GABUNGAN ADVANCED ENCRYPTION STANDARD DAN VIGENERE CIPHER UNTUK PENGAMANAN DOKUMEN DIGITAL

Eko Hari Rachmawanto[1], Christy Atika Sari[2]

[1,2] Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
[1]eko.hari@dsn.dinus.ac.id[1], christy.atika.sari@dsn.dinus.ac.id

Abstrak

Penggunaannya yang kian massif dan banyakya data dan informasi yang tersebar di internet yang mungkin saja terdapat data yang bersifat rahasia, menjadikan data tersebut rawan untuk disalahgunakan dari tindakan illegal oleh pihak yang tidak bertanggung jawab. Faktor keamanan menjadi hal yang sangat penting agar data tersebut tetap aman dan terjamin keasliannya. Maka dibutuhkan metode agar data tetap aman dan asli. Kriptografi adalah metode untuk mengamankan data digital dengan cara mengubah dan mengacak data asli (plainteks) menjadi bentuk yang tidak dikenali (cipherteks). Maka dari itu dipilihlah menggunakan kombinasi algoritma Vigenere dan Advanced Encryption Standard (AES) dalam mengamankan data agar tetap asli. Vigenere digunakan sebagai pembangkit kunci karena aman, cepat dan tidak banyak menghabiskan sumber daya, menghasilkan ciphertext yang bervariasi. AES dipilih sebagai algoritma yang akan mengenkripsi file dokumen karena menggunakan sistem cycle atau putaran, yang bervariasi terhadap panjang kunci. Sehingga ketika variasi panjang kunci yang berbeda, AES akan mengenkripsi file dokumen dengan jumlah putaran yang disesuaikan. Dengan adanya program kombinasi algoritma Vigenere dan AES ini diharapkan dapat membantu dalam menyembunyikan dan mengamankan data agar data tetap terjamin keasliannya. Berdasarkan hasil eksperimen pada proses enkripsi dan dekripsi, dihasilkan nilai Avalanche effect yang cukup baik. Nilai Aevalache Effect diperngaruhi oleh pajnag kunci yang digunakan. Pada Analisa kebutuhan waktu enkripsi dekripsi, diketahui bahwa proses dekripsi pesan membutuhkan waktu yang lebih lama disbanding proses enkripsi.

Kata kunci : Kriptografi, Enkripsi, Dekripsi, Vigenere, Advanced Encryption Standard

1. Pendahuluan

Dalam era globalisasi yang kian pesat, peran teknologi menjadi peran penting dalam kehidupan sehari-hari. Penyebaran informasi dan pertukaran informasi disebarkan melalui internet, membuat internet menjadi media komunikasi digital yang mutakhir. Pada dasarnya jaringan internet adalah seluruh komputer yang berada di berbagai belahan dunia yang terhubung dan saling terkoneksi satu sama lain dan dapat memberi, menerima, meyebarkan dan bertukar data atau informasi satu sama lain. Internet memuat berbagai macam informasi yang dirangkum oleh mesin pencari dimana informasi tersebut dapat berupa berita, artikel, gambar, audio, video dan media digital lainnya. Meski jaringan internet bersifat publik dan semua orang yang memiliki akses dapat membuka internet secara bebas, konten digital bisa saja memuat informasi atau data penting yang diharapkan hanya bisa diakses oleh beberapa pihak karena bersifat rahasia (Vittal Kumar Mittal | Manish Mukhija, 2019). Maka dari itu sebuah kerahasian, kevalidan dan keaslian data harus tetap terjaga dan terlindungi meskipun berada di jaringan yang mudah dibuka dan diakses tanpa campur tangan pihak ketiga dan pihak yang tidak kredibel.

Faktor keamanan data menjadi hal yang sangat harus dipertimbangkan guna mengatasi masalah pembajakan dan penyalahgunaan data agar data tetap bersifat rahasia dan tidak jatuh ke pihak yang salah. Untuk menjaga data agar tetap bersifat privasi, tertutup dan terhindar dari penyalahgunaan data dibutuhkan sebuah metode untuk mengamankan data (Ajmera, Ghosh and Vijayetha, 2018; Mathur, Pathak and Bandil, 2019). Untuk menghindari ancaman kejahatan siber seperti pengaksesan paksa, pencurian dan pemalsuan data, dibutuhkan cara agar data tetap aman dan terjaga keasliannya.

Kriptografi adalah salah satu metode untuk mengamankan dan menyembuyikan data dengan cara mengubah data asli menggunakan struktur algoritma khusus menjadi sebuah data atau informasi yang tidak bisa dikenali oleh siapapun dan perangkat digital apapun. Kriptografi merupakan singkatan dari "crypto" dan "graphia" yang dalam bahasa Yunani crypto yang artinya rahasia dan graphia yang memiliki arti tulisan. Dengan demikian secara umum kriptografi memiliki arti "tulisan rahasia". Dalam artian yang sebenarnya kriptografi berarti ilmu yang mempelajari tentang kerahasian data agar data tetap aman, valid dan terjaga keabsahannya. Pada penelitian ini yang didasarkan pada latar belakang

yang telah penulis jabarkan sebelumnya, penulis akan membangun dan mengimplementasikan sebuah sistem file berbagi dokumen bebasis Web Services yang dilengkapi dengan keamanan tambahan menggunakan kriptografi dengan metode Vigenere Cipher dan AES 256. Web Service dipilih dengan alasan lebih efisien dan tidak menghabiskan memori dikarenakan semua proses dilakukan secara online. Sehingga proses menyimpan dan berbagi data bisa dilakukan di mana saja, kapan saja dan dengan gawai apa saja tanpa melakukan proses pemasangan paket aplikasi, dengan syarat gawai terhubung dengan jaringan internet ketika website dieksekusi. Sehingga proses penyimpanan dan pengiriman data menjadi lebih ringkas, cepat, nyaman namun tetap aman dengan hanya memasukkan url file sharing yang sudah dijabarkan di atas.

Pemilihan algoritma vigenere digunakan sebagai membangkitkan kunci karena cukup aman, cepat dan tidak banyak menghabiskan sumber daya. Vigenere Cipher akan digunakan sebagai pembangkit kunci baru yang sebelumnya diambil dari nama file. Karena termasuk cipher polialfabetik (Susanto *et al.*, 2019; TOUIL, AKKAD and SATORI, 2020), vigenere menghasilkan ciphertext yang berbeda di setiap karakter plainteks meskipun menggunakan kunci yang sama. Kemudian kunci hasil generasi dari Vigenere Cipher akan digunakan oleh AES untuk mengunci dan mengacak file dokumen yang akan diunggah. Sehingga file dokumen yang akan diunggah dan dibagikan telah diproteksi dengan Algoritma Vigenere Cipher dan AES. Kemudian algoritma yang akan digunakan untuk mengenkripsi dokumen yang akan diunggah adalah algoritma Advanced Encryption Standard. AES dipilih sebagai algoritma yang akan mengenkripsi file dokumen karena menggunakan sistem cycle atau putaran, yang bervariasi terhadap panjang karakter kunci (Sangeeta and Kaur, 2017; Sharma, Prabhjot and Kaur, 2017; Ajmera, Ghosh and Vijayetha, 2018), sehingga ketika memasukkan variasi panjang kunci yang berbeda, AES akan mengenkripsi file dokumen dengan jumlah putaran yang disesuaikan. AES saja atau Vigenere saja sudah pernah diimplementasikan pada plainteks berupa teks ASCII sesuai penelitian oleh (Latif, 2015), (Tulloh, Permanasari and Harahap, 2016), (Maricar and Sastra, 2018) dan (Arrijal, Efendi and Susilo, 2016). Pada beberapa artikel tersebut, baik AES maupun Vigenere baru di uji menggunakan waktu tempuh prosesing saja, sedangkan nilai ketahanan belum diuji. Beberapa artikel mengenai AES dan kombinasinya dengan algortima lain juga telah diterapkan namun masih menggunakan AES 128 bit, sedangkan pada artikel ini telah menggunakan AES 256 bit. AES-Vigenre pernah dikombinasikan namun dengan model dua kali enkripsi sehingga kurang efektif. Dengan demikian penulis memilih dan menggunakan AES sebagai algoritma untuk mengenkripsi file dokumen dan algoritma vigenere sebagai pembangkit kunci.

Tujuan penelitian ini adalah untuk mengetahui bagaimana implementasi algoritma vigenere dan AES, menguji seberapa efektif algoritma Vigenere dan AES, kombinasi antara algoritma klasik dan cipher modern, serta mengetahui kekuatan kunci simetris dan statis yang diskenario menjadi kunci simetris namun dinamis memanfaatkan nama file yang dienkripsi dengan kunci dari sistem menggunakan algoritma vigenere sehingga menghasilkan kunci yang berbeda untuk setiap filenya.

2. Landasan Teori

2.1 Kriptografi

Kriptografi adalah ilmu yang mempelajari tentang teknik penyandian dengan cara mengubah dan mengacak plaintext atau naskah asli menggunakan kunci dan algoritma khusus menjadi naskah acak yang sulit dikenali bahkan tidak bisa dibaca (ciphertext) oleh seseorang yang tidak memiliki kunci untuk mengembalikan informasi kembali ke naskah asli (Sari *et al.*, 2017). Proses untuk mengubah dan mengacak naskah asli menjadi naskah yang tidak dikenali disebut enkripsi, sedangkan dekripsi adalah sebuah proses mengembalikan naskah yang tidak dikenali menjadi naskah asli. Kedua proses utama kriptografi tersebut membutuhkan kunci untuk mengacak dan mengembalikan informasi. Sehingga ketika seseorang yang menerima data atau informasi tersebut tidak memiliki kunci, akan membutuhkan waktu yang sangat lama untuk mengembalikan ke bentuk asli dan kemungkinan tidak bisa dikembalikan sama sekali. Metode yang digunakan dalam teknik enkripsi kriptografi klasik menggunakan enkripsi simetris. Enkripsi simetris adalah proses enkripsi dimana kunci yang digunakan untuk dekripsi sama seperti dengan kunci yang digunakan untuk proses enkripsi. Kriptogarfi klasik menggunakan kunci yang dibuat melalui permutasi karakter atau subtitusi karakter.

2.2 Vigenere Cipher

Vigenere cipher adalah kriptografi klasik dan bagian dari kriptografi polialfabetik yang dirancang oleh diplomat perancis bernama Blaise de Vigenere pada tahun 1586. Algoritma vigenere cipher menggunakan tabel vigenere sebagai media dalam mengenkripsi pesan. Tabel vigenere terdiri dari 26 alfabetik standar yang dimulai dari A – Z dan tiap barisnya akan digeser satu huruf ke kiri. Kunci pada algoritma vigenere dipakai berulang sepanjang plainteks yang akan dienkripsi. Algoritma vigenere sendiri termasuk kriptografi klasik karena belum menggunakan kalkulasi, rumus dan proses komputasi yang kompleks (Nasution *et al.*, 2017; Isfahani and Nugraha, 2019; Susanto *et al.*, 2019). Algoritma Vigenere termasuk kriptorafi klasik namun dikenal

karena sulit untuk ditembus. Algoritma ini dikatakan tidak dapat dipecahkan oleh pernyataan Charles utwidge Dodgson seorang matematikawan. Seorang ilmuan amerika sempat menyatakan bahwa algoritma vigenere cipher adalah salah satu algoritma yang tidak mungkin dapat ditembus. Namun hal tersebut berhasil dibantah oleh Kasiski karena berhasil menembus algoritma vignere pada abad ke-19 menggunakan sebuah tabel dalam melakukan proses enkripsi. Tabel tersebut berisi kumpulan alfabet dari A – Z dan setiap barisnya bergeser ke kiri sebanyak 1 karakter. Pada tabel tersebut, bagian paling atas baris tabel menyatakan untuk plainteks. Sedangkan kolom bagian kiri tabel menyatakan kunci. Kemudian karakter yang lain yang berada di dalam tabel merupakan karakter dari cipherteks.

Proses Enkripsi algoritma vigenere sendiri menggunakan metode password berulang, di mana plainteks yang akan dienkripsi lebih panjang dari panjang kunci. Untuk proses enkripsinya sendiri yaitu memecah plainteks dan kunci per karakter kemudian mencari pertemuan antara karakter plainteks dan kunci menggunakan tabel vigenere. Proses itu dilakukan sampai akhir karakter plainteks hingga semua karakter plainteks berubah mejadi cipherteks.

2.3 Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) adalah algoritma kriptografi kunci simetris yang dibuat dan dirancang unttuk menggantikan algoritma DES atau Data Encryption Standard. Advanced Encryption Standard (AES) dipublikasikan secara resmi pada tahun 2001 oleh National Institute of Standard and Technology sebagai algoritma kunci simetris yang telah disepakati menjadi standar pada saat ini. Algoritma AES adalah algoritma kriptografi kunci simetris dimana kunci yang digunakan untuk dekripsi sama dengan kunci yang digunakan untuk enkripsi. AES memiliki 3 buah kategori kunci yakni AES 128 bit, 192 bit dan 256 bit (Ali and Hasan, 2019). Pada algoritma AES 128 bit, setiap blok data asli sebesar 128 bit dirubah ke dalam bentuk state yaitu matriks heksadesimal berukuran 4x4. Putaran enkripsi dan dekripsi pada algoritma AES dipengaruhi oleh panjang kunci. Sehingga ketika menggunakan kunci 128 bit, proses enkripsi atau dekripsi lebih cepat karena perputaran yang lebih sedikit. Algoritma AES sendiri menggunakan sistem putaran atau cycle dalam proses penyandian. Setiap putaran dipengaruhi oleh panjang kunci yang terbagi menjadi 10, 12 dan 14 putaran. Untuk proses enkripsi AES terdiri dari 4 proses yaitu SubBytes, Shiftrows, MixColumns, dan AddRoundKey. Dalam proses enkripsi yang pertama kali dijalankan adalah proses AddRoundKey, kemudian masuk ke proses putaran SubBytes, ShiftRows, MixColumns, dan AddRoundKey dan terus berulang sesuai jumlah putarannya.

3. Metode Penelitian

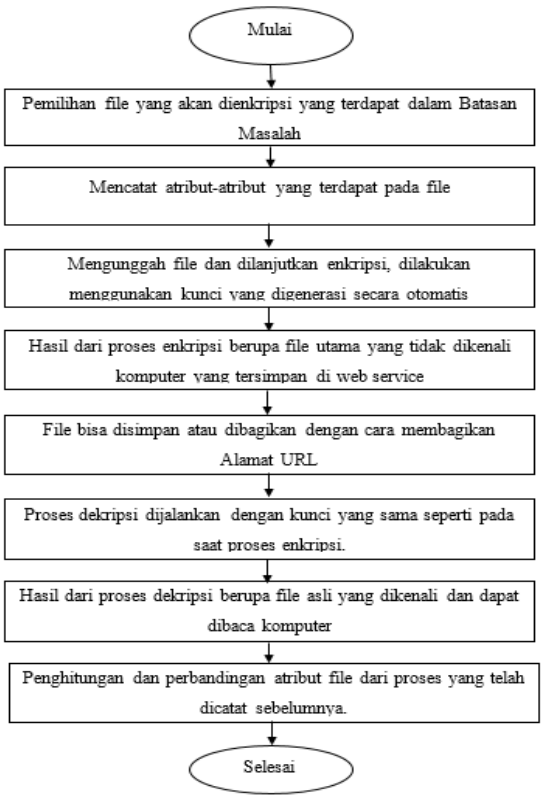
3.1 Jenis Data

Jenis data yang digunakan dalam penelitian ini adalah dokumen digital. Semua data dokumen diatas berukuran tidak lebih dari 3MB. Untuk detail dari masing-masing dokumen yang akan digunakan adalah berikut:

- Dokumen word dan pdf, file akan berisi lima ribu (5000) hingga sepuluh ribu (10.000) kata, memuat berupa seperti diagram, gambar, tabel dan semua komponen yang dapat dimuat oleh file word.
- Dokumen spreadsheet akan berisi diagram, gambar, rumus dan komponen-komponen yang dapat dimuat oleh dokumen spreadsheet.
- Dokumen presentation berisi gambar, diagram, video, media digital dan komponen yang dapat dimuat oleh file presentation.

3.2 Tahapan Penelitian

Metode yang diusulkan dalam penelitian ini yaitu menggunakan algoritma Vigenere Cipher dan AES, sesuai Gambar 1.



Gambar 1. Gabungan Vigenere Cipher dan AES

Gambar 1 merupakan tahapan penelitian dalam mengimplementasikan Vigenere Cipher dan AES, adapun detail langkah dapat dijabarkan sebagai berikut :

1. Peneliti melakukan pengujian menggunakan file-file yang tercantum pada Batasan Masalah.

2. Melakukan pencatatan atribut-atribut file seperti ukuran file dalam satuan paling terkecil (byte) untuk selanjutnya sebagai pembanding dengan file yang telah dienkripsi dan didekripsi.
3. Memilih file dan mengunggah ke website kemudian mengeksekusi proses enkripsi yang dilakukan menggunakan kunci berupa alfabet A – Z tanpa menggunakan karakter spesial seperti simbol. Proses enkripsi dilakukan dengan memproses algoritma Vigenere yang digenerasi dari nama file kemudian dilanjutkan dengan algoritma AES dan file enkripsi tersimpan ke dalam folder penyimpanan web service.
4. Proses enkripsi selesai dan file yang telah dienkripsi tersimpan di dalam folder yang terdapat pada web service dan link dapat dibagikan.
5. Melakukan pencatatan atribut-atribut file yang telah dienkripsi seperti ukuran file dalam satuan paling terkecil (byte) dan waktu yang telah dihabiskan untuk enkripsi untuk selanjutnya sebagai pembanding.
6. Dekripsi dilakukan menggunakan kunci yang sama seperti saat proses enkripsi dilakukan. Proses dekripsi dilakukan dengan memproses algoritma Vigenere untuk membangkitkan kunci kemudian dilanjutkan dengan algoritma AES.
7. Hasil dari proses dekripsi berupa file asli seperti sebelum proses enkripsi. Kemudian diuji dengan cara menjalankan file yang telah didekripsi dengan tujuan untuk mengetahui apakah file kembali seperti semula atau mengalami kerusakan.
8. Melakukan penghitungan dan perbandingan atribut file seperti ukuran file dalam satuan paling terkecil (byte) dan waktu yang telah dihabiskan untuk dekripsi untuk mengetahui apakah ada perbedaan atau tidak.

4. Pembahasan Hasil

4.1 Pengujian Enkripsi-Dekripsi

Untuk menguji algoritma vigenere, dilakukan pengujian dengan menggunakan pengujian kasiski. Pengujian Kasiski adalah sebuah metode dimana pengujian tersebut mampu membantu menemukan length-key atau panjang kunci. Pengujian Kasiski memanfaatkan keuntungan dengan menghitung pengulangan dan kemunculan huruf, huruf berpasangan dan tripel. Dengan memanfaatkan perulangan karakter, memungkinkan untuk menghasilkan chiperteks yang berulang. Pengujian dilakukan dengan bantuan tools yaitu menggunakan "Kasiski Test" yang dapat diakses melalui https://planetcalc.com/8550/. Pengujian dilakukan dengan menyiapkan plainteks dan cipherteks, kemudian mengihtung tingkat kemunculan karakter berpasangan dan tripel. Selanjutnya penguji akan menyiapkan plainteks berupa 1 paragraf berbahasa inggris yang diambil dari arti "Filosofi logo" yang dari website resmi UDINUS yaitu pada halaman https://dinus.ac.id/vision/. Kemudian dienkripsi dengan kunci "udinus" seperti ilustrasi pada Tabel 1, dimana P adalah plainteks, K adalah kunci, dan C adalah cipherteks.

Tabel 1. Perubahan Plainteks Menjadi Cipherteks dengan Kunci "udinus"

P	The symbol of University of Dian Nuswantoro (UDINUS) is a combination of letter D and N, which was abbreviated of Dian Nuswantoro. Letter N is symbolized curved down which means Udinus will always pray to God. The Golden yellow of circle in the middle has the meaning of harmony, strong will, and life dynamics. It means that by the harmony and strong will from civitas academica, UDINUS will always be ready to move forward to support government in educating the nation.
K	udinus
C	Nkm fsevrt bz Mhldrlkcwg bz Vcdv Aokqdvgiji (XLVHMM) la n wggeqaulcrv bz dywbrl V uql A, qzcfp juk uejeyncdbrx gz Gqnh Fovenhliuw. Yylnhz A ck mbuoidccmq wmlymq xgqq eucub pmnhk Ogqaok qlty udqdgf jjub bb Agx. Wpr Agfgma swfowj ix wlzpfw cq buy ecglyy zuv buy eydvvhy ii pnleiqg, fnjiqo jcdf, dvq fazh llhsglkf. Cl ghiam lbdb os lbh pnleiqg nhv mwzbhy qlty zjip kvpanda nwsxhuvws, OGQAOK qlty udqdgf vw lhiqs li pwiy xiuenlv nr ahjhiub tinyuvzyfn lv rxmwdbvhy nkm aulcrv.

Tabel 2. Kemunculan Frekuensi pada Vigenere

Tripel	Kemunculan ke 1	Kemunculan berikutnya	Frekuensi	Faktor Pembagi
AOK	27	120, 282	162	{1, 2, 3, 6, 9, 18}
OKQ	28	120, 282	162	{1, 2, 3, 6, 9, 18}
QLT	123	150, 162	12	{1, 2, 3, 4, 6, 12}
LTY	123	150, 162	12	{1, 2, 3, 4, 6, 12}

Pada Tabel 2, frekuensi adalah hasil dari pengurangan nilai kemunculan terbesar dengan nilai kemunculan paling besar kedua. Ketika sudah didapatkan nilai dari frekuensi, selanjutnya adalah menentukan himpunan nilai faktor pembagi dari nilai frequency tersebut. Proses selanjutnya adalah melakukan proses eliminasi yaitu menghilangkan nilai tidak sama. Setelah melihat hasil dari faktor pembagi yang terdapat pada Tabel 2, dapat disimpulkan bahwa dengan metode pengujian

kasiski, pengujian tersebut mampu menentukan panjang kunci. Dari hasil tersebut didapatkan bahwa panjang password yang mendekati benar adalah sepanjang 6 karakter. Panjang kunci yang digunakan untuk percobaan di atas adalah "udinus", kunci tersebut memiliki panjang 6 karakter. Dapat disimpulkan bahwa dengan percobaan kasiski dapat menebak panjang kunci vigenere yang benar dengan persentase kebenaran hingga 93%. Meskipun begitu, kunci dengan panjang 6 karakter tanpa kombinasi angka memiliki jumlah kombinasi lebih dari 300.000.000 (300 juta) kombinasi password dengan kombinasi spesifik 308.915.776 kombinasi kunci. Sedangkan algoritma AES sendiri mampu menyimpan rata-rata 16 karakter dengan maksimal kunci 32 karakter. Dengan demikian pihak yang tidak bertanggung jawab akan membutuhkan waktu yang sangat lama dengan kombinasi kunci sepanjang 32 karakter dengan probabilitas kombinasi kunci sebanyak 1.901.722.457.268.488 e+45 kombinasi kunci.

4.2 PengujianAvalanche Effect

Avalanche effect adalah suatu metode pengujian yang digunakan untuk menentukan seberapa baik suatu algoritma dimana perubahan 1-bit dari kunci maupun plainteks memberikan dampak yang signifikan dalam ciphertextnya, dan perubahan 1-bit pada cipherteks memberikan dampak yang besar pada plainteksnya. Avalanche effect dapat dihitung dengan persamaan (1).

$$AE = \frac{perubahan\ bit\ ciphertext}{jumlah\ bit\ pada\ ciphertext}\ x\ 100\% \qquad (1)$$

Tabel 3 merupakan hasil pengujian AE dengan percobaan pergeseran 1 bit pada karakter paling akhir pada kalimat plainteks. Plainteks berupa kata "jayalahDINUS2020" (merubah karakter '0' (00110000) menjadi '1' (00110001)) seperti pada Tabel 3.

Tabel 3. Pengujian AE ke-1

Plainteks	
jayalahDINUS2020 6a 61 79 61 6c 61 68 44 49 4e 55 53 32 30 32 30	jayalahDINUS2021 6a 61 79 61 6c 61 68 44 49 4e 55 53 32 30 32 31
Perubahan bit	
48	49
Kunci	
nuswantoro21!*?# 6e 75 73 77 61 6e 74 6f 72 6f 32 31 21 2a 3f 23	
Cipherteks	
Ynjn67hEAKFaS9B2q UlzMYnYB2tVIyt0MN +BcRyr3VU=	2tkE55UolKPbMq9qu6 nlKYnYB2tVIyt0MN+ BcRyr3VU=
Avalanche effect	
37,50%	38,28%

Pengujian kedua adalah pengujian kepada kunci yaitu merubah satu karakter pada akhir kunci. Kemudian perubahan karakter '#' (00100011) menjadi '@' (01000000) seperti pada Tabel 4.

Tabel 4. Pengujian AE ke-2

Plainteks	
jayalahDINUS2020 6a 61 79 61 6c 61 68 44 49 4e 55 53 32 30 32 30	
Perubahan bit	
48	50
Kunci	
nuswantoro21!*?# 6e 75 73 77 61 6e 74 6f 72 6f 32 31 21 2a 3f 23	nuswantoro21!*?@ 6e 75 73 77 61 6e 74 6f 72 6f 32 31 21 2a 3f 40
Cipherteks	
Ynjn67hEAKFaS9B2qUl zMYnYB2tVIyt0MN+Bc Ryr3VU=	wsNqh8qoXjAJAsP6 75Yt6by5XPxGWqp qbtyqM57UFZI=
Avalanche effect	
37,5%	39,06%

Pengujian ketiga focus pada kunci dengan merubah satu karakter pada tengah kunci. Kemudian perubahan karakter kunci "nuswantoro21!*?#" merubah karakter 'n'(01101110) menjadi 'm' (01101101) seperti pada Tabel 5.

Tabel 5. Pengujian AE ke-3

Plainteks	
jayalahDINUS2020 6a 61 79 61 6c 61 68 44 49 4e 55 53 32 30 32 30	
Perubahan bit	
48	57
Kunci	
nuswantoro21!*?# 6e 75 73 77 61 6e 74 6f 72 6f 32 31 21 2a 3f 23	nuswamtoro21!*?# 6e 75 73 77 61 6d 74 6f 72 6f 32 31 21 2a 3f 23
Cipherteks	
Ynjn67hEAKFaS9B2q UlzMYnYB2tVIyt0MN +BcRyr3VU=	67JMxDlLsaY080OS gSt4FweI7j5DH1woT 0+XoFfpL5s=
Avalanche effect	
37,5%	44,53%

4.3 Pengujian Lama Waktu Enkripsi Dekripsi

Algoritma diuji dengan dataset yang telah diperoleh sebelumnya dimana setiap dataset diuji dengan karakter kunci yang berbeda. Pengujian dilakukan 3 kali dengan panjang karakter kunci 8, 16, dan 32 karakter. Dengan alur pemrosesan yaitu pencatatan atribut file, eksekusi proses enkripsi, pencatatan atribut file cipher, proses dekripsi, pencatatan file hasil dari proses dekripsi. Pengujian yang pertama adalah pengujian file dokumen dengan panjang kunci 8 karakter. Kunci berupa alfabet 'A – Z' tanpa kombinasi angka dan symbol, sehingga penulis memutuskan untuk menggunakan kunci "dinuss" untuk dokumen PDF dan "dinus" untuk dokumen office seperti pada Tabel 6.

Tabel 6. Pengujian Lama Waktu Enkripsi Dekripsi dengan panjang kunci 8, 16, dan 32

Jenis File	Enkripsi			Dekripsi		
	Waktu (Detik)			Waktu (Detik)		
	Kunci 8	Kunci 16	Kunci 32	Kunci 8	Kunci 16	Kunci 32
.docx	0,2319	0,2411	0,2443	0,4243	0,4243	0,2754
.pdf	0,2216	0,2433	0,2597	0,3152	0,3177	0,4263
.xlsx	0,1843	0,1888	0,1827	0,2435	0,2861	0,2056
.pptx	0,1545	0,1583	0,1541	1,1417	1,3083	1,1894
Rata-rata	0,198	0,20788	0,210	0,531	0,584	0,524
	0,205			0,546		

5. Kesimpulan dan Saran

Dari hasil percobaan yang telah dilakukan pada aplikasi ini, program dapat mengamankan data dengan baik menggunakan kunci algoritma Vigenere dan algoritma AES. Penggabungan antara 2 algoritma tersebut data menjadi semakin aman dan tidak ada kendala yang terjadi, file dienkripsi dan diderkipsi dengan baik. Waktu yang dibutuhkan untuk proses enkripsi dan dekripsi kombinasi algoritma Vigenere dan AES pada dokumen powerpoint cenderung lebih lama dibandingkan dengan dokumen yang lain. Pada penelitian ini telah dilakukan 3 kali percobaan untuk mengetahui nilai Avallanche Effect. Pada pengujian ke 3 diketahui, nilai AE merupakan yang tertinggi dengan perolegan 44,53% menggunakan perubahan bit sebanyak 57, meskipun pada AE percobaab ke 1 dan ke 2 masih mendapat nilai baik. Untuk meningkatkan performa pada penelitian lebih lanjut dapat dilakukan penggabungan dengan algoritma lain maupun penggunakan jenis data yang lebih bervariasi.

Daftar Pustaka :

Ajmera, A., Ghosh, S. S. and Vijayetha, T. (2018) 'Secure LSB Steganography over Modified Vigenère-AES Cipher and Modified Interrupt Key-AES Cipher', in *2018 IEEE Punecon*. IEEE, pp. 1–7. doi: 10.1109/PUNECON.2018.8745393.

Ali, S. M. A. and Hasan, H. F. (2019) 'Novel encryption algorithm for securing sensitive information based on feistel cipher', *Test Engineering and Management*, 2019(November), pp. 10–16.

Arrijal, I. M., Efendi, R. and Susilo, B. (2016) 'Penerapan Algoritma Kriptografi Kunci Simetris Dengan Modifikasi Vigenere Cipher Dalam Aplikasi Kriptografi Teks', *Pseudocode*, 3(1), pp. 69–82. doi: 10.33369/pseudocode.3.1.69-82.

Isfahani, F. Al and Nugraha, F. (2019) 'Implementasi Steganografi LSB dengan Enkripsi Base64 Pada Citra dengan Ruang Warna CMYK', *ScientiCO : Computer Science and Informatics Journal*, pp. 1–8. doi: 10.22487/j26204118.2018.v1.i2.11221.

Lapid, B. and Wool, A. (2019) 'Cache-Attacks on the ARM TrustZone Implementations of AES-256 and AES-256-GCM via GPU-Based Analysis', in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. Springer International Publishing, pp. 235–256. doi: 10.1007/978-3-030-10970-7_11.

Latif, A. (2015) 'IMPLEMENTASI KRIPTOGRAFI MENGGUNAKAN METODE ADVANCED ENCRYPTION STANDAR (AES) UNTUK PENGAMANAN DATA TEKS', *Jurnal Ilmiah Mustek Anim Ha*, 4(2), p. 32.

Maricar, M. A. and Sastra, N. P. (2018) 'Efektivitas Pesan Teks Dengan Cipher Substitusi, Vigenere Cipher, dan Cipher Transposisi', *Majalah Ilmiah Teknologi Elektro*, 17(1), p. 59. doi: 10.24843/mite.2018.v17i01.p08.

Mathur, R., Pathak, V. and Bandil, D. (2019) *Emerging Trends in Expert Applications and Security*, *Emerging Trends in Expert Applications and Security*. Edited by V. S. Rathore et al. Singapore: Springer Singapore (Advances in Intelligent Systems and Computing). doi: 10.1007/978-981-13-2285-3.

Nasution, S. D. *et al.* (2017) 'Data Security Using Vigenere Cipher and Goldbach Codes Algorithm', *International Journal of Engineering Research & Technology (IJERT)*, 6(01), pp. 360–363.

Nilesh, D. and Nagle, M. (2014) 'The new cryptography algorithm with high throughput', in *2014 International Conference on Computer Communication and Informatics*. IEEE, pp. 1–5. doi: 10.1109/ICCCI.2014.6921739.

Sangeeta and Kaur, E. A. (2017) 'A Review on Symmetric Key Cryptography Algorithms', *International Journal of Advanced Research in Computer Science*, 8(4), pp. 358–362.

Sari, W. S. *et al.* (2017) 'A Good Performance OTP Encryption Image based on DCT-DWT Steganography', *TELKOMNIKA*, 15(4), pp. 1987–1995. doi: 10.12928/TELKOMNIKA.v15i4.5883.

Sharma, N., Prabhjot and Kaur, H. (2017) 'A Review of Information Security using Cryptography Technique.', *International Journal of Advanced Research in Computer Science*, 8(4), pp. 323–326. Available at: http://web.a.ebscohost.com/ehost/detail/detail?vid=0&sid=852854fe-f74a-47d8-b2c5-

36c892e545ea%40sessionmgr4006&bdata=Jmxhbmc9ZXMmc2l0ZT1laG9zdC1saXZl#AN=123430611&db=aci.

Subandi, A. *et al.* (2018) 'Vigenere cipher algorithm modification by adopting RC6 key expansion and double encryption process', *IOP Conference Series: Materials Science and Engineering*, 420(1), p. 012119. doi: 10.1088/1757-899X/420/1/012119.

Susanto, A. *et al.* (2019) 'Dual Security Method for Digital Image using HBV Encryption and Least Significant Bit Steganography', in *Journal of Physics: Conference Series*. doi: 10.1088/1742-6596/1201/1/012024.

TOUIL, H., AKKAD, N. EL and SATORI, K. (2020) 'Text Encryption: Hybrid cryptographic method using Vigenere and Hill Ciphers', in *2020 International Conference on Intelligent Systems and Computer Vision (ISCV)*. IEEE, pp. 1–6. doi: 10.1109/ISCV49265.2020.9204095.

Triandi, B. *et al.* (2018) 'Improve Security Algorithm Cryptography Vigenere Cipher Using Chaos Functions', in *2018 6th International Conference on Cyber and IT Service Management (CITSM)*. IEEE, pp. 1–5. doi: 10.1109/CITSM.2018.8674376.

Tulloh, A. R., Permanasari, Y. and Harahap, E. (2016) 'Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen', *Jurnal Matematika UNISBA*, 2(1), pp. 118–125. Available at: https://ejournal.unisba.ac.id/index.php/matematika/article/view/4067.

Vittal Kumar Mittal | Manish Mukhija (2019) 'Cryptosystem Based on Modified Vigenere Cipher using Encryption Technique', *International Journal of Trend in Scientific Research and Development (IJTSRD) International Journal of Trend in Scientific Research and Development*, 3(5), pp. 1936–1939. doi: https://doi.org/10.31142/ijtsrd27878.