A-2

Proses Enkripsi dan Dekripsi *Email* menggunakan Algoritma *Advanced Encryption Standard* (AES)

Ricky Antonius Leohani[1], Imaludin Agus[2]

[1]Program Studi Pascasarjana Pendidikan Matematika,Universitas Negeri Yogyakarta
[2] Program Studi Pascasarjana Pendidikan Matematika,Universitas Negeri Yogyakarta
imal.udin@yahoo.co.id

Abstrak-Artikel ini bertujuan untuk mengkaji secara teoritik proses enkripsi dan dekripsi *email* menggunakan algoritma *Advanced Encryption Standard* (AES). *Email* adalah salah satu alat komunikasi berbasis web. Untuk menjaga *privacy* dan keamanan dalam pengiriman informasi, maka diperlukan proses enkripsi. Salah satu metode enkripsi informasi yang dapat digunakan yaitu algoritma AES. AES merupakan algoritma kriptografi yang digunakan untuk mengamanakan data sebagai pengganti algoritma *Data Encryption Standart* (DES) yang dianggap sudah tidak aman. Keamanan algoritma AES ini terletak pada penggunaann kunci kriptografi hingga 128, 192 dan 256 bit. Selain itu algoritma AES menggunakan *blokchipertext* simetrik yang dapat mengenkripsi dan deskripsi informasi. Informasi yang akan dikirim disebut dengan *Plaintext*, kemudian informasi ini dienkripsikan menjadi *chipertext*. Dengan menggunakan *privat key*, penerima informasi dapat mendeskripsikan *chipertext* ke bentuk *Plaintext*.

Kata kunci: Enkripsi, dekripsi, email, algoritma AES

I. PENDAHULUAN

Email memiliki peranan penting dalam proses komunikasi. *Email* dapat digunakan untuk mengirim atau menerima data yang berupa dokumen, pesan *text*, gambar, dan file-file lainnya. Tidak jarang data-data yang dikirimkan adalah data-data privasi yang bersifat penting, *urgent*, dan rahasia. Namun, sistem pengamanan akun *email* hanya mencakup *id* dan *password user*, sedangkan data-data dalam *email* tidak di enkripsi, sehingga berpotensi untuk di sadap oleh pihak yang tidak bertanggung jawab [1]. Melihat berharganya data-data yang dikirim, maka perlu dilakukan proteksi tambahan pada data user yaitu dengan cara mengenkripsi dan mendekripsi data. Proses enkripsi dan deskripsi data tersebut menggunakan kriptografi.

Salah satu jenis algoritma kriptografi yang diyakini memiliki tingkat keamanan yang baik yaitu *Advance Enkription Standart* (AES). AES adalah standar terkini yang digunakan untuk mengenkripsikan kunci rahasia. AES pertama kali dikembangkan oleh vincen rijmen dan joan daemon sebagai pengganti Data Enkripstion Standar (DES) yang dianggap sudah tidak aman lagi. AES memiiliki manfaat dalam proteksi data, sebab dalam penerapannya, proses enkripsi AES mnggunakan panjang kunci 128, 192, dan 256 bit, yang berarti memiliki pengamanan data yang sangat kuat [2].

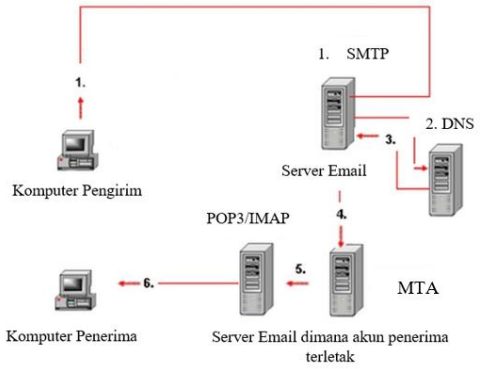
Memperhatikan pentingnya proteksi data-data dalam *email* serta relevansi AES dalam pengamanan data, maka AES dapat diterapkan dalam pengamanan data *email*. Oleh karena itu, dalam artiket ini akan membahas tentang proses enkripsi dan dekripsi pada data-data *email* dengan menggunakan algoritma AES.

II. PEMBAHASAN

A. *Email*

Email adalah singkatan dari elektronik mail, yang pada prinsipnya memiliki sifat yang relatif sama dengan pengiman surat biasa, yang membedakan hanyalah *email* menggunakan internet [3]. Proses pengiriman *email* sangat cepat, dimana pesan dapat dikirim dalam hitungan menit bahkan terkadang detik keseluruh dunia tanpa adanya biaya tambahan [1]. Pendapat lainnya, *email* merupakan aplikasi TCP/IP yang paling banyak digunakan. *Email* adalah pesan yang terdiri dari kumpulan string ASCII dalam format RFC 822 yang dikembangkan tahun 1982 [4].

Adapun cara kerja *email* adalah sebagai berikut:



GAMBAR 1. CARA KERJA *EMAIL*

Proses kerja *email* diawali dengan pengiriman *email* oleh user, kemudian *email* tersebut akan dikirim oleh clien ke mail server melalui SMTP (*Simple Mail Transfer Protocol*). Dimana SMTP ini bisa diibaratkan sebagai kotak pos yang bertugas memeriksa perangko, alamat, dan membantu proses pengiriman. Selanjutnya, SMTP akan meneruskan ke server *Domain Name System* (DNS). DNS akan mengubah domain alamat *email* yang dituju menjadi bentuk alamat *Internet Protocol* (IP) serta mengecek ketersediaan MX atau *Excahange*. Secara sederhana DNS berfungsi untuk memverifikasi kevalidan alamat *email* yang dituju. Setelah alamat berhasil diverifikasi, maka *email* akan diteruskan ke server mail exchange pada domain tersebut. Server ini disebut dengan *Mail Transfer Agent* (MTA). Kemudian Penerima *email* dapat menerima pesan yan dikirim melalui client yang bekerja melalui POP atau IMAP [3].

B. Advance Enkription Standart (AES) pada Pesan Email

AES merupakan algoritma kriptografi yang bisa digunakan untuk memproteksi data. Algoritma ini ditetapkan oleh *National Institute of Standarts and Technology* (NIST) menjadi pengganti DES dalam algoritma enkripsi simteri yang baru [5]. Hal ini disebabkan karena DES hanya menggunakan pengolahan data 64-Bit dan kunci 56-bit yang dianggap sudah tidak memadai lagi untuk pengamanan data. Maka pada tahun 1997 diadakanlah kontes pemilihan standar algoritma baru, hingga pada akhirnya di tahun 2000 algoritma yang dikembangkan oleh Vincent Rijndael dan Joan Daemen ditetapkan sebagai standar algoritma yang baru. Algoitma ini dikenal sebagai AES [6].

AES menggunakan chiper blok simteri yang dapat memproses blok data 128 bit, dengan menggunakan kunci chiper yang panjangnya 128, 192, dan 256 bit [7]. Berdasrakan hal tersebut, perbedaan panjang kunci akan mempengaruhi jumlah putaran yang akan diimplementasikan dalam algoritma AES. Secara ringkas akan ditampilkan pada tabel 1 berikut [8]:

TABEL. 1 PERBANDINGAN JUMLAH PUTARAN DAN KUNCI

	Jumlah Kunci (Nk)	**Ukuran Blok (Nb)**	**Jumlah Putaran (Nr)**
AES-128	**4**	**4**	**10**
AES-192	**6**	**4**	**12**
AES-256	**8**	**4**	**14**

Adapun langkah-langkah enkripsi dan dekripsi AES sebagai berikut [9]:

Enkripsi:

1. *Addroundkey*: Pada tahap ini pesan yang dikirim (*plain text*) akan di XOR kan dengan cipher key. Tahap ini disebut juga dengan *Initial round.*
2. *Round* : Selanjutnya akan dilakukan putran sebanyak Nr-1 kali. Proses yang dilakukan sebagai berikut:
   a) *Subbytes* : pada proses ini hasil dari add*round* key akan dikonversikan menggunakan nilai s-box seperti gambar 2 beriku [5]:

x \ 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	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

GAMBAR. 2 NILAI S-BOX

b) *Shiftrows* : Hasil dari *Subbytes* digeser secara *wrapping*.

c) *Mixcolumns :* Mengacak data dengan melakukan perkalian antara matriks publik keys dengan matriks hasil *Shiftrows*.

Adapun matriks publik keys untuk enkripsi data sebagai berikut [5]:

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \tag{1}$$

d) *Addroundkey* : state yang dihasilkan sebelumnya di XOR kan dengan *Round* key

3. Final Round : untuk putaran ke Nr, dilakukan tahap-tahap yang sama dengan *round* namun tidak melalui proses *Mixcolumns*. Adapun prosesnya sebagai berikut :
   a) *Subbytes*
   b) *Shiftrows*
   c) *Addroundkey*

Dekripsi:

1. *Addroundkey*: Pada tahap ini pesan yang diterima (plain text) akan di XOR kan dengan cipher key. Tahap ini disebut juga dengan *Initial round.*
2. *Round* : Selanjutnya akan dilakukan putaran sebanyak Nr-1 kali. Proses yang dilakukan sebagai berikut:
   a) *InvShiftrows* : Hasil dari *Subbytes* digeser secara *wrapping*.
   b) *InvSubbytes*: pada proses ini hasil dari *addroundkey* akan dikonversikan menggunakan nilai *Inv*erse sbox seperti gambar 3 berikut [5]:

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

GAMBAR 3. NILAI *INVERSE* S-BOX

c) *InvMixcolumns :* Mengacak data dengan melakukan perkalian antara matriks publik keys dengan matriks hasil *Shiftrows*.

Adapun matriks publik keys untuk dekripsi data sebagai berikut [5]:

$$\begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} \tag{2}$$

ISBN. 978-602-73403-1-2

d) *Addroundkey* : state yang dihasilkan sebelumnya di XOR kan dengan *Round* key

3. *Final Round* : untuk putaran ke Nr, dilakukan tahap-tahap yang sama dengan *round* namun tidak melalui proses *Mixcolumns*. Adapun prosesnya sebagai berikut :
   a) *InvShiftrows*
   b) *InvSubbytes*
   c) *Addroundkey*

Contoh simulasi enkripsi dan dekripsi AES:

Plaintext **: Teori_Pengkodean**

Chiperkey **: Djogja_Istimewa0**

1. *Addroundkey*

Masukkan ke kolom 4x4

Plain Text

T	E	o	r
i	_	P	e
n	G	k	o
d	E	a	n

Chiper key

D	j	o	G
j	a	_	I
s	t	i	M
e	w	a	0

Konversi ke hexadesimal

54	65	6F	72
69	5F	50	65
6E	67	6B	6F
64	65	61	6E

44	6A	6F	67
6A	61	5F	49
73	74	69	6D
65	77	61	30

Plain Text XOR *Chiper key*

54	65	6F	72
69	5F	50	65
6E	67	6B	6F
64	65	61	6E

⊕

44	6A	6F	67
6A	61	5F	49
73	74	69	6D
65	77	61	30

=

10	0F	00	15
03	3E	0F	28
1D	13	02	02
01	02	00	0E

2. *Sub-Bytes*

10	0F	00	15
03	3E	0F	28
1D	13	02	02
01	02	00	0E

➔

CA	76	63	59
7B	B2	76	34
A4	7D	77	77
7C	77	63	AB

3. *Shift-Row*

CA	76	63	59
7B	B2	76	34
A4	7D	77	77
7C	77	63	AB

➔

CA	76	63	59
7B	B2	76	34
A4	7D	77	77
7C	77	63	AB

CA	76	63	59
7B	B2	76	34
A4	7D	77	77
7C	77	63	AB

➔

CA	76	63	59
B2	76	34	7B
A4	7D	77	77
7C	77	63	AB

CA	76	63	59
B2	76	34	7B
A4	7D	77	77
7C	77	63	AB

➔

CA	76	63	59
B2	76	34	7B
77	77	A4	7D
7C	77	63	AB

CA	76	63	59
B2	76	34	7B
A4	7D	77	77
7C	77	63	AB

➔

CA	76	63	59
B2	76	34	7B
77	77	A4	7D
7C	77	63	AB

CA	76	63	59
B2	76	34	7B
77	77	A4	7D
AB	7C	77	63

4. *Mix Column*

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

×

CA	
B2	=
77	
AB	

2	x	CA	=	10	*xor*	11001010	$= X \text{ xor } X^7 + X^6 + X^3 + X$ $= X^8 + X^7 + X^4 + X^2 \bmod$ $X^8 + X^4 + X^3 + X + 1$ $= X^7 + X^3 + X^2 + X + 1$ = 10001111	10001111

3	x	B2	=	11	*xor*	10110010	$= (X+1)\text{xor}\ (X^7+X^5+X^4+X)$ $= (X^8+X^7+X^6+X^4+X^2+X \bmod X^8+X^4+X^3+X+1)$ $= X^7+X^6+X^3+X^2+X+1$ = 11001111	11001111
1	x	77	=	1	*xor*	01110111	01110111	01110111
1	x	AB	=	1	*xor*	10101011	10101011	10101011
							Jumlah (XOR)	10010100
							Bentuk Hexa	94

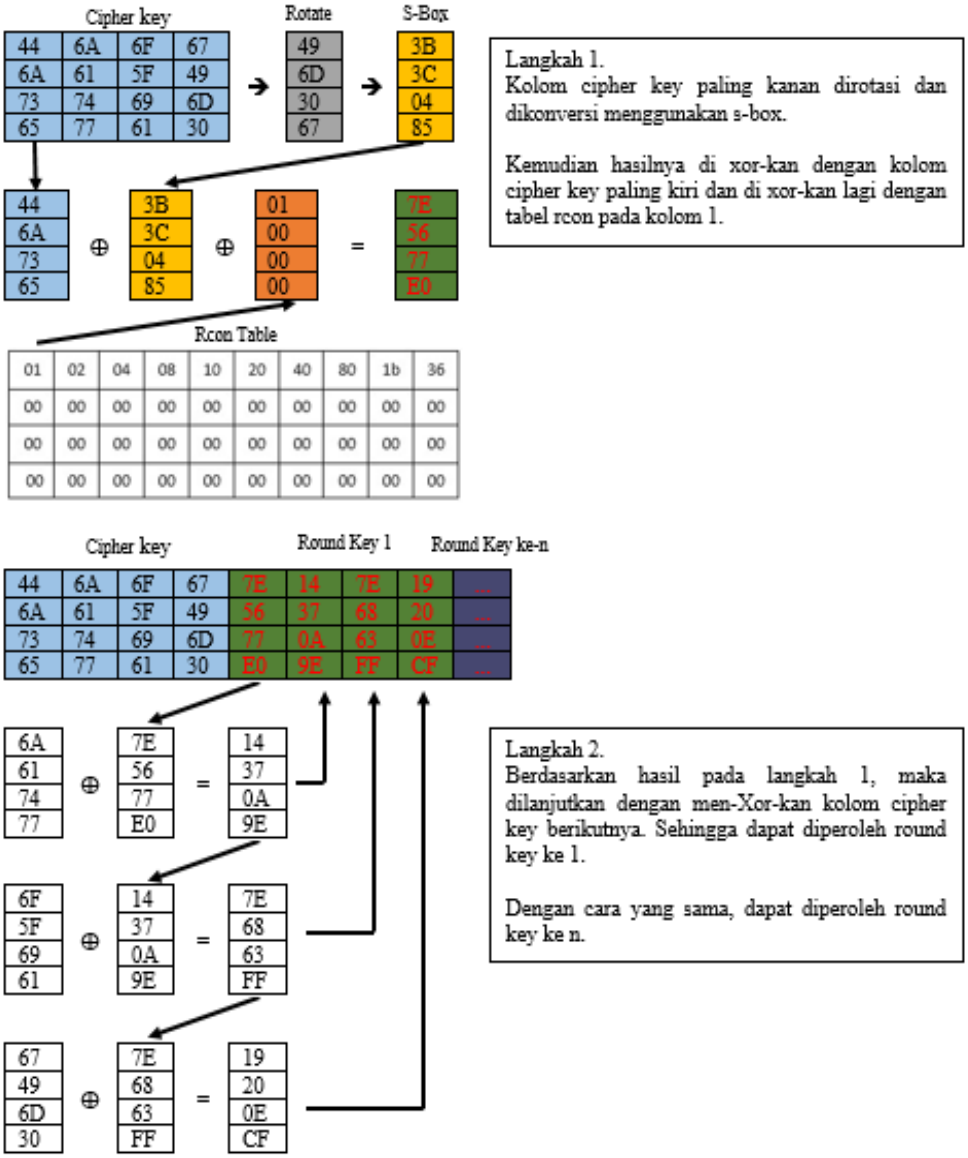
Dengan cara yang sama diperoleh untuk nilai baris dan kolom yang lain. Dimana untuk mixcolumn *round* 0 adalah sebagai berikut:

10010100	01111101	01001001	00100001
10100101	01111111	10001001	01100101
01110001	01101010	10011110	01111110
11001101	01100011	11011011	00101011

Hexa

94	7D	49	21
A5	7F	89	65
71	6A	9E	7E
CD	63	DB	2B

Pada proses selanjutnya dilanjutkan dengan add *round* key, dimana cipher key yang telah ada akan diexpansikan terlebih dahulu, langkah-langkahnya seperti gambar 4 berikut:



GAMBAR 4. LANGKAH-LANGKAH *EXPANTION KEY*

Proses *Round* dilakukan higga putaran ke 9, dengan mengulang cara yang sama seperti *Round* 1. Sedangkan untuk putaran ke 10 dilakukan proses *final round* dimana dilakukan tahap-tahap yang sama dengan *round* namun tidak melalui proses *Mixcolumns*.

Pada proses dekripsi, langkah-langkah yang diakukan hampir sama dengan proses enkripsi. Namun yang membedakan adalah pada dekripsi menggunakan *Inv*erse s-box, dan *Inv*ers matriks mix columns. Selain itu,pada proses *round* dan *final round*nya dimulai dengan melakukan proses *Inv*Shiftrow kemudin dilanjutkan proses Invsubbyte.

III. KESIMPULAN

Berdasarkan kajian teori yang dipaparkan dapat ditarik beberapa kesimpulan yaitu penggunaan algoritma AES melibatkan proses *Addroundkey*, *Subbytes*, *Shiftrows* dan *mixcolumns* pada setiap *round*nya. Untuk panjang kunci 128 bit mengalami *round* sebanyak 10 kali, kemudian untuk panjang kunci 192 bit terdapat 12 *round*, dan panjang kunci 256 bit sebanyak 14 *round*. Hal in menyebabkan algoritma AES sulit untuk dipecahkan.

Oleh karena itu, untuk menjamin keamanan pesan yang dikirim dan diterima pada *email*, maka penggunaan algoritma AES merupakan pilihan yang tepat. Meskipun pesan yang dikirim diketahui oleh orang lain, mereka tetap tidak dapat memahami pesan tersebut, sebab pesan yang tertampil berupa kode hexadecimal yang hanya bisa dibaca oleh orang memegang private key.

UCAPAN TERIMA KASIH

Ucapan terima kasih kepada Ibu Dr. Karyati, S.Si.,M.Si selaku pembimbing dalam pembuatan artikel ini.

DAFTAR PUSTAKA

[1] University of north carolina at chapel hill libraries, “Introduction to *email*: Gmail and Yahoo mail basics”, California, Juli 2013, pp. 3.

[2] J. Daemon & V. Rijmen, “The Rijndael Block Cipher”,Belgium, September 2003,pp 8.

[3] http://winpoin.com/winexplain-bagaimana-cara-kerja-*email*

[4] Y. Taufan, I. Winarno, K. Fatonah, “Enkripsi *email* dengan menggunakan metode elgamal pada perangkat mobile,” unpublished.

[5] R. Pahal & V. Kumar, “Efficience implementation of AES”, IJARCSSE, Haryana, Vol. 3, Juli 2013, pp.290-295

[6] D. Surian, “ Algoritma kriptografi AES Rijndael”,TESLA, Vol. 8 No. 2, Oktober 2006, pp.97-101.

[7] Federal Information Processing Publications, “Announcing the Advanced Encryption Standard (AES)”, New York, November 2001.

[8] M. Rinaldi, “Kriptografi”. Bandung, Penerbit Informatika, 2006.

[9] S. Murdowo, “Mengenal proses perhitungan enkripsi menggunakan algoritma Advance Encription Standard (AES) Rijdnael”, INFOKAM, Semarang, Maret 2014, pp.32-41