IMPLEMENTASI KRIPTOGRAFI SUPERENKRIPSI *VIGENERE CIPHER* DAN *ADVANCED ENCRYTION STANDARD* (AES) PADA PENGAMANAN DATA RIWAYAT PASIEN RUMAH SAKIT

Fitri Nuraeni[1], Yuda Purnama Putra[2], Indri Hendriyani[3]
[1,2,3]Program Studi Teknik Informatika, STMIK Tasikmalaya, Tasikmalaya
e-mail: [1]nufi3@stmik-tasikmalaya.ac.id, [2] yudaestilo@gmail.com, [3]indri4998@gmail.com

Abstrak

Rekam medis merupakan dokumen yang berisi data riwayat kesehatan pasien, dimana datanya perlu dijamin kerahasiaannya dalam proses pengolahan data melalui sistem informasi. Dengan memanfaatkan kriptografi, sistem informasi dapat mengamankan informasi riwayat rekam medis pasien dari orang yang tidak berhak untuk mengetahui apalagi memanipulasi data tersebut. Untuk memberikan jaminan kerahasiaan yang lebih kuat, perlu digunakan sistem kriptografi berupa super enkripsi, salah satunya kolaborasi antara Vigenere Cipher dan AES-128-CBC. Untuk implemantasi super enkripsi ini, ditambahkan suatu fungsi enkripsi dan dekripsi pada sistem informasi rekam medis berbasis web. Sedangkan untuk mengetahui kualitas enkripsi sistem kriptografi super enkripsi ini dilakukan eksperimen dengan membandingkan ukuran file sample plainteks dengan cipherteks, membandingkan waktu enkripsi dan dekripsi, nilai entropi, nilai korelasi dan grafik histogram. Hasil eksperimen didapat sistem kriptografi dengan Super Enkripsi Vigenere Cipher dan AES-128-CBC memiliki keunggulan dari nilai korelasi dan entropi, namun masih memiliki waktu proses yang lebih lama daripada menggunakan 1 algoritma.

Kata Kunci-- aes, kriptografi, rekam medis, super enkripsi, vigenere

Abstract

Medical records are documents that contain patient's medical history data, where the data needs to be guaranteed confidentiality in the processing of data through information systems. By utilizing cryptography, the information system can secure information on the patient's medical history from people who have no right to know let alone manipulate the data. To provide a guarantee of stronger confidentiality, it is necessary to use a cryptographic system in the form of super encryption, one of which is collaboration between Vigenere Cipher and AES-128-CBC. For the implementation of super encryption, an encryption and decryption function is added to the web-based medical record information system. Meanwhile, to determine the encryption quality of the super encryption cryptographic system, an experiment was carried out by comparing the size of the plaintext sample file with the ciphertext, comparing the time of encryption and decryption, entropy values, correlation values and histogram graphics. The experimental results obtained by the cryptographic system with Super Encryption Vigenere Cipher and AES-128-CBC have the advantage of correlation and entropy values, but still have a longer processing time than using 1 algorithm.

Keywords— aes, cryptography, medical record, super encryption, vigenere

1. PENDAHULUAN

Rekam Medis merupakan fakta yang berkaitan dengan keadaan pasien, riwayat penyakit dan pengobatan masa lalu serta saatu ini yang tertulis oleh profesi kesehatan

yang memberi pekayanan kepada pasien. Fasilitas Pelayanan Kesehatan berkewajiban menjaga kerahasiaan rekam medis karena memuat data pribadi pasien[1], berupa "catatan dan dokumen tentang identitas pasien, pemeriksaan, pengobatan, tindakan dan pelayanan lain yang diberikan kepada pasien pada sarana pelayanan kesehatan"[2]. Tujuan terselengaranya pelayanan rekam medis adalah untuk menunjang tercapainya tertib administrasi. Tanpa adanya suatu sistem pengolahan rekam medis yang baik dan benar, mustahil tertib administrasi rumah sakit berhasil sebagaimana yang diharapkan. Dalam praktik pengelolaan rekam medis, banyak fasilitas pelayanan kesehatan menggunakan sistem informasi manajemen (SIM) karena sangat membantu dalam pencarian data pasien dan mendukung pada proses pelayanan kesehatan lainnya[3]. Namun, penggunaan SIM ini masih belum memperhatikan masalahan keamanan data seperti kerahasiaan, integritas data dan otentifikasi data[4]. Oleh karena itu, perlu dilakukan suatu upaya pengamanan untuk menjaga informasi dari pihak-pihak yang tidak memiliki otoritas atau hak akses.

Pengamanan data rekam medis pada suatu sistem informasi manajemen dapat menggunakan algoritma Vigenere Cipher karena algoritma ini cukup popular karena mudah dipahami dan diimplementasikan[4]. Akan tetapi algoritma ini menjadi lemah dengan adanya kunci yang pendek sehingga harus digunakan secara berulang[5], hal ini dapat memudahkan kriptanalisis dalam menebak kunci dengan metode kasiski.

Untuk lebih meningkatkan tingkat kesulitan kriptanalisis, vigenere cipher dapat dikombinasikan dengan algoritma lainnya[5]. Kombinasi dua algoritma dalam sistem kriptografi yang disebut super enkripsi dapat meningkatkan keamanan data karena sistem kriptografi menjadi lebih kuat[6]. Banyak sekali algoritma kriptografi yang dapat digunakan bersama vigenere cipher untuk membangun super enkripsi khusus untuk data teks, salah satunya DES, AES, IDEA dan Blowfish. Namun pada hasil penelitian yang membandingkan algoritma-algoritma tersebut diketahui bahwa untuk proses enkripsi dan dekripsi data teks AES merupakan algoritma tercepat dibandingkan 3 algortima tersebut[7].

Kombinasi Vigenere Cipher & AES-128 untuk data berupa teks telah dapat diimplementasikan dengan baik[8]. AES-128 bits merupakan ukuran blok yang tercepat dalam proses pemrosesan enkripri[9], karena semakin kecil kunci blok yang digunakan maka semakin cepat dalam pemrosesannya. Oleh karena itu, proses super enkripsi vigenere cipher & AES-128 memungkinkan untuk dilakukan pada pengamanan data rekam medis. Namun, untuk memastikan berapa besar peningkatan kualitas enkripsi dari super enkripsi ini, maka dilakukan eksperimen enkripsi pada sampel data rekam medis, kemudian hasil enkripsi tersebut dibandingkan dengan penggunaan cipher tunggal vigenere saja, tidak hanya dari waktu proses, namun dari perbandingan nilai korelasi dengan teks asli, nilai entropi serta perbandingan histogramnya.

2. METODE PENELITIAN

2.1. Algoritma Vigene Chiper

Vigenere Cipher pada dasarnya menggunakan teknik yang sama dengan Caesar Cipher, bedanya dalam Vigener Cipher setiap karakter pada plainteks dapat dienkripsikan dengan kunci yang berbeda. Karakter pertama pada plainteks dienkripsikan dengan kunci berupa karakter pertama dari kata kunci dan seterusnya, sifat *polyalphabetic* yang dimiliki oleh Vigener Cipher diimplementasikan dengan bujursangkar Vigenere Cipher. Sifat periodiknya terlihat apabila panjang kunci lebih kecil dari pada panjang plainteks, kunci dapat di ulang penggunanya sampai panjang kunci sama dengan panjang plainteks jika panjang kunci hanya satu karakter, enkripsinya sama dengan Caesar Cipher biasa.

Enkripsi Vigenere Cipher secara matematis dapat ditulis dalam bentuk:

$$C_i = (P_i + K_i) mod\ n \quad (1)$$

Ket :

n = jumlah karakter alphabet
c = cipherteks
p = plainteks
k = kunci
i = 1,2,3,..., posisi karakter

Sedangkan untuk proses dekripsinya adalah sebagai berikut:

$$P_i = (C_i - K_i) mod\ n \quad (2)$$

Ket :
n = jumlah karakter alphabet
c = cipherteks
p = plainteks
k = kunci
i = 1,2,3,..., posisi karakter

2.2. Algoritma Advanced Encryption Standard (AES)

Algoritma AES termasuk pada algoritma kriptografi modern simetris dengan menggunakan blok ukuran tertentu dalam proses enkripsi dan dekripsinya. Algoritma AES ini menggunakan kunci kriptografi 128, 192, dan 256 bits untuk mengenkripsi dan dekripsi data pada blok 128 bits.

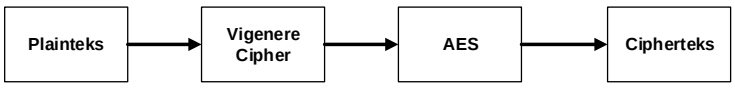
Setiap masukan 128 bit *plaintext* dimasukan ke dalam state yang berbentuk bujursangkar 4x4 byte, state ini di XOR dengan key dan selanjutnya diolah 10 kali dengan subtitusi-transformasi linear-*addkey*, dan diakhir diperoleh *ciphertext*. Berikut ini adalah operasi Rijndael (AES) yang menggunakan 128 bit kunci:

1) Ekspansi kunci utama (dari 128 bit menjadi 1408 bit);
2) Pencampuran subkey;
3) Ulang dari i=1 sampai i=10 Transformasi : ByteSub (subtitusi per byte) ShiftRow (pergeseran byte perbaris) MixColumn (Operasi perkalian GF(2) per kolom);
4) Pencampuran subkey dengan XOR;
5) Pencampuran subkey.

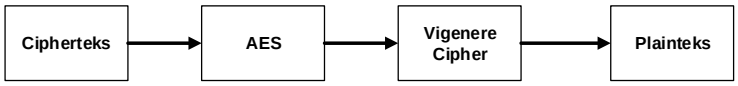
2.3. Algoritma Superenkripsi Vigenere + Advanced Encryption Standard (AES)

Proses perancangan Enkripsi dan Deskripsi pada penggabungan algoritma *Vigenere Cipher* dan *Advanced Enkripsi Standard* (AES) diantaranya :

Enkripsi



Deskripsi



Gambar 2 Skema proses enkripsi dan dekripsi super enkripsi

Dengan adanya penggabungan dua buah cipher hal tersebut bertujuan untuk mendapatkan Cipher yang lebih kuat sehingga tidak mudah untuk dipecahkan, dan juga untuk mengatasi penggunaan Cipher tunggal yang secara komparatif lemah. Untuk melakukan teknik super enkripsi seperti pada gambar 2, pertama pesan dienkripsi dengan algoritma vigenere cipher, dan kode yang didapat dari proses pertama tersebut dienkripsi lagi dengan menggunakan AES-128.

Begitupun sebaliknya untuk proses dekripsi, *ciphertext* diproses menggunakan AES-128 yang kemudian dilanjutkan dengan *vigenere cipher*, dan didapatkan kembali *plaintext* semula.

Contoh plainteks:

No Rekam Medis : rm-20190522.0001
NIK : 221018291029102
Tanggal kunjungan : 2019-05-02
Jenis Perawatan : Rawat Inap
Poliklinik : Poli Anak
Diagnosa : of dd thyfoid
Tindakan : Inpus Putrolit 25 tpm
Obat : probiokid 1x1, nendia 4x1, sanmol 4x1/4

Proses pertama adalah melakukan enkripsi menggunakan vigenere cipher dengan menggunakan kunci “rekam medis rahasia”, dan didapatkan cipherteks 1 yaitu:

4s 1ewmq pmvzs : ym-k81q4f2e.c439
5zk : 92j81p6j1ced48k
aaugyil 1yxj6zkdv : kh1g-0n-82
0ixi4 1iuierthn : 9iwrx snm1
trt01lpn0s : p5ps azmo
gqsxnvss : wf uh 3harsll
bznka2in : zrzu4 1ywz62i0 2n 1p3
sla5 : 1vrj05kpd j51, 4ixdum 809, arnto3 cxi/8

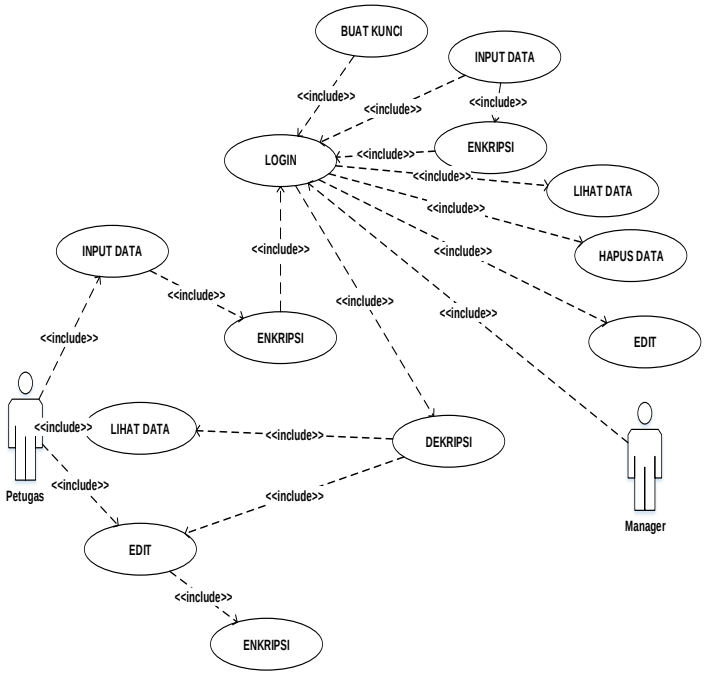
Cipherteks tersebut kemudian diproses menggunakan AES-128 menggunakan kunci yang sama, dan menghasilkan cipherteks akhir seperti berikut:

aCNwpg+4GnNSqrch2JDL0Aqi6KLvYVM5xBArBEIuZdaViHF29sdORPjXo6B3yfS3dabxiecBvAPiui
6kViNEshm2N2tTCvPXKI+jXzzk+3/SDwTvI3dO5RZ/ZvNTV0nq2cNVdXkBZzFyVztKfbla+cl3Q7h/
zSakH/53FVPVmHKUXLO+AutPTgaD/ZbHDXyUeEOV4ivt+5EXPUCKYMve7lWTBBz2u2zuRB39
GMDQgm1QkdFF4vZuhLYeepl441AsRkt7JQih47jcQyy6Z343B6zaTuiEjf87qeV9vuq4pIhDZnaHfgR
WqS1y2ha1LOZ6MkNxNZK1ZokWV2NI4zBRYw==

Hasil super enkripsi yaitu penggabungan dua algoritma yaitu Vigenere Cipher dan AES, dengan cara dua kali di proses pertama di proses oleh Vigenere Cipher dan menghasilkan Cipherteks, lalu Cipherteks tersebut di proses oleh AES dan menghasilkan pengkodean yang sangat sulit di pecahkan karena bentuknya yang sudah jauh berbeda dengan bentuk asli plainteksnya.

3. HASIL DAN PEMBAHASAN

Untuk mengimplementasikan superenkripsi ini, maka dibuatkan suatu fungsi enkripsi dan dekripsi yang ditambahkan pada suatu sistem informasi arsip rekam medis. Gambar 3 merupakan alur yang terdapat di rekam medis dengan data yang terenkripsi, tentunya harus login terlebih dahulu. Petugas hanya bisa melakukan input, lihat, dan edit data. Sedangkan Kepala Bagian Rekam Medis bisa buat kunci, input data, lihat data, hapus data dan edit. Untuk melihat data tentunya data harus di dekripsikan terlebih dahulu, untuk mengdekripsikan nya petugas harus memasuki kata sandi yang hanya diketahui oleh petugas dan kepala bagian rekam medis.

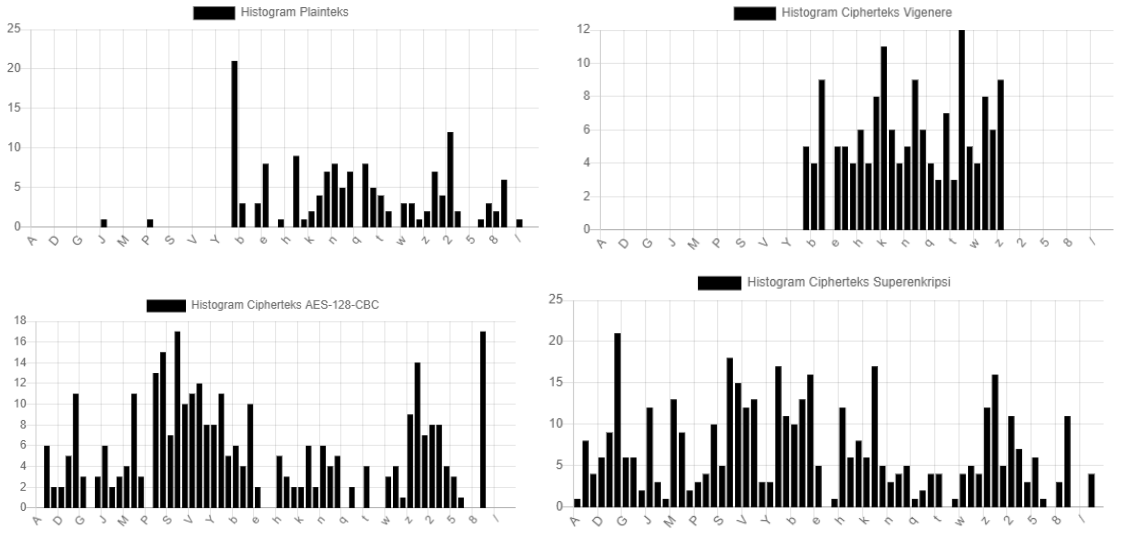


Gambar 3 usecase diagram sistem informasi rekam medis dengan super enkripsi

Untuk mengetahui kualitas enkripsi dari super enkripsi ini, dilakukan uji coba proses enkiprsi pada sampel data rekam medis sebanyak 3 kali yaitu 1) enkripsi vigenere cipher; 2) enkripsi AES-128; 3) Superenkripsi vigenere-AES128. Kemudian dicari lama proses, besar file hasil, nilai entropi file hasil, nilai korelasi dan grafik histogram file hasil masing-masing enkripsi, seperti pada gambar 4 berikut.

Hasil Pengujian Waktu Eksekusi, Besar File, Nilai Entropi & Koefisien Korelasi

File Plainteks	Size Plainteks	Entropi Plainteks	Kunci	Algoritma	Waktu Enkripsi	Waktu Dekripsi	Size Cipherteks	Entropi Cipherteks	Korelasi
data.txt	185 byte	4,6793	kunci	Vigenere	2,863 ms	2,909 ms	175 byte	4,5783	0,2304
data.txt	185 byte	4,6793	kunci	AES-128-CBC	0,185 ms	0,069 ms	330 byte	5,3664	0,2458
data.txt	185 byte	4,6793	kunci	Superenkripsi	4,236 ms	4,303 ms	442 byte	5,5591	0,0097



Gambar 4 Hasil pengujian pada sampel data

Untuk hasil uji coba salah satu sampel proses enkripsi dari super enkripsi *vigenere* cipher dan AES-128 ini, dilihat dari waktu dan ukuran hasilnya lebih lama dan besar. Tetapi melihat hasil korelasi dan entropi bagus, karena semakin kecil ukuran korelasi semakin bagus dan semakin besar ukuran entropi mendekati 8 maka semakin bagus. Begitupun dari perbandingan grafik histogram, file hasil superenkripsi memiliki persebaran karakter yang lebih merata disbanding dengan file hasil proses lainnya. Hal ini bagus, karena cipherteks dari superenkripsi lebih kuat dari serangan analisis frekuensi, karena tidak memunculkan karakter-karakter tertentu yang terlalu sering muncul.

Tabel 1 Perbandingan Ukuran File Hasil & Waktu Proses Enkripsi Vigenere Cipher, AES-128, Super enkripsi Vigenere+AES-128

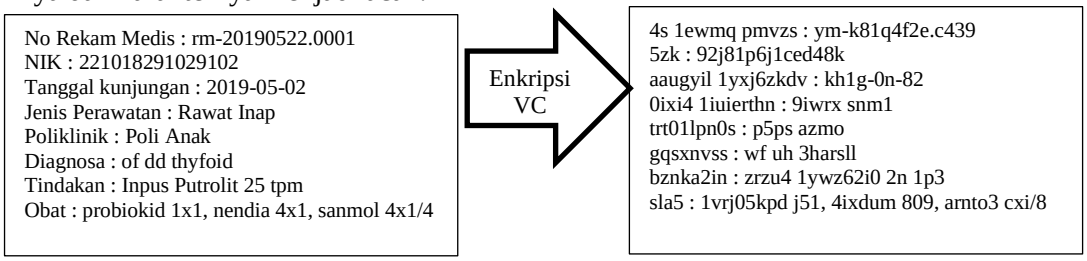
Plainteks	Ukuran Plainteks (bytes)	Ukuran Cipherteks (bytes)			Waktu Enkripsi (ms)		
		V.C	AES	SE	V.C	AES	SE
File 1	119	109	330	358	4,727	0,103	4,999
File 2	133	235	330	610	10,270	0,095	10,342
File 3	158	148	330	414	5,027	0,129	5,203
File 4	227	217	330	526	8,751	0,077	8,390
File 5	255	245	330	586	10,638	0,082	8,831
File 6	262	252	330	624	9,037	0,078	9,476
File 7	273	263	330	614	11,466	0,077	9,397
File 8	282	272	330	666	9,915	0,087	9,776
File 9	282	272	330	642	12,185	0,096	11,115
File 10	286	276	330	638	11,863	0,080	9,825
Rata-rata		**229**	**330**	**568**	**9,388**	**0,090**	**8,735**

Pada tabel 1 dapat dilihat hasil perbandingan antara vigenere cipher, AES, dan SuperEnkripsi, waktu enkripsi superenkripsi (SE) lebih besar karena plainteks diproses sebanyak dua kali, yaitu proses enkripsi vigenere cipher kemudian dilanjutkan dengan AES seperti pada gambar 2. Jika dibandingkan dengan sistem kriptografi yang menggunakan 1 algoritma, sistem kriptografi superenkripsi jelas menjadi lebih lama. Lama proses enkripsi ini juga sangat dipengaruhi oleh *coding* program masing-masing sistem kriptografi yang digunakan, seperti lama proses enkripsi AES lebih cepat karena program sistem kriptografi tersebut, menggunakan sistem konversi simbol karakter ke angka desimal ASCII kemudian mengkonversi ke rangkaian binner digital (bit). Sedangkan pada program pada sistem kriptografi vigenere cipher (VC) memiliki waktu yang lebih lama, karena programnya menggunakan sistem pencarian indeks pada deret/ array alphabet. Sehingga makin besar file maka karakter dalam file tersebut semakin banyak, dan proses pencarian indeks alphabet diulang sebanyak karakter dalam file sehingga waktu lebih lama. Lamanya proses pada vigenere cipher (VC) ini terbawa pada proses super enkripsi (SE), karena sistem kriptografi dengan SE menggabungkan VC dan AES.

Tabel 2 Perbandingan Nilai Entropi Dan Nilai Korelasi Hasil Proses Enkripsi Vigenere Cipher, Aes-128, Super Enkripsi Vigenere+Aes-128

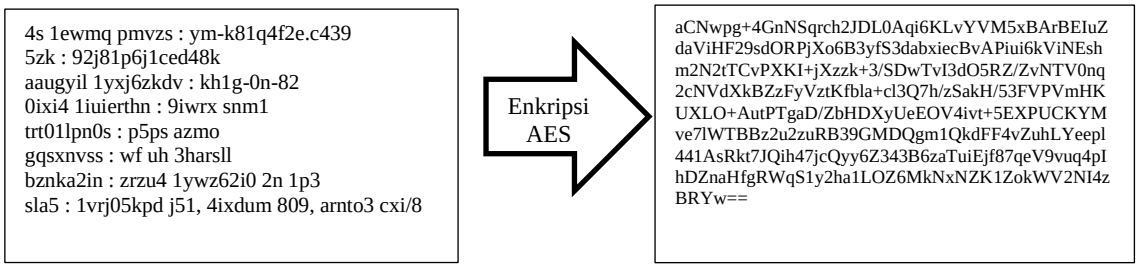
Plainteks	Nilai Entropi			Nilai Korelasi		
	V.C	AES	SE	V.C	AES	SE
File 1	4,4595	5,4136	5,4247	0,2850	0,3562	0,1807
File 8	4,5533	5,4312	5,6250	0,2143	0,2804	0,2435
File 2	4,5298	5,4172	5,5427	0,2607	0,3864	0,2234
File 7	4,4895	5,4441	5,6006	0,2572	0,3553	0,2286
File 10	4,4058	5,4246	5,5980	0,2784	0,4026	0,4270
File 4	4,5350	5,4155	5,6072	0,3158	0,3559	0,3023
File 5	4,5247	5,4155	5,6301	0,2958	0,2549	0,2746
File 3	4,5386	5,4502	5,6110	0,2467	0,3568	0,3258
File 9	4,5546	5,3595	5,6277	0,2854	0,2990	0,2802
File 6	4,5546	5,4270	5,6162	0,2846	0,4487	0,2093
Rata-Rata	4,5145	5,4198	**5,5883**	0,2724	0,3496	**0,2695**

Namun, pada tabel 2 dapat dilihat bahwa hasil perbandingan antara korelasi dengan entropi, Super enkripsi memiliki nilai korelasi kecil atau mendekati 0 dan nilai entropi besar atau mendekati angka 8, sehingga SE memiliki kualitas enkripsi yang lebih bagus dibandingkan dengan sistem kriptografi 1 algoritma yang lainnya. Hal ini dikarenakan file cipherteks yang dihasilkan SE mengandung karakter yang lebih acak dibandingkan hasil dari algoritma lainnya. Pada sistem kriptografi super enkripsi (SE), fase pertama setiap karakter yang ada diplainteks diproses oleh vigenere cipher sehingga disubsitusikan dengan karakter lain yang ada pada alphabet, seperti pada gambar 5 dibawah ini. File yang dihasilkan menjadi berbeda dengan file aslinya dan karakternya menjadi acak.



Gambar 5 Fase 1 Sistem Kriptografi Superenkripsi

Selanjutnya memasuki fase ke-2, file hasil dari fase 1 diproses dengan algoritma AES, masing-masing dibagi-bagi pada blok 128 bit kemudian diproses dengan kunci dengan ukuran blok 128 juga. Karena AES memproses rangkaian bit data sehingga semua karakter ikut terproses dan menghasilkan deretan bit yang berbeda dengan file sebelumnya kemudian dirubah kembali menggunakan fungsi base64 encode, sehingga file yang dihasilkan pada fase 2 ini menjadi makin acak dan berbeda dengan file aslinya. Hal inilah yang menyebabkan nilai korelasi SE menjadi lebih kecil dibandingkan dengan yang lainnya. File hasil fase 2 ini juga memiliki tingkat acak yang sangat tinggi sehingga nilai entropi lebih besar dibandingkan yang lainnya.



Gambar 6 Fase 2 Sistem Kriptografi Superenkripsi

4. KESIMPULAN

Berdasarkan hasil dari penelitian super enkripsi ini, dapat diambil kesimpulan yaitu :

1) Dari hasil pengujian Super Enkripsi dibandingkan dengan Vigenere Cipher dan AES 128-CBC, dari segi waktu masih lama dan dari ukuran file masih besar. Tetapi dari hasil Korelasi dan entropi Super Enkripsi mengahsilkan hasil yang bagus, karena semakin kecil ukuran korelasi semakin bagus, dan semakin besar ukuran entropi semakin bagus.
2) Dengan dirancangnya implementasi Super Enkripsi pada Pengamanan data rekam medis mengurangi resiko terjadinya pembocoran data/pencurian data, karena menggunakan kriptografi dengan dua algoritma yaitu vigenere cipher dan aes mempersulit orang yang tidak

memiliki wewenang untuk memanipulasi data atau menghapus data tanpa persetujuan yang bersangkutan.

5. SARAN

Untuk pengembangan selanjutnya, dapat dipilih pasangan algoritma Vigenere Cipher dengan algoritma lain agar hasil super enkripsi memiliki kekuatan dari entropi dan korelasi yang baik lagi. Serta dapat juga menambahkan proses kompresi agar ukuran lebih kecil dan menghemat tempat penyimpanan dan proses pengolahan data.

DAFTAR PUSTAKA

[1] R. H. Gemala, *Pedoman Manajemen Informasi Kesehatan di Sarana Pelayanan Kesehatan*. Jakarta: Universitas Indonesia, 2008.

[2] M. K. R. Indonesia, *Peraturan Menteri Kesehatan Republik Indonesia Nomor 269/Menkes/Per/III/2008 tentang Rekam Medis*. Indonesia, 2008, pp. 1–7.

[3] S. Gunawan and Sukadi, "Sistem Informasi Rekam Medis Pada Rumah Sakit Umum Daerah (RSUD) Pacitan Berbasis Web Base," *J. Speed – Sentra Penelit. Eng. dan Edukasi*, vol. 4, no. 4, pp. 18–24, 2011.

[4] E. Gunadhi and A. Sudrajat, "Pengamanan data rekam medis pasien menggunakan kriptografi vigenere cipher," *J. Algoritm.*, vol. 13, no. 1, 2016.

[5] A. M. H. Padede, H. Manurung, and D. Filina, "Algoritma Vigenere Cipher Dan Hill Cipher Dalam Aplikasi Keamanan Data Pada File Dokumen," *J. Tek. Inform. Kaputama*, vol. 1, no. 1, pp. 26–33, 2017.

[6] E. Setyaningsih, C. Iswahyudi, and N. Widyastuti, "Konsep Super Enkripsi untuk Meningkatkan Keamanan Data Citra," in *Prosiding Seminar Nasional Sistem & Teknologi Informasi (SNASTI) 2011*, 2011, p. ISLP 7-ISLP 10.

[7] D. A. Meko, "Perbandingan Algoritma DES, AES, IDEA Dan Blowfish dalam Enkripsi dan Dekripsi Data," *J. Teknol. Terpadu*, vol. 4, no. 1, pp. 8–15, 2018.

[8] M. Arifin and M. Mufti, "IMPLEMENTASI KRIPTOGRAFI CHATTING MENGGUNAKAN METODE VIGENERE DAN AES 128 BERBASIS WEB," *SKANIKA*, vol. 1, no. 1, pp. 102–109, 2018.

[9] A. F. Marisman and A. Hidayati, "Pembangunan Aplikasi Pembanding Kriptografi Dengan Caesar Cipher Dan Advance Encryption Standard (Aes) Untuk File Teks," *J. Penelit. Komun. dan Opini Publik*, vol. 19, no. 3, pp. 213–222, 2015.