Pengkajian Metode dan Implementasi AES

Hans Agastyra 13509062
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
solvethistrick@yahoo.com

Abstrak : **Dunia kriptografi teruslah berkembang dalam rangka pemenuhan kebutuhan akan melindungi informasi yang merupakan hal yang amat krusial di era global seperti saat ini. Informasi adalah sebuah hal penting yang layaknya sebuah harta yang juga harus terlindungi, privasi memang sangat dibutuhkan untuk tidak menimbulkan kekacauan serta melindungi hak, oleh karena itulah kriptografi menjadi salah satu hal yang berkembang dengan sangat pesat untuk mendukung kebutuhan akan hal itu. Salah satu metode kriptografi adalah algoritma kunci simetris yang salah satu jenisnya adalah menggunakan algoritma enkripsi Advanced Encryption Standard (AES) yang sudah sangat mendunia. Makalah ini akan menganalisis dan juga membahas tentang metode serta aplikasi dari algoritma enkripsi AES tersebut yang sebelumnya akan mengenalkan terlebih dahulu hal-hal dasar yang terkait dengan hal tersebut antara lain adalah kriptografi, enkripsi, dekripsi, dan algoritma kunci simetris.**

Kata Kunci : **Advanced Encryption Standard, kriptografi, enkripsi, dekripsi, algoritma kunci simetris**

I. PENDAHULUAN

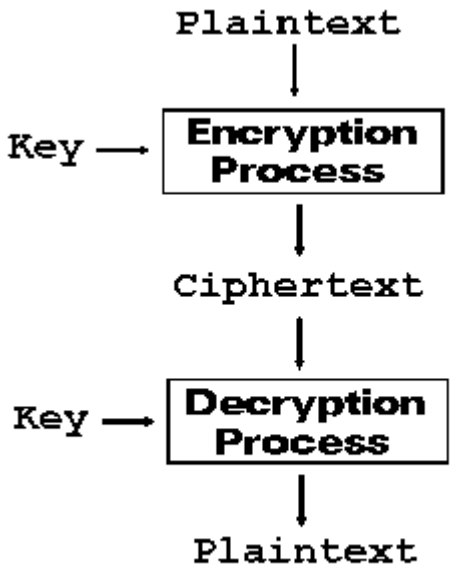
Sebelum lebih jauh membahas seperti apa metode yang digunakan dalam algoritma kriptografi Advanced Encryption Standard (yang seterusnya akan disingkat dengan AES) ada baiknya mengenal beberapa hal yang berkaitan erat dengan perkembangan serta munculnya algoritma tersebut sebagai salah satu solusi dari permasalahan di dunia kriptografi.

Hal pertama yang penting diketahui adalah mengenai kriptografi. Kriptografi adalah sebuah ilmu untuk menyembunyikan informasi. Seperti yang didefinisikan oleh Wikipedia. Kriptografi masuk ke dalam disiplin ilmu dari matematika, sains komputer, dan teknik elektro. Awalnya ilmu kriptografi digunakan dan diperkenalkan dalam dunia perang sejak tahun 400 SM oleh tentara Sparta di Yunani, setelah itu pun ilmu ini kerap digunakan dalam peperangan-peperangan seperti perang dunia II karena sifatnya yang khas yaitu melindungi atau menyembunyikan informasi yang merupakan hal penting dalam sebuah peperangan. Seiring berkembangnya zaman dan teknologi informasi. Kriptografi tidak lagi hanya digunakan dalam peperangan. Semua hal yang berkaitan dengan informasi digital yang ada sekarang hampir semuanya berkaitan dengan kriptografi hal ini karena komputer hanya dapat mengolah suatu informasi dalam bentuk biner. Selain komputer, contoh lain dalam penggunaan ilmu kriptografi adalah pada kartu ATM dan privasi dalam email.

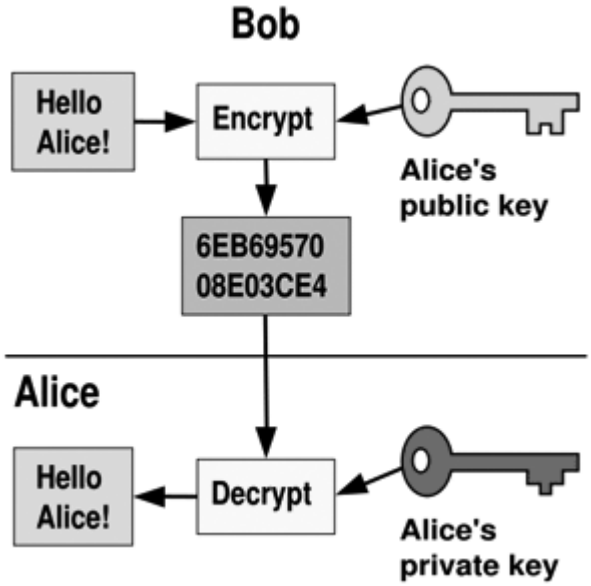
Kriptografi sendiri dibagi menjadi beberapa kategori metode penyusunannya , antara lain : Algoritma kunci simetris, algoritma kunci asimetris, dan fungsi hash. Semuanya memiliki keunggulan, kekurangan, dan karakteristik yang unik yang menjadi ciri khas dari masing-masing metode tersebut sehingga dapat digunakan untuk tujuan yang berbeda-beda sesuai kebutuhan.

Setelah secara umum dijelaskan mengenai kriptografi, sekarang hal lebih lanjut dari kriptografi adalah metode dasar di dalamnya, yaitu enkripsi dan dekripsi, kedua hal inilah yang mendasari adanya kriptografi. Sebuah teks biasa yang biasanya mempunyai istilah plainteks yang akan dijadikan kode akan dienkripsi menjadi sebuah kode yang biasa disebut chiperteks dan chiperteks ini nantinya akan didekripsi agar dapat menjadi sebuah plainteks lagi dan dibaca oleh orang lain. Seperti itulah prinsip dasar dari kriptografi. Dengan kata lain ekripsi adalah sebuah proses yang merubah plainteks menjadi chiperteks dan dekripsi adalah sebuah proses yang mengubah chiperteks menjadi plainteks. Dalam melakukan fungsinya, agar privasi dapat terjaga, proses enkripsi dan dekripsi diberi sebuah kunci agar dapat bekerja, kunci inilah yang mendasari perbedaan antara algoritma kunci simetris dengan algoritma kunci asimetris. Dalam algoritma kunci simetris, kunci yang digunakan pada proses enkripsi sama dengan kunci yang digunakan dalam proses dekripsi dan dalam algoritma kunci asimetris, kunci yang digunakan dalam proses enkripsi dan proses dekripsi adalah dua buah kunci yang berbeda.

Seperti apa yang telah dijelaskan, kunci simetris sifatnya lebih ke public karena si pengirim dan penerima akan sama-sama bisa melihat konten dari informasi yang dienkripsi, berbeda dengan kunci asimetris yang terdapat kunci publik dan kunci pribadi dimana si pengirim memiliki dua buah kunci yang satu untuk mengenkripsi dan yang satu lagi adalah untuk mendekripsi sehingga membuat kunci asimetris memiliki kerahasiaan yang lebih dari kunci simetris dan hal ini sangat berguna di kehidupan sehari-hari yang memanfaatkan sifat tersebut.



Gambar 1.1 Ilustrasi Enkripsi dan Dekripsi



Gambar 1.2 Kunci Asimetris

Gambar 1.1 dan 1.2 memperlihatkan ilustrasi bagaimana kriptografi, enkripsi, dan dekripsi bekerja serta memberikan penjelasan tentang kunci dalam proses tersebut. Setelah membahas mengenai apa itu kriptografi dan jenis-jenisnya dan sebelum masuk ke dalam pembahasan utama mengenai metode AES, hal lain yang perlu diketahui adalah tentang bagaimana AES ini terbentuk.

AES diumumkan pertama kali pada 26 November 2001 oleh Institut Nasional Standard an Teknologi (NIST) yang diperuntukkan sebagai Standar Pemrosesan Informasi Federal (FIPS). Ada 15 desain yang diajukan pada saat itu untuk dikaji dan diperiksa. Algoritma yang terpilih dan cocok dijadikan sebagai standar adalah algoritma Rijndael. Oleh karena itu algoritma Rijndael sekarang lebih dikenal dengan sebutan AES karena sudah ditetapkan sebagai standar ekripsi internasional.

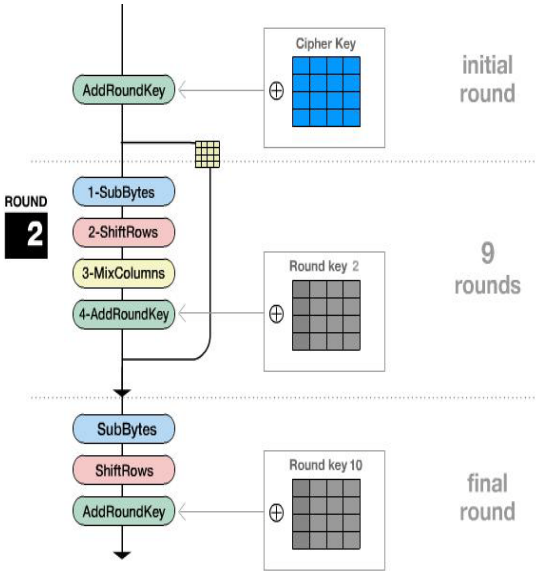
II. METODE

AES adalah sebuah standar enkripsi yang diadopsi oleh Amerika Serikat. Hal ini menjadikan Hal ini membuat algoritma Rijndael lebih spesial karena memiliki kedudukan tersebut. Algoritma ini dipilih bukan karena tanpa alasan, hal ini dikarenakan Rijndael memiliki sebuah metode yang dapat diandalkan serta efektif.

AES memiliki beberapa macam tipe size kunci dan digolongkan menjadi AES-128, AES-192, dan AES-256. Ketiganya memiliki ukuran blok chiper 128 bits dan yang membedakan adalah ukuran kuncinya yaitu 128 bits untuk AES-128, 192 bits untuk AES-192, dan 256 bits untuk AES-256. Blok chiper tersebut dalam pembahasan ini akan diasumsikan sebagai sebuah kotak.

Setiap plainteks akan dikonversikan terlebih dahulu ke dalam blok-blok tersebut dalam bentuk heksadesimal. Barulah kemudian blok itu akan diproses dengan metode yang akan dijelaskan.

Secara umum metode yang digunakan dalam pemrosesan enkripsi dalam algoritma ini dapat dilihat melalui Gambar 2.1.

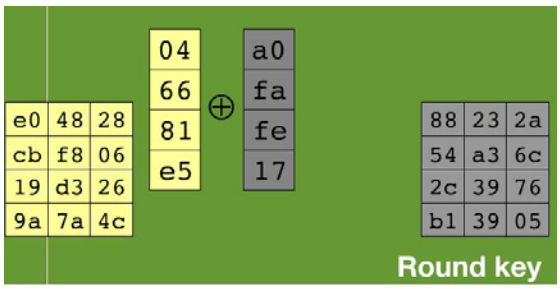


Gambar 2.1 Diagram AES

Terlihat dari Gambar 2.1 terdapat beberapa istilah asing yang perlu dijelaskan agar membuat semuanya lebih terjelaskan. Istilah-istilah tersebut adalah Add Round Key, Sub Bytes, Shift Rows, dan Mix Columns.

A. ADD ROUND KEY

Add Round Key pada dasarnya adalah mengkombinasikan chiper teks yang sudah ada dengan chiper key yang chiper key dengan hubungan XOR. Bagannya bisa dilihat pada gambar 2.1.1.



Gambar 2.1.1 Add Round Key

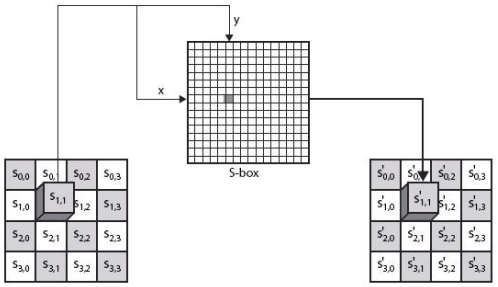
Pada gambar tersebut di sebelah kiri adalah chiper teks dan sebelah kanan adalah round key nya. XOR dilakukan per kolom yaitu kolom-1 chiper teks di XOR dengan kolom-1 round key dan seterusnya.

B. SUB BYTES

Prinsip dari Sub Bytes adalah menukar isi matriks/tabel yang ada dengan matriks/tabel lain yang disebut dengan Rijndael S-Box. Di bawah ini adalah contoh Sub Bytes dan Rijndael 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 2.2.1 Rijndael S-Box

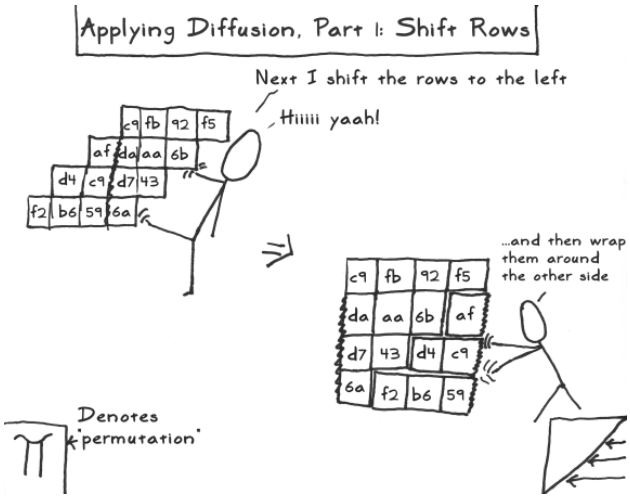


Gambar 2.2.2 Ilustrasi Sub Bytes

Gambar 2.2.1 adalah contoh dari Rijndael S-Box, di sana terdapat nomor kolom dan nomor baris. Seperti yang telah disebutkan sebelumnya, tiap isi kotak dari blok chiper berisi informasi dalam bentuk heksadesimal yang terdiri dari dua digit, bisa angka-angka, angka-huruf, ataupun huruf-angka yang semuanya tercantum dalam Rijndael S-Box. Langkahnya adalah mengambil salah satu isi kotak matriks, mencocokkannya dengan digit kiri sebagai baris dan digit kanan sebagai kolom. Kemudian dengan mengetahui kolom dan baris, kita dapat mengambil sebuah isi tabel dari Rijndael S-Box. Langkah terakhir adalah mengubah keseluruhan blok chiper menjadi blok yang baru yang isinya adalah hasil penukaran semua isi blok dengan isi langkah yang disebutkan sebelumnya.

C. SHIFT ROWS

Shift Rows seperti namanya adalah sebuah proses yang melakukan shift atau pergeseran pada setiap elemen blok/tabel yang dilakukan per barisnya. Yaitu baris pertama tidak dilakukan pergeseran, baris kedua dilakukan pergeseran 1 byte, baris ketiga dilakukan pergeseran 2 byte, dan baris keempat dilakukan pergeseran 3 byte. Pergeseran tersebut terlihat dalam sebuah blok adalah sebuah pergeseran tiap elemen ke kiri tergantung berapa byte tergesernya, tiap pergeseran 1 byte berarti bergeser ke kiri sebanyak satu kali. Ilustrasi dari Tahap ini diperlihatkan oleh gambar di bawah ini.



Gambar 2.3.1 Ilustrasi dari Shift Row

Seperti yang terlihat pada Gambar 2.3.1, tahap shift row sama sekali tidaklah rumit, karena ini adalah proses standar yang hanya berupa pergeseran. Langkah terakhir adalah Mix Column.

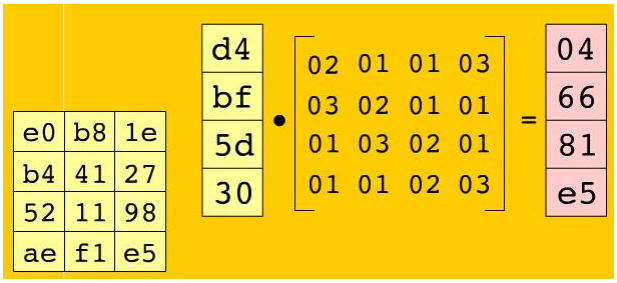
D. MIX COLUMNS

Yang terjadi saat Mix Column adalah mengalikan tiap elemen dari blok chiper dengan matriks yang ditunjukkan oleh Gambar 2.4.1. Tabel sudah ditentukan dan siap pakai. Pengalian dilakukan seperti perkalian matriks biasa yaitu menggunakan dot product lalu perkalian keduanya dimasukkan ke dalam sebuah blok chiper baru. Ilustrasi 2.4.2 akan menjelaskan mengenai bagaimana perkalian ini seharusnya dilakukan. Dengan begitu seluruh rangkaian proses yang terjadi pada AES telah dijelaskan dan selanjutnya adalah menerangkan mengenai penggunaan tiap-tiap proses tersebut.

02	01	01	03

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

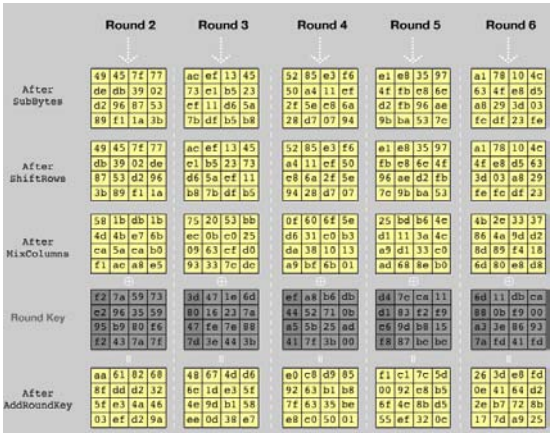
Gambar 2.4.1 Tabel untuk Mix Columns



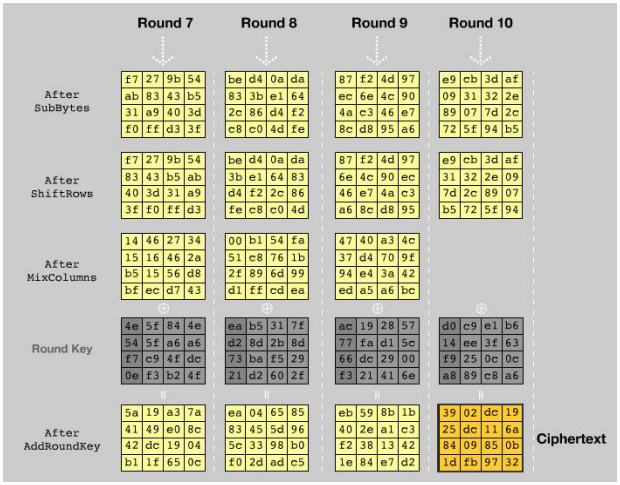
Gambar 2.4.2 Ilustrasi Mix Columns

E. DIAGRAM ALIR AES

Kembali melihat diagram yang ditunjukkan oleh Gambar 2.1. Seperti yang terlihat semua proses yang telah dijelaskan sebelumnya terdapat pada diagram tersebut. Yang artinya adalah mulai dari ronde kedua, dilakukan pengulangan terus menerus dengan rangkaian proses Sub Bytes, Shift Rows, Mix Columns, dan Add Round Key, setelah itu hasil dari ronde tersebut akan digunakan pada ronde berikutnya dengan metode yang sama. Namun pada ronde kesepuluh, Proses Mix Columns tidak dilakukan, dengan kata lain urutan proses yang dilakukan adalah Sub Bytes, Shift Rows, dan Add Round Key, hasil dari Add Round Key inilah yang dijadikan sebagai chiperteks dari AES. Lebih jelasnya bisa dilihat dengan Gambar 2.5.1 dan 2.5.2 yang akan menerangkan mengenai kasus tersebut.



Gambar 2.5.1Ilustrasi Ronde 2 hingga Ronde 6



Gambar 2.5.2 Ilustrasi Ronde 7 hingga Ronde 10

Dengan mengetahui semua proses yang ada pada AES, maka kita dapat menggunakannya dalam berbagai contoh kasus yang muncul di kehidupan sehari-hari.

III. IMPLEMENTASI AES

AES atau algoritma Rijndael sebagai salah satu algoritma yang penting tentu memiliki berbagai kegunaan yang sudah diaplikasikan atau diimplementasikan di kehidupan sehari-hari yang tentu saja membutuhkan suatu perlindungan atau penyembunyian informasi di dalam prosesnya.

Salah satu contoh penggunaan AES adalah pada kompresi 7-Zip. Salah satu proses di dalam 7-Zip adalah mengenkripsi isi dari data dengan menggunakan metode AES-256. Yang kuncinya dihasilkan melalui fungsi Hash. Perpaduan ini membuat suatu informasi yang terlindungi dan tidak mudah rusak terutama oleh virus yang merupakan salah satu musuh besar dalam dunia komputer dan informasi karena sifatnya adalah merusak sebuah data.

Hal yang serupa digunakan pada WinZip sebagai salah satu perangkat lunak yang digunakan untuk melakukan kompresi. Tapi prinsip kompresi pun tidak sama dengan prinsip enkripsi. Karena kompresi adalah mengecilkan ukuran suatu data, biasanya digunakan kode Huffman dalam melakukan hal tersebut.

Contoh penggunaan lain adalah pada perangkat lunak DiskCryptor yang kegunaannya adalah mengenkripsi keseluruhan isi disk/partisi pada sebuah komputer. Metode enkripsi yang ditawarkan adalah menggunakan AES-256, Twofish, atau Serpent.

IV. KESIMPULAN

Algoritma Rijndael yang ditetapkan sebagai AES memiliki karakteristik yang istimewa yang menjadikannya mendapat status tersebut. Dalam hal ini pula maka algoritma ini perlu lah untuk dipelajari karena

penggunaannya di kehidupan sehari-hari sudah sangatlah banyak dan hal ini akan berguna dalam pengembangan dari teknologi kriptografi agar dapat menemukan terobosan-terobosan baru. Tujuan utama dari kriptografi adalah melindungi sebuah informasi, begitu pula dengan AES yang dengan serangkaian tahap atau ronde yang dilakukan dengan menggunakan kunci simetris. Penggunaan AES pun bukan hanya digunakan dalam hal yang sederhana melainkan perannya sangatlah krusial dalam sebuah perangkat lunak ataupun dalam hal lain dimana AES tersebut digunakan.

REFERENSI

[1] Munir, Rinaldi, *Matematika Diskrit (Edisi Ketiga)*, Penerbit Informatika, Bandung, hal. 203-210.

[2] http://www.nonfictioncomics.net/category/technology/page/2/, waktu akses 16 Desember 2010.

[3] http://en.wikipedia.org/wiki/Cryptography , waktu akses 16 Desember 2010.

[4] http://en.wikipedia.org/wiki/Symmetric-key_algorithm , waktu akses 16 Desember 2010.

[5] http://en.wikipedia.org/wiki/Advanced_Encryption_Standard , waktu akses 16 Desember 2010.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 17 Desember 2010

ttd

Hans Agastyra
13509062