Perbandingan Algortima Stream Cipher RC4 dan Block Cipher AES dengan Mode CBC untuk Penyembunyian Data pada File Log

M. Rian Fakhrusy / 13511008
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
rian.fakhrusy@students.itb.ac.id

***Abstract*—Pada makalah ini, akan dibandingkan implementasi algortima stream cipher RC4 dengan algoritma blcok cipher AES dengan mode CBC pada file log. RC4 menggunakan aliran bit yang dibentuk dari umpan kunci masukan sehingga cocok dengan karakteristik file log yang besarnya terus bertambah. AES dengan mode CBC menggunakan block sebelumnya untuk melakukan enkripsi sehingga cocok untuk karakteristik file log yang teks masukannya serupa untuk tiap kali masukan. Pengujian dilakukan dengan membandingkan waktu enkripsi dan deskripsi serta analisis terhadap cipher text.**

***Index Terms*—AES, Block Cipher, File Log, RC4, Stream Cipher.**

I. PENDAHULUAN

File log banyak digunakan pada berbagai aplikasi dalam keseharian. Contoh penggunaan file log pada aplikasi adalah log sistem operasi, catatan operasi server, catatan perubahan data, catatan kompilasi program dan berbagai keperluan pencatatan lainnya. Log file ini biasanya digunakan untuk melakukan analisa terhadap aktivitas.

Namun, terkadang ada file log yang berisi informasi sensitif. Informasi ini tidak diinginkan untuk dapat dimengerti oleh pihak tertentu meskipun mereka bisa membacanya. Oleh karena itu, ingin digunakan teknik kriptografi untuk penyembuyian data pada file log tersebut.

Algoritma RC4 dan AES dengan mode CBC adalah algortima yang diharapkan dapat menyembuyikan file log tersebut dengan baik. Algortima RC4 yang menggunakan aliran bit dalam proses enkripsi dan tidak menggunakan bit padding akan dibandingkan dengan algortima AES dengan mode CBC yang dapat menyembunyikan text masukann yang mirip dengan baik, jika kedua algortima tersebut digunakan dalam penyembunyian file log.

II. DASAR TEORI

A.RC4

RC4 termasuk dalam salah satu algoritma kriptografi stream cipher yang banyak digunakan pada protokol internet. Algortima ini didesain oleh Ron Rivest pada tahun 1987.

Dalam melakukan enkripsi dan deskripsi, algortima ini mengambil kunci masukan pengguna sebagai umpan untuk membangkitkan stream bit yang kemudian dilakukan operasi x-or dengan plain text.

Aliran kunci dibentuk dari permutasi angka 0-255 pada S0, S1...S255 yang diinisialisasi dengan algortima

```
for i = 0 to 255 do S[i] = i;
```

Lalu permutasi keystream dibuat dengan algoritma :

```
i, j = 0;
while (true)
i = (i + 1) mod 256;
j = (j + S[i]) mod 256;
Swap (S[i], S[j]);
```

Apabila panjang kunci kurang dari 256 akan dilakukan bit padding dengan perulangan masukan kunci.

B.AES mode CBC

AES adalah algortima kriptografi yang dibuat untuk menggantikan DES yang dianggap sudah tidak aman. Nama asli algoritma ini adalah Rijndael yang menjadi pemenang sayembara algoritma kriptografi baru yang diadakan NIST. AES dibuat dengan menggabungkan teknik SubByte, ShiftRow, MixColumn dan AddRoundKey disertai optimasi serta beberapa ronde putaran. Enkripsi AES cepat dan fleksible. Cara untuk membongkar algoritma ini adalah dengan melakukan serangat bruteforce yang memakan waktu lama.

CBC adalah mode yang menggunakan ketergantungan antarblok dalam enkripsinya. Hasil enkripsi menggunakan block terakhir sebagai umpan untuk enkripsi blok yang akan dienkripsi selanjutnya. Enkripsi blok pertama memerlukan IV (Initialization Value) yang dibentuk dari masukan kunci pengguna.

C.File Log

File log adalah catatan kumpulan aksi yang dilakukan oleh perangkat lunak. Contohnya pada web server yang mencatat request yang masuk untuk melakukan analisa.

Analisa yang dilakukan misalnya terhadap lokasi asal pengunjung yang melakukan akses ke server tersebut.

III. PERSIAPAN IMPLEMENTASI

A.Desain Metode

Terdapat kelemahan yang cukup besar jika enkripsi data dilakukan dengan cara seperti biasa yaitu dengan enkripsi tiap baris secara sendiri-sendiri lalu disambungkan ke akhir dari file log. Dengan menggunakan cara ini, masukan yang memiliki plain text yang mirip akan memiliki cipher text yang serupa pula jika menggunakan kunci yang sama. Contoh berikut akan mengilustrasikan kelemahan tersebut:

Algortima : RC4
Kunci : himalaya
Entri pertama (menekan tombol add):
Plain text : Tombol 'add' ditekan oleh pengguna
Cipher text (dalam hexadecimal) :
4795E635C5B440AA050F61B6E14BAABC7A55388C7
E3AB29483FB180B4F765AFB8103
Entri Kedua (menekan tombol edit) :
Plain text :
Tombol 'add' ditekan oleh pengguna
Tombol 'edit' ditekan oleh pengguna
Cipher text :
4795E635C5B440AA050F61B6E14BAABC7A55388C7
E3AB29483FB180B4F765AFB8103
4795E635C5B440AA010F6CE5E60FA7A16B5B328330
75B19D8EB3481E447F5AE99A0C5C

Algortima : AES mode CBC
Kunci :
0x00,0x01,0x02,0x03,0x04,0x05,0x06,0x07,0x08,0x09,
0x00,0x01,0x02,0x03,0x04,0x05
Entri pertama :
Plain text : Tombol 'add' ditekan oleh pengguna
Cipher text (dalam hexadecimal) :
B63F0462A8D069C8FDD2880FC5913573145BF82390
D066D9C44C48F8933889E76C5C00CB76A7B3AEA8D
02AAC31152E3B
Entri Kedua :
Plain text :
Tombol 'add' ditekan oleh pengguna
Tombol 'edit' ditekan oleh pengguna
Tombol 'add' ditekan oleh pengguna
Cipher text :
B63F0462A8D069C8FDD2880FC5913573145BF82390
D066D9C44C48F8933889E76C5C00CB76A7B3AEA8D
02AAC31152E3B
33EFA936610FE158CC0E98CDBC34A6A569B53303C
071C355BD2349571BBC8FF60C6FFDC3C991E9530B3
8B0E0EF374DC3
B63F0462A8D069C8FDD2880FC5913573145BF82390
D066D9C44C48F8933889E76C5C00CB76A7B3AEA8D
02AAC31152E3B

Kelemahan yang terdapat jika menggunakan algoritma RC4 adalah cipher text yang mirip untuk plain text yang mirip sehingga lebih rawan terhadap serangan. Sementara untuk algoritma AES dengan metode CBC, plain text yang sama akan selalu menghasilkan cipher text sama sehingga dapat dilihat pola perulangan pada file log tersebut walaupun tidak diketahui operasi apa yang diulang. Namun hal ini tidak terjadi jika tiap kali masukan file log memiliki input plain text yang berbeda.

Kelemahan yang terlihat pada ciphertext algoritma RC4 ini, terjadi karena menggunakan keystream yang sama dari kunci yang sama untuk melakukan enkripsi. Untuk memperbaiki kelemahan pada RC4 ini, akan digunakan keystream lanjutan dari keystream pada entri pertama. Contohnya jika pada input text pertama keystream yang digunakan adalah stream ke 1 sampai stream ke 112, maka input selanjutnya akan menggunakan stream ke 113.

Kelemahan pada ciphertext algortima AES mode CBC diatasi dengan menyimpan IV pada blok terakhir untuk melakukan deskripsi blok terakhir saja (karena ada bit padding) lalu melanjutkan enkripsi dimulai dari block terakhir yang disambung dengan plaintext sehingga tetap ada hubungan antara satu baris dengan baris lain dan dapat dilakukan deskripsi secara bersamaan

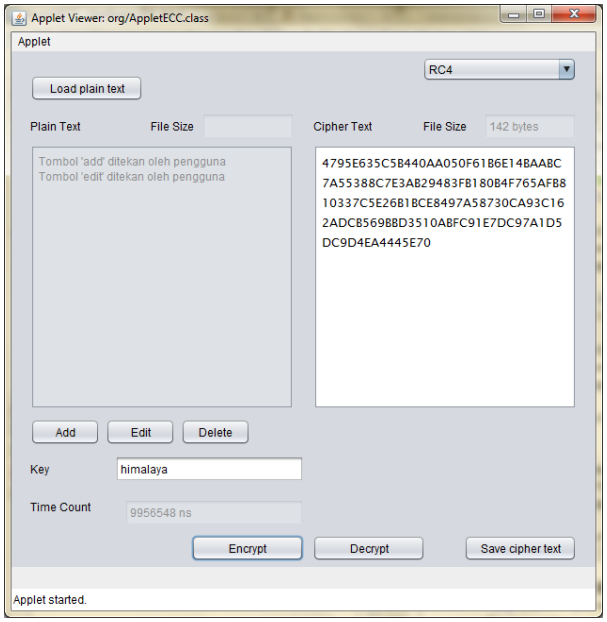
B. Langkah Pengujian

Untuk pengujian, dibuat aplikasi yang menggunakan algoritma RC4 dan AES mode CBC. Kemudian, akan diambil suatu file log yang dimasukkan sebagai input aplikasi. Aplikasi akan melakukan proses dengan mekanisme sebagai berikut :

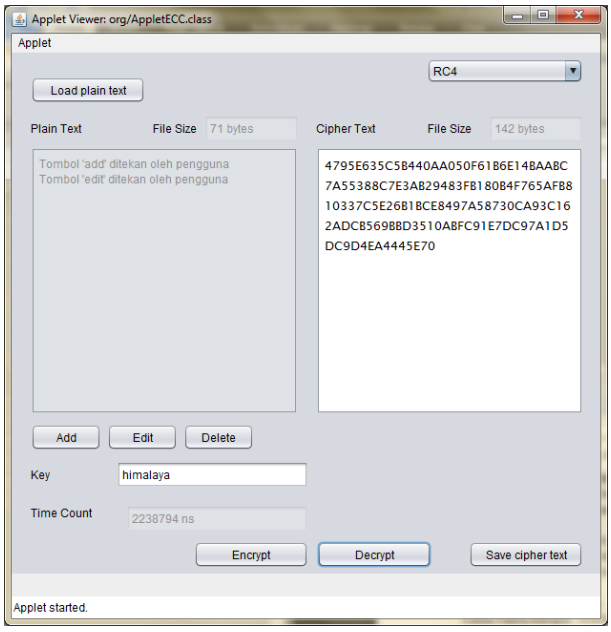
1) Dipilih algortima RC4 dengan menggunakan drop-down list.
2) Dimasukkan kunci yang diinginkan.
3) Ditekan satu tombol pada aplikasi yang membentuk satu baris kalimat pada file log.
4) Kalimat tersebut akan langsung dienkripsi dan hasil enkripsi dapat dilihat langsung pada program.
5) Kembali ditekan salah satu tombol yang menghasilkan baris file log yang baru.
6) Kalimat baru yang dihasilkan akan langsung dienkripsi dengan menggunakan algoritma dan kunci yang sama.
7) Dicatat waktu enkripsi dan file ciphertext beserta besarnya.
8) Ditekan tombol ‘decrypt’ untuk melihat kebeneran isi file.
9) Dicatat waktu deskripsi
10) Lakukan langkah 2-9 untuk algoritma AES dengan mode CBC

IV. HASIL PENGUJIAN

A.Hasil Pengujian dengan RC4



Gambar 1 Hasil Enkripsi dengan RC4



Gambar 2 Hasil Deskripsi dengan RC4

Plain Text : "Tombol 'edit' ditekan oleh pengguna" (telah ada plain text "Tombol 'add' ditekan oleh pengguna" terenkripsi sebelumnya)

Kunci : Himalaya

Cipher text :
"4795E635C5B440AA050F61B6E14BAABC7A55388C
7E3AB29483FB180B4F765AFB810337C5E26B1BCE84
97A58730CA93C162ADCB569BBD3510ABFC91E7DC
97A1D5DC9D4EA4445E"

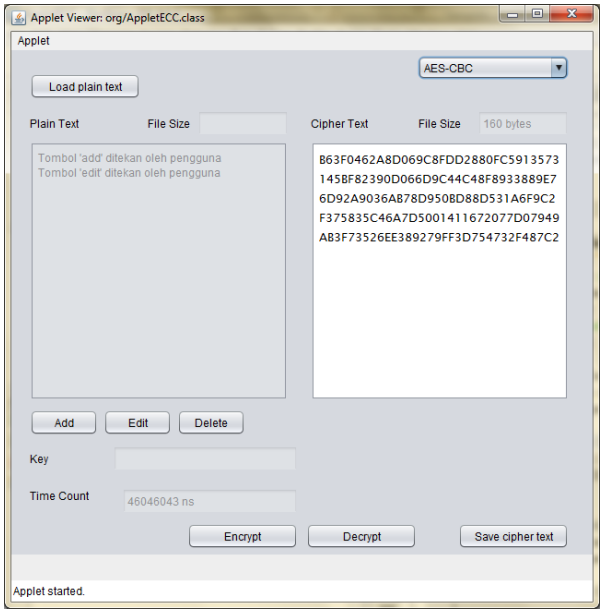
Besar ciphertext : 142 byte

Lama waktu enkripsi : 9956548 ns = 9.96 ms

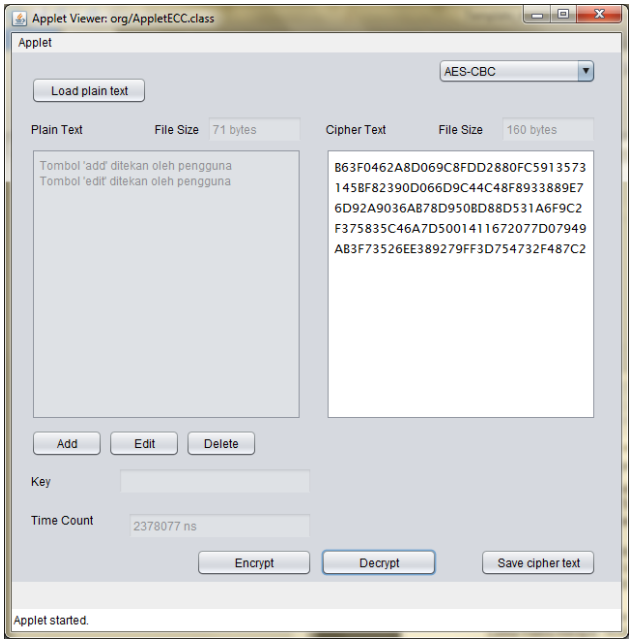
Besar plaintext : 71 byte

Lama waktu deskripsi : 2238794 ns = 2,24 ms

B.Hasil Pengujian dengan AES mode CBC



Gambar 3 Hasil Enkripsi dengan AES mode CBC



Gambar 4 Hasil Deskripsi dengan AES mode CBC

Plain Text : "Tombol 'edit' ditekan oleh pengguna" (telah ada plain text "Tombol 'add' ditekan oleh pengguna" terenkripsi sebelumnya)

Kunci :
0x00,0x01,0x02,0x03,0x04,0x05,0x06,0x07,0x08,0x09,
0x00,0x01,0x02,0x03,0x04,0x05

Cipher text :
"B63F0462A8D069C8FDD2880FC5913573145BF82390
D066D9C44C48F8933889E76D92A9036AB78D950BD
88D531A6F9C2F375835C46A7D5001411672077D0794
9AB3F73526EE389279FF3D754732F487C2"

Besar ciphertext : 160 byte

Lama waktu enkripsi : 46046043 ns = 46,3 ms
Besar plaintext : 71 byte
Lama waktu deskripsi : 2378077 ns = 2,37 ms

V. PERBANDINGAN

A.Waktu Enkripsi dan Deskripsi

Waktu yang dibutuhkan RC4 dan AES mode CBC untuk enkripsi lebih besar daripada waktu waktu yang dibutuhkan untuk deskripsi. Waktu deskripsi yang dibutuhkan RC4 dan AES mode CBC hampir sama, namun waktu enkripsi yang dibutuhkan AES mode CBC lebih lama daripada waktu yang dibutuhkan RC4.

Waktu enkripsi yang lebih lama ini disebabkan AES mode CBC memerlukan deskripsi block yang memilki bit padding terlebih dahulu sebelum digabungkan dengan plain text baru dan memulai enkripsi lagi. Selain itu enkripsi pada block cipher dilakukan dengan beberapa tahap putaran, tidak seperti stream cipher yang langsung mengoperasikan plain text dan stream key dengan x-or.

B.Panjang Cipher Text

Cipher text yang dihasilkan oleh AES mode CBC lebih panjang dibandingkan cipher text yang dihasilkan oleh RC4, hasil ini disebabkan adanya bit padding pada akhir cipherteks AES mode CBC.

C.Kriptanalisis

RC4 sangat rentan terhadap serangan berupa known plain-text attack, apalagi dengan banyaknya perulangan kata pada file log. Ditambah lagi dengan adanya perulangan key stream pada RC4 setelah periode tertentu yang berbahaya ketika ukuran file log besar sehingga dapat ditemukan pola yang sama pada cipher text.

AES mode CBC lebih aman terhadap kriptanalisis karena serangan terhadap algoritma ini adalah dengan brute force yang memakan waktu lama.

VI. KESIMPULAN

1) Lebih disarankan menggunakan algortima AES dengan mode CBC daripada menggunakan algoritma RC4 dalam penyembunyian data pada log file. Walaupun RC4 memiliki kelebihan dalam lebih sedikitnya waktu yang dibutuhkan untuk enkripsi dan panjang ciphertext yang lebih kecil tetapi RC4 rawan terhadap serangan known plain text yang menjadi lebih berbahaya dengan banyaknya perulangan teks.
2) Penyambungan ciphertext dimungkinkan pada algoritma AES mode CBC dan RC4. Pada algoritma RC4 dilakukan dengan mencatat keystream terakhir yang digunakan, lalu digunakan keystream setelahnya untuk enkripsi plaintext yang baru. Pada algoritma AES mode CBC dilakukan dengan mencatat IV block terakhir, melakukan deskripsi block terakhir untuk membuat bit padding, menyambungkan dengan plain text baru, lalu melakukan enkripsi block terakhir dan plain text baru tersebut.

REFERENCES

[1] Rinaldi Munir, Review Beberapa Algortima Kriptografi Modern (2013) diakses dari http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2012-2013/Review%20Beberapa%20Algoritma%20Kriptografi%20Modern%20(2013).ppt pada 10 Mei 2015

[2] William Stalling. The RC4 Stream Enccryption Algortihm.diakses dari http://www.vanilla47.com/PDFs/Cryptography/RC4%20Stream%20Cipher/Tutorials/THE%20RC4%20STREAM%20ENCRYPTION%20ALGORITHM.pdf pada 10 Mei 2015

[3] Rinaldi Munir, Advanced Encrytion Standard (AES) diakses dari http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2012-2013/Advanced%20Encryption%20Standard%20(AES).ppt pada 10 Mei 2015

[4] Singh, Simar Preet dan Maini, Raman. Comparison of Data Encrytion Algorithms. IJSCS diakses dari http://www.csjournals.com/IJCSC/PDF2-1/Article_22.pdf pada 10 Mei 2015

[5] Rinaldi Munir, Algoritma Kriptografi Modern diakses dari http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2014-2015/Algoritma%20Kriptografi%20Modern%20(2015).ppt pada 11 Mei 2015

[6] Logfile. Diakses dari http://www.webopedia.com/TERM/L/log_file.html pada pada 11 Mei 2015

[7] El Jung. Stream Cipher. usfCS. Diakses dari http://www.cs.usfca.edu/~ejung/courses/686/lectures/03stream.pdf pada 11 Mei 2015

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, 11 Mei 2015

M. Rian Fakhrusy
13511008