KRIPTOGRAFI *SYMMETRIC-KEY CRYPTOSYSTEM* DENGAN METODE AES (*ADVANCED ENCRYPTION STANDARD*) 256bit

Willy Riyadi
Program Studi Sistem Informasi, STIKOM Dinamika Bangsa, Jambi
Jl. Jendral Sudirman Thehok – Jambi
Email : wriyadi5@gmail.com

ABSTRAK

Kriptografi merupakan suatu teknik guna mengamankan suatu data maupun informasi dengan menyembunyikan isi pesan atau dokumen sehingga digunakan untuk mengamankan kerahasiaan dalam komunikasi komputerisasi interpersonal. Kriptografi terdiri dari metode enkripsi yang bertujuan mengubah bentuk dari pesan atau dokumen yang dapat dibaca disebut plaintext menjadi bentuk yang tidak terbaca disebut cyphertext dan metode dekripsi yang bertujuan mengubah bentuk cyphertext menjadi plaintext. Berbagai algoritma kriptografi telah diciptakan oleh para ahli kriptografi, namun hal tersebut juga diiringi dengan banyaknya keberhasilan usaha dilakukan oleh para cracker guna memecahkannya metode kriptografi tersebut. Untuk itu, peneliti membahas salah satu metode kriptografi yang paling umum dipakai dan menjadi standar kriptografi hingga saat ini adalah Symmetric-Key Cryptosystem dengan metode AES (Advanced Encryption Standard) dengan panjang kunci 256bit yang memberikan tingkat keamanan maksimum bagi pengguna metode kriptografi AES.

Kata Kunci : kriptografi, Symmetric-Key Cryptosystem, AES (Advanced Encryption Standard) 256bit

ABSTRACT

Cryptography is a technique in order to safeguard a data and information to conceal the contents of the message or document which used to secure confidentiality in computerized interpersonal communications. Cryptography consists of encryption method that aims to change the form of the message or document that can be read called plaintext into illegible form called cyphertext and decryption method that aims to change cyphertext forms into plaintext. Various cryptographic algorithms have been created by experts cryptography, but it is also accompanied by a number of successful business conducted by the cracker in order to solve the cryptographic methods. To that end, researchers discuss one of the most common cryptographic methods used and become standard cryptography today is Symmetric-Key Cryptosystem by using AES (Advanced Encryption Standard) with 256bit key length that provides the maximum level of security for AES Cryptography users.

Keywords: cryptography, Symmetric-Key Cryptosystem, AES (Advanced Encryption Standard)

1. PENDAHULUAN

Kebutuhan akan kerahasiaan data maupun informasi yang dikirimkan melalui berbagai media komunikasi seperti jaringan telepon, gelombang radio, jaringan TV kabel, jaringan komputer lokal, internet, media cetak. baik secara *on-line* maupun *off-line* selalu mendapat banyak perhatian dalam berbagai konteks politik atau militer selama ini. Kerahasiaan telah menjadi kebutuhan umum guna mendapatkan privasi, oleh karena itulah di tercipta teknik kriptografi sebagai akibat berkembangnya kesadaran hak-hak seseorang untuk itu. Kriptografi, merupakan bagian dari keamanan komputer yang digunakan untuk mengamankan kerahasiaan dalam komunikasi komputerisasi interpersonal saat ini.

Stallings (2011) berdasarkan NIST *Computer Security Handbook* [NIST95] dikatakan bahwa "Keamanan komputer merupakan perlindungan yang diberikan untuk sistem informasi otomatis untuk mencapai tujuan yang diinginkan dengan menjaga integritas, ketersediaan, dan kerahasiaan sumber daya sistem informasi (termasuk perangkat keras, perangkat lunak, *firmware*, informasi / data, dan telekomunikasi)".

Menurut Klein (2014) "Kriptografi merupakan suatu teknik guna mengamankan suatu data maupun informasi dengan menyembunyikan isi pesan atau dokumen. Sebuah *cryptosystem* adalah sistem untuk melakukannya yang terdiri dari dua bagian: metode enkripsi dan metode dekripsi dengan mengubah bentuk dari pesan atau dokumen yang dapat dibaca disebut *plaintext* atau teks-jelas. menjadi bentuk yang tidak terbaca disebut *cyphertext*."

Kościelny., Kurkowski., & Srebrny (2013) mengemukakan bahwa "kriptografi adalah ilmu mengubah, atau *encoding,* informasi menjadi bentuk yang tidak dipahami bagi siapa saja yang tidak mengetahui kunci yang

tepat. Dalam bentuk seperti informasi dapat dengan aman dikirimkan melalui setiap saluran komunikasi ataupun disimpan dalam arsip data dengan akses terbatas atau bahkan dilarang untuk diakses (dengan alasan tertentu)".

Kriptografi adalah seni dan ilmu enkripsi. Enkripsi merupakan tujuan asli dari kriptografi. Enkripsi simetris adalah salah satu dari dua bentuk kriptografi di mana enkripsi dan dekripsi dilakukan dengan menggunakan kunci yang sama atau dikenal sebagai enkripsi konvensional. AES Rijndael termasuk dalam jenis algoritma kriptografi yang sifatnya simetris dan cipher block. Dengan demikian algoritma ini mempergunakan kunci yang sama saat enkripsi dan dekripsi serta masukan dan keluarannya berupa blok dengan jumlah bit tertentu. Oleh karena itu Jurnal ini akan membahas tentang salah satu enkripsi simetris yang paling umum digunakan yaitu *Advanced Encryption Standard* (AES) dengan panjang kunci 256bit.

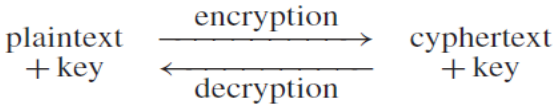
2. METODE PENELITIAN

a. Studi Literatur
   Pada studi literatur ini penulis lakukan untuk mempelajari dan memahami tentang konsep-konsep kriptografi *symmetric-key cryptosystem* dengan metode AES (Advanced Encryption Standard) 256bit dari literatur terkalit berupa e-book, jurnal, maupun sumber dari internet guna membantu proses penelitian berjalan dengan baik.
b. Analisis kriptografi AES (*Advanced Encryption Standard*)
   Analisis kriptografi berupa proses enkripsi dan dekripsi dengan AES dengan ukuran kunci 256bit dalam mengamankan *plaintext* agar hanya bisa dibaca oleh pihak yang mengetahui *secret key* saja.
c. Hasil Analisis dan Pembahasan
   Setelah dilakukannya analisis kriptografi *symmetric-key cryptosystem* dengan metode AES (*Advanced Encryption Standard*) maka bisa ditarik sebuah kesimpulan guna memperoleh tingkat keamanan maksimum dalam pengiriman pesan tersebut.

3. PEMBAHASAN

3.1 Kriptografi

Kriptografi (*Cryptography*) adalah cabang ilmu matematika tentang persandian untuk menjaga keamanan data. *Cryptographic system* atau *cryptosystem* adalah suatu fasilitas untuk mengkonversikan plaintext ke *ciphertext* dan sebaliknya. *Plaintext* adalah data asli, data yang masih bisa dibaca dan dimengerti. Sedangkan *ciphertext* adalah data yang tidak bisa dibaca maupun dimengerti. Penggunaan yang paling familiar dari kriptografi adalah menyembunyikan isi pesan atau dokumen. *Cryptosystem* adalah sistem untuk mengubah bentuk yang dapat dibaca dari pesan atau dokumen disebut *plaintext* atau *cleartext*. Diubah menjadi bentuk yang sulit terbaca disebut *cyphertext*. (Nama lain untuk *cryptosystem* adalah *cypher*). Proses enkripsi dan dekripsi pada kriptografi modern saat ini sangat cepat. Kriptografi bertujuan untuk mengamankan pesan yang dikirim melalui jaringan internet dengan memanfaatkan program algoritma komputer guna memperoleh *cyphertext* berdasarkan *secret key* yang dipakai seperti dapat dilihat pada gambar 1 berikut :



Gambar 1: Proses Kriptografi (sumber: Philip N. Klein (2014 : 1))

Metode *Cryptosystem* terdiri dari dua bagian: metode enkripsi dan metode dekripsi. Enkripsi adalah proses mendapatkan cyphertext dari plaintext. Metode enkripsi membutuhkan dua input: *plaintext* dan *secret key*. Demikian pula, dekripsi membutuhkan dua input: *cyphertext* dan *secret key*. Setiap *cryptosytem* yang baik harus memiliki karakteristik sebagai berikut :

1) Keamanan sistem terletak pada kerahasiaan kunci dan bukan pada kerahasiaan algoritma yang digunakan.
2) *Cryptosystem* yang baik memiliki ruang kunci (*keyspace*) yang besar.
3) *Cryptosystem* yang baik akan menghasilkan ciphertext yang terlihat acak dalam seluruh tes statistik yang dilakukan terhadapnya.

Cryptographic systems di karakterisasikan menjadi 3 (tiga) dimensi yaitu :

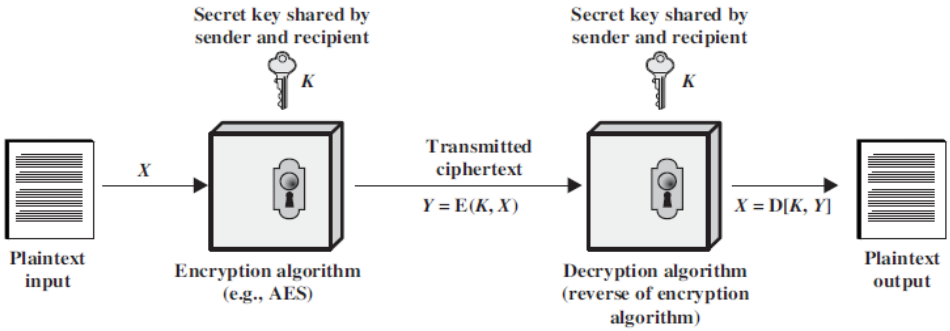
1) Jenis Operasi yang digunakan untuk mengubah *plaintext* ke *ciphertext*. Semua algoritma enkripsi didasarkan pada dua kategori umum: Pergantian (*substitution*), setiap elemen pada *plaintext* (bit, letter, group of bits or letters) dipetakan menjadi elemen lain, dan Perpindahan (*transposition*), setiap elemen pada *plaintext* disusun ulang. Kebutuhan mendasarnya bahwa tidak ada informasi yang hilang (dan semua operasi tersebut

dapat di balik). Kebanyakan sistem, direferensikan sebagai *product systems*, melibatkan beberapa tahapan dari Pergantian (*substitutions*) and Perpindahan(*transpositions*).

2) Jumlah Kunci yang digunakan. Jjika pengirim dan penerima menggunakan kunci yang sama, system tersebut di definisikan sebagai *symmetric*, *single-key*, *secret-key*, atau enkripsi konvensional. Jika pengirim dan penerima menggunakan kunci yang berbeda maka sistem tersebut didefinisikan sebagai *asymmetric*, *two-key*, atau *public-key encryption*.
3) Cara memproses *plaintext*. *Block cipher* memproses masukan (*input*) satu blok elemen secara bersamaan, menghasilkan keluaran (*output*) blok untuk setiap blok *input*. Sedangkan *stream cipher* memproses elemen masukan secara simultan, menghasilkan *output* satu elemen secara bersamaan, begitu pun seterusnya.

3.2 Symmetric Encryption

Dalam kriptografi tradisional, kunci yang sama digunakan untuk mengenkripsi dan mendekripsi disebut *cryptosystem symmetric-key* atau *symmetric encryption*. Metode *symmetric encryption* digunakan untuk menyembunyikan isi blok atau aliran data dari berbagai ukuran, termasuk pesan, file, kunci enkripsi, dan password. Model *symmetric encryption* dapat dilihat pada gambar 2 berikut :

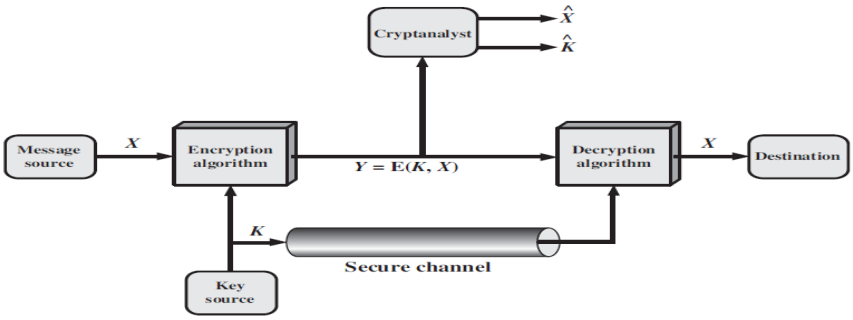


Gambar 2 : Model sederhana dari enkripsi simetrik (Sumber: William Stallings (2011 : 33))

Dari gambar 2 diatas dapat diketahui bahwa enkripsi simetris memiliki lima penyusun, yaitu:

1) *Plaintext*: ini adalah pesan asli yang dimengerti atau data yang dimasukkan ke dalam algoritma sebagai masukan.
2) *Encryption algorithm*: algoritma enkripsi melakukan berbagai substitusi dan transformasi pada plaintext.
3) *Secret Key*: merupakan kunci rahasia dan sebagai masukan pada algoritma enkripsi. Kunci tersebut berisi nilai tertentu yang berbeda dari *plaintext* dan berguna untuk menghasilkan *ciphertext* yang berbeda-beda jika nilai yang menjadi kunci tersebut juga berbeda-beda untuk algoritma yang digunakan.
4) *Ciphertext*: ini adalah pesan acak yang diproduksi sebagai keluaran (*output*) yang tergantung pada hasil kombinasi *plaintext* dan *Secret Key*. Untuk pesan yang diberikan, dua kunci yang berbeda akan menghasilkan dua ciphertexts yang berbeda pula.
5) *Decryption algorithm*: algoritma dekripsi pada dasarnya adalah algoritma enkripsi berjalan secara terbalik. Diperlukan *ciphertext* dan *Secret Key* guna menghasilkan *plaintext* yang dapat dibaca.

Dalam metode *symmetric encryption* hal yang paling utama dalam mengamankan data yaitu menjaga kerahasiaan kunci yang digunakan/dipakai. Sehingga apabila seseorang *Cryptanalysist* (seseorang yang dapat melakukan proses dekripsi *Ciphertext* tanpa mengetahui *Secret Key* yang digunakan) mengetahui algoritma enkripsi yang digunakan, dia memerlukan waktu yang lama untuk melakukan dekripsi *Ciphertext* tersebut menjadi *plaintext*. Untuk lebih jelasnya dapat dilihat pada gambar 3 berikut :



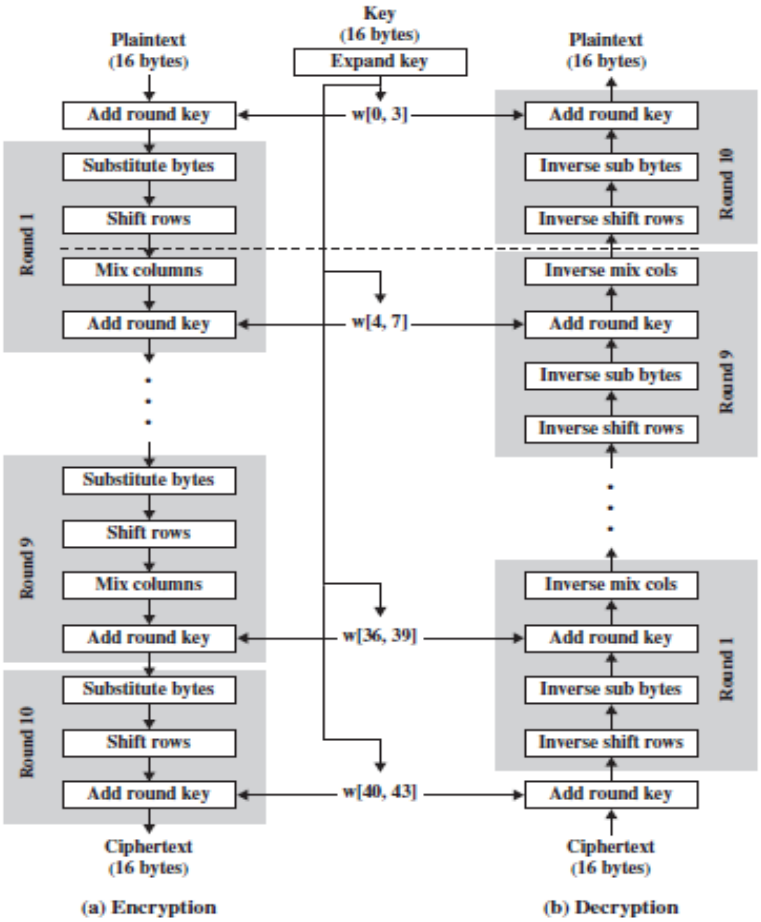
Gambar 3: Model Symmetric Cryptosystem (Sumber: William Stallings (2011 : 34))

Berdasarkan gambar 3 diatas, diketahui ada dua kebutuhan dalam mengamankan *symmetric encryption* yaitu :

1) Diperlukan algoritma enkripsi yang kuat. Setidaknya dengan algoritma tersebut walaupun semua orang yang mengetahui *Ciphertext* yang dikirimkan mereka tidak dapat melakukan dekripsi pada ciphertext tersebut atau menebak nilai pada *Secret Key*.
2) Pengirim dan penerima pesan wajib menyimpan *secret key* secara aman. Jika seseorang menemukan kunci tersebut dan mengetahui algoritma nya maka semua komunikasi yang menggunakan kunci tersebut dapat terbaca.

3.3 AES (*ADVANCED ENCRYPTION STANDARD*)

Advanced Encryption Standard (AES), dikenal sebagai Rijndael merupakan cipher dengan kunci dan blok ukuran yang berbeda, ditemukan oleh dua kriptografer Belgia, Joan Daemen dan Vincent Rijmen. Algoritma yang digunakan oleh AES merupakan algoritma kunci simetris, artinya kunci yang sama digunakan untuk kedua enkripsi dan mendekripsi data. AES merupakan *modern block cipher* yang mendukung tiga ukuran kunci yang berbeda yaitu 128, 192 dan 256 bit. Sehingga menjadikannya sistem keamanan jangka panjang yang baik dalam mencegah *brute-force attacks* dan sangat efisien dalam penggunaan *software* dan *hardware*. Proses enkripsi dan



dekripsi *plaintext* menjadi *ciphertext* seperti pada gambar 4:

Gambar 4: Proses enkripsi dan dekripsi pada AES (Sumber: William Stallings (2011 : 154))

AES tidak menggunakan menggunakan struktur *feistel* karena struktur *feistel* tidak mengenkripsi seluruh blok per iterasi, misalnya, dalam DES, 64/2 = 32 bit dienkripsi dalam satu putaran. Sedangkan AES mengenkripsi semua 128 bit dalam satu iterasi yang merupakan salah satu alasan mengapa AES memiliki *comparably rounds* yang kecil. Sebaliknya, pada setiap *full round* terdiri dari empat fungsi yang terpisah: substitusi byte, permutasi, operasi aritmatika dengan *field* terbatas, dan XOR dengan kunci. AES terdiri dari lapisan (*layer*) dan menggunakan *Galois field arithmetic* pada setiap *layer*-nya, khususnya pada S-Box dan *layer* MixColumn layer. Setiap *layer* memanipulasi semua 128 bit jalur data. Jalur data juga disebut sebagai keadaan algoritma. *Advanced Encryption Standard* (AES) menggunakan aritmatika dengan karakteristik 2 bidang yang terbatas dengan 256 elemen, yang juga bisa disebut *Galois field* (2^8), dengan *irreducible polynomial* $m(x) = x^8 + x^4 + x^3 + x + 1$.

Misalkan, {53} • {CA} = {01} jika dihitung dengan *Galois Field* maka :

$(x^6 + x^4 + x + 1)\ (x^7 + x^6 + x^3 + x)$

$= (x^{13} + x^{12} + x^9 + x^7) + (x^{11} + x^{10} + x^7 + x^5) + (x^8 + x^7 + x^4 + x^2) + (x^7 + x^6 + x^3 + x)$

$= x^{13} + x^{12} + x^9 + x^{11} + x^{10} + x^5 + x^8 + x^4 + x^2 + x^6 + x^3 + x$

$= x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + x^2 + x$

dan

$= x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + x^2 + x$ modulo $x^8 + x^4 + x^3 + x^1 + 1$

= (11111101111110 mod 100011011) = {3F7E mod 11B} = {01} = 1 (desimal).

3.3.1 Proses Enkripsi pada AES

3.3.1.1 *Byte Substitution Layer*

Layer pertama pada setiap round yaitu *byte substitution layer* yang dapat dilihat pada gambar 4, setiap byte pada *State* dipetakan menjadi byte baru dengan cara : 4 bit yang paling kiri menggunakan nilai pada baris S-Box dan 4 bit yang paling kanan menggunakan nilai pada kolom S-Box. Nilai pada baris dan kolom di cocokkan dengan nilai pada S-Box sehingga di dapat nilai 8-bit yang unik. Misal: input byte pada S-Box *Ai* = (*C*2)*hex*, maka nilai substitusinya yaitu *S* ((*C*2)*hex*) = (25)*hex* atau *S* $(11000010)_{bin} = (00100101)_{bin}$. AES S-Box untuk proses enkripsi dapat dilihat pada gambar 5 berikut :

	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
x 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 5: AES S-Box (Sumber: Christof Paar dan Jan Pelzl (2010 : 101))

S-Box pada AES memiliki struktur matematika sederhana yang tidak hanya membantu melindungi terhadap *cryptanalysis* yang diferensial, tetapi juga meyakinkan pengguna bahwa itu belum direkayasa dengan beberapa pintu jebakan tersembunyi. Setiap byte s = [s7, . . . , s0] dari *state* matriks AES diambil pada gilirannya dan dipertimbangkan sebagai elemen dari *Galois Field*(2^8). S-Box dapat dideskripsikan secara matematis dengan dua cara :

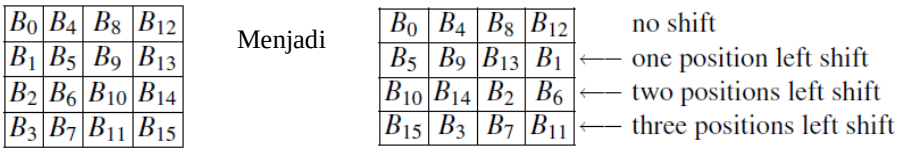
1) Invers perkalian dari *Galois Field*(2^8) dihitung, untuk menghasilkan byte baru x = [x7,. . . , X0]. Untuk elemen [0,. . . , 0], yang tidak memiliki invers perkalian, satu menggunakan konvensi bahwa ini dipetakan ke nol, sehingga dapat menjaga pemetaan *one-to-one* dari input ke output dari S-Box.
2) Bitvector x kemudian dipetakan, melalui transformasi matriks *Galois Field* (2^8) berikut, dengan bitvector b_i seperti gambar 6 berikut:

$$\begin{bmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

Gambar 6: Transformasi matriks AES(Sumber: William Stallings (2011 : 159))

3.3.1.2 *Diffusion Layer*

Diffusion layer terdiri dari dua sublayer yaitu *ShiftRows transformation* dan *MixColumn transformation*. Pada *ShiftRows transformation* matriks pada baris pertama tidak mengalami pergeseran nilai, pergeseran nilai dilakukan mulai pada baris kedua dengan pergeseran satu byte ke kanan, baris ketiga dengan pergeseran dua byte ke kanan dan baris ke empat dengan pergeseran tiga byte ke kanan seperti pada gambar 7 berikut:



Gambar 7: *ShiftRows transformation* pada *state* matriks

Sedangkan pada *MixColumn transformation* merupakan transformasi secara linier yang mengkombinasikan setiap kolom dari *state* matriks. Karena setiap byte *input* mempengaruhi empat byte *output*, operasi pada *MixColumn* merupakan elemen difusi utama dalam AES. Kombinasi layer *ShiftRows* dan *MixColumn* me mungkinkan setelah tiga *rounds* setiap byte pada *state* matriks bergantung pada setiap 16 bytes pada *plaintext*. Setiap kolom 4-byte dianggap sebagai vektor dan dikalikan dengan tetap dengan matriks 4 × 4 yang berisi entri konstan, perkalian dan penambahan koefisien dilakukan dalam *Galois Field*(2^8). Seperti pada gambar 8 berikut :

$$\begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} 02\ 03\ 01\ 01 \\ 01\ 02\ 03\ 01 \\ 01\ 01\ 02\ 03 \\ 03\ 01\ 01\ 02 \end{pmatrix} \begin{pmatrix} B_0 \\ B_5 \\ B_{10} \\ B_{15} \end{pmatrix}$$

Gambar 8: Perkalian matriks 4x4 AES (Sumber: Christof Paar dan Jan Pelzl (2010 : 105))

Setiap *state* byte *Ci* dan *Bi* adalah nilai 8-bit yang mewakili unsur dari *Galois Field*(2^8). Semua aritmatika yang melibatkan koefisien dilakukan dalam bidang Galois ini. Untuk konstanta dalam matriks notasi heksadesimal digunakan: "01" mengacu pada *Galois Field* (2^8) polinomial dengan koefisien (00000001), yaitu elemen 1 dari bidang Galois; "02" mengacu pada polinomial dengan bit vector (00000010), dengan x polinomial; dan "03" mengacu pada polinomial dengan bit vector (00000011), yaitu elemen *Galois Field* x + 1. Sebagai contoh jika input *state* pada *MixColumn layers* adalah B = (25,25, . . . ,25). Maka hanya dua perkalian pada *Galois Field*(2^8) yang bisa dilakukan yaitu 02 · 25 dan 03 · 25, yang dapat ditulis dengan persamaan berikut:

$02 \cdot 25 = x \,.\, (x5 + x2 + 1)$
$= x6 + x3 + x$
$03 \cdot 25 = (x+1) \,.\, (x5+x2+1)$
$= (x6 + x3 + x)+(x5 + x2 + 1)$
$= x6 + x5 + x3 + x2 + x + 1$

Karena kedua nilai memiliki nilai lebih kecil dari 8, tidak diperlukan pengurangan modular dengan P (x). Hasil output byte dari C dari penambahan berikut dalam *Galois Field* (2^8):

$01 \,.\, 25 = x5 + x2 + 1$
$01 \,.\, 25 = x5 + x2 + 1$
$02 \,.\, 25 = x6 + x3 + x$
$03 \,.\, 25 = x6 + x5 + x3 + x2 + x + 1$

$Ci = x5 + x2 + 1$, Dimana $i = 0, \ldots, 15$. Yang menghasilkan output state $C = (25,25, \ldots ,25)$.

3.3.1.3 *Key Addition Layer*

Pada *Key Addition Layer* terdapat tiga jenis input kunci utama dengan panjang yang berbeda yaitu 128, 192 atau 256 bit, dimana 128 bit dari *State* di XOR kan dengan ukuran kunci nya 128, 192 atau 256 bits sehingga dihasilkan nilai *state* baru pada matriks 4x4 dari hasil pengolahan sebelumnya. Ukuran kunci yang digunakan untuk cipher menentukan jumlah pengulangan (*rounds*) seperti pada tabel 1 berikut :

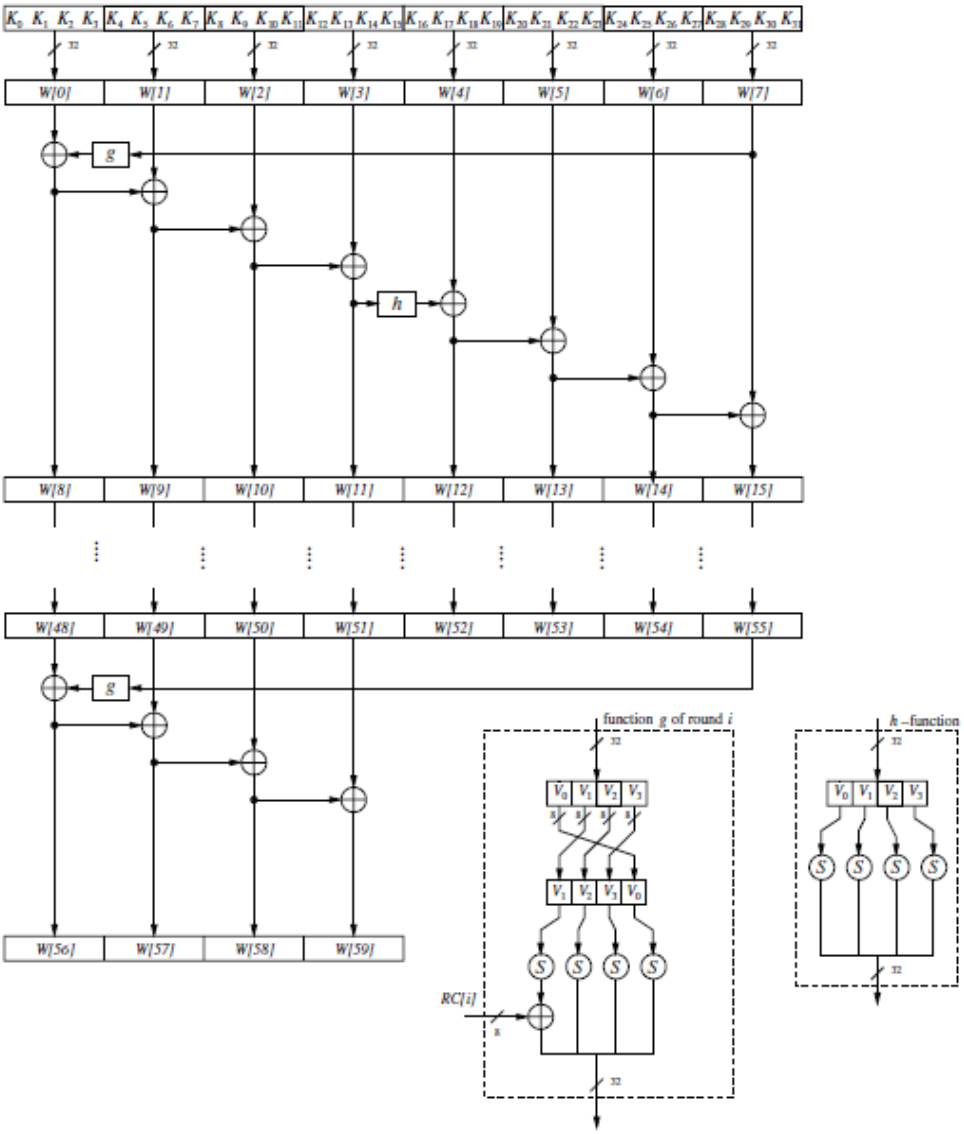
Tabel 1:
Panjang kunci dan jumlah *rounds* untuk AES

Panjang Kunci	**# Jumlah *rounds* = nr**
128 bit	10 *Rounds*
192 bit	12 *Rounds*
256 bit	14 *Rounds*

AES *key schedule* merupakan variabel *word*, dimana 1 word = 32 bit. Subkeys disimpan pada *key expansion array* W yang berisi variabel *words*. Ada perbedaan *key schedules* untuk tiga ukuran kunci yang berbeda pada AES 128, 192 and 256 bit walaupun semuanya hampir terlihat sama. AES dengan kunci 256-bit memiliki 15 buah *subkey* yang disimpan dalam 60 words W[0], . . . ,W[59]. *Key schedule* memiliki tujuh iterasi, dimana setiap iterasi menghitung delapan kata untuk *subkey*. *Subkey* untuk AES putaran pertama dibentuk oleh elemen array (W [0], W [1], W [2], W [3]), subkey kedua oleh elemen (W [4], W [5], W [6], W [7]), dan seterusnya sehingga dihasilkan tujuh koefisien bulat RC [1],. . . , RC [7] dalam fungsi *g* () yaitu :

$RC[1] = x0 = (00000001)_2$,
$RC[2] = x1 = (00000010)_2$,
$RC[3] = x2 = (00000100)_2$,
...
$RC[10] = x9 = (00110110)_2$.

Fungsi *g*() ada dua tujuan. Pertama, menambah *key schedule* secara non linier. Kedua, menghilangkan algoritma simetris pada AES. Keduanya diperlukan untuk menggagalkan serangan pada blok cipher tertentu. Seperti pada gambar 9 berikut :



Gambar 9: *Key Addition Layer* dengan kunci 256 Bit (Sumber: Christof Paar dan Jan Pelzl (2010 : 110))

3.3.2 Proses Dekripsi pada AES

3.3.2.1 *Inverse MixColumn Sublayer*

Setelah penambahan subkey, langkah ***Inverse MixColumn Sublayer*** diterapkan pada state (kecuali pada proses dekripsi putaran pertama). Dalam rangka untuk membalikkan operasi MixColumn, kebalikan dari matriks yang harus digunakan. Input adalah kolom 4-byte dari state C yang dikalikan dengan kebalikan 4 × 4

matriks yang berisi entri konstan. Perkalian dan penambahan koefisien dilakukan dalam *Galois Field*(2^8) seperti gambar 10:

$$\begin{pmatrix} B_0 \\ B_1 \\ B_2 \\ B_3 \end{pmatrix} = \begin{pmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{pmatrix} \begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{pmatrix}$$

Gambar 10: ***Inverse MixColumn Sublayer*** (Sumber: Christof Paar dan Jan Pelzl (2010 : 112))

Kolom kedua output byte (B4, B5, B6, B7) dihitung dengan mengalikan empat byte input (C4, C5, C6, C7) oleh matriks konstan yang sama, dan sebagainya. Setiap nilai B_i, C_i dan konstanta adalah elemen dari *Galois Field*(2^8). Notasi untuk konstanta adalah heksadesimal dan sama seperti yang digunakan untuk lapisan *MixColumn*, misalnya:

$0B = (0B)_{hex} = (00001011)_2 = x^3 + x + 1$.

3.3.2.2 *Inverse ShiftRows Sublayer*

Dalam rangka untuk membalikkan algoritma *ShiftRows* pada operasi enkripsi AES, diharuskan menggeser baris dari *state* matriks ke arah yang berlawanan. Baris pertama tidak berubah pada *Inverse ShiftRows*. Jika input dari *ShiftRows sublayer* diberikan sebagai state matriks B = (B0, B1,, B15...) maka perubahannya dapat dilihat pada gambar 11 berikut:

B_0	B_4	B_8	B_{12}
B_1	B_5	B_9	B_{13}
B_2	B_6	B_{10}	B_{14}
B_3	B_7	B_{11}	B_{15}

Menjadi

B_0	B_4	B_8	B_{12}	no shift
B_{13}	B_1	B_5	B_9	⟶ one position right shift
B_{10}	B_{14}	B_2	B_6	⟶ two positions right shift
B_7	B_{11}	B_{15}	B_3	⟶ three positions right shift

Gambar 11: *Inverse shiftrows sublayers* S-Box (Sumber: Christof Paar dan Jan Pelzl (2010 : 113))

3.3.2.3 *Inverse Byte Substitution Layer*

Inverse S-Box digunakan ketika mendekripsi *ciphertext*. Karena AES S-Box adalah sebuah bijective dengan kata lain pemetaan *one-to-one*, sehingga memungkinkan untuk membuat *inverse* S-Box dengan menghitung kebalikan dari transformasi yang relatif sama dengan rumus : $A_i = S{-}1(B_i) = S{-}1(S(A_i))$, dimana A_i dan B_i merupakan elemen dari *state matrix*, entri dari inverse S-Box dapat dilihat pada gambar 12 :

	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
x 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 12 : AES *Inverse* S-Box (Sumber: Christof Paar dan Jan Pelzl (2010 : 114))

Untuk melakukan *inverse* pada *S-Box substitution*, harus dihitung dulu *inverse* pada *affine transformation*. Untuk itu, setiap input byte B_i dipertimbangkan debagai elemen dari Galois Field (2^8). *Inverse affine transformation* pada setiap byte B_i didefinisikan seperti pada gambar 13 :

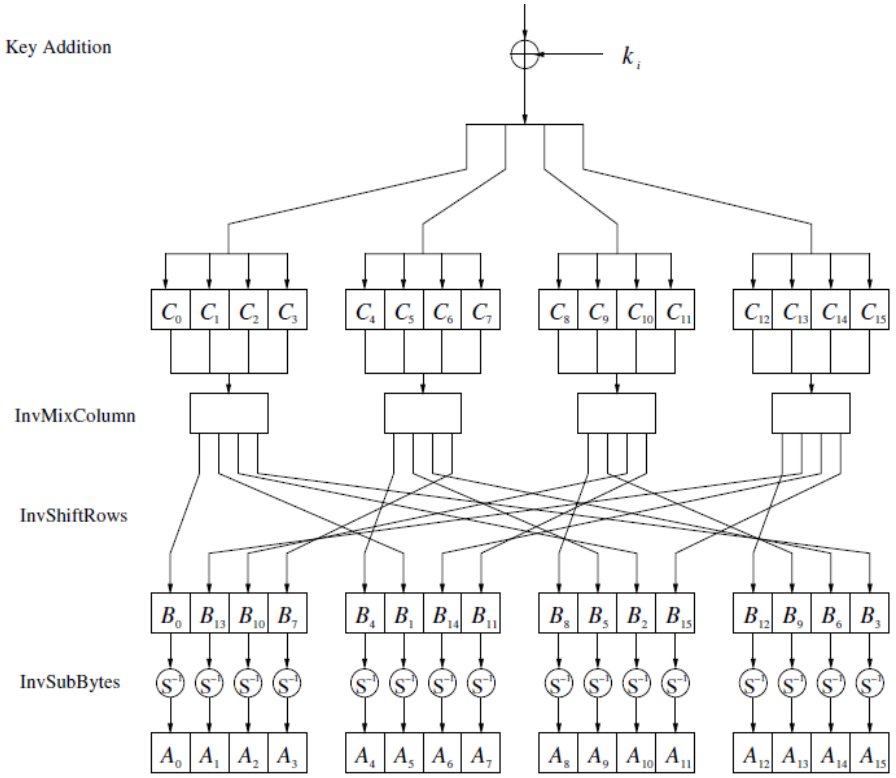
$$\begin{pmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{pmatrix} \equiv \begin{pmatrix} 0\,1\,0\,1\,0\,0\,1\,0 \\ 0\,0\,1\,0\,1\,0\,0\,1 \\ 1\,0\,0\,1\,0\,1\,0\,0 \\ 0\,1\,0\,0\,1\,0\,1\,0 \\ 0\,0\,1\,0\,0\,1\,0\,1 \\ 1\,0\,0\,1\,0\,0\,1\,0 \\ 0\,1\,0\,0\,1\,0\,0\,1 \\ 1\,0\,1\,0\,0\,1\,0\,0 \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} \bmod 2$$

Gambar 13: *Inverse Byte Substitution Layer* (Sumber: Christof Paar dan Jan Pelzl (2010 : 112))

Dimana ($b_7, \ldots, b_0$) merupakan representasi *bitwise vector* dari $B_i(x)$, dan ($b'_7, \ldots, b'_0$) yang merupakan hasil setelah *inverse affine transformation*.

3.3.2.4 *Decryption Key Schedule*

Algoritma *key expansion* pada AES memerlukan input kunci sebesar empat word (16-byte) dan menghasilkan array yang linier dengan 44 words (176 bytes). Hal ini cukup untuk menyediakan *round key* sebesar empat word untuk inisialisasi pada *AddRoundKey stage* dan setiap 10 *round* pada cipher. Proses *round* pertama dekripsi pada AES membutuhkan *subkey* terakhir, dekripsi pada *round* kedua juga membutuhkan *subkey* kedua dari yang *key* terakhir, dan seterusnya. Pada prakteknya proses *decryption key schedule* dapat diperoleh dengan komputasi semua *key schedule* terlebih dahulu dan menyimpan *round* 11, 13 atau 15 dari semua *subkeys*, tergantung dari jumlah *round* AES yang digunakan (tergantung pada tiga buah panjang kunci yang digunakan pada sistem AES). Biasanya proses dekripsi pada AES memerlukan waktu yang sedikit lebih lama dari proses enkripsinya. Keseluruhan proses dekripsi dapat dilihat pada gambar 14 berikut :



Gambar 14 : Round dekripsi pada AES (Sumber: Christof Paar dan Jan Pelzl (2010 : 112))

4. Hasil Enkripsi dan Dekripsi AES Dengan Ukuran Kunci 256 Bit

Hasil kriptografi dengan AES yang penulis lakukan pada situs http://aesencryption.net/ didapati bahwa hasil enkripsi dengan metode AES 256 bit dapat dilihat pada tabel 2 berikut ini :

Tabel 2 :
Hasil Enkripsi Dengan Metode AES Ukuran Kunci 256bit

Plaintext	KRIPTOGRAFI SYMMETRIC-KEY CRYPTOSYSTEM DENGAN METODE AES (ADVANCED ENCRYPTION STANDARD) 256bit
Secret Key	ABCDEFGH

Ukuran kunci	256 Bit
Hasil Enkripsi	awD9qSa2sKTZHGrY6xkc8fKZ277aAKQkxVmkri8f31xFLT10K9woikGRRj1GsU2No8 HoKCxMUTqJREkS6zzP8vwDLbSpKVzwZlTlR6iEKfQUdyoTOOxZo54D1DJrN9ne

Hasil enkripsi *plaintext* yang sama dengan *secretkey* yang berbeda didapat hasil seperti tabel 3 berikut:

Tabel 3 :
Hasil Enkripsi Dengan Metode AES Dengan Secret Key Yang Berbeda

Plaintext	KRIPTOGRAFI SYMMETRIC-KEY CRYPTOSYSTEM DENGAN METODE AES (ADVANCED ENCRYPTION STANDARD) 256bit
Secret Key	WILLY
Ukuran kunci	256 Bit
Hasil Enkripsi	c+N86NFrQQ99GplguP3YrHbUh8MhT5a62+3U9zQTsjAGDONpuJG0bYBBjdi8+oDBp sWo9rMUatTCUG4neXdj6CyX4vyXx+mY6E5pPLtsc3+hQlay3FB790WjHOpAbh8c

Begitu pula jika *ciphertext* hasil enkripsi tadi di dekripsikan dengan *Secret Key* yang sama dengan metode AES 256 bit akan menghasilkan plaintext yang sama seperti pada tabel 4 berikut ini:

Tabel 4 :
Hasil Dekripsi Dengan Metode AES Dengan *Secret Key* Yang Sama

Ciphertext	awD9qSa2sKTZHGrY6xkc8fKZ277aAKQkxVmkri8f31xFLT10K9woikGRRj1GsU2No8H oKCxMUTqJREkS6zzP8vwDLbSpKVzwZlTlR6iEKfQUdyoTOOxZo54D1DJrN9ne
Secret Key	ABCDEFGH
Ukuran kunci	256 Bit
Hasil Dekripsi	KRIPTOGRAFI SYMMETRIC-KEY CRYPTOSYSTEM DENGAN METODE AES (ADVANCED ENCRYPTION STANDARD) 256bit

Jika *ciphertext* hasil enkripsi tadi di dekripsikan dengan *Secret Key* yang berbeda pula dengan metode AES 256 bit akan menghasilkan plaintext yang tidak bisa dibaca seperti pada tabel 5 berikut ini:

Tabel 5:
Hasil Dekripsi Dengan Metode AES Dengan *Secret Key* Yang Berbeda

Ciphertext	awD9qSa2sKTZHGrY6xkc8fKZ277aAKQkxVmkri8f31xFLT10K9woikGRRj1GsU2No8H oKCxMUTqJREkS6zzP8vwDLbSpKVzwZlTlR6iEKfQUdyoTOOxZo54D1DJrN9ne
Secret Key	STIKOM
Ukuran kunci	256 Bit
Hasil Dekripsi	��.������w:s�m�-#T8�t�tHc%��\�� • ����G�8/c��&�tr�jQ;C ��/�,m�fgc�������hE)vu�%��+���

5. PENUTUP

5.1 Kesimpulan

Dari hasil penelitian diatas dapat diambil beberapa kesimpulan yaitu :

1. Pada *Advanced Encryption Standard* (AES) dengan ukuran kunci 256bit, dalam proses enkripsi maupun dekripsi *ciphertext* memerlukan *secret key* yang sama. Sehingga dalam melakukan pertukaran *secret key* antar pengirim dan penerima diperlukan jalur komunikasi yang benar-benar aman.
2. Algoritma Kriptografi pada AES cukup handal hingga saat ini karena serangan terbaik terhadap algoritma AES dengan ukuran kunci 256bit pada tahun 2006 hanya sampai ke-9 putaran. Sehingga tahun 2006 National Security Agency (NSA) pernah menyatakan bahwa AES cukup aman digunakan untuk mengamankan data-data pemerintah Amerika Serikat yang bukan tergolong sangat rahasia.

5.2 Saran

Adapun saran-saran yang berguna untuk perkembangan lebih lanjut adalah sebagai berikut :

1. Ada baiknya metode AES dikombinasikan dengan sistem keamanan tambahan seperti *firewall* dan *Secure Socket Layer* (SSL) maupun metode lainnya guna menghindari terjadinya pencurian data saat pertukaran data (*eavesdropping*).
2. Seiring dengan berkembang pesatnya teknologi tidak tertutup kemungkinan metode kriptografi AES akan bisa direntas dalam beberapa tahun mendatang sehingga pengguna metode ini harus aktif secara berkala dalam mencari informasi tentang risiko celah-celah keamanan dengan metode ini.

DAFTAR PUSTAKA

[1] Surian, D. (2006). Algoritma Kriptografi AES Rijndael, Jurnal Teknik Elektro Puslit PETRA, 8(2), 97 – 101.

[2] Klein, P. N., 2014. *A Cryptography Primer Secrets And Promises*. United States of America : Cambridge University Press.

[3] Ko´scielny, C., Kurkowski, M., Srebrny, M., 2013. *Modern Cryptography Primer*. Berlin : Springer.

[4] Paar, C., Pelzl, J., 2010. *Understanding Cryptography*. Berlin : Springer.

[5] Stallings, W., 2011. *Cryptography And Network Security Principles And Practice.* 5th ed. United States of America: Prentice Hall.

[6] Wikipedia. 2015. *Advanced Encryption Standard* (AES). (*https://en.wikipedia.org/wiki/Advanced_Encryption_Standard*), diakses 20 Desember 2015.

[7] AES encryption Encrypt and decrypt text with AES algorithm. (http://aesencryption.net), diakses 20 Desember 2015.

[8] Voni, Y., Gani, I., Antonius, R. (2009). Enkripsi Dan Dekripsi Dengan Algoritma AES 256 Untuk Semua Jenis File, Jurnal Informatika Universitas Kristen Duta Wacana Yogyakarta, 5 (1), APRIL 2009, 22 – 31.