Analisis Perbandingan Algoritma AES Dan RC4 Pada Enkripsi Dan Dekripsi Data Teks Berbasis CrypTool 2

Risa Naili Fitriana[1], Djuniadi Djuniadi[2]

[1]Sistem Informasi, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Negeri Semarang,
[2]Teknik Elektro, Fakultas Teknik, Universitas Negeri Semarang

risanaili@students.unnes.ac.id[1], djuniadi@mail.unnes.ac.id[2]

Kata Kunci

Kata kunci
Keamanan Data, Advanced Encryption Standard, Rivest Cipher4

Abstrak

*Berkembangnya teknologi diikuti dengan bertambahnya data yang cukup besar. Data tersebut tidak semuanya disajikan untuk khalayak umum, beberapa data sangat dijaga kerahasiannya karena kepentingan tertentu. Penelitian ini bertujuan untuk melakukan uji coba enkripsi dan dekripsi pada data teks (dengan format *.txt) untuk menjaga kerahasiannya dan membandingkan kinerja dari algoritma AES dengan RC4. Penelitian ini menggunakan metode algoritma AES dan RC4 dengan panjang kunci 256 bit menggunakan CrypTool 2 untuk proses enkripsi dan dekripsi. Hasilnya uji coba pertama yaitu dilakukan uji coba enkripsi dan dekripsi algortima AES pada data teks menghasilkan ukuran ciphertext yang berbeda dari data teks asli. Sedangkan uji coba kedua dilakukan enkripsi dan dekripsi algoritma RC4 pada data teks dihasilkan ukuran ciphertext yang sama sebelum dilakukan proses simulasi. Sehingga dari penelitian ini diperoleh algoritma RC4 menghasilkan ukuran ciphertext lebih kecil dari pada menggunakan algoritma AES.*

Keywords

Data Security, Encryption, Description, Advanced Encryption Standard, Rivest Cipher4

Abstract

*The development of technology is followed by a large amount of data. Not all of the data is presented to the general public, some data are strictly kept confidential because of certain interests. This study aims to test the encryption and decryption of text data (with *.txt format) to maintain confidentiality and compare the performance of the AES algorithm with RC4. This study uses the AES and RC4 algorithms with a key length of 256 bits using CrypTool 2 for encryption and decryption processes. The result of the first trial is that the encryption and decryption test of the AES algorithm on text data results in a different ciphertext size from the original text data. While the second trial was carried out by encryption and decryption of the RC4 algorithm on text data, resulting in the same ciphertext size before the simulation process was carried out. So from this research, the RC4 algorithm produces a smaller ciphertext size than using the AES algorithm.*

1. Pendahuluan

Pekerjaan manusia mulai berubah seiring dengan perkembangan teknologi. Adanya teknologi membantu dalam melakukan berbagai aktivitas atau pekerjaan sehingga lebih akurat, cepat, efektif, dan efisien. Manfaat adanya perkembangan teknologi tersebut dilakukan pada berbagai macam bidang, salah satunya penyimpanan data atau informasi penting.

Banyaknya dokumen yang disimpan pada sebuah perusahaan atau instansi diperlukan sebuah keamanan agar dokumen tersebut tidak diakses oleh orang yang tidak berwenang. Pada dasarnya semua informasi tidak disajikan secara umum, akan tetapi beberapa informasi hanya ditujukan bagi golongan tertentu, sehingga kerahasiaan pada data tersebut perlu dijaga keamanan datanya agar tidak sampai pada pihak yang tidak berwenang untuk menghindari kebocoran atau penyalahgunaan[1]. Dengan adanya perkembangan teknologi, dalam menjaga informasi tersebut saat ini dapat dilakukan salah satunya dengan menggunakan algoritma kriptografi.

Pengamanan data menggunakan algoritma kriptografi salah satunya teknik kriptografi modern yaitu menggunakan teknik substitusi dan teknik transposisi diantaranya yaitu algoritma AES dan RC4 [2]. Penelitian sebelumnya banyak yang sudah membahas tentang pengamanan terhadap informasi atau data dengan algoritma kriptografi tersebut. Saat ini, banyak yang menggunakan algoritma AES untuk mengamankan data yang hanya dapat diketahui oleh orang tertentu atau bersifat rahasia [3]. AES adalah salah satu satu algoritma kriptografi modern yang berfungsi untuk mengenkripsi (encipher) dan dekripsi (decipher) informasi dalam bentuk blok ciphertext simetris [4].

Selain menggunakan algoritma AES, pengamanan data juga dapat dilakukan menggunakan algoritma RC4. Algoritma RC4

DOI : 10.29080/systemic.v7i2.1263

adalah algoritma kriptografi yang mempunyai bentuk *stream cipher* yang digunakan untuk menginput data atau informasi pada saat tertentu, dan data tersebut biasanya berbentuk byte [2]. RC4 memiliki kelemahan yaitu salah satunya *Bit-Flipping Attack* (BFA) yang dapat mengakibatkan seorang penyerang mendapatkan *plaintext* tanpa mengetahui kunci enkripsi [5].

Penelitian sebelumnya banyak yang sudah membahas tentang pengamanan data menggunakan RC4. Seperti penelitian yang dilakukan Taliasih and Afrianto [6] mereka menggunakan kombinasi antara RC4 dengan Base64 untuk mengamankan basis data pada klien P.T. Infokes. Selanjutnya penelitian lain juga dilakukan oleh Suryani [5] melakukan proses enkripsi dengan menggunakan algoritma RC4.

Algoritma AES dan RC4 dalam melakukan proses memiliki perbedaan tingkat kerumitan. Sehingga perlu dilakukan penelitian keberlanjutan terkait dua algoritma tersebut. penelitian ini akan melakukan simulasi pada proses enkripsi dekripsi data teks (format *.txt) dengan dua algoritma tersebut menggunakan cryptool 2. Penelitian ini menggunakan Algoritma AES dan RC4 dengan kunci 256 bit karena pada dasarnya dua algoritma tersebut samasama dapat diproses dengan kunci 256 bit. Sehingga dengan melakukan enkripsi dan dekripsi menggunakan AES dan RC4 peneliti memiliki tujuan untuk membandingkan kinerja dari dua algoritma tersebut untuk mengetahui proses kerjanya dan hasil dari algoritma mana yang lebih unggul dalam hal ukuran *ciphertext* dari kedua algoritma tersebut

2. Landasan Teori

2.1. Algoritma *Advanced Encryption Standard* (AES)

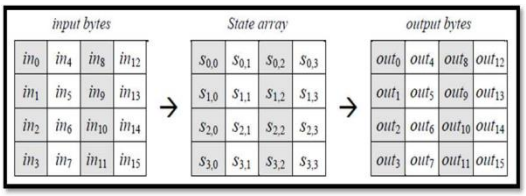
Algoritma *Advanced Encryption Standard* (AES) adalah *block cipher* yang menggunakan kunci simetri dan bersifat simetri dalam melakukan enkripsi dan dekripsi [3]. Algoritma AES mempunyai empat komponen dasar, yang dapat bekerja pada blok data diantaranya 8 bit. 128 bit diinput kedalam algoritma sehingga dapat diproses ke dalam matriks 4 4 yang biasanya disebut *state*, jika ingin mendapatkan blok 8 bit, maka dilakukan proses transformasi pada data masukan untuk menghasilkan teks sandi blok [7]

Panjang kunci yang dimiliki algoritma AES terdapat bermacam-macam diantaranya 128, 192, dan 256 bit [8]. Panjang kunci tersebut memiliki perbedaan dan dapat mempengaruhi hasil dari jumlah *round* (perputaran), seperti pada Tabel 1. (Rinaldi Munir, 2006).

Tabel 1. Tabel Perbedaan Jumlah Round dan Key [3]

	Panjang Kunci	Panjang Blok	Jumlah Putaran
AES-128	4	4	10
AES-129	6	4	12
AES-256	8	4	14

Terdapat data masukan in0 hingga in15 disalin pada array state pada enkripsi AES, dan setelah disalin dilakukan tahapan enkripsi atau dekripsi, sehingga menghasilkan output yang diletakkan pada array out [9]. Proses tersebut seperti yang ditunjukkan pada Gambar 1.



Gambar 1. Tahapan memasukkan *bytes, state array, output bytes* [3]

2.1.1. Enkripsi AES

Enkripsi merupakan proses yang digunakan untuk membuat suatu pesan asli (plaintext) sehingga menghasilkan output berupa bahasa sandi (ciphertext) [10]. Proses tersebut terdapat beberapa jenis transformasi bytes diantaranya, *Mixcolumns, AddRoundKey, SubBytes,* dan *ShiftRows*. Langkah pertama yaitu teks asli disusun menjadi sebuah *state*, selanjutnya dilakukan penggabungan antara blok teks asli dengan kunci round ke-0 (*AddRoundKey*), dan yang terakhir dilakukan proses round 1 sampai ke-(Nr-1) [11].

2.1.2. Dekripsi AES

Dekripsi adalah suatu proses yang melakukan input dari data berupa bahasa sandi sehingga menghasilkan output berupa pesan asli seperti semula [10]. Algoritma dekripsi AES menggunakan transformasi dasar dari algoritma ekripsi AES atau transformasi *invers*, transformasi byte pada *invers cipher* diantaranya *InvMixColumn, InvSubBytes,* dan *InvShiftRows.* Sedangkan *AddRoundKey* termasuk transformasi *self-invers* yang mempunyai syarat dengan memakai kunci serupa [11].

2.2. Algoritma *Rivest Cipher* (RC4)

Algoritma RC4 merupakan cipher yang mempunyai kunci simetris dan dapat melakukan proses enkripsi berupa *plaintext* yang dilakukan secara per digit atau per byte dan dapat menggabungkan dengan operasi biner (XOR) dan menggunakan angka semiacak [5]. Kunci yang digunakan pada algoritma RC4 yaitu dari 1 sampai dengan 256 byte berfungsi menginisialisasikan tabel dengan panjang 256 byte [12].

Metode enkripsi RC4 memiliki kecepatan yang sangat tinggi hingga melebihi kecepatan DES [12]. RC4 memiliki S-Box, S0, S1 ,...,S255, dengan permutasi yang terdapat mulai bilangan 0 hingga 255, sedangkan permutasi adalah sebuah fungsi dari kunci yang mempunyai panjang variabel [13].

RC4 tidak hanya memiliki kelebihan dengan kecepatannya, akan tetapi RC4 juga terdapat kelemahan diantaranya terdapat nilai-nilai pada array S yang memiliki nilai yang sama, karena pada karakter kunci dicopy secara berulang dan dapat

mudah diserang dengan *known-plaintext* attack jika penyerang mengetahui beberapa buah *plaintext* dan *ciphertext* yang berkorespondensi [14].

2.3. CrypTool 2

CrypTool2 adalah sebuah perangkat lunak yang dapat melakukan pendeskripsian terhadap konsep kriptografi dan kriptoanalisis [15]. Perangkat lunak tersebut biasanya digunakan dalam proses enksripsi dan dekripsi pada algoritma yang ada pada perangkat lunak tersebut. Terdapat beberapa algoritma yang ada di cryptool 2 diantaranya TEA, Caesar, MD5, AES, Vigenere, RSA, DES, dan 300 algoritma lainnya[15].

2.4. Tujuan Penelitian

Banyaknya dokumen yang disimpan pada sebuah perusahaan atau instansi diperlukan sebuah keamanan agar dokumen tersebut tidak diakses oleh orang yang tidak berwenang. Saat ini banyak yang menggunakan algoritma kriptografi modern seperti AES dan RC4 untuk mengamankan data tersebut. Berdasarkan permasalahan yang telah disampaikan, penelitian ini memiliki tujuan diantaranya.

1. Melakukan enkripsi dan dekripsi pada data teks (dengan format *.txt) dengan algoritma AES
2. Melakukan enkripsi dan dekripsi pada data teks (dengan format *.txt) dengan algoritma RC4
3. Melakukan analisa perbandingan kinerja antara algoritma AES dengan algoritma RC4.

3. Metode

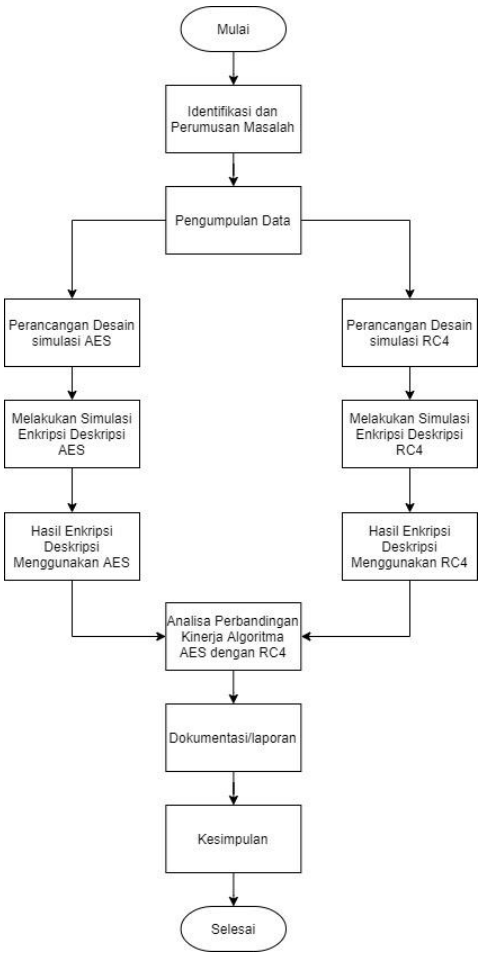
3.1. Tahapan penelitian

Metode penelitian ini dijelaskan pada gambar 2. sesuai dengan tahapan yang dilakukan selama proses penelitian.

Tahap penelitian pada gambar 2. Yang dilakukan pertama kali yaitu mengidentifikasi dengan merumuskan masalah untuk menemukan solusi yang diinginkan. Selanjutnya dilakukan pengumpulan data sesuai yang dibutuhkan selama proses penelitian. Setelah data terkumpul maka dilakukan simulasi enkripsi dan dekripsi menggunakan AES dan RC4. Hasil dari simulasi tersebut dilakukan analisa perbandingan antara dua algoritma tersebut. Selama proses simulasi dilakukan dokumentasi sebagai laporan pada penelitian ini. Tahapan yang terakhir yaitu membuat kesimpulan dari hasil penelitian.

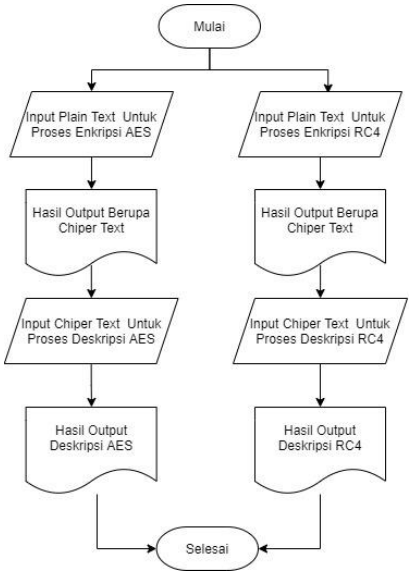
3.2. Tahapan Simulasi

Tahapan simulasi pada panelitian yaitu melakukan pengujian dengan algoritma AES dan RC4 dengan CrypTool2 seperti pada gambar 3.



Gambar 2. Tahapan Penelitian

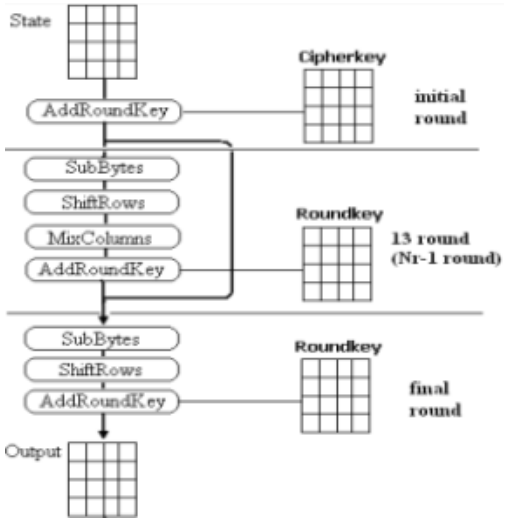
Simulasi dilakukan dengan 2 algoritma yang dimulai dengan proses enkripsi pada data teks (dengan format *.txt). Hasil dari enkripsi data teks berupa *ciphertext* dilakukan percobaan dekripsi pada *ciphertext* dari hasil data teks yang sudah terenkripsi untuk kembali pada data teks awal, dan tahapan yang terakhir yaitu analisa hasil pengujian dan membandingkan kinerja dari dua algoritma tersebut.



Gambar 3. Alur Tahapan Simulasi

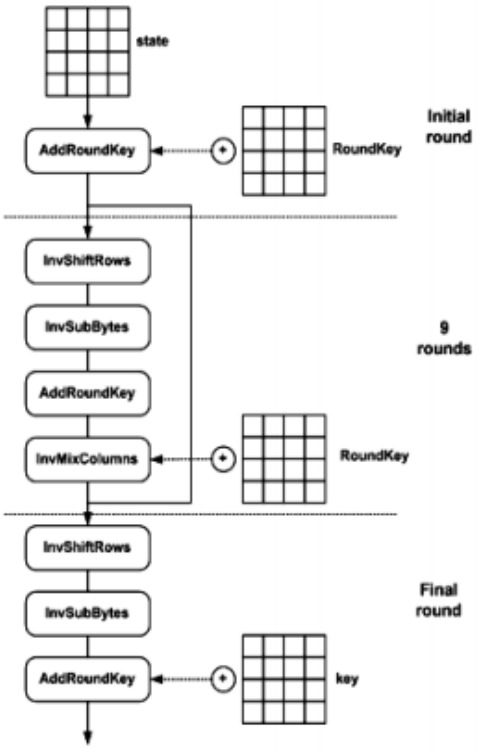
3.3. Desain Simulasi

Tahapan pertama yang dilakukan pada proses simulasi yaitu melakukan enkripsi pada algoritma AES 128, dengan proses seperti Gambar 4.



Gambar 4. Skema enkripsi AES 128 [16]

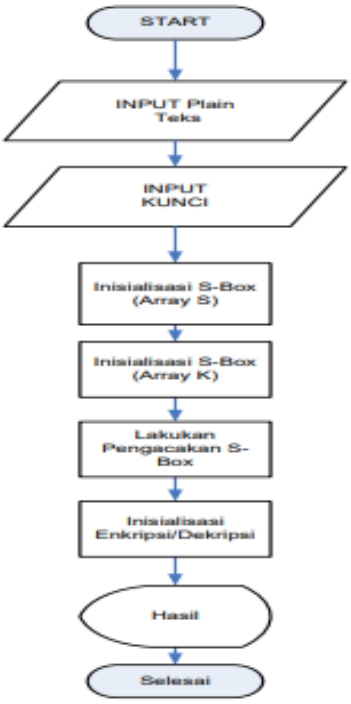
Hasil proses enkripsi berupa *ciphertext* digunakan uji coba untuk proses dekripsi seperti pada gambar 5.



Gambar 5. Skema dekripsi AES 128 [17]

Setelah dilakukukan enkripsi dan dekripsi dengan algoritma AES, selanjutnya dilakukan proses dengan menggunakan algoritma RC4 seperti pada gambar 6. yang hasilnya akan dilakukan analisis perbandingan kinerja dari dua algoritma tersebut.

Proses simulasi pada RC4 dimulai dengan memasukkan plain teks dan kunci. Sistem akan otomatis membaca dan mengubah teks yang ada pada S-Box ke Array S dan Array K. Selanjutnya dilakukan pengacakan pada S-Box dan jika sudah selesai maka sistem akan bekerja melakukan proses enkripsi atau dekripsi.



Gambar 6. Proses enkripsi/dekripsi RC4 [18]

4. Hasil Dan Pembahasan

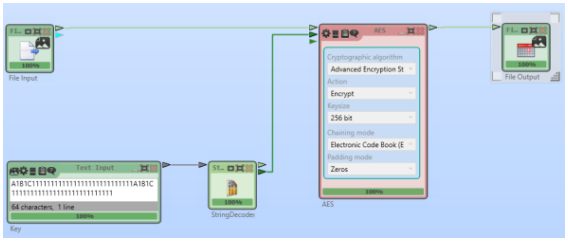
Penelitian ini menggunakan beberapa file yang berisi *plaintext* (dengan format *.txt) untuk dilakukan uji enkripsi dekripsi menggunakan algoritma AES dan RC4. Data teks (dengan format *.txt) yang akan digunakan diantaranya sebagai berikut.

Tabel 2. Nama file yang akan di simulasi

No	Nama File (*.txt)
1.	Teori Pembelajaran 1
2.	Teori Pembelajaran 2
3.	Teori Pembelajaran 3
4.	Teori Pembelajan 4
5.	Teori Pembelajan 5
6.	Teori Pembelajan 6
7.	Teori Pembelajan 7
8.	Teori Pembelajan 8

4.1. Simulasi Enkripsi *Advanced Encryption Standard* (AES)

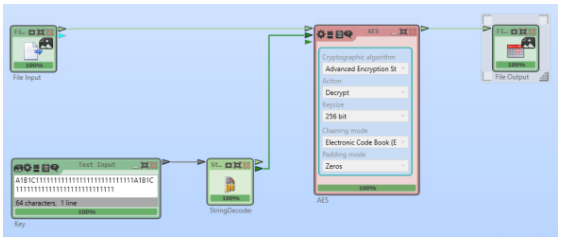
Simulasi yang dilakukan pada penelitian menggunakan Cryptool 2, data teks tersebut dilakukan proses enkripsi dan dekripsi untuk mengamankan file, seperti pada Gambar 7. Menunjukkan proses uji coba dari simulasi Enkripsi pada data teks (dengan format *.txt) dengan Algoritma AES menggunakan CrypTool 2.



Gambar 7. Simulasi enkripsi AES

4.2. Simulasi Dekripsi *Advanced Encryption Standard* (AES)

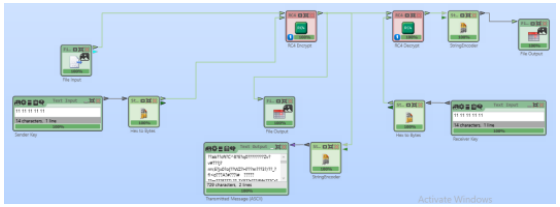
Perubahan pada *ciphertext* dilakukan dengan arah berlawanan sehingga output yang dihasilkan berupa *inverse cipher*. Output dari proses dekripsi yaitu berupa *plaintext*, dan hasilnya sesuai dengan sebelum dilakukan proses enkripsi. Pada gambar 8. Menunjukkan hasil simulasi dekripsi dari salah satu data teks (dengan format *.txt) yang digunakan pada penelitian ini.



Gambar 8. Simulasi dekripsi AES

4.3. Simulasi Enkripsi Dekripsi *Rivest Cipher* (RC4)

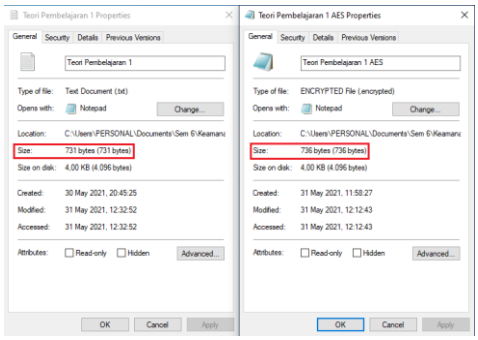
Simulasi menggunakan RC4 dalam proses enkripsi dan dekripsi dapat dilakukan secara bersama dalam satu proses menggunakan cryptool 2. Data teks yang berisikan *plaintext* dapat di transformasikan menjadi *ciphertext*, dan sebaliknya data berupa *ciphertext* dapat secara langsung di transformasikan menjadi data teks semula sebelum dilakukan proses enkripsi, seperti pada gambar 9.



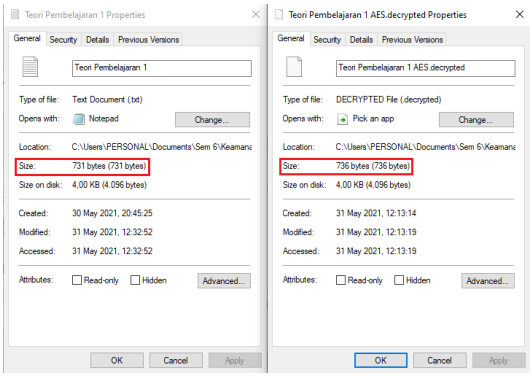
Gambar 9. Simulasi enkripsi dekripsi RC4

4.4. Perbandingan Ukuran Data Asli Dengan Data Simulasi

Berdasarkan hasil simulasi terdapat beberapa data yang memiliki ukuraan yang sama seperti data asli, akan tetapi juga terdapat beberapa data yang berubah ukurannya setelah dilakukan proses simulasi, Pada gambar 10. dan gambar 11. menunjukkan ukuran data teks hasil dari proses simulasi menggunakan AES

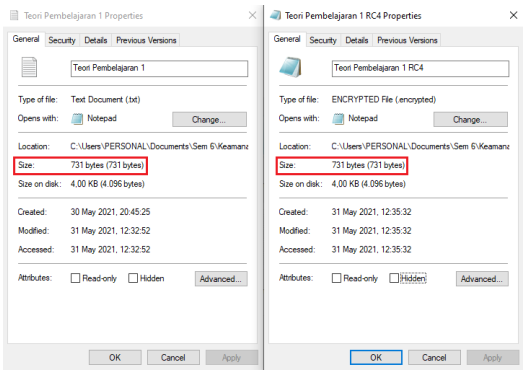


Gambar 10. Perbandingan ukuran hasil enkripsi AES

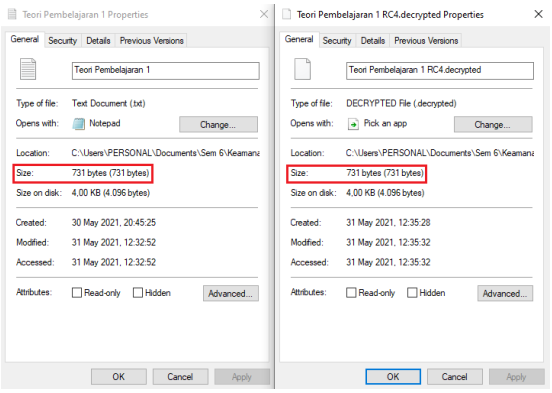


Gambar 11. Perbandingan ukuran hasil dekripsi AES

Simulasi menggunakan RC4 didapatkan hasil ukuran byte seperti yang dijelaskan pada gambar 12. dan gambar 13.



Gambar 12. Perbandingan ukuran hasil enkripsi RC4



Gambar 13. Perbandingan ukuran hasil dekripsi RC4

Tabel 3. Perbandingan kinerja AES dengan RC

No	Data Teks Asli Nama File (*.txt)	Ukuran Data Teks Asli	Enkripsi		Dekripsi	
			Ukuran (Byte) Menggunakan AES	Ukuran (Byte) Menggunakan RC4	Ukuran (Byte) Menggunakan AES	Ukuran (Byte) Menggunakan RC4
1.	Teori Pembelajaran 1	731 Bytes	736 Bytes	731 Bytes	736 Bytes	731 Bytes
2.	Teori Pembelajaran 2	366 Bytes	368 Bytes	366 Bytes	368 Bytes	366 Bytes
3.	Teori Pembelajaran 3	368 Bytes	368 Bytes	368 Bytes	368 Bytes	368 Bytes
4.	Teori Pembelajan 4	269 Bytes	272 Bytes	269 Bytes	272 Bytes	269 Bytes
5.	Teori Pembelajan 5	520 Bytes	528 Bytes	520 Bytes	528 Bytes	520 Bytes
6.	Teori Pembelajan 6	229 Bytes	240 Bytes	229 Bytes	240 Bytes	229 Bytes
7.	Teori Pembelajan 7	119 Bytes	128 Bytes	119 Bytes	128 Bytes	119 Bytes
8.	Teori Pembelajan 8	276 Bytes	288 Bytes	276 Bytes	288 Bytes	276 Bytes

4.5 Perbandingan Kinerja Simulasi Algoorima AES dengan RC4

Hasil dari simulasi algoritma AES dengan RC4 ditunjukkan pada tabel 3. Dijelaskana bahwa dari proses simulasi enkripsi algoritma AES menggunakan 256 bit rata-rata menghasilkan ukuran byte yang berbeda dari file sebelum di enkripsi, akan tetapi hasil dari dekripsi menggunakan AES menghasilkan ukuran byte yang sama pada saat file sudah terenkripsi yaitu sama dengan ukuran *ciphertext* sebelum di dekripsi. Sedangkan pada simulasi algoritma RC4 juga sama seperti simulasi sebelumnya menggunakan 256 bit diperoleh bahwa setelah dilakukan proses enkripsi dan dekripsi dihasilkan ukuran byte sama seperti saat sebelum dilakukan proses enkripsi maupun dekripsi.

Kesimpulan

Berdasarkan hasil dari simulasi pada data teks (dengan format *.txt) menggunakan algoritma AES dan RC4 dengan panjang 256 bit diperoleh bahwa kedua algoritma tersebut dapat melakukan enkripsi dan dekripsi pada data teks. Simulasi algoritma AES menghasilkan rata-rata ukuran byte yang berbeda dari data teks asli. Sedangkan pada algoritma RC4 dihasilkan ukuran yang sama seperti data teks asli sebelum dilakukan proses simulasi. Sehingga dapat disimpulkan bahwa pada algoritma RC4 dalam hal ukuran dihasilkan ciphertext lebih kecil dari pada menggunakan algoritma AES, karena algoritma AES merubah ukuran data teks sedangkan pada algoritma RC4 dalam proses enkripsi dan dekripsi tidak merubah ukuran data teks tersebut dari data teks asli.

Daftar Pustaka

[1.] Sihotang, D., *Perancangan Aplikasi Keamanan Data Text Dengan Metode IDEA dan Kompresi Menggunakan Algoritma Huffman.* Informasi dan Teknologi Ilmiah (INTI), 2017. **4**(2).

[2.] Prakoso, R.G.I. and S. Suhartono, *ANALISA KINERJA ALGORITMA RIJNDAEL DAN RC4 DENGAN INPUTAN TEKS DAN FILE TEKS*. 2016, Universitas Diponegoro.

[3.] Yuniati, V. and G. Indriyanta, *Enkripsi dan dekripsi dengan algoritma AES 256 untuk semua jenis file.* Jurnal Informatika, 2009. **5**(1).

[4.] Haryanto, H., R. Wiryadinata, and M. Afif, *Implementasi Kombinasi Algoritma Enkripsi Aes 128 Dan Algoritma Kompresi Shannon-Fano.* Setrum: Sistem Kendali-Tenaga-elektronika-telekomunikasi-komputer, 2016. **3**(1): p. 16-25.

[5.] Suryani, K.N., *Algoritma RC4 sebagai metode enkripsi.* Jurnal Umum, Program Studi Teknik Informatika-Sekolah Teknik Elektro Dan Informatika ITB, Bandung, 2009.

[6.] Taliasih, N. and I. Afrianto, *Sistem Keamanan Basis Data Klien PT Infokes Menggunakan Kriptografi Kombinasi RC4 Dan Base64.* 2020.

[7.] Van Dyken, J. and J.G. Delgado-Frias, *FPGA schemes for minimizing the power-throughput trade-off in executing the Advanced Encryption Standard algorithm.* Journal of Systems Architecture, 2010. **56**(2-3): p. 116-123.

[8.] Putra, S.H., et al., *IMPLEMENTASI ALGORITMA KRIPTOGRAFI ADVANCED*

ENDRYPTION STANDARD (AES) PADA KOMPRESI DATA TEKS. Jurnal Ilmu Komputer Universitas Brawijaya, 2013.

[9.] Munir, R., *Kriptografi.* Informatika, Bandung, 2006.

[10.] Rosyadi, A., *Implementasi Algoritma Kriptografi AES Untuk Enkripsi Dan Dekripsi Email.* Transient: Jurnal Ilmiah Teknik Elektro, 2012. **1**(3): p. 63-67.

[11.] Rahmawati, S., I. Taufik, and G. Sandi. *Implementasi algoritma AES (Advanced Encryption Standard) 256 bit dan kompresi menggunakan algoritma Huffman pada aplikasi voice recorder*. in *Prosiding-Seminar Nasional Teknik Elektro UIN Sunan Gunung Djati Bandung*. 2018.

[12.] Nugroho, N.B., Z. Azmi, and S.N. Arif, *Aplikasi Keamanan Email Menggunakan Algoritma Rc4.* Jurnal SAINTIKOM, 2016.

[13.] Pandiangan, H., *Perancangan Media Pengiriman Pesan Teks Dengan Penyandian Pesan Menggunakan Algoritma RC4 Berbasis WEB.* Jurnal Mantik Penusa, 2016. **19**(1).

[14.] Purba, B., et al. *Pengamanan File Teks Menggunakan Algoritma RC4*. in *Seminar Nasional Teknologi Komputer & Sains (SAINTEKS)*. 2020.

[15.] Mulya, M.F. and N. Rismawati, *Analisi dan Simulasi Algoritma TEA (Tiny Encryption Algorithm) untuk Enkripsi dan Dekripsi Pesan Text menggunakan Cryptool2.* Jurnal SISKOM-KB (Sistem Komputer dan Kecerdasan Buatan), 2019. **3**(1): p. 31-38.

[16.] Kurniawan, Y.C., *Penerapan algoritma kriptografi DES, AES dan RSA serta algoritma kompresi data LZM untuk pengamanan berkas digital*. 2007, Petra Christian University.

[17.] Gumira, G. and A. Erlanshari, *IMPLEMENTASI METODE ADVANCED ENCRYPTION STANDARD (AES) & MESSAGE DIGEST 5 (MD5) PADA ENKRIPSI DOKUMEN (Studi Kasus LPSE UNIB).* Rekursif: Jurnal Informatika, 2016. **4**(3).

[18.] Sihombing, P. and W. Ginting, *Perancangan dan Implementasi Enkripsi dan Dekripsi File dengan Algoritma RC4–One Time Pad pada Jaringan LAN.* KAKIFIKOM: Kumpulan Artikel Karya Ilmiah Fakultas Ilmu Komputer, 2020. **2**(1): p. 1-10.