408 bit key .To expand the number of keys to use of the key then done key schedule .



Picture 1.4 Process Algoritm Rijndael

At process file tugas-tugas encryption there are:

1. *Load text file that will encrypted .Format text used is .txt , .doc , and .pdf .While to a measure filenya no its limit , the great size filenya so the more it message that can be encrypted*
2. To the process encryption and decryption rijndael the process key schedule same, took the key ciphers and do routine expansion a lock (key expansion) to form key schedule.Expansion key brought total nb (nr + 1) word.This algorithm need the opening set key consisting of nb word, and every round nr need data key as many as nb word.The results of key schedule consisting of array 4 byte word linear denoted by wi.Subword is a function that takes 4 byte word input and apply s-box to every data 4 byte to produce word output.Function rotword take word a0, a1, a2, a3 as input, do the permutations cyclic, and restore word a1, a2, a3, a0.

01	02	04	08	10	20	40	80	1b	36
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00

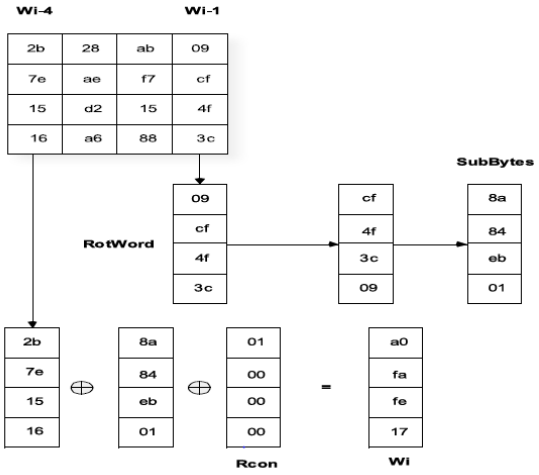
Picture 1.5 *Rcon*

Of pictures 1.5 shows that rcon i consisting of nilai-nilai given by xi-1 , { 00 } , { 00 } , { 00 } , with xi-1 as a rank of of x (x notated as { 02 }

2b	28	ab	09
7e	ae	f7	cf
15	d2	15	4f
16	a6	88	3c

Picture1.6 *Cipher Key*

1.6 of pictures can be seen that a key cryptography used by routine expansion key to produce a set of keys of the round , can be described as a rectangular array of bytes , having four rows and columns nk .6 of pictures can be seen that a key cryptography used by routine expansion key to produce a set of keys of the round , can be described as a rectangular array of bytes , having four rowsand columns nk



Picture 1.7 Process *Key Schedule*

Of pictures 1.7 can be seen that word to nk first expansion of the key contains key ciphers .Every word next , w i , same with xor of the word earlier , w i-1 and nk word that were on a previous position , w i-nk .To word in a position that is a multiple nk , a transformation apply to w i-1 before xor , and continued by xor with konstantaround , rcon i .The transformation of it consists of this shift in cyclic bytes of data in a word rotword , and then follow up application of lookup table for all 4 bytes data from subword word . During calculations plainteks be cipherteks , current status from the data stored in array of byte two dimensions , state , and its size of nrows x ncols .Array elements state referenced as follows:s[r,c] = in[r+4c] to 0 ≤ r < 4 dan 0 ≤ c < Nb

19	a0	9a	e9
3d	f4	c6	f8
e3	e2	8d	48
be	2b	2a	08

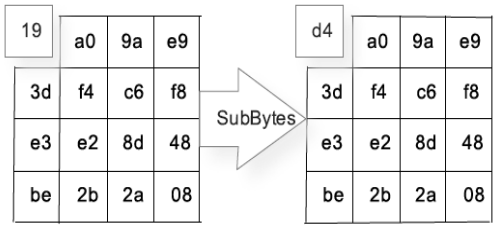
Picture 1.8 Charging *Array State*

Of a picture 1.8 can be seen that (nb is a long block divided 32).In aes, nb = 128 / 32 = 4.Every elements of array state filled with 8 bits text (1 bytes) in notation hex.Following charge array state done, do transformation subbytes where transformation bytes on each element in state will mapped by using a table substitution (s-box).Table substitution s-box will be presented in Tabel 3.2.

hex	y															
	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	3	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

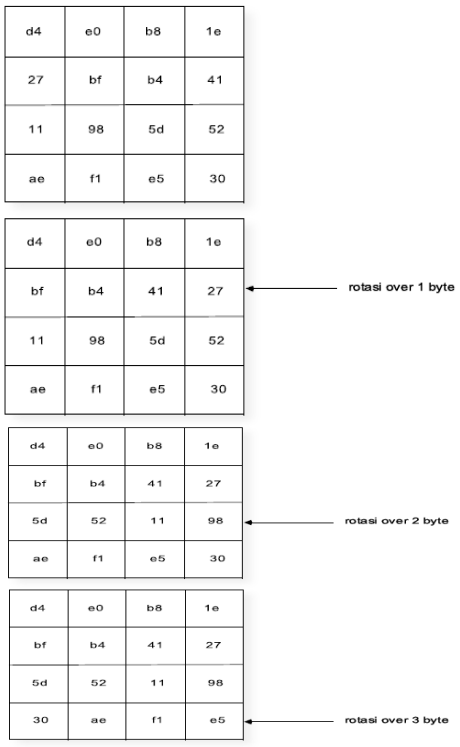
x

Following the results of the array of state who is already in the transformation of subbytes:



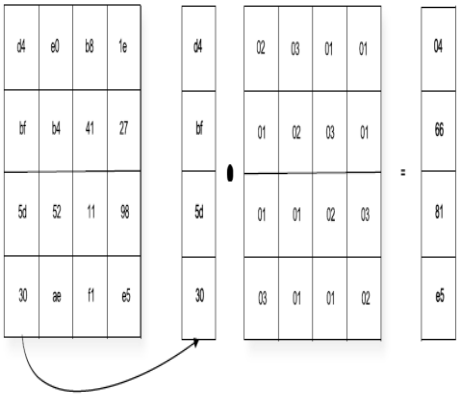
Picture 1.9 Transformasi *SubBytes*

Of a picture 1.9 can be seen that s-box used in subbytes ( ) a transformation presented in the form of hexadecimal in table 3.1 .For example , if = 1,9s { d4 } , this value substitution to be decided by intersection of line with an index ' 1' and columns with an index ' 9' .Do transformation shiftrows that fundamentally the process shift bit where bit most left will be moved into bit most on the right rotation bit .The process shift shiftrows to be demonstrated in a picture 1.10 the following:



Picture 1.10 Transformasi *ShiftRows*

After transforming shiftrows done, do scrambling array state by conducting the multiplication of matrices that is the transformation of multiplication polynomial between every column with polynomial 4 the in gf (28), a (x) mod (x4 + 1).



Picture 1.11 *MixColumns*

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

Picture 1.12 ***Galois Field By a Given Matrix***

04	e0	48	28
66	cb	f8	06
81	19	d3	26
e5	9a	7a	4c

Picture 1.13 final result ***MixColumns***

To the process encryption and decryption rijndael the process addroundkey same, a round key added at state by operation xor.Every round key consisting of nb word where every word is to be totaled word align or column on which against one another of state so :
[S'0,c,S'1,c,S'2,c,S'3,c] = [S0,c,S1,c,S2,c,S3,c] [Wround*Nb+c] For $0 \leq c \leq Nb$
[Wi] Is the key word of that corresponded where:

i = round*Nb+c

Transformation addroundkey at process encryption the first time at the round = 0 to round next round = round +

04	e0	48	28
66	cb	f8	06
81	19	d3	26
e5	9a	7a	4c

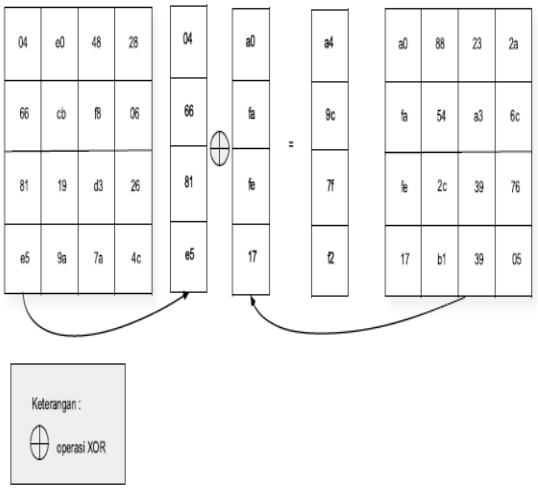
1

Gambar 1.14 ***Array State*** **Sekarang**

a0	88	23	2a
fa	54	a3	6c
fe	2c	39	76
17	b1	39	05

Picture 1.55 ***Round Key***

The following the result of array state and round key out of transformation addroundkey:

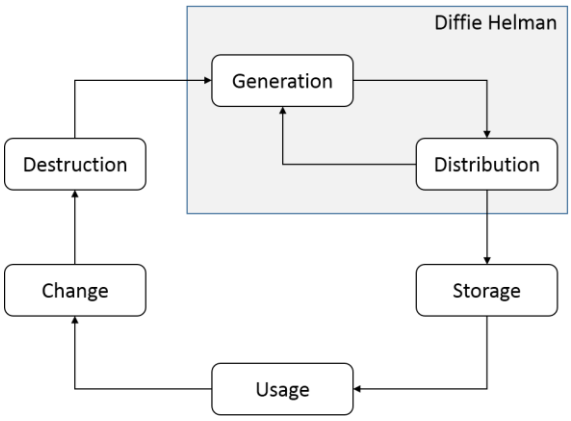


Picture 1.16 Transformation ***AddRoundKey***

a4	68	6b	02
9c	9f	5b	6a
7f	35	ea	50
f2	2b	43	49

Picture 1.17 final result ***AddRoundKey***

After completed to all measures above so save the file as cipherteks (text file that have encrypted)



Picture 3.18 Key management system

There are six the process main where 2 process is the application of algorithm diffie helman namely the process generation and distribution.The rest those are the process storage, usage, change and destruction.

A. Generation

This process is impelementasi of an algorithm diffie helman .Variable raised namely : variable *g* dan *n*, $X = g^x \bmod n$, $Y = g^y \bmod n$, $K = Y^x \bmod n$, $K' = X^y \bmod n$.

B. Distribution

This process is part of the implementation on diffie algorithm helman.Variable in spread namely :variable *X* dan *Y*.

C. Storage

This process is stages by which after private key obtained .Private key and kept in a database servers and secured .

D. Usage

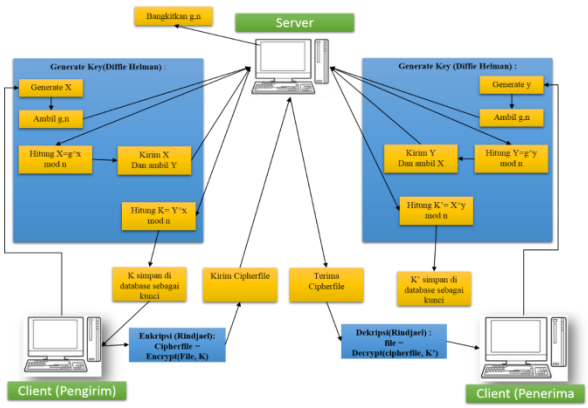
This process is the use of key stage taken from the database for the encryption and decryption process.

E. Change

This process is a process to do replacement key if client feel the need to replace key with perform the process generation back .

F. Destruction

This process to walk when client have replace .Key that is in a database removed .



Picture 1.19 The process of working system

That there are on the imagery of common system divide three main process , namely .Tahapan-stage every the process that is as follows:Proses Generate Key

a. Server excite the number of g and n.
b. Client (the sender) evoking numbers x take numbers as well as g and n of the server .Counting next x = gx mod n. value of x resulting sent to the server
c. Client (the recipient resurrection the number of he and take the number of g and n from the server.Next counting y = gy mod n. value of y produced sent to the server.
d. client (the sender take value of y sent by client recipients , and calculate k = yx mod n and storing k in a database as private key to encrypt .
e. client (the recipient) takes the value x sent by client the sender, and calculate K' = Xy mod n and storing K' in a database as private key to; s been decrypting.client (the recipient) takes the value x sent by client the sender, and calculate K' = Xy mod n and storing K' in a database as private key to; s been decrypting.

1. Process encryption
   a. Client determine the sender address client (receiver) (ip / hostname)
   b. Client (sender encryption) do on file chosen by private key
   c. Client (sender) to send a file server
2. Proses Dekripsi
   a. Client (recipients) choses files on the server .
   b. Client (recipients) take private key .
   c. Client (the recipient) do dekripi on file were chosen in private key.

Based on the results of testing and evaluation have done before , it can be obtained conclusion as follows: after going through stage design , implementation and testing cryptography applications for security data by using the method key is invalid diffie-hellman and algorithms rijndael (a case study in the state human resources agency regional iii) , so a conclusion can be drawn that:

1. This application meet the needs of that is required in bkn (the state human resources agency regional III aimed at to secure the documents that are considered important .

2. On the application this file is will can be opened it is encrypted and the file will not be able to in salahgunakan by irresponsible parties.

literature:

[1] Ramdan, Mangunpraja. 2010. Peningkatan Keamanan Pertukaran Kunci DiffieHellman dengan Pengimbuhan Algoritma RSA, Bandung:STIE.

[2] Kurniawan J., Ir. , M.T., *Kriptografi, Keamanan Internet dan Jaringan Komunikasi*, Informatika ,April 2004.

[3] Sadikin, Rifki. 2012. Kriptografi Untuk Keamanan Jaringan.Yogyakarta: Penerbit Andi Offset.

[4] N. Penchalaiah , "Effective Comparison and evaluation of DES and Rijndael Algorithm (AES)", International Journal on Computer Science and Engineering, Vol. 02, No. 05, 2010, pp.1641-1645.