SNESTIK

Seminar Nasional Teknik Elektro, Sistem Informasi, dan Teknik Informatika

https://ejurnal.itats.ac.id/snestik dan https://snestik.itats.ac.id

Informasi Pelaksanaan :
SNESTIK V - Surabaya, 26 April 2025
Fakultas Teknik Elektro dan Teknologi Informasi, Institut Teknologi Adhi Tama Surabaya

Informasi Artikel:
DOI : 10.31284/p.snestik.2025.7425

Prosiding ISSN 2775-5126

Fakultas Teknik Elektro dan Teknologi Informasi-Institut Teknologi Adhi Tama Surabaya
Gedung A-ITATS, Jl. Arief Rachman Hakim 100 Surabaya 60117 Telp. (031) 5945043
Email : snestik@itats.ac.id

Implementasi Kriptografi Super Enkripsi Vigenere Cipher Dan Data Encryption Standard (Des) Pada Pengamanan Data Data Rekam Medis Pasien Rumah Sakit

Alief Saputra Lumban Gaol, Hafidz Anggara Amiral, S. Nurmuslimah

Institut Teknologi Adhi Tama Surabaya
e-mail: alief.saputra2526@gmail.com

ABSTRACT

Medical records are confidential data documents containing facts that depict the patient's condition that the healthcare professionals in the hospital have created. Due to the lack of proper medical record data processing, the hospital may face difficulties in managing administration. One method to secure medical record data in the management information system (MIS) is by employing the Vigenère Cipher algorithm. However, the Vigenère Cipher algorithm has weaknesses, so it requires combining it with other algorithms. The combination of two or more encryption algorithms in cryptography is called super encryption, which enhances the data security of the cryptographic system. In this research, the Vigenère cipher algorithm is combined with the Data Encryption Standard (DES). The DES algorithm has several advantages, including a relatively high level of security, easy implementation, and capability in different operating modes such as electronic codebook (ECB), cipher block chaining (CBC), and output feedback (OFB). This study is entitled "Implementing Super Encryption Cryptography: Vigenère Cipher and Data Encryption Standard (DES) to Secure Hospital Patient Medical Record Data. The test applied the Avalanche effect with average values as follows: Vigenère Cipher 5.96%, DES 20.14%, and Vigenère Cipher and DES 20.35%. Among the three tested methods, the highest Avalanche Effect (AE) value existed in the Vigenère Cipher and DES tests at 20.35%. Due to its highest complexity and randomness, it is suitable for use in securing hospital patient medical record data.

Keywords: *cryptography, encryption, Vigenère Cipher, DES, Avalanche Effect.*

ABSTRAK

Rekam medis adalah dokumen data confidential berisikan fakta yang menggambarkan keadaan pasien yang dibuat oleh petugas kesehatan di rumah sakit. Dengan tidak adanya pengolahan data rekam medis yang benar, rumah sakit akan menjadi lebih susah dalam mengatur administrasi sebagaimana yang diharapkan. Salah satu cara yang dapat digunakan untuk mengamankan data rekam medis pada sistem informasi manajemen (SIM) adalah dengan menggunakan algoritma Vigenère Cipher. Algoritma Vigenère Cipher memiliki kelemahan sehingga diperlukan penggabungan dengan algoritma lainnya. Kombinasi dari dua atau lebih algoritma enkripsi dalam kriptografi disebut super enkripsi, yang mana menjadikan sistem kriptografi menjadi lebih kuat dalam meningkatkan keamanan data. Dalam penelitian ini algoritma Vigenère Cipher digabungkan dengan DES (Data Encryption Standards). Algoritma DES memiliki beberapa kelebihan yaitu Tingkat keamanan yang cukup tinggi, implementasi mudah, dan kemampuan dalam mode operasi berbeda-beda seperti operasi Electronic Codebook (ECB), Cipher Block Chaining (CBC) dan Output Feedback (OFB). Pada penelitian "Implementasi Kriptografi Super Enkripsi Vigenère Cipher dan Data Encryption Standard (DES) Pada Pengamanan Data Rekam Medis Pasien Rumah Sakit" dilakukan pengujian dengan menggunakan Avalanche effect dengan nilai rata-rata : Vigenère Cipher 5,96%, DES 20,14%, dan Vigenère Cipher & DES 20,35%. Dari tiga metode yang diujikan, diperoleh nilai AE tertinggi yaitu pada pengujian Vigenère Cipher & DES sebesar 20,35%. Sehingga memiliki tingkat kerumitan dan keacakan tertinggi yang menjadikannya cocok untuk digunakan dalam pengamanan data rekam medis pasien rumah sakit.

Kata kunci: Kriptografi, Enkripsi, Vigenère Cipher, DES, Avalanche Effect.

PENDAHULUAN

Menjaga kerahasiaan rekam medis pasien sudah menjadi kewajiban dan tanggung jawab Fasilitas pelayanan Kesehatan karena rekam medis mengandung data pribadi pasien, berupa "dokumen serta catatan identitas pasien, penyakit, pengobatan, pemeriksaan, pelayanan dan tindakan lain yang diberikan kepada pasien. Oleh karena itu, menjaga kerahasiaan rekam medis pasien yang diberikan di fasilitas pelayanan kesehatan merupakan hal yang sangat penting [1]. Salah satu cara yang dapat digunakan untuk mengamankan data rekam medis pada sistem informasi manajemen (sim) adalah dengan menggunakan algoritma Vigenère Cipher. RS Kasih herlina memiliki sebuah program sistem informasi manajemen yang digunakan untuk mengolah data pasien, tetapi sistemnya hanya digunakan untuk mengolah pasien tanpa adanya keamanan terhadap privasi pasien sehingga dinilai belum memadai untuk melindungi data rekam medis pasien dengan baik. Hal ini menimbulkan risiko terhadap kebocoran informasi data pasien yang dilakukan oleh pihak atau sekelompok orang yang tidak memiliki otoritas yang dapat mengancam privasi dan keamanan pasien. Dengan tidak adanya pengolahan data rekam medis yang benar, rumah sakit akan menjadi lebih susah dalam mengatur administrasi dari sebagaimana yang diharapkan. Oleh sebab itu Dibutuhkan adanya upaya dalam pengamanan untuk menjaga informasi data rekam medis dari orang atau sekelompok orang yang tidak memiliki hak akses atau otoritas. Terdapat banyak algoritma kriptografi yang dapat gabungkan bersama algoritma vigenere chiper untuk membuat suatu super enkripsi terlebih khususnya pada data teks, salah satu algoritma yang akan cocok untuk digabungkan antara lain : IDEA, BLOWFISH, AES dan DES [1]. Penelitian mengenai super enkripsi kombinasi Vigenère Cipher dan Advanced Encryption Standard (AES) telah dilakukan sebelumnya dan menunjukkan hasil yang cukup baik dalam mengamankan data teks [1]. Namun, hingga saat ini belum banyak penelitian yang membandingkan efektivitas kombinasi Vigenère Cipher dengan algoritma kriptografi lainnya, seperti Data Encryption Standard (DES), dalam konteks pengamanan data rekam medis. Algoritma Des (Data Encryption Standard) dapat digunakan dalam aplikasi sistem informasi manajemen (SIM) rekam medis. DES merupakan kriptografi simetris dan termasuk dalam jenis cipher block. Des dapat mengenkripsi 64 bit plaintext menjadi 64 bit ciphertext dengan memakai 56 bit subkey (subkunci). Subkunci ini diperoleh dari external key (kunci eksternal) yang berukuran 64 bit [2]. Penelitian ini bertujuan untuk mengetahui seberapa besar peningkatan

kualitas enkripsi dari penggunaan Super enkripsi kombinasi algoritma Vigenere Cipher dan Data Encryption Standard (DES) dalam pengamanan data rekam medis pasien di rumah sakit.

METODE

Algoritma Vigenere Cipher

Dalam proses pengerjaannya Vigenère Cipher sangat mirip dengan Caesar Cipher, adalah dengan menggeser setiap huruf dalam pesan (plainteks) sesuai dengan nilai kunci dalam deret alphabet. Namun, Vigenère Cipher menggunakan metode pertukaran abjad majemuk, dimana setiap huruf dalam pesan dienkripsi dengan memakai kunci yang berbeda (sesuai dengan pertukaran abjad), sedangkan dalam pengerjaan algoritma Caesar Cipher menerapkan metode pertukaran abjad tunggal di mana semua huruf di dalam pesan (plaintext) yang akan dienkripsi memakai kunci yang sama. Algoritma ini adalah salah satu algoritma kriptografi klasik yang banyak dipakai karena mudah diterapkan dan relatif aman jika kunci yang digunakan tidak diketahui oleh pihak yang tidak memiliki hak [4].

Enkripsi:

Enkripsi Vigenère Cipher dapat dijabarkan secara matematis dengan menggunakan persamaan :
$Ci = (Pi + Ki)mod\ n$

Dekripsi:

Sementara itu untuk proses dekripsi adalah sebagai berikut :

$Pi = (Ci - Ki)mod\ n$

Keterangan:

C = Cipherteks

P = Plainteks

K = Kunci

n = Jumlah karakter alphabet

i = 1,2,3,..., posisi karakter

Algoritma Data Encryption Standard (DES)

Algoritma Data Encryption Standard (DES) merupakan sistem kriptografi simetri dan termasuk dalam jenis cipher blok. DES bekerja pada blok 64 bit dan mengenkripsi 64 bit plaintext menjadi 64 bit ciphertext dengan memakai 56 bit internal key (kunci internal) atau subkey [5]. Kunci internal ini dihasilkan dari external key (kunci eksternal) yang memiliki panjang 64 bit. Untuk proses enciphering (enkripsi) terhadap blok plaintext dikerjakan setelah dibagi awal menjadi dua bagian (setiap blok plaintext) mengalami 16 putaran enkripsi yang masing-masing merupakan jaringan Feistel yang dinyatakan matematis dengan persamaan sebagai berikut :

Enkripsi :

Li= Ri – 1

Ri = Li – 1 $\oplus$ f(Ri – 1, Ki)

E(Ri – 1) $\oplus$ Ki = A

Pada setiap putaran enkripsi, fungsi ekspansi digunakan untuk memperbesar blok Ri–1 yang berukuran 32 bit menjadi blok 48 bit. Hasil dari perluasan tersebut kemudian enkripsi dengan XOR dengan kunci Ki yang menghasilkan vektor A. Vektor A kemudian dibagi menjadi 8 kelompok 6 bit yang masing-masing akan disubstitusikan menggunakan 8 kotak S-Box (S1

hingga S8). Masing-masing kotak S-Box akan memperoleh inputan 6 bit dan mengeluarkan keluaran 4 bit. Setiap 6 bit pertama akan disubstitusikan ke dalam kotak S-Box1, 6 bit kedua akan disubstitusikan ke dalam kotak S-Box2, dan seterusnya.

Dekripsi :

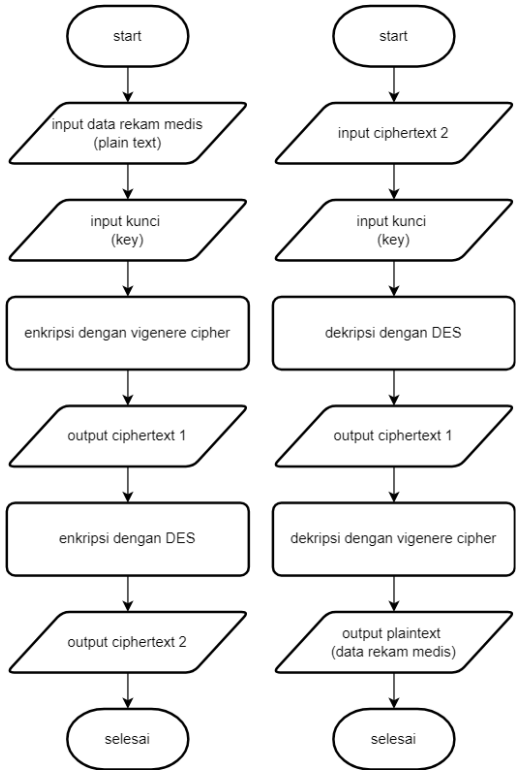
Untuk Proses dekripsi ciphertext adalah kebalikan dari proses enkripsi yang telah dijelaskan. Kunci yang akan dipakai pada proses dekripsi merupakan kebalikan daripada kunci yang dipakai pada proses enkripsi, yaitu K[16], K[15] hingga K[1]. Setiap putaran 1, 2, hingga 16, hasil dari setiap putaran dekripsi diperoleh dengan cara yang sama dengan proses enkripsi, adalah :

$Li = Ri - 1$

$Ri = Li - 1 \oplus f(Ri - 1, Ki)$

ANALISIS DAN PERANCANGAN

Pada tahap ini menjelaskan tentang bagaimana suatu sistem dibentuk mulai dari penggambaran, perencanaan dan pembuatan sketsa program, yang bertujuan untuk memudahkan dan memperjelas jalannya suatu pembuatan program atau aplikasi.



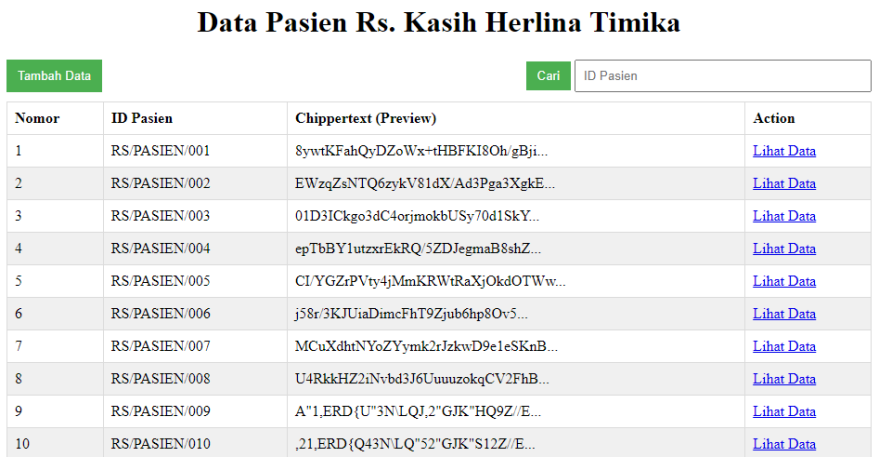
Gambar 1. *Flowchart* Algoritma Enkripsi dan Dekripsi

Gambar 1 menggambarkan flowchart enkripsi dan dekripsi dari algoritma Vigenere Cipher dan Data Encryption Standard (DES). Awalnya pengguna akan memasukkan data rekam medis (plaintext) terlebih dahulu, selanjutnya pengguna akan memasukkan kunci (key) untuk mengacak plaintext yang akan dienkripsi. Setelah itu, proses enkripsi akan dilakukan menggunakan algoritma vigenere cipher dengan menggunakan kunci yang dimasukkan pada langkah ke-2. Setelah menjadi chipertext, proses enkripsi akan dilakukan lagi menggunakan

algoritma DES dengan menggunakan kunci yang dimasukkan pada langkah ke-2. Setelah melalui enkripsi Vigenere Cipher dan DES, data rekam medis berhasil di enkripsikan. Sedangkan proses deskripsinya dilakukan dengan cara memasukkan Ciphertext yang didapat dari data rekam medis. Selanjutnya, pengguna akan memasukkan kunci Vigenere Cipher dan Data Encryption Standard (DES). Proses dekripsi DES akan dilakukan menggunakan kunci yang telah dimasukkan. Setelah itu, hasil Ciphertext akan didekripsi lagi menggunakan Vigenere Cipher. Proses dekripsi Vigenere Cipher akan dilakukan. Hasil dekripsi adalah plaintext (data rekam medis).

HASIL DAN PEMBAHASAN

Tampilan Program



Gambar 2. Laman Dashboard program

Gambar 2 menjelaskan terkait tampilan dashboard dari program enkripsi data rekam medis, *button* tambah data berfungsi untuk *user* menambah data pasien yang hendak di enkripsi, untuk kolom pencarian berfungsi untuk mencari data rekam medis pasien berdasarkan ID pasien yang hendak dideskripsikan, untuk tabel didalam program berfungsi untuk menampilkan data rekam medis yang telah di enkripsikan berurutan berdasarkan ID Pasien.

Skenario Pengujian Untuk mengetahui kompleksitas dari kombinasi algoritma Vigenere Cipher dengan Data Encryption Standard (DES), penulis menggunakan Avalanche Effect. Avalanche effect merupakan sebuah cara untuk mengukur seberapa efektif proses enkripsi dalam mengubah pesan asli dengan melihat perbandingan antara jumlah bit cipherteks yang berubah dan jumlah bit plainteks sebelum diubah. Semakin besar persentase perubahan yang terjadi, semakin baik enkripsi yang dihasilkan [6]. Hal ini dikarenakan perubahan pada bit membuat perbedaan yang cukup sulit untuk dilakukan sebuah penyerangan. Pada pengujian ini digunakan rumus [7].

$$\text{Avalanche Effect} = \frac{Jumlah\ perubahan\ bit}{Jumlah\ bit\ total\ Cipherteks} \text{ x } 100\%$$

Berikut adalah hasil perhitungan Avalanche effect menggunakan 5 dataset dengan metode super enkripsi yakni kombinasi Vigenere cipher dan DES :

Tabel 1. Tabel nilai *Avalanche effect Vigenere-DES*

No	Data	Perubahan Bit	Total Bit	Nilai (AE)
1a	RS/PASIEN/001	1486	7232	20,547%
1b	RS/PASIEN/002			
2a	RS/PASIEN/003	1472	7424	19,827%
2b	RS/PASIEN/004			
3a	RS/PASIEN/005	1501	7424	20,218%
3b	RS/PASIEN/006			
4a	RS/PASIEN/007	1659	8064	20,572%
4b	RS/PASIEN/008			
5a	RS/PASIEN/009	1660	8064	20,585%
5b	RS/PASIEN/010			
Nilai Rata-Rata *Avalanche effect*				20,35%

Tabel 1 menampilkan nilai *Avalanche effect* metode *Vigenere-Des* dari 5 dataset (10 data berpasangan) dengan menggunakan rumus avalanche effect yang terdapat pada bab 4.4 perhitungannya sebagai berikut :

$$AE = \frac{1486}{7232} \text{ x } 100\% = 20{,}547\ \%$$

Setelah mendapat nilai avalanche effect 5 dataset, lakukan perhitungan untuk mencari rata-rata nilai avalanche effect (X) dengan menggunakan rumus :

$$X = \frac{Jumlah\ nilai\ AE}{Banyaknya\ Pengujian}$$

Dengan demikian, lakukan perhitungan nilai rata-rata avalanche effect dengan menggunakan data Vigenere-Des :

$$X = \frac{101{,}749}{5} \text{ x } 100\% = 20{,}35\%$$

Jadi, data Vigenere-Des menunjukkan rata-rata Avalanche effect 20,35%, Sebagai pembanding, rata-rata nilai Avalanche Effect untuk metode Vigenère adalah 5,96%, sedangkan untuk metode DES adalah 20,14%.

Hasil ini menunjukkan bahwa kombinasi Vigenère-DES memberikan peningkatan yang signifikan terhadap efek difusi (*Avalanche Effect*) jika dibandingkan dengan penggunaan Vigenère Cipher secara tunggal, dan sedikit lebih tinggi dari penggunaan DES secara mandiri. Hal ini mengindikasikan bahwa super enkripsi Vigenère-DES mampu memberikan perlindungan data yang lebih baik dalam konteks pengamanan data rekam medis.

KESIMPULAN

Berdasarkan analisis dan pengujian dalam pengamanan data rekam medis pasien menggunakan metode super enkripsi Vigenere Cipher dan Data Encryption Standards (DES) dapat disimpulkan sebagai berikut:

1. Penggunaan Enkripsi pada data rekam medis pasien data digunakan untuk melindungi informasi sensitif terkait data rekam medis pasien dengan mengubah plaintext menjadi ciphertext atau sekumpulan karakter acak yang rumit.
2. Metode Super enkripsi Vigenere-Des lebih baik dalam meningkatkan keamanan data rekam medis, jika dibandingkan dengan metode Vigenere cipher atau Des saja, hasil dari nilai Avalanche effect metode super enkripsi kombinasi Vigenere cipher dan Des sebesar 20,35% sedangkan untuk metode Vigenere dan Des masing-masing memperoleh 5,96% serta 20,14%.
3. Dengan hasil Avalanche sebesar 20,35% menunjukkan bahwa metode vigenere-Des bisa digunakan untuk melindungi data rekam medis pasien, namun dengan hasil avalanche kurang dari 50% menunjukkan bahwa metode super enkripsi vigenere-des kurang optimal untuk digunakan hal ini disebabkan oleh keterbatasan kunci (Alfabet dan tidak lebih dari 8 byte) sehingga nilai avalanche yang dihasilkan hanya sebesar 20,35%.

DAFTAR PUSTAKA

[1] Nuraeni, F., Purnama Putra, Y., Hendriyani, I., Studi Teknik Informatika, P., & Tasikmalaya, S. (n.d.). IMPLEMENTASI KRIPTOGRAFI SUPER ENKRIPSI VIGENERE CIPHER DAN ADVANCED ENCRYTION STANDARD (AES) PADA PENGAMANAN DATA RIWAYAT PASIEN RUMAH SAKIT.

[2] Sentosa, Y. (2010). Algoritma DES untuk Keamanan Informasi pada Aplikasi Rekam Medis Elektronik.

[3] Sudrajat, A., & Gunadhi, E. (2016). PENGAMANAN DATA REKAM MEDIS PASIEN MENGGUNAKAN KRIPTOGRAFI VIGÈNERE CIPHER. http://jurnal.sttgarut.ac.id

[4] Dedi Irawan, M. (2017). IMPLEMENTASI KRIPTOGRAFI VIGENERE CIPHER DENGAN PHP. In JURNAL TEKNOLOGI INFORMASI (JurTI) (Vol. 1, Issue 1).

[5] Rusri Yanti, N., Afrida Ritonga, D., Prorgram Studi Teknik Informatika STMIK Budidarma Medan, M., Sisingamangaraja No, J., & Limun Medan, S. (2018). Implementasi Algoritma Data Encryption Standard Pada Penyandian Record Database. In Jurnal Sains Komputer & Informatika (J-SAKTI (Issue 2). http://tunasbangsa.ac.id/ejurnal/index.php/jsakti

[6] Budi Handoko, L. (2022). PENGUJIAN AVALANCE EFFECT PADA KRIPTOGRAFI TEKS MENGGUNAKAN AUTOKEY CIPHER. 2 St Proceeding STEKOM, 2022.

[7] D. H. Sulaksono, “Multiple Encryption Dengan Menggunakan,” vol. XI, pp. 25–30, 2016.

Halaman ini sengaja dikosongkan