Jurnal Ilmiah Informatika (JIF)
| ISSN (Print) 2337-8379 | ISSN (Online) 2615-1049 |
Jurnal online di akses di http://ejournal.upbatam.ac.id/index.php/jif

ANALISIS ALGORITMA AES DALAM MENGAMANKAN DATA PADA KANTOR WALIKOTA PEMATANGSIANTAR

Eko Hartato[a], Indra Gunawan[b], Iin Parlina[c,] Solikhun[d], Anjar Wanto[e]

[A,b,c,d,e]*Stikom TUNAS BANGSA Pematangsiantar, Jln. Sudirman Blok A No. 1,2,3 Pematangsiantar, 21111- Indonesia, Telp : (0622) 22431*

INFORMASI ARTIKEL

Sejarah Artikel
Diterima Redaksi: 18 Februari 2020
Revisi Akhir: 10 Maret 2020
Diterbitkan *Online*: 25 Maret 2020

KATA KUNCI

Data
Security
AES
Encryption
Decryption

KORESPONDENSI

E-mail: ekohartato2611@gmail.com

A B S T R A C T

Data is information that is kept very confidential because it contains important information about the company or agency. Computers are currently the main component in the company that is able to store data, speed up work, improve the quality and quantity of services, simplify the transaction process, and others. But in terms of computer security still has several loopholes that allow a person or group to easily retrieve data or information on the computer. To avoid theft and manipulation of data, it is necessary to implement a security system. Cryptography is the study of how to change information from normal conditions / forms (can be understood) into a form that cannot be understood. One method that can be used to secure messages / information is the Advanced Encryption Standard (AES). The application of the AES cryptographic algorithm in securing data at the Pematangsiantar Mayor's Office shows that this algorithm can generate encryption that cannot be understood by humans and produces the exact decryption with the initial plaintext input.

1. PENDAHULUAN

Data merupakan salah satu bagian terpenting dalam berlangsungnya suatu perusahaan, institusi - institusi pendidikan, instansi - instansi pemerintahan, dan untuk pribadi. Sehingga memerlukan berbagai macam pertimbangan untuk melakukan penyimpanan data, terlebih dalam segi keamanan dan kerahasiaannya. Sering sekali terjadi kasus pembocoran data rahasia oleh pihak – pihak tidak berwenang seperti *hacker* maupun *cracker* yang menyebabkan kerugian besar bagi sang pemilik data. Kantor Walikota Pematangsiantar merupakan kantor pemerintahan yang memiliki banyak sekali data, baik itu data pegawai, data keuangan, data penduduk, dan data pemerintah daerah. Hal ini tentunya akan menjadi pertimbangan dalam melakukan penyimpanan data karena perlindungan keaslian suatu data maupun informasi menjadi kebutuhan yang sangat penting dimasa sekarang dan seterusnya.

Dari hasil pengamatan penulis Kantor Walikota Pemaangsiantar belum menerapkan sistem keamanan data. Komputer yang digunakan dapat diakses oleh siapapun sehingga sangat beresiko apabila ketika ada orang yang tidak bertangung jawab mengakses informasi yang sensitif dan berharga tersebut. Kemungkinan lainnya adalah informasi yang berada di dalamnya bisa saja berubah sehingga menyebabkan perubahan atau kerusakan data dan dapat disalahgunakan untuk kepentingan yang tidak baik bagi si pemilik data.

Upaya proteksi data dapat dilakukan dengan mengaplikasikan bidang kriptografi. Kriptografi merupakan sebuah teknik dalam mengamankan dan mengirimkan data dalam bentuk yang sulit untuk dibaca, sehingga dapat mengamankan data - data penting baik yang tersimpan dalam media penyimpanan maupun yang ditransmisikan melalui jaringan komunikasi[1]. Kriptografi merupakan ilmu mengamankan data dengan teknik enkripsi dimana data asli diacak menggunakan suatu kunci enkripsi menjadi suatu data yang hanya bisa dimengerti oleh seorang yang memiliki kunci dekripsi.

Penelitian sebelumnya membahas tentang Penerapan Algoritma AES : Rijndael Dalam Pengenkripsian Data Rahasia [2]. Di dalam penelitian tersebut membahas tentang pengaplikasian algoritma kriptografi Rijndael dalam pengamanan data. Diawali dengan menganalisa cara kerja algoritma Rijndael kemudian merancang aplikasi yang dapat mengenkripsi dan mendekripsi plainteks yang di-*input user*. Hasil evaluasi memperlihatkan bahwa algoritma Rijndael dapat menghasilkan enkripsi yang tidak dapat dimengerti manusia biasa, dan menghasilkan dekripsi yang sama persis dengan *plainteks* awal yang di-*input user*. Disini penulis menerapkan sebuah metode pengamanan data yaitu AES (*Advanced Encryption Standard*) yang mana merupakan standar enkripsi dengan kunci-simetris yang

diadopsi oleh pemerintah Amerika Serikat. Algoritma AES merupakan sistem penyandian blok yang bersifat *non-feistel* kerena AES menggunakan komponen yang selalu memiliki invers dengan panjang blok 128. Penyandian Algoritma AES menggunakan proses yang berulang disebut dengan ronde. jumlah ronde yang digunakan oleh AES tergantung panjang kunci yang dipakai. Setiap ronde membutuhkan kunci ronde dan masukan dari ronde berikut nya[3].

2. TINJAUAN PUSTAKA

Analisis

Analisis merupakan suatu proses tahapan pekerjaan sebelum riset didokumentasikan melalui tahapan penulisan laporan menguraikan suatu pokok menjadi beberapa bagian dan menelaah bagian itu sendiri serta hubungan antar bagian untuk memperoleh pengertian yang tepat dan pemahaman arti keseluruhan [4].

Analisis kriptografi AES *(Advanced Encryption Standard)* berupa proses enkripsi dan dekripsi dengan AES dengan ukuran kunci 128-bit dalam mengamankan *plaintext* agar hanya bisa dibaca oleh pihak yang mengetahui *secret key* saja. dalam hal ini data yang akan dienkripsi pada aplikasi kriptografi ini adalah *file* berjenis dokumen teks, gambar, video, dan musik.

Kriptografi

Kriptografi merupakan ilmu dan seni untuk menjaga kerahasiaan pesan agar isi pesan yang disampaikan tersebut aman sampai ke penerima pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya'. Orang yang mendalami ilmu dan seni dalam memecahkan suatu algoritma kriptografi tanpa harus mengetahui kuncinya disebut kriptanalis, sedangkan orang yang melakukan penyandian disebut kriptografer [5].

4 aspek keamanan pada algoritma kriptografi [6]:

1. Kerahasiaan. Pesan *(plaintext)* hanya dapat dimengerti oleh pihak yang memliki kewenangan.
2. Autentikasi. Pengirim pesan harus dapat menetapkan dengan pasti, bahwa penyusup harus dipastikan tidak bisa diam-diam menjadi orang lain.
3. Integritas. Penerima pesan harus dapat menetapkan bahwa pesan yang diterima tidak ada perubahan ketika sedang dalam proses pengiriman data.
4. *Non-Repudiation*. Pengirim pesan harus tidak bisa membantah pesan yang dia kirimkan.

Berikut 3 fungsi dasar Algoritma kriptografi [7] :

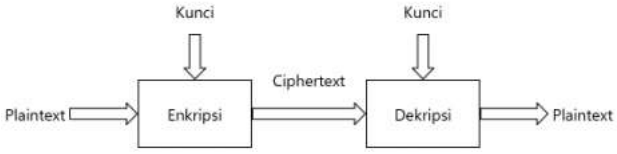
1. Enkripsi, merupakan pengamanan data yang dikirimkan terjaga rahasianya, plainteks yang dirubah menjadi kode-kode yang tidak dimengerti. Enkripsi bisa diartikan dengan *cipher* atau kode.
2. Dekripsi, merupakan kebalikan dari proses enkripsi, pesan yang telah dienkripsi menjadi kode-kode dikembalikan kebentuk asalnya *(plainteks).*
3. Kunci, yang digunakan untuk melakukan enkripsi dan dekripsi, kunci ini terbagi jadi 2 bagian yaitu kunci pribadi *(private key)* dan kunci umum *(public key).*

Konsep matematis yang mendasari kriptografi adalah relasi antara 2 (dua) buah perkumpulan yaitu perkumpulan yang berisi elemen-elemen plainteks dan perkumpulan yang berisi cipherteks. Proses enkripsi dan dekripsi merupakan fungsi yang memetakan elemen-elemen antar kedua perkumpulan tersebut.

Advanced Encryption Standard (AES)

AES merupakan algoritma kriptografi bernama Rijndael yang dirancang oleh dua orang kriptografer yang berasal dari Belgia yaitu Vincent Rijmen dan John Daemen. Mereka merupakan pemenang kontes algoritma kriptografi pengganti *Data Encryption Standard* (DES) yang diadakan oleh *National Institutes of Standards and Technology* (NIST) di Amerika Serikat pada tanggal 26 November 2001. Algoritma Rijndael inilah yang kemudian dikenal sebagai AES. Pada tanggal 22 Mei 2006 AES mengalami proses penyesuaian oleh NIST, kemudian diangkat menjadi ukuran algoritma kriptografi[8]. Menurut [9] Rijndael memiliki panjang kunci 128 sampai 256 bit dengan step 32 bit. Karena Algoritma AES memiliki tiga pilihan kunci yaitu tipe :128, 192, dan 256 serta dukungan penuh dari algoritma Rijndael yang fleksibel maka AES saat ini dikenal dengan AES-128, AES-192, AES-286.

Berikut merupakan skema proses enkripsi dan dekripsi dalam pertukaran informasi:



Gambar 1. Skema Enkripsi dan Dekripsi

Java

Java merupakan bahasa pemrograman berorientasi objek atau sering disebut OOP *(Object Oriented Program)* dan *multi platform* yang diperkenalkan oleh James Gosling dari *Sun Microsystems Inc*. Tujuan dari pembuatan bahasa pemrograman Java adalah untuk meningkatkan kemampuan bahasa pemrograman C++ yang sebelumnya telah ada sehingga aplikasi-aplikasi yang dikembangkan dengan bahasa tersebut dapat berjalan diatas platform hardware dan software yang berbeda[10]. Aplikasi berbasis Java biasanya diubah ke dalam p-code (*bytecode*) dan dapat dioperasikan pada berbagai Mesin Virtual Java (JVM).

NetBeans

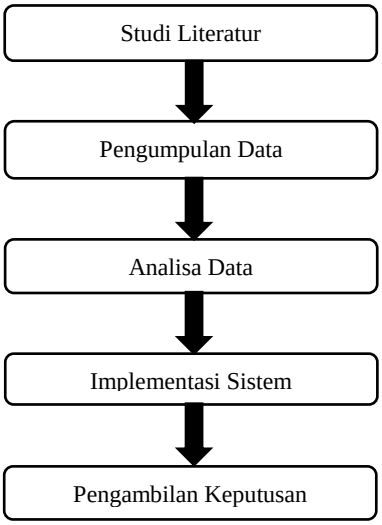
Netbeans adalah *Intregrated Development Environment* (IDE) berbasiskan Java dari *Sun Microsystem* yang berjalan di atas *Swing. Swing* merupakan teknologi Java untuk pengembangan aplikasi *dekstop* yang dapat berjalan di berbagai macam *platform* seperti Windows, Linux, Mac OS X dan Solaris [11]

Netbeans merupakan *software development* yang *Open Source*, dengan kata lain *software* ini dibawah pengembangan bersama. Netbeans memiliki beberapa fitur yaitu *source code, refactoring*

dan *profiling*. *Refactoring* pada netbeans cukup lengkap, hal ini membantu programmer untuk mengubah nama *class*, *method* dan *variable* dengan cepat. Fitur *profiling* pada netbeans dapat digunakan untuk memantau aktifitas memori dan CPU di saat aplikasi Java yang dibuat dijalankan. Netbeans juga mendukung plugin untuk menambah fungsionalitas aplikasi.

3. METODOLOGI

Tahapan ini merupakan tahapan bagaimana proses penelitian ini dilakukan yang dibuat dalam bentuk langkah – langkah kerja untuk mencapai tujuan dan menentukan jawaban atas masalah yang diajukan secara sistematis.



Gambar 2. Diagram Blok Metode Penelitian

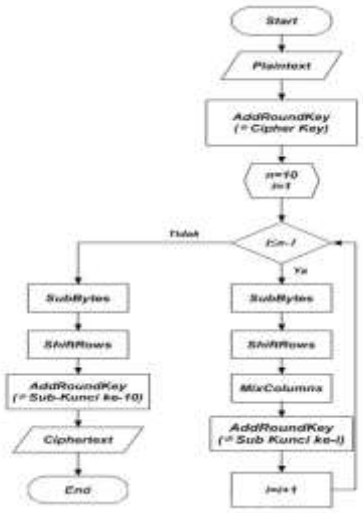
Berdasarkan gambar 2 langkah yang dilakukan dalam penelitian ini yaitu:

1. Melakukan studi literatur yang berkaitan dengan implementasi metode AES.
2. Melakukan pengumpulan data dari hasil studi kasus pada Kantor Walikota Pematangsiantar.
3. Melakukan analisa data untuk membantu dan memudahkan pihak yang bersangkutan dalam mengamankan data.
4. Mengajukan pengujian terhadap perangkat lunak.
5. Melakukan evaluasi pada *Output* yang dihasilkan perangkat lunak.

Rancangan Penelitian

Rancangan dari penelitian yang dilakukan penulis dibagi ke dalam dua buah *flowchart* sebagai berikut.

a. Enkripsi Algoritma AES

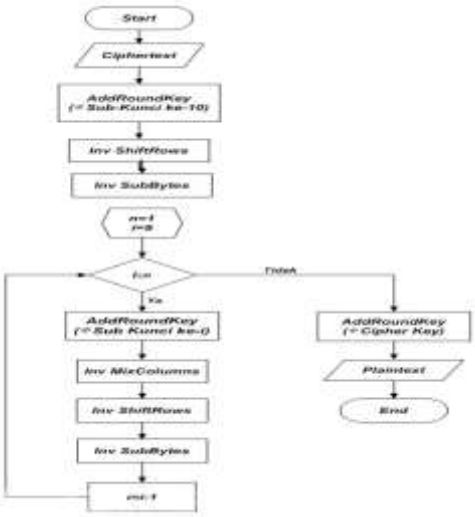


Gambar 3. Proses Enkripsi Algoritma AES

Gambar 3 menunjukkan *flowchart* proses enkripsi algoritma *AES*, langkah-langkah proses enkripsi tersebut dapat dijelaskan sebagai berikut:

1. Menginputkan *plaintext*
2. Melakukan transformasi *AddRoundKey*, yaitu melakukan operasi *XOR* terhadap sebuah *round key* dengan *array state*
3. Mempersiapkan dan mendeklarasikan nilai awal dari n atau jumlah *round key*
4. Melakukan empat proses terstruktur sebanyak sembilan iterasi yang tersusun atas :
   - *SubBytes*, yaitu memetakan setiap *byte* dari *array state* dengan menggunakan tabel substitusi *S-Box Rijndael*
   - *ShiftRows*, yaitu melakukan pergeseran secara *wrapping* pada tiga baris terakhir dari *array state*
   - *MixColumns*, yaitu mengalikan setiap kolom dari *array state* dengan matriks *MixColumns Rijndael*
   - *AddRoundKey*
5. Akhir proses enkripsi yaitu iterasi kesepuluh tersusun atas tiga proses terurut,yaitu :
   - *SubBytes*
   - *ShiftRows*
   - *AddRoundKey*
6. Menghasilkan *ciphertext*

b. Dekripsi Algoritma AES



Gambar 4. Proses Dekripsi Algoritma AES

Gambar 4 menunjukkan *flowchart* proses dekripsi algoritma *AES*, langkah-langkah proses dekripsi tersebut dapat dijelaskan sebagai berikut:

1. Menginputkan *ciphertext*
2. Melakukan transformasi *AddRoundKey*, yaitu melakukan operasi *XOR* antara *ciphertext* dengan *round key* yang digunakan pada saat enkripsi.
3. Melakukan transformasi *InvShiftRows*, yaitu kebalikan dari proses *ShiftRows* dimana proses pergeseran baris dari *array state* dimulai dari baris paling bawah.
4. Melakukan transformasi *InvSubBytes* yaitu memetakan setiap *byte* dari *array state* dengan menggunakan tabel substitusi *Inverse S-Box Rijndael*
5. Mempersiapkan dan mendeklarasikan nilai awal dari n atau jumlah *round key*
6. Melakukan empat proses terstruktur sebanyak sembilan iterasi yang tersusun atas :
   - *AddRoundKey*
   - *InvMixColumns*, yaitu mengalikan setiap kolom dari *array state* dengan matriks *InvMixColumns Rijndael*
   - *InvShiftRows*
   - InvSubBytes
7. Proses dekripsi diakhiri dengan melakukan transformasi *AddRoundKey*
8. Menghasilkan *plaintext*

Pengujian dan Evaluasi

Tahapan ini merupakan tahapan pengujian terhadap aplikasi yang dibuat. Setelah dilakukan pengujian hasil dari sistem aplikasi tersebut, maka tahapan selanjutnya yaitu mengevaluasi hasil dari kinerja sistem aplikasi tersebut apakah sistem aplikasi yang telah dibuat berjalan dengan baik dan sesuai berdasarkan desain yang telah dibuat.

4. HASIL DAN PEMBAHASAN

Hasil

Terdapat 2 fungsi utama pada aplikasi ini, yaitu fungsi enkripsi dan fungsi dekripsi, yang mana keduanya dapat kita akses melalui menu utama, seperti gambar 5. berikut.

Gambar 5.. Tampilan Menu Utama

Proses enkripsi *file* dengan program kriptografi ini adalah sebagai berikut :

1. Pilih fungsi enkripsi untuk mengenkripsi *file*.
2. Pilih *file* yang akan dienkripsi.
3. Masukkan kunci dan konfirmasi kunci. Kunci yang dimasukkan sesuai dengan keinginan user.
4. Program akan melakukan proses enkripsi *file* dan kemudian menghasilkan *file output*. *File* hasil enkripsi akan tersimpan secara langsung di direktori yang sama dan *file* asli akan terhapus secara otomatis. Namun jika *file* asli masih terbuka saat melakukan enkripsi maka *file* asli tidak terhapus, jika ingin menghapusnya bisa dilakukan dengan cara manual langsung ke direktori penyimpanan *file* tersebut.

Adapun panjang kunci yang di-*input* harus sesuai atau tidak melebihi panjang kunci yang ditentukan. Untuk AES dengan panjang 128 *bit* berarti 16 *byte* (16 karakter). Apabila melanggar aturan tersebut maka program akan mengeluarkan pesan *warning* "Masukkan Kunci Sebanyak 16 karakter"

Gambar 6. Tampilan Masukkan Kunci

Dan selanjutnya kita akan diminta meng-input ulang *password* yang sama untuk proses verifikasi, jika *password* yang di-*input*-kan berbeda maka akan muncul pesan *warning* "Kedua kunci berbeda!"

Gambar 7. Tampilan Masukkan Kunci Pesan 1

Setelah kedua *password* cocok maka proses enkripsi akan dilakukan dan akan muncul notifikasi yang menyatakan proses berhasil.

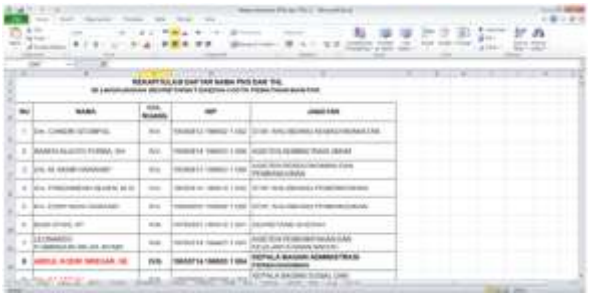
Gambar 8. Tampilan Proses Enkripsi Berhasil

Pengujian Sistem

Proses enkripsi adalah proses mengubah *plaintext* menjadi *ciphertext* yang bertujuan untuk mengamankan data atau isi pesan agar tidak dapat dipahami oleh pihak lain sehingga, perlu dilakukan analisis isi *file* untuk melihat apakah *file* yang akan dienkripsi dapat terjaga kerahasiaannya. Berikut ini contoh analisis pada beberapa *file* dengan ekstensi berbeda.

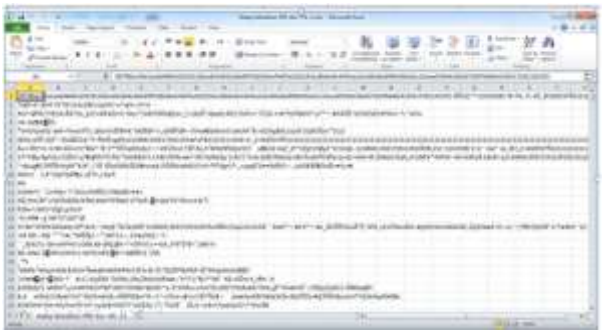
1. *File* Dokumen*Ms. Excel (.xls/.xlsx)*

a. *File* Asli (Rekap Kehadiran PNS dan THL-2.*xlsx.*)



Gambar 9. *File* Rekap Kehadiran PNS dan THL-2.xlsx

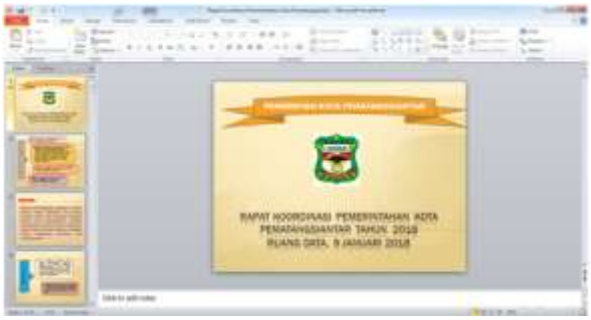
b. *File* Hasil Enkripsi (Rekap Kehadiran PNS dan THL-2.*xlsx.enc*)



Gambar 10. *File* Rekap Kehadiran PNS dan THL-2.xlsx.enc

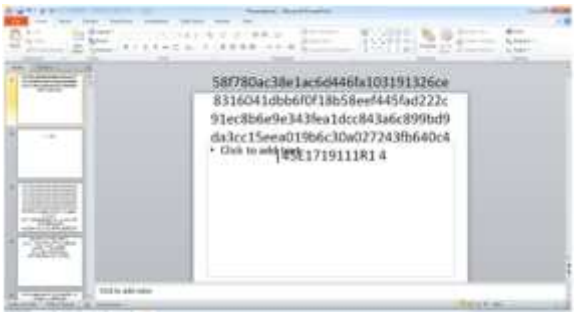
2. File Dokumen Power Point (.ppt/.pptx)

a. File Asli (Rapat Koordinasi Pemerintahan KotaPematangsiantar.pptx)



Gambar 11. Rapat Koordinasi Pemerintahan Kota Pematangsiantar.pptx

b. File Hasil Enkripsi (Rapat Koordinasi Pemerintahan Kota Pematangsiantar.pptx.enc)



Gambar 12. Rapat Koordinasi Pemerintahan Kota Pematangsiantar.pptx.enc

Beberapa *file* di atas menunjukkan bahwa setelah dilakukan proses enkripsi, *file-file* tersebut tidak dapat dibaca dan dimengerti maknanya.

Analisis Waktu Enkripsi dan Dekripsi

Waktu adalah salah satu faktor pendukung dalam melakukan proses enkripsi dan dekripsi. Dengan adanya waktu, kecepatan proses enkripsi dan dekripsi dapat diketahui. Berikut ini akan diberi tabel perbandingan waktu enkripsi dan dekripsi pada beberapa tipe file.

Tabel 1 dibawah Hubungan antara Ukuran File dengan Waktu Proses Enkripsi dan Proses Dekripsi

No	Nama *File*	Kunci	Ukuran *File* (bytes)	Waktu Enkripsi (ms)	Waktu Dekripsi (ms)
1.	Rekap Kehadiran PNS dan THL-2.xlsx	pematang_siantar	133.986	53	119
2.	Rekap Kehadiran PNS dan THL-2.xlsx	1234567 8123456 78	133.986	70	75
3.	Daftar Kehadiran PNS dan THL.docx	pematang_siantar	4.553.85 6	573	460
4.	Daftar Kehadiran PNS dan THL.docx	1234567 8123456 78	4.553.85 6	502	483
5.	Rapat Koordinasi Pemerintahan Kota Pematangsiantar.pptx	pematang_siantar	2.882.63 3	345	341
6.	Rapat Koordinasi Pemerintahan Kota Pematangsiantar.pptx	1234567 8123456 78	2.882.63 3	359	441
7.	Evjab Kota Pematangsiantar 2.pdf	pematang_siantar	269.978	76	158
8.	Evjab Kota Pematangsiantar 2.pdf	1234567 8123456 78	269.978	110	126
9.	Logo Kota Pematangsiantar.png	pematang_siantar	203.692	135	53
10.	Logo Kota Pematangsiantar.png	1234567 8123456 78	203.692	76	105
11.	Peta kota pematangsiantar.jpg	pematang_siantar	333.618	80	51
12.	Peta kota pematangsiantar.jpg	1234567 8123456 78	333.618	74	119
13.	Siantar The Most Tolerance City.Mp4	pematang_siantar	1.944.00 0	1286	1357
14.	Siantar The Most Tolerance City.Mp4	1234567 8123456 78	1.944.00 0	1400	1345
15.	Siantar Kota Toleransi. Mp3	pematang_siantar	1.944.00 0	270	439
16.	Siantar Kota Toleransi. Mp3	1234567 8123456 78	1.944.00 0	262	272

Tabel 1. di atas menunjukkan kecenderungan kenaikan waktu yang dibutuhkan untuk melakukan proses enkripsi dan dekripsi. Perbedaan kunci yang digunakan ikut mempengaruhi waktu yang dibutuhkan untuk melakukan proses enkripsi dan dekripsi. Dan apabila semakin besar ukuran suatu *File* maka semakin lama pula waktu yang dibutuhkan untuk melakukan proses enkripsi dan dekripsi.

5. KESIMPULAN DAN SARAN

Kesimpulan

Aplikasi yang dibuat menggunakan NetBeans IDE 8.0.2. dengan algoritma AES berhasil diaplikasikan untuk mengenkripsi *file* dengan berbagai ekstensi seperti :.doc, .xls, .ppt, .pdf,.jpg, .png. .Mp4, dan .Mp3 serta dapat mengembalikan plaintext sama seperti *file* aslinya.

Data yang diamankan melalui metode kriptografi AES tidak menjadi rusak dengan syarat tidak melakukan perubahan meliputi penambahan atau pengapusan teks, pemotongan (*cropping*), penambahan kecerahan (*brightness*), dan hal hal yang dapat merubah data yang telah di enkripsi lainnya.

Saran

Menambah fitur untuk mengenkripsi *file* dengan ekstensi yang lebih beragam dan Penelitian ini dapat di implementasikan pada instansi lain yang memiliki data/dokumen yang dirahasiakan, serta melakukan pengembangan dengan bahasa pemrograman lain, agar tidak hanya bisa di implementasikan pada dekstop saja melainkan juga pada mobile, web, dan lainnya.

DAFTAR PUSTAKA

[1] A. sFauzi, Novriyenni, Y. Maulita, And A. M. H. Pardede, "Analisis Hybrid Cryptosystem Algoritma Algoritma Rsa Dan Triple Des," Vol. 1, No. 2, Pp. 36–44, 2017.

[2] D. Alyanto, "Pengenkripsian Data Rahasia," 2016.

[3] R. R. M, "Desain Dan Implementasi Aplikasi Sms (Short Message Service) Pada Android Menggunakan Algoritma Aes," Vol. 2, No. 2, Pp. 3318–3326, 2015.

[4] A. Wedianto, H. L. Sari, And Y. S. H, "Analisa Perbandingan Metode Filter Gaussian , Mean Dan Median Terhadap Reduksi Noise," Vol. 12, No. 1, Pp. 21–30, 2016.

[5] N. Afifah, "Perancangan Aplikasi Kriptografi Image Menggunakan Metode Advanced Encryption Standard (Aes)," 2018.

[6] T. T. W. Aziz, "Perbandingan Algoritma Fermat , Lehman , The Sieve Of Eratosthenes Dan The Sieve Of Atkins Dalam Pembangkitan Bilangan Prima Pada Rsa," 2018.

[7] R. A. Harahap, "Implementasi Algoritma Vigenere Cipher Dan Rivest Shammer Adleman (Rsa) Dalam Keamanan Data Teks," Vol. 1, No. 2, Pp. 156–160, 2016.

[8] D. Kurniawan, R. Afyenni, And R. Hidayat, "Implementasi Algoritma Aes Dalam Mengenkripsi Berkas Terintegrasi Dengan Layanan Cloud Storage Berbasis Android," No. September, Pp. 237–245, 2018.

[9] P. Arif, Ahmad; Mandarani, "Rekayasa Perangkat Lunak Kriptografi Menggunakan Algoritma Advanced Encryption Standard (Aes) 128 Bit Pada Sistem Keamanan Short Message Service (Sms) Berbasis Android," Vol. 4, No. 1, 2016.

[10] A. Abdullah And E. Utami, "Analisis Dan Perancangan Sistem Informasi Skb Kab Kubu Raya Menggunakan Konsep Mvc Dalam Bahasa Pemrograman Java," Vol. 1, No. 1, Pp. 51–57, 2017.

[11] A. Suryono And R. Kardian, "Aplikasi Penilaian Kompetensi O Shore Instalation Manager (Oim) Bidang Industri Minyak Dan Gas Dengan Metode Ahp Dan Rating Scale (Studi Kasus : Pt . Benchmark Training)," Vol. 16, Pp. 235–248, 2017.

BIODATA PENULIS

Eko Hartato
Mahasiswa Sarjana di Jurusan Teknik Informatika STIKOM Tunas Bangsa Pematangsiantar.

Indra Gunawan
Dosen Program Studi Teknik Informatika, STIKOM Tunas Bangsa Pematangsiantar.

Iin Parlina
Dosen Program Studi Teknik Informatika, STIKOM Tunas Bangsa Pematangsiantar.

Solikhun
Dosen Program Studi Teknik Informatika, STIKOM Tunas Bangsa Pematangsiantar.

Anjar Wanto
Dosen Program Studi Teknik Informatika, STIKOM Tunas Bangsa Pematangsiantar.