IMPLEMENTASI SISTEM KEAMANAN AES 256-BIT GCM GUNA MENGAMANKAN DATA PRIBADI

Ega Shela Marsiani[1], Irawan Setiadi[2], Alqomari Cahyo[3]
Program Studi Teknik Informatika, Fakultas Teknik dan Ilmu Komputer,
Universitas Indraprasta PGRI
Jalan Raya Tengah No 80, Kelurahan Gedong, Pasar Rebo, Jakarta Timur
egashela@gmail.com[1], irawan.setiadi91@gmail.com[2], alqomari.cahyo@gmail.com[3]

Abstrak

Perkembangan teknologi yang semakin cepat dapat dimanfaatkan oleh manusia. Pemanfaatan teknologi yang dilakukan manusia adalah untuk berkomunikasi, mempermudah pekerjaan, dan memperoleh informasi. Tetapi dibalik semuanya itu, teknologi memiliki kelemahan. Kelemahan dari teknologi ialah kurangnya keamanan terhadap data pribadi. Keamanan data merupakan hal yang perlu diperhatikan karena data tersebut bisa dicuri oleh pihak ketiga apabila tidak memiliki sistem keamanan data. Salah satu cara agar data dapat diamankan oleh sistem adalah dengan Kriptografi. Kriptografi adalah penerapan dan studi tentang teknik pengamanan komunikasi maupun data terhadap pihak ketiga/musuh. AES-256 Bit merupakan algoritma kriptografi yang dapat digunakan untuk mengamankan data. AES-256 Bit merupakan *blokchipertext* simetrik yang dapat mengenkripsi dan dekripsi data/informasi dengan ukuran kunci 256 bit. Dengan menggunakan AES-256 Bit keamanan data tersebut dapat terjaga karena algoritma tersebut melakukan pengamanan dan penyandian yang berlapis-lapis.

Kata Kunci : Kriptografi, AES-256 Bit, Enkripsi, Dekripsi

Abstract

The rapid development of technology can be utilized by humans. Human technology is used to communicate, facilitate work, and obtain information. But behind it all, technology has its drawbacks. The downside of technology is the lack of security over personal data. Data security is a concern because it can be stolen by third parties if it does not have a data security system. One way that data can be secured by the system is by Cryptography. Cryptography is the application and study of communication and data security techniques against third parties / enemies. AES-256 Bit is a cryptographic algorithm that can be used to secure data. AES-256 Bit is a symmetric blokchipertext that can encrypt and decrypt data/information with a key size of 256 bits. By using AES-256 Bit data security can be maintained because the algorithm performs multi-layered security and encoding.

***Keyword** : Cryptography, AES-256 Bit, Encryption, Decryption*

PENDAHULUAN

Di zaman sekarang, teknologi terus berkembang dengan pesat. Perkembangan teknologi ini dimanfaatkan oleh setiap manusia untuk mempermudah pekerjaan, berkomunikasi, hingga memperoleh informasi. Kemudahan yang diberikan teknologi, memang sangat bermanfaat untuk setiap manusia. Tetapi dibalik kemudahan yang diberikan, teknologi memiliki kelemahan. Kelemahan dari teknologi ialah kurangnya keamanan ataupun kerahasiaan data pribadi. Sistem keamanan mempunyai peranan penting dalam penggunaan teknologi. Para pengguna akan mempertimbangkan sistem keamanan dalam teknologi tersebut sebelum menggunakannya. Jika keamanan dalam teknologi tidak terjamin, maka akan merugikan para pengguna maupun yang membuat teknologi tersebut. Salah satunya ialah kebocoran data-data pribadi para pengguna. Untuk itu, penulis akan memperkenalkan salah satu sistem keamanan guna mengamankan data-data pribadi yaitu algoritma kriptografi AES-256 Bit GCM.

PENELITIAN RELEVAN

Menurut penelitian Agustan Latif yang berjudul "*IMPLEMENTASI KRIPTOGRAFI MENGGUNAKAN METODE ADVANCED ENCRYPTION STANDAR (AES) UNTUK PENGAMANAN DATA TEKS*" adalah sebegai berikut :

1. Sistem kriptografi AES-128 bit dapat berjalan dengan baik mulai dari plainteks dienkripsi dan

menghasilkan teks yang terenkripsi menggunakan metode AES 128 bit, kemudian ketika teks tersebut dilakukan proses dekripsi menjadi plainteks berhasil dilakukan dan menghasilkan teks sesungguhnya atau teks asli.

2. Berdasarkan hasil pengujian kapasitas enkripsi dan dekripsi diperoleh hasil bahwa kapasitas data teks yang telah dienkripsi lebih besar daripada data teks sebelum di enkripsi. Sedangkan untuk kecepatan komputasi diperoleh hasil bahwa kecepatan komputasi dekripsi lebih cepat di bandingkan dengan waktu komputasi untuk proses enkripsi.

Menurut kami, penelitian tersebut sangat bermanfaat karena dapat mengetahui bagaimana cara mengamankan data teks dengan menerapkan algoritma kriptografi AES-128 Bit. Namun akan lebih baik apabila algoritma yang digunakan adalah algoritma kriptografi AES-256 Bit karena algoritma tersebut memiliki sistem keamanan yang lebih terjamin. Bukan hanya data teks saja yang dapat diamankan tetapi seluruh file yang ada secara khusus file pribadi akan mendapatkan keamanan yang lebih terjamin dibandingkan dengan algoritma kriptografi AES-128 Bit.

METODE PENELITIAN

Penulisan jurnal ini menggunakan metode penelitian kepustakaan yang mengumpulkan informasi dan data dari berbagai macam sumber. Adapun sumber materi pada jurnal ini berupa jurnal ilmiah, situs internet, serta sumber lain yang memiliki relevansi dengan isi jurnal ini. Tujuan kami menggunakan metode ini yaitu, untuk memberikan solusi agar sistem keamanan pada teknologi semakin efektif dan efisien guna mengamankan data-data pribadi para pengguna**.**

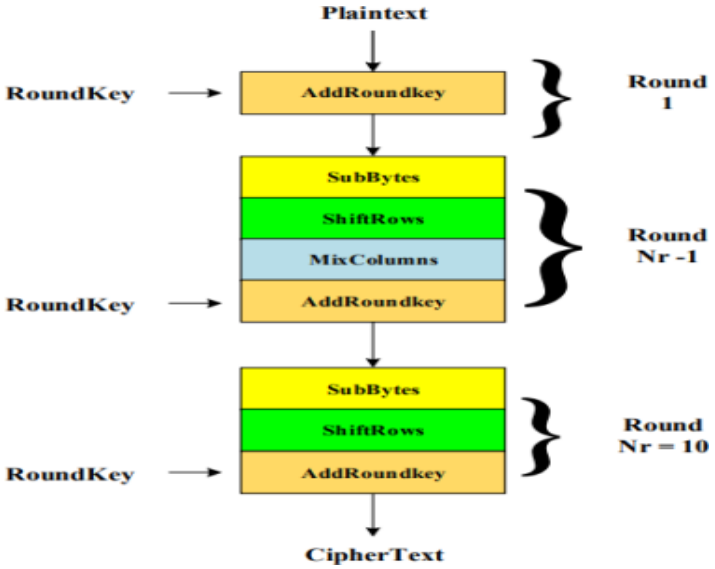
HASIL DAN PEMBAHASAN

Key Size	Possible combinations
1-bit	2
2-bit	4
4-bit	16
8-bit	256
16-bit	65536
32-bit	4.2×10^{9}
56-bit (DES)	7.2×10^{16}
64-bit	1.8×10^{19}
128-bit (AES)	3.4×10^{38}
192-bit (AES)	6.2×10^{57}
256-bit (AES)	1.1×10^{77}

Key size	Time to Crack
56-bit	399 seconds
128-bit	1.02×10^{18} years
192-bit	1.872×10^{37} years
256-bit	3.31×10^{56} years

Gambar 1. *Possible combinations and Time to Crack* AES-256 Bit

Proses enkripsi algoritma AES 256 (gambar 2) terdiri dari 4 (empat) jenis transformasi yang akan dijalankan, yaitu *SubBytes, ShiftRows, MixColumns* dan *AddRoundKey* awal proses enkripsi, input yang telah disamakan atau diduplikasi ke dalam state akan mengalami transformasi *SubBytes, ShiftRows, Mixcolumns* dan *AddRoundKey* secara berulang sesuai banyaknya Nr=10, jumlah kunci Nk = 8 dan ukuran blok Nb=4.



Gambar 2. Proses Enkripsi AES-256 Bit

AddRoundKey

Pada proses transformasi enkripsi dan dekripsi AES 256-bit, sebuah round key ditambahkan pada state dengan operasi XOR. Setiap round key terdiri dari Nb word di mana tiap word tersebut akan dijumlahkan dengan word atau kolom yang bersetaraan wi [9] dari state sehingga :

$$[s'o,c\ ,\ s'1,c\ ,\ s'2,c\ ,\ s'3,c\ ]\ *$$

$$[so,c\ ,\ s1,c\ ,\ s2,c\ ,\ s3,c] \oplus [wround*Nb+c\ ] \qquad (1)$$

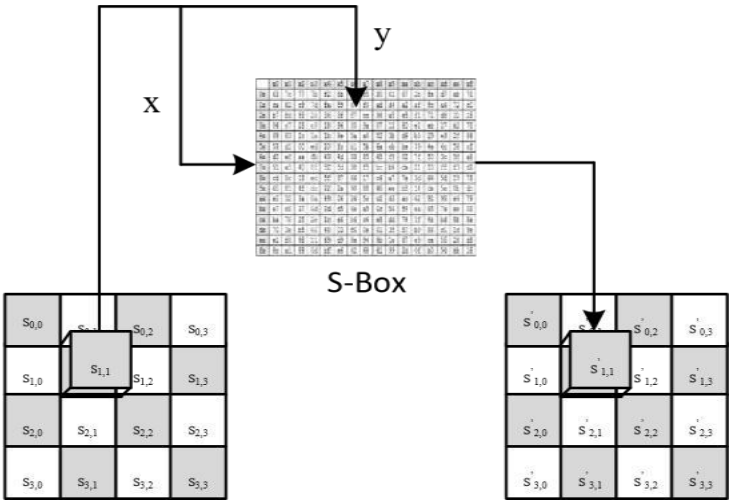
Dengan i = round*Nb+c.

SubBytes

SubBytes merupakan transformasi byte dimana setiap elemen pada state akan dipetakan dengan menggunakan sebuah tabel subtitusi (S-Box). Tabel subtitusi S-Box akan dipaparkan dalam tabel 1. Untuk setiap byte pada array state, misalkan S[r,c]=xy, yang dalam hal ini xy adalah digit heksadesimal dari nilai S[r,c], maka nilai subtitusinya, dinyatakan dengan S[r,c], adalah elemen di dalam tabel subtitusi yang merupakan pengaruh pemetaan byte pada setiap byte dan state.

Tabel 1. S-Box

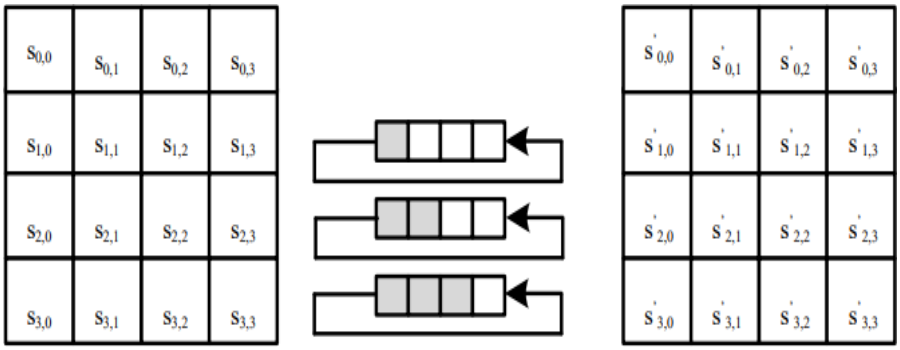
	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xa	xb	xc	xd	xe	xf
0x	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1x	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2x	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3x	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4x	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5x	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6x	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7x	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8x	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9x	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
ax	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
bx	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
cx	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
dx	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
ex	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
fx	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16



Gambar 3. Pengaruh Pemetaan pada setiap byte dalam state

ShiftRows

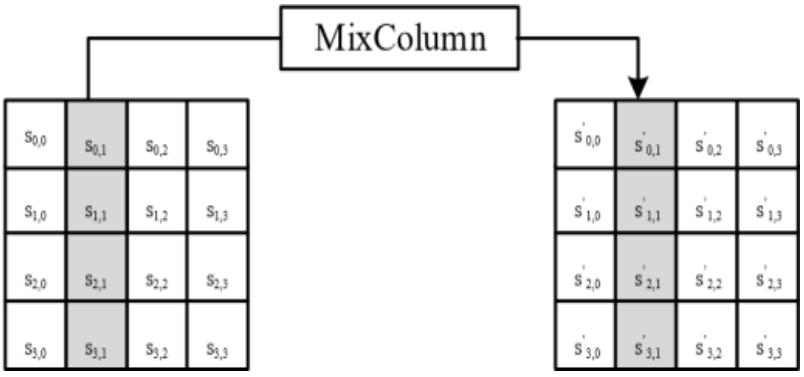
Shift Rows adalah sebuah proses yang melakukan pergeseran dalam elemen blok/tabel yang harus dilakukan per baris, baris pertama tidak harus dilakukan pergeseran 2 byte lalu setelah itu baris yang keempat dilakukan pergeseran 3 bytes, berikut pada gambar 4.



Gambar 4. Proses *ShiftRows*

MixColumns

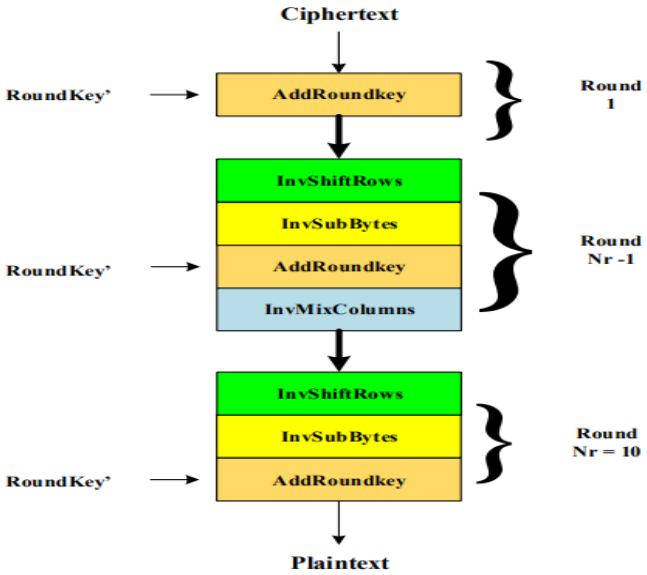
MixColumn adalah proses perkalian tiap elemen dari blokcipher dengan matriks (gambar 5 dan persamaan 2).



Gambar 5. *MixColumn*

$$\begin{pmatrix} s'0,1 \\ s'1,1 \\ s'2,1 \\ s'3,1 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix} \begin{pmatrix} s0,1 \\ s1,1 \\ s2,1 \\ s3,1 \end{pmatrix} \quad (2)$$

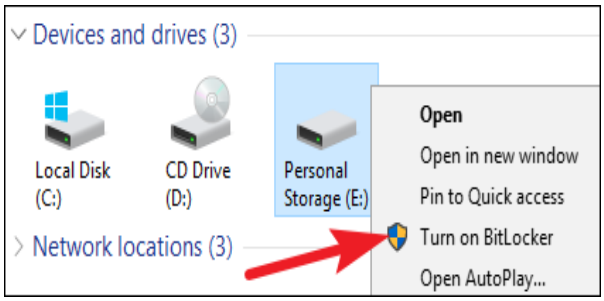
Proses Dekripsi AES-256 bit, tahapan transformasi byte digunakan proses invers cipher ke plaintext adalah InvShiftRows, InvSubBytes, InvMixColumns, dan AddRoundKey. Algoritma dekripsi dapat dilihat pada skema (gambar 6)



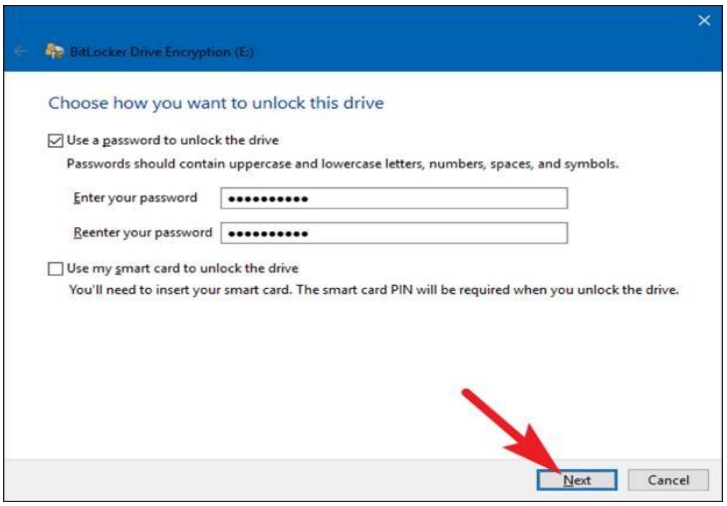
Gambar 6. Proses Dekripsi AES-256 Bit

Semua pengguna komputer atau pun smartphone memiliki banyak data pribadi dan juga memiliki data penting yang merupakan milik perusahaan. Semua pengguna tidak ingin data yang dimiliki hilang. Apabila data tersebut hilang hal itu akan merepotkan para penggunanya karena harus mencari atau membuat data yang baru yang menyerupai dengan data sebelumnya. Penjelasan diatas merupakan cara kerja sistem keamanan AES-256 Bit. Sistem keamanan tersebut dapat dipakai guna mengamankan semua data-data yang dimiliki pengguna.

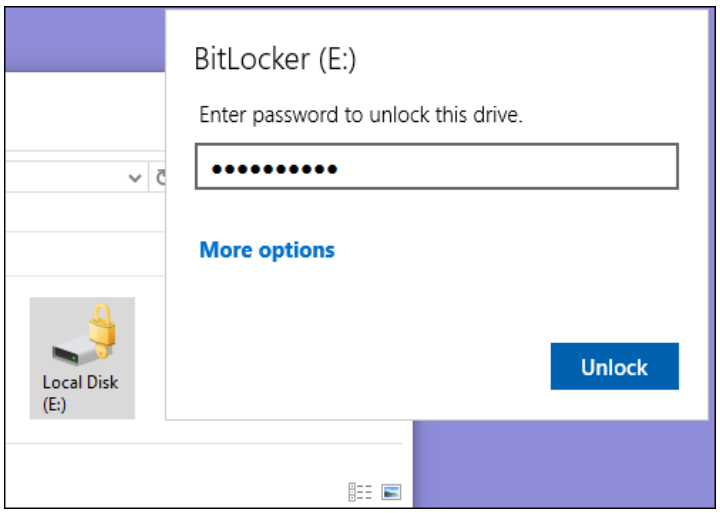
Windows memiliki fitur yang bernama BitLocker. Fitur ini menggunakan algoritma kriptografi AES- 256 Bit yang mana fitur ini berfungsi untuk mengenkripsi partisi sehingga data data tersebut dapat diamankan dan hanya bisa diakses apabila pengguna memiliki atau mengetahui password untuk mengakses partisi tersebut. Fitur ini hanya terdapat pada Windows Vista, 7, 8, dan 10 edisi Professional, Enterprise, dan Education. Berikut ini adalah tampilan penggunaan fitur *BitLocker* dengan metode AES-256 bit:



Gambar 7. Sebelum Enkripsi



Gambar 8. Pembuatan Enkripsi



Gambar 9. Sesudah Enkripsi

Gambar 7-9 merupakan tampilan pembuatan enkripsi pada partisi yang terdapat di windows. Apabila seseorang ingin mengakses partisi yang sudah di enkripsi, orang tersebut harus mengetahui password untuk mengakses partisi tersebut.

SIMPULAN

Berdasarkan hasil dan pembahasan diatas, enkripsi data atau file merupakan hal penting karena data yang kita enkripsi akan aman. Salah satunya adalah dengan menggunakan metode AES-256 Bit. Dengan menggunakan AES-256 Bit data tersebut akan kebal menghadapi serangan konvensional yang menggunakan statistik untuk memecahkan sandi. Salah satu program yang sudah menggunakan metode AES 256-bit adalah windows. Dengan mengoptimalkan sistem keamanan yang ada di windows data yang dimiliki pengguna akan aman terhadap ancaman.

DAFTAR PUSTAKA

[1] N. Anwar, M. Munawwar, M. Abduh, and N. B. Santosa, "Komparatif Performance Model Keamanan Menggunakan Metode Algoritma AES 256 bit dan RSA," J. RESTI (Rekayasa Sist. dan Teknol. Informasi), 2018.

[2] G. Bhaudhayana and I. Widiartha, "Implementasi Algoritma Kriptografi Aes 256 Dan Metode Steganografi Lsb Pada Gambar Bitmap," J. Ilmu Komput., 2015.

[3] A. Marisman and A. Hidayati, "PEMBANGUNAN APLIKASI PEMBANDING KRIPTOGRAFI DENGAN CAESAR CIPHER DAN ADVANCE ENCRYPTION STANDARD (AES) UNTUK FILE TEKS," J. Penelit. Komun. dan Opini Publik, 2015.

[4] F. Nuraeni and Y. H. Agustin, "The IMPLEMENTASI CAESAR CIPHER & ADVANCED ENCRYPTION STANDAR (AES) PADA PENGAMANAN DATA PAJAK BUMI BANGUNAN," J. Ilm. Matrik, 2020.

[5] F. N. Pabokory, I. F. Astuti, and A. H. Kridalaksana, "Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard," Inform. Mulawarman J. Ilm. Ilmu Komput., 2016.

[6] A. R. Tulloh, Y. Permanasari, and E. Harahap, "Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen," J. Mat. UNISBA, 2016.

[7] A. Prameshwari and N. P. Sastra, "Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen," Eksplora Inform., 2018.

[8] O. K. Sulaiman, K. Nasution, and S. Y. Prayogi, "Enkripsi Surat Elektronik Menggunakan Metode XXTEA," Comput. Eng. Sci. Syst. J., 2019.