Pengamanan Kunci Jawaban Sertifikasi CCNA Menggunakan Advanced Encryption Standard (AES) dan Mode Operasi Cipher Block Chaining

Miko Prasetya Widi, Aisyatul Karima, S.Kom, MCS

Teknik Informatika

Universitas Dian Nuswantoro Semarang

111201005551@mhs.dinus.ac.id, aisyatul.karima@gmail.com

ABSTRAK

Perkembangan teknologi yang semakin pesat dapat membantu pekerjaan dapat diselesaikan dengan cepat dan efisien. Namun tidak semua dengan kecanggihan teknologi sekarang ini memberikan dampak positif bagi pengguna. Dampak negatif yang bisa terjadi adalah masalah keamanan data, pesan, ataupun informasi. Untuk mengurangi atau mencegah tindakan tersebut dibutuhkan metode keamanan data atau lebih dikenal dengan istilah kriptografi. Kriptografi mendukung kebutuhan untuk menjaga aspek keamanan seperti integritas data, keaslian entitas dan keaslian data. Dalam kriptografi mengenal beberapa teknik dalam pengamanan data, namun dalam penelitian ini kriptografi yang digunakan adalah Algoritma AES dan mode operasi CBC. Kedua metode ini dipilih karena menggunakan cukup banyak kunci dalam enkripsi dan dekripsi. Dengan banyaknya kunci yang digunakan akan memperkuat algoritma kriptografi dan dapat menambah kesulitan bagi kriptanalis dalam memecahkan hasil enkripsi tersebut. Salah satu dokumen yang perlu diperhatikan adalah pada sertifikasi CCNA. CCNA merupakan sertifikasi dalam bidang Computer Networking. Dalam hal ini banyak kunci jawaban yang tersebar di media untuk tiap-tiap chapter yang diberikan, dengan demikian dikhawatirkan akan mempermudah peserta untuk mencari jawaban tanpa harus berfikir lebih untuk menyelesaikan soal yang diujikan dan hal ini akan mengurangi kualitas dari pemegang sertifikasi itu sendiri dalam hal pengetahuan tentang mengoperasikan dan memecahkan permasalahan.

Kata kunci : Kriptografi, Algoritma AES, Mode Operasi CBC, CCNA.
xiv + 70 halaman + 23 gambar + 4 tabel + 2 lampiran

I. PENDAHULUAN

A. Latar Belakang

Seiring dengan perkembangan teknologi komputer, banyak pekerjaan dapat diselesaikan dengan cepat dan efisien. Namun tidak semua dengan kecanggihan teknologi sekarang ini memberikan dampak positif bagi pengguna. Dampak negatif yang bisa terjadi adalah penyadapan dan pencurian data. Di dalam dunia informasi terdapat data-data yang berisi informasi yang tidak terlalu penting jadi tidak terlalu

masalah jika diketahui oleh publik, akan tetapi apabila data itu milik pemerintah ataupun militer dan itu bersifat rahasia. Kerahasiaan dan keamanan data adalah hal penting dalam hal ini. Untuk dapat menjaga keamanan dan kerahasiaan data, maka dapat dilakukan teknik enkripsi guna untuk penyembunyian pesan, Teknik pengamanan data tersebut dikenal dengan istilah kriptografi.

Kriptografi merupakan ilmu dan seni untuk menjaga suatu pesan atau data informasi agar data tersebut aman.Kriptografi mendukung kebutuhan untuk menjaga aspek keamanan suatu informasi seperti integritas data, keaslian entitas dan keaslian data. Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain[1]. Metode pengamanan informasi dengan menggunakan kriptografi melalui enkripsi ini akan penulis terapkan dalam pengamanan kunci jawaban sertifikasi CCNA..

CCNA (Cisco Certified Network Associate) adalah sertifikasi di bidang Computer Networking (level II). Sertifikat ini dikeluarkan oleh perusahaan Cisco Systems. Untuk mendapatkan sertifikasi ini harus melewati beberapa soal dari tiap-tiap chapter yang diberikan. Dalam hal ini banyak kunci-kunci jawaban yang tersebar di media sehingga dikhawatirkan akan mempermudah peserta untuk mencari jawaban tanpa harus berfikir lebih untuk menyelesaikan soal yang ujikan. Untuk mengatasi hal seperti ini teknik enkripsi diperlukan untuk melindungi data (kunci jawaban) dari pihak yang ingin melakukan jalan pintas dalam memperoleh kunci jawaban, selain itu seandainya ada data yang diunggah agar lebih ter-protect sehingga susah untuk membukanya. Hal ini dimaksudkan agar pemegang sertifikasi benar-benar menyelesaikan dengan kemampuan sendiri sehingga kelak menghasilkan kemampuan yang sudah teruji tentang pengetahuan dalam mengoperasikan dan memecahkan permasalahan khususnya dalam bidang networking.

Dalam kriptografi, ada berbagai algoritma kriptografi yang sudah banyak diciptakan, namun dalam penelitian akan menggunakan dua metode yaitu Algoritma AES (*Advanced Encryption Standard*) dan mode operasi CBC (*Cipher Block Chaining*), ini dilakukan karena dengan menggunakan dua metode akan menggunakan cukup banyak kunci, pada CBC mempunyai dua kunci yaitu IV dan kunci CBC itu sendiri, sedangkan pada AES menggunakan satu kunci. Dengan cukup banyak kunci yang digunakan akan memperkuat algoritma kriptografi dan dapat menambah kesulitan bagi kriptanalis dalam memecahkan hasil enkripsi.

B. Rumusan Masalah

Dari masalah yang telah dipaparkan, maka rumusan masalah yang mendasari penelitian ini adalah:

1. Bagaimana menjaga keamanan kunci jawaban sertifikasi CCNA yang tersebar di media?
2. Bagaimana mengembalikan data yang telah dienkripsi menjadi file asli?

C. Batasan Masalah

Adapun dalam menyelesaikan permasalahan diatas akan dibatasi sebagai berikut:

1. Algoritma yang dipakai adalah Advanced Encription Standard (AES) 128 bit.
2. Menggunakan mode Cipher Block Chaining (CBC).
3. Enkripsi dan dekripsi hanya dilakukan untuk file berekstensi .txt.
4. Panjang IV pada proses CBC yang digunakan adalah 8 bit.
5. Panjang kunci AES yang digunakan 128 bit.
6. MenggunakanVisual Basic sebagai tool untuk implementasi algoritma AES dan mode operasi CBC.

D. Tujuan

Tujuan yang akan dalam penelitian ini adalah:

1. Mengimplementasikan algoritma AES, dan mode operasi CBC untuk memperkuat algoritma dalam pengamanan kunci jawaban sertifikasi CCNA yang tersebar di media.
2. Mendekripsikan pesan yang telah dienkripsi menggunakan algoritma AES dan mode operasi CBC.

II. TINJAUAN PUSTAKA

A. Tinjauan Studi

Ada beberapa penelitian terkait dengan metode keamanan data pada kriptografi, diantaranya adalah penelitian oleh Deni Rosmala dan Riki Aprian pada tahun 2012tentang Implementasi Mode Operasi CBC pada Pengamanan Data [3]. Hasil pengujian yang dilakukan pada data teks dapat merahasiakan data menjadi cipherteks sehingga data tidak dapat dimengerti. Sedangkan pada file gambar setelah dienkripsi file tidak dapat dibuka karena datanya telah rusak. Pada file PDF setelah dienkripsi menampilkan pesan error karena datanya dianggap corrupt. Dengan mode ini setiap blok cipherteks bergantung tidak hanya pada blok plainteksnya tetapi juga pada seluruh blok plainteks sebelumnya.

Penelitian oleh R. Kristoforus dan Stefanus Aditya pada tahun 2012 tentang implementasi algoritma Rijndael untuk enkripsi dan dekripsi pada citra digital[4]. Pengujian dilakukan pada file citra digital dengan kedalaman warna 24 bit. Hasil dari proses enkripsi yang diperoleh masih terlihat kemiripan dengan citra asli. Hal ini disebabkan karena citra yang diuji didominasi oleh warna tunggal. Untuk hasil dari kecepatan proses enkripsi, semakin panjang kunci yang digunakan, maka waktu proses semakin lama.

Penelitian oleh Soni Harza Putra, Edy Santoso, S.Si., M.Kom. dan Lailil Muflikhah, S.Kom., M.Sc. pada tahun 2013 tentang Implementasi Algoritma Kriptografi AES pada Kompresi Data Teks[5]. Proses kompresi dilakukan pada Header file terkompresi saja. Hal ini dilakukan agar proses kriptografi dapat lebih efisien dalam memberikan pengamanan pada hasil kompresi. Hasil penelitian menunjukkan bahwa algoritma AES 128 bit dapat menyandikan isi header dari file terkompresi sehingga dapat mengamankan file tersebut. Sementara rasio hasil kompresi pada kompresi yang mengimplementasikan metode kriptografi AES menjadi sistem terpadu adalah sebesar 41,80% untuk file uji *.txt dan 25,09% untuk file uji *.htm

B. Landasan Teori

Ancaman Keamanan

Fungsi keamanan komputer adalah menjaga tiga karakteristik, yaitu:

1. Secrecy, adalah isi dari program komputer hanya dapat diakses oleh orang yang berhak. Tipe yang termasuk di sini adalah reading, viewing, printing, atau hanya yang mengetahui keberadaan sebuah objek.
2. Integrity, adalah isi dari komputer yang dapat dimodifikasi oleh orang yang berhak, yang termasuk disini adalah writing, changing status, deleting, dan creating.
3. Availability, adalah isi dari komputer yang tersedia untuk beberapa kelompok yang diberi hak. Data yang aman adalah data yang memenuhi ketiga karakteristik keamanan data tersebut.

Kriptografi

Kriptografi berasal dari bahasa Yunani, crypto dan graphia. Crypto berarti secret (rahasia) dan graphia berarti writing (tulisan). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain[7].

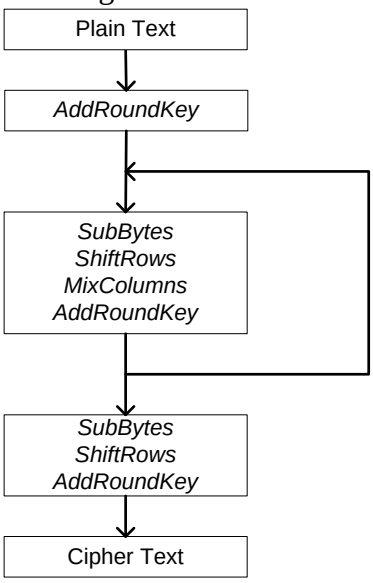
Kriptografi bertujuan untuk member layanan keamanan. Aspek-aspek keamanan dalam kriptografi adalah kerahasiaan (*confidentiality*), integritas data (*data integrity*), Otentikasi (*authentication*), dan nir-penyangkalan (*non-repudiation*)[8].

Algoritma AES

Algoritma AES (*Advanced Encryption Standard*) ditemukan oleh Vincent Rijnmen dan Joan Daeman dar Belgia. AES sendiri dipilih jadi pemenang bukan karena algoritma paling aman, namun karena memiliki keseimbangan antara keamanan dan fleksibilitas dalam berbagai paltform software dan hardware [9]. AES mempunyai panjang kunci yang bervariasi, yaitu 128 bit, 192 bit, dan 256 bit. Pemilihan ukuran blok data dan kunci akan menentukan jumlah proses yang harus dilalui untuk proses enkripsi dan dekripsi.

Enkripsi Algoritma AES

Proses enkripsi pada algoritma AES terdiri dari 4 jenis transformasi bytes, yaitu *SubBytes, ShiftRows, Mixcolumns,* dan *AddRoundKey.* Pada awal proses enkripsi, input yang telah dikopikan ke dalam state akan mengalami transformasi byte *AddRoundKey*. Setelah itu, state akan mengalami transformasi *SubBytes, ShiftRows, MixColumns*, dan *AddRoundKey* secara berulang-ulang sebanyak *Nr*. Proses ini dalam algoritma AES disebut sebagai round function. Round yang terakhir agak berbeda dengan round-round sebelumnya dimana pada round terakhir, state tidak mengalami transformasi *MixColumns*[10].



Gambar 1. Diagram Alir Proses Enkripsi

SubBytes

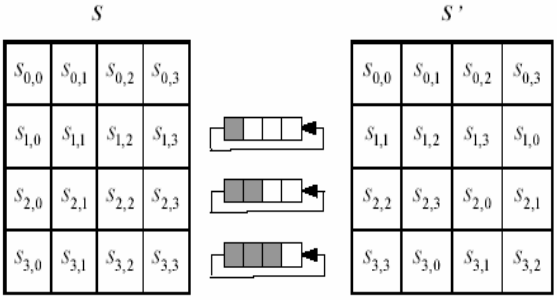
SubBytes merupakan transformasi byte dimana setiap elemen pada state akan dipetakan dengan menggunakan sebuah tabel substitusi (S-Box).

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. Tabel S-Box

ShiftRows

Transformasi Shiftrows pada dasarnya adalah proses pergeseran bit dimana bit paling kiri akan dipindahkan menjadi bit paling kanan (rotasi bit).transformasi ini diterapkan pada baris 2, baris 3, dan baris4. Baris 2 akan mengalami pergeseran bit sebanyak satukali, sedangkan baris 3 dan baris 4 masing-masingmengalami pergeseran bit sebanyak dua kali dan tiga kali.



Gambar 4. Transformasi ShiftRows

MixColumns

MixColumns mengoperasikan setiap elemen yang berada dalam satu kolom pada state.

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix}$$

Melakukan proses penambahan pada operasi ini berarti melakukan operasi bitwise XOR. Maka hasil dari perkalian matriks diatas dapat dianggap seperti perkalian yang ada di bawah ini :

$$s'_{0,c} = (\{02\} \bullet s_{o,c}) \oplus (\{03\} \bullet s_{1,c}) \oplus s_{2,c} \oplus s_{3,c}$$

$$s'_{1,c} = s_{0,c} \oplus (\{02\} \bullet s_{1,c}) \oplus (\{03\} \bullet s_{2,c}) \oplus s_{3,c}$$

$$s'_{2,c} = s_{0,c} \oplus s_{1,c} \oplus (\{02\} \bullet s_{2,c}) \oplus (\{03\} \bullet s_{3,c})$$

$$s'_{3,c} = (\{03\} \bullet s_{0,c}) \oplus s_{1,c} \oplus s_{2,c} \oplus (\{02\} \bullet s_{3,c})$$

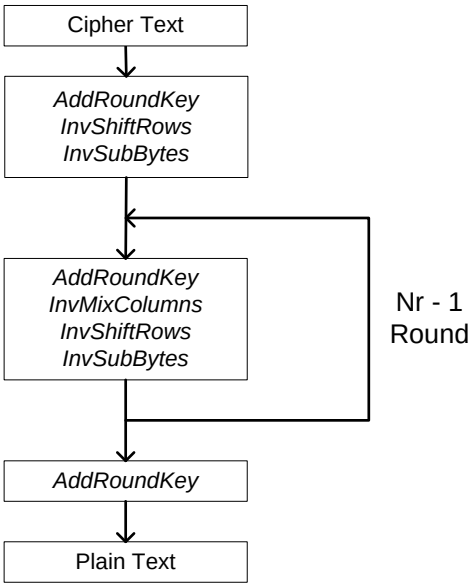
AddRoundKey

Pada proses enkripsi dan dekripsi AES proses AddRoundKey sama, sebuah round key ditambahkan pada state dengan operasi XOR. Setiap round key terdiri dari Nb word dimana tiap word tersebut akan dijumlahkan

dengan word atau kolom yang bersesuaian dari state.

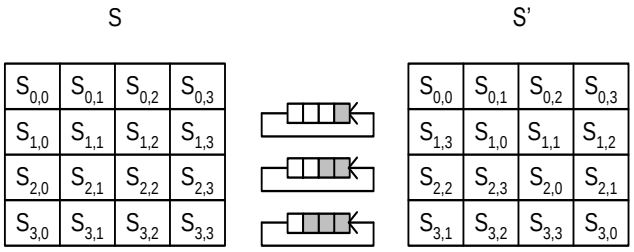
Dekripsi Algoritma AES

Pada dasarnya proses dekripsi algoritma AES merupakan kebalikan dari proses enkripsi. Transformasi cipher dapat dibalikkan dan diimplementasikan dalam arah yang berlawanan untuk menghasilkan inverse cipher yang mudah dipahami untuk algoritma AES. Transformasi byte yang digunakan pada invers cipher adalah InvShiftRows, InvSubBytes, InvMixColumns, dan AddRoundKey[7].



Gambar 5. Diagram Alir Proses Dekripsi

InvShiftRows



Gambar 6. Transformasi InvShiftRows

InvSubBytes

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 7. Tabel Invers S-Box

InvMixColumns

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix}$$

Hasil dari perkalian dalam matriksadalah :

$$s'_{0,c} = (\{0E\} \bullet s_{o,c}) \oplus (\{0B\} \bullet s_{1,c}) \oplus (\{0D\} \bullet s_{2,c}) \oplus (\{09\} \bullet s_{3,c})$$

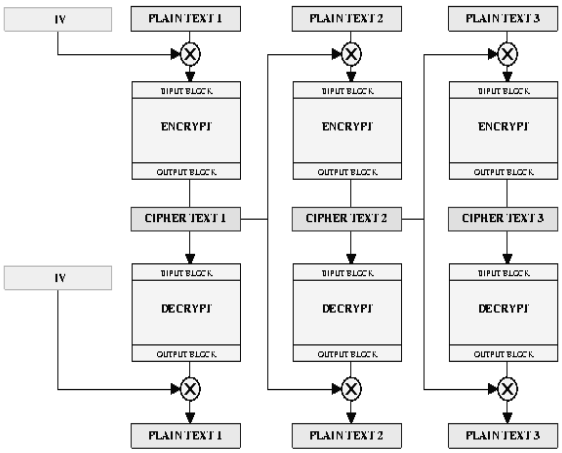
$$s'_{1,c} = (\{09\} \bullet s_{o,c}) \oplus (\{0E\} \bullet s_{1,c}) \oplus (\{0B\} \bullet s_{2,c}) \oplus (\{0D\} \bullet s_{3,c})$$

$$s'_{2,c} = (\{0D\} \bullet s_{o,c}) \oplus (\{09\} \bullet s_{1,c}) \oplus (\{0E\} \bullet s_{2,c}) \oplus (\{0B\} \bullet s_{3,c})$$

$$s'_{3,c} = (\{0B\} \bullet s_{o,c}) \oplus (\{0D\} \bullet s_{1,c}) \oplus (\{09\} \bullet s_{2,c}) \oplus (\{0E\} \bullet s_{3,c})$$

Mode Operasi CBC

Mode (*Cipher Block Chainning*) adalah plaintext yang sama akan di enkripsi ke dalam bentuk cipher yang berbeda, disebabkan blok cipher yang satu tidak berhubungan dengan blok cipher yang lain. Melainkan tergantung pada cipher yang sebelumnya. CBC menggunakan operasi umpan balik atau dikenal dengan operasi berantai (chaining). Hasil enkripsi dari blok sebelumnya adalah feedback untuk enkripsi dan dekripsi pada blok berikutnya. Dengan kata lain, setiap blok ciphertext dipakai untuk memodifikasi proses enkripsi dan dekripsi pada blok berikutnya.



Gambar 8. Mode Operasi CBC

Pada CBC diperlukan data acak sebagai blok pertama untuk enkripsi. Blok data acak ini sering disebut initialization vector atau IV. IV dapat diberikan oleh pengguna atau dibangkitkan secara acak oleh program. Untuk menghasilkan blok cipher pertama, IV digunakan untuk menggantikan blok cipherteks sebelumnya. Sebaliknya pada dekripsi, blok plainteks pertama diperoleh dengan cara meng- XOR-kan IV dengan hasil dekripsi terhadap blok cipherteks pertama[8].

BAB III
METODE PENELITIAN

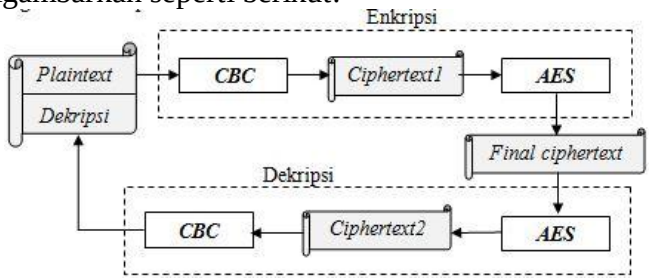
A. Pengumpulan Data

Dalam penelitian ini penulis menggunakan beberapa metode untuk memperoleh data dan informasi dalam menyelesaikan permasalahan. Adapun metode yang dilakukan adalah :

1. Studi pustaka
   Melalui metode ini penulis memperoleh data ataupun informasi dengan mengumpulkan, mempelajari dan membaca referensi baik dari buku, jurnal, makalah, internet dan berbagai sumber lainnya yang berkaitan dengan penelitian yang dibuat.
2. Eksperimen
   Setelah mendapatkan data secara studi pustaka, penulis melakukan eksperimen atau percobaan. Dalam eksperimen ini pengumpulan data dapat diambil secara langsung, sehingga penulis akan lebih mendalami dalam melakukan penelitian.

B. Metode yang diusulkan

Dalam penelitian yang digunakan untuk menyelesaian permasalahan yang ada dalam penelitian adalah menggunakan model seperti digambarkan seperti berikut:



Gambar 9. Metode yang diusulkan

BAB IV
ANALISIS HASIL PENELITIAN DAN PEMBAHASAN

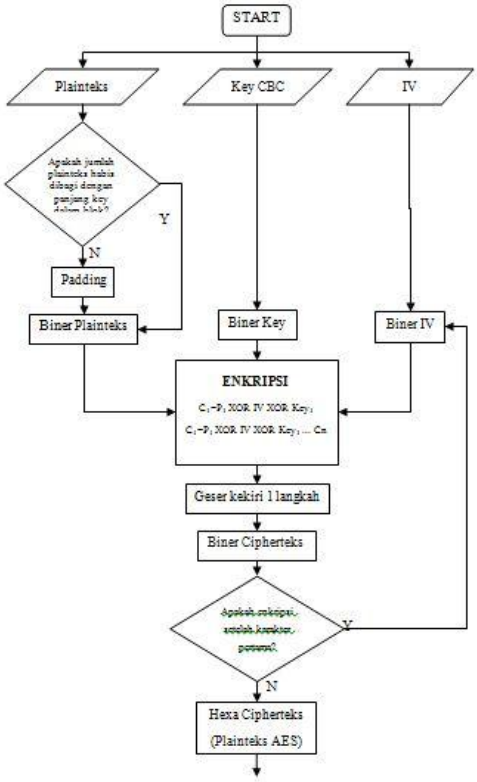
A. Desain Program

Proses enkripsi akan dimulai dari CBC kemudian diteruskan menggunakan algortima AES, sebaliknya untuk mendekripsikan kembali dari hasil enkripsi, proses akan dimulai dari algoritma AES dilanjutkan pada proses CBC.

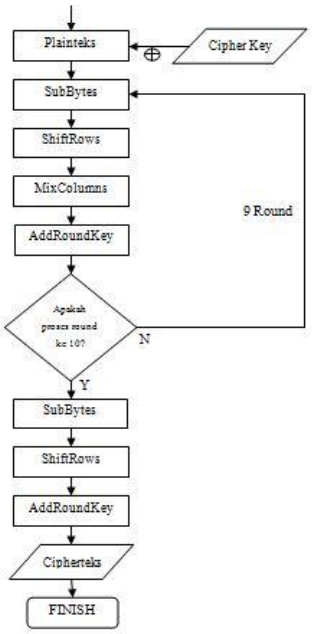
Untuk masing-masing algoritma mempunyai cara yang berbeda dalam mengenkripsi maupun mendekripsi. Pada mode CBC menggunakan setidaknya dua kunci, dimana kunci pertama disebut dengan Initial Vector (IV) yang akandigunakan untuk perhitungan byte pertama pada proses enkripsi yang selanjutnya hasil perhitungan tersebut akan di XOR-kan kembali dengan kunci yang telah ditetapkan. Sebaliknya pada dekripsi IV dilakukan pada proses yang terakhir.

Dibawah ini akan dijelaskan dengan flowchart bagaimana proses enkripsi berjalan:

Proses enkripsi CBC :

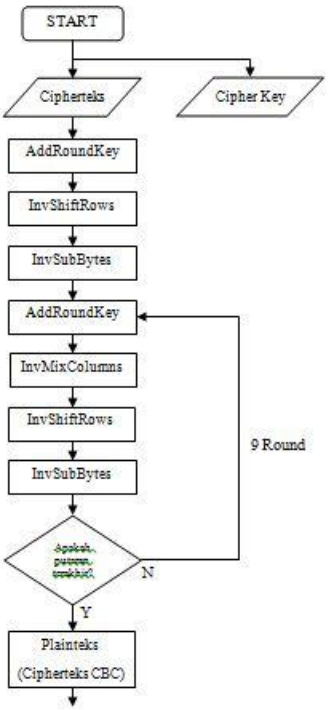


Proses enkripsi algoritma AES :

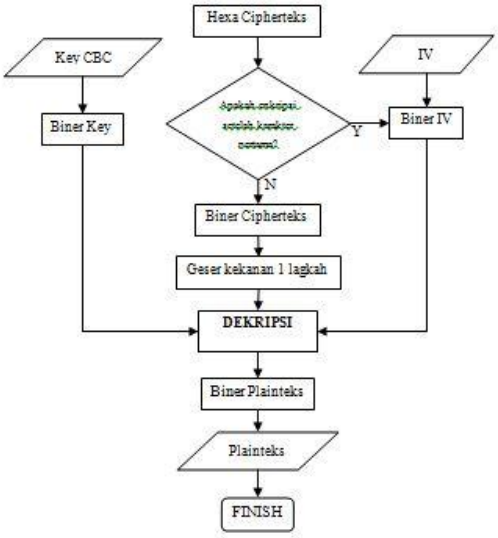


Dibawah ini adalah flowchart proses dekripsi berjalan :

Proses dekripsi algoritma AES :



Proses dekripsi pada CBC :



B. Simulasi enkripsi dan dekripsi

Eksperimen dilakukan dengan pesan sebagai berikut :

Plainteks : FIKDINUSSEMARANG
IV : x
Key CBC : 2010
Key AES : MikoPrasetyaWidi

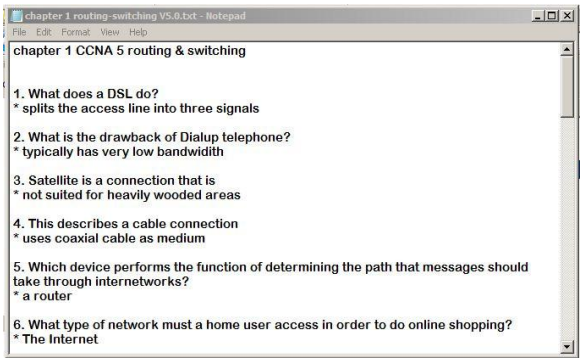
	F	I	K	D
Plainteks	01000110	01001001	01001011	01000100
IV	01111000	00011000	11000010	01110001
	00111110	01010001	10001001	00110101
Key	00110010	00110000	00110001	00110000
	00001100	01100001	10111000	00000101
wrapping	00011000	11000010	01110001	00001010
	18	**C2**	**71**	**0A**
	I	**N**	**U**	**S**
	01001001	01001110	01010101	01010011
	00001010	11100010	00111001	10111010
	01000011	10101100	01101100	11101001
	00110010	00110000	00110001	00110000
	01110001	10011100	01011101	11011001
	11100010	00111001	10111010	10110011
	E2	**39**	**BA**	**B3**
	S	**E**	**M**	**A**
	01010011	01000101	01001101	01000001
	10110011	10100101	10100001	10111011
	11100000	11100000	11101100	11111010
	00110010	00110000	00110001	00110000
	11010010	11010000	11011101	11001010
	10100101	10100001	10111011	10010101
	A5	**A1**	**BB**	**95**
	R	**A**	**N**	**G**
	01010010	01000001	01001110	01000111
	10010101	11101011	00110101	10010100
	11000111	10101010	01111011	11010011
	00110010	00110000	00110001	00110000
	11110101	10011010	01001010	11100011
	11101011	00110101	10010100	11000111
	EB	**35**	**94**	**C7**

Selanjutnya hasil enkripsi CBC diproses kembali pada algoritma AES untuk dijadikan plainteks, dengan Key AES dalam hexa : 4D 69 6B 6F 50 72 61 73 65 74 79 61 57 69 64 69.

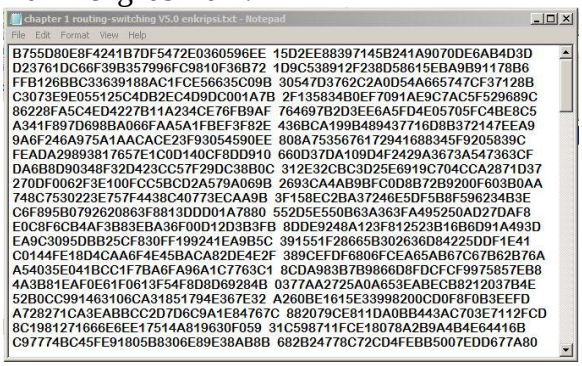
Dalam algoritma AES input dan output menggunaka hexa, untuk AES 128 proses enkripsi berlangsung sebanyak 10 kali putaran (*round*) yang meliputi proses *SubBytes, ShiftRows, Mixcolumns,* dan *AddRoundKey* kecuali pada *round* terakhir yang tidak melalui proses *Mixcolumn*. Hasil akhir proses enkripsi CBC dan AES dengan pesan diatas menghasilkan output :
B0 FB E9 8D 55 CE 52 EC 13 2C 9A 87 75 55 60 8A.

C. Pengujian pada file .txt

Berikut akan dilakukan proses enkripsi pada file "chapter 1 routing-switching V5.0.txt" dengan menggunakan Key CBC yaitu "2010", dengan IV "x" dan Key "MikoPrasetyaWidi" untuk algoritma AES. Dan hasil akhir dari output yang dihasilkan seperti pada file "chapter 1 routing-switching V5.0 enkripsi.txt".



Dan menghasilkan :



D. Penggunaan Key CBC, IV dan Key AES

Dalam proses enkripsi dan dekripsi pada proses CBC mengguakan panjang kunci bebas, panjang kunci yang digunakan menentukan banyaknya pula blok pada sebuah plainteks.

Untuk IV mengunakan 1 karakter saja (8bit), hal ini dimaksudkan agar proses enkripsi per karakter lebih bervariasi, kerena hasil perhitungan IV pada karakter pertama akan digunakan untuk proses selanjutnya sehingga setiap karakter yang akan dienkripsi akan mempunyai IV yang berbeda.

Penggunaan Key pada algoritma AES menggunakan kunci tidak lebih dan tidak kurang sepanjang 16 karakter, karena dalam penyusunan tugas akhir ini algoritma AES yang digunakan adalah 128 bit.

BAB V
KESIMPULAN DAN SARAN

Kesimpulan

Dari hasil perancangan dan pembuatan program aplikasi dengan menggabungkan dua metode yaitu algoritma AES dan mode operasi CBC ini, maka dapat diambil kesimpulan sebagai berikut :

1. Dalam implementasi, algoritma AES dapat digabungkan dengan mode operasi CBC dalam pengamanan kunci jawaban sertifikasi CCNA.

2. Program dapat berjalan dengan baik dalam mengenkripsi dan mendekripsikan kembali file berekstensi .txt.
3. CBC dapat dijadikan sebagai kunci AES sehingga dapat menambah variasi kunci yang acak, dimana kunci yang acak dapat memperkuat algoritma kriptografi.
4. Banyaknya kunci yang digunakan dapat menambah kesulitan bagi kriptanalis sehingga akan merepotkan untuk memecahkan hasil enkripsi.
5. Dengan terlalu banyak menggunakan kunci, maka diperlukan daya ingat yang kuat.
6. Panjang plainteks CBC menyesuaikan panjang plainteks AES dalam proses enkripsi/dekripsi, sehingga jika isi dari blok CBC kurang memenihi maka perlu dilakukan padding.

DAFTAR PUSTAKA

[1] Dony Ariyus, *Pengantar Ilmu Kriptografi Teori, Analisis dan Implementasi*. Yogyakarta: Andi, 2008.

[2] Dony Ariyus, *Kriptografi Keamanan Data dan Komunikasi*. Yogyakarta: Graha Ilmu, 2006.

[3] Doni Rosmala and Rika Aprian, "Implementasi Mode Operasi CBC pada Pengamanan Data," *Informatika*, vol. 3, p. 2, Mei - Agustus 2012.

[4] R. Kristoforus and Stefanus Aditya, "Implementasi Algoritma Rijndael untuk Enkripsi dan Dekripsi pada Citra Digital," Sekolah Tinggi Teknik Musi, Yogyakarta, Juni 2012.

[5] Soni Harza Putra, S.Si., M.Kom, Edy Santoso S.Kom., M.Sc, and Lailil Muflikah, "Implementasi Algoritma Kriptografi AES pada Kompresi Data Teks," Universitas Brawijaya Malang, Malang, 2013.

[6] I Putu Heryawan, *Keamanan Data*. Bali, 2010.

[7] Dony Ariyus, *Kriptografi Keamanan Data dan Komunikasi*. Yogyakarta: Andi Offset, 2005.

[8] Rinaldi Munir, *Kriptografi*. Bandung: Informatika Bandung, 2006.

[9] Yusuf Kurniawan, *Kriptografi Keamanan Internet dan Jaringan Komunikasi*. Bandung: Informatika Bandung, 2004.

[10] Wihartantyo Ari Wibowo, *ADVANCED ENCRYPTION STANDARD, ALGORITMA RIJNDAEL*. Bandung: Departemen Teknik Elektro ITB, 2004.