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.2025.7226

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

Multiple Encryption Menggunakan Electronic Code Book dan Modifikasi Algoritma Playfair Cipher 9x9 untuk Keamanan Data Teks

Jonathan Anandar Cahyadi[1], Citra Nurina Prabiantissa[2]
Institut Teknologi Adhi Tama Surabaya[1,2]
e-mail: jonathana4017@gmail.com

ABSTRACT

Over the past decade, the increasing use of computer networks has brought new challenges related to privacy and security, especially for sensitive data such as psychiatric patient medical records. Cryptography has emerged as a solution to maintain the confidentiality of information. This study aims to address the security of text data by combining the Modified 9x9 Playfair Cipher algorithm and Electronic Code Book (ECB) in the encryption process to improve the security of psychiatric patient medical data. The results of the study showed that the average results of the Avalanche Effect test conducted by the researcher were 32.32% for the Playfair 9x9 method, 50.47% for the ECB method and 50.70 for the combination of both. It can be seen that there is an alignment of the increase in the number of different bits with the percentage of Avalanche Effect which shows that for each bit length of the data row, there is a limit to the percentage of Avalanche Effect that will be obtained. With the highest percentage of Avalanche Effect, namely 58.75%.

Keywords: *Multiple Encryption, Cryptography, 9x9 Modified Playfair Cipher, Electronic Code Book (ECB)*

ABSTRAK

Selama dekade terakhir, peningkatan penggunaan jaringan komputer telah membawa tantangan baru terkait privasi dan keamanan, terutama untuk data sensitif seperti catatan medis pasien psikiatri. Kriptografi muncul sebagai solusi untuk menjaga kerahasiaan informasi. Penelitian ini bertujuan untuk mengatasi keamanan data teks dengan menggabungkan algoritma Modified 9x9 Playfair Cipher dan Electronic Code Book (ECB) dalam proses enkripsi untuk meningkatkan keamanan data medis pasien psikiatri. Hasil penelitian menunjukkan bahwa rata-rata hasil pengujian Avalanche Effect yang dilakukan oleh peneliti adalah 32,32% untuk metode Playfair 9x9, 50,47 %untuk metode ECB dan 50,70 untuk gabungan keduanya. Dapat dilihat bahwa ada

keselarasan dari kenaikan jumlah bit yang berbeda dengan persentase Avalanche Effect yang menunjukkan bahwa pada setiap panjang bit baris data maka ada batas persentase Avalanche Effect yang akan didapatkan. Dengan persentase Avalanche Effect paling tinggi yaitu 58,75%.
Kata kunci: Multiple Encryption, Kriptografi, Playfair Cipher modifikasi 9x9, Electronic Code Book (ECB)

PENDAHULUAN

Penggunaan jaringan komputer dalam berbagai sektor, seperti pemerintahan, bisnis, dan pendidikan, telah meningkat dalam sepuluh tahun terakhir, memunculkan tantangan privasi dan keamanan. Kriptografi, terutama enkripsi, menjadi kunci untuk menjaga kerahasiaan pesan, memerlukan upaya berkelanjutan dan partisipasi para ahli [1]. Keamanan informasi sensitif menjadi faktor penting dalam era teknologi informasi, terutama dalam komunikasi berbasis teks yang rentan terhadap penyalahgunaan [2].

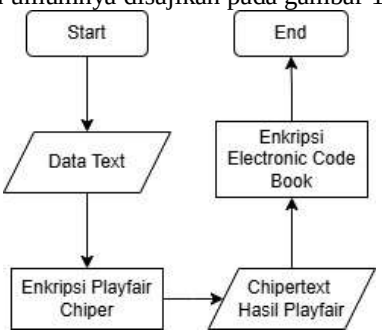
Data sensitif, seperti rekam medis, memerlukan perlindungan ekstra melalui enkripsi untuk mematuhi peraturan privasi. Penggunaan teknik kriptografi membantu melindungi data dan komunikasi di tengah perubahan lanskap digital [3]. Keamanan data medis juga menjadi krusial dalam praktik klinis, di mana enkripsi digunakan untuk melindungi privasi pasien dan integritas informasi kesehatan mental [4].

Beberapa algoritma seperti Electronic Code Book telah terbukti efektif dalam melindungi data privasi seperti data pegawai dari akses yang tidak sah di PDAM Tirta Sanita Sumber [6]. Penggabungan Electronic Code Book dengan Playfair Cipher dapat mengatasi kerentanan umum dalam enkripsi simetris, seperti analisis frekuensi dan uji Kasiski. Algoritma Playfair Cipher adalah algoritma kriptografi yang digunakan secara luas, tetapi perlu diperkuat dan ditingkatkan keamanannya untuk menghadapi serangan kriptoanalisis yang berkembang. Penggabungan Playfair Cipher dengan algoritma kriptografi kontemporer seperti RSA atau AES [7].
Menggabungkan Electronic Code Book dengan Playfair Cipher dapat mengatasi kerentanan umum dalam enkripsi simetris, memberikan tingkat keamanan yang diperlukan untuk melindungi informasi sensitif dalam lingkungan digital [5].

Penggabungan *Electronic Code Book* dengan metode enkripsi *Playfair Cipher* menawarkan solusi terhadap sejumlah masalah umum yang sering dihadapi oleh teknik enkripsi simetris secara umum. Masalah keamanan ini berkaitan dengan kerentanan terhadap serangan seperti analisis frekuensi dan uji Kasiski. Dengan bantuan *Playfair Cipher*, pendekatan ini diharapkan dapat mengatasi potensi kerentanan keamanan.

METODE

Program yang dikembangkan dalam penelitian ini menggabungkan teknik enkripsi *Playfair Cipher* berukuran 9x9 dengan mode *Electronic Code Book (ECB).* Pada tahap enkripsi, algoritma Playfair Cipher dimodifikasi untuk meningkatkan tingkat keamanan dan ketidakdugaan dari hasil ciphertext. Gambaran umumnya disajikan pada gambar 1.



Gambar 1. Diagram Alir Sistem

Proses enkripsi dan dekripsi dengan mencoba melakukan perhitungan pada data melalui ekstraksi tabel atau perhitungan manual dengan algoritma Playfair Cipher dan Electronic Code Book:

1. Data Teks
   Data yang digunakan dalam penelitian ini berasal dari *Kaggle* dengan jumlah 142 data pemeriksaan pasien psikiatri dengan jumlah pasien yang di observasi sebanyak 50 pasien.
2. Algoritma Playfair Chiper
   Playfair cipher diklasifikasikan sebagai cipher poligram, khususnya menggunakan bigram untuk menggantikan dua huruf secara simultan, membedakannya dari cipher klasik lain yang beroperasi pada huruf tunggal. Berikut langkah - langkah untuk menggunakan metode sandi Playfair untuk mengenkripsi data:
   1. Setiap huruf digantikan dengan huruf di bawahnya jika terdapat dua huruf dalam kolom kunci yang sama.
   2. Setiap huruf digantikan dengan huruf di sebelah kanannya jika dua huruf berada dalam baris kunci yang sama.
   3. Huruf pada perpotongan baris huruf pertama dan kolom huruf kedua akan menggantikan huruf pertama jika dua huruf tidak berada dalam baris atau kolom yang sama. Huruf pada sudut keempat dari persegi panjang yang dihasilkan oleh tiga huruf pertama kemudian digunakan untuk menggantikan huruf kedua.
4. Algoritma Electronic Code Book (ECB)
   Selama proses enkripsi, sebuah kunci tertentu (K) dan sebuah fungsi enkripsi (Ek) digunakan untuk mengubah setiap blok plainteks (Pi) menjadi blok cipherteks (Ci) yang sesuai. Dalam proses dekripsi, blok-blok cipherteks (Ci) dapat dikembalikan menjadi blok-blok plainteks (Pi) dengan menggunakan fungsi dekripsi (Dk) yang menggunakan kunci yang sama (K). Representasi matematis dari enkripsi dalam mode Electronic Codebook (ECB) dapat dijelaskan sebagai berikut:
   $Ci = Pi \otimes K$ (1)

   Dimana rumus XOR sebagai berikut :
   $A \otimes B$ = (A AND (NOT B) OR ((NOT A) DAN B) (2)

HASIL DAN PEMBAHASAN

Pengujian terhadap algoritma yang sudah diterapkan dalam melakukan enkripsi dan dekripsi terhadap data yang didapat, yaitu dengan melakukan pengujian terhadap keamanannya (Avalanche Effect). Semua pengujian dilakukan menggunakan 3 kunci yang memiliki perbedaan panjang bit yaitu :

aBcD123! dengan 64 bit
L0g1c@lP@ssw0rd! dengan 128 bit
R@nd0mC0mplex1oCkK3y!Symb0ls2024 dengan 256 bit

Pengujian Avalanche Effect dilakukan untuk metode Playfair 9x9, Electronic Code Book dan Gabungan keduanya. Pengujian dilakukan pada saat data sudah terenkripsi lalu dilakukan dekripsi, dengan demikian data dapat dibandingkan dari bentuk plaintext dengan bentuk ciphertext-nya. Tabel 1 merupakan berisikan data siswa beserta nilai Avalanche Effect :

Tabel 1. Avalanche Effect Playfair Cipher

Data ke-	Jumlah Bit Plaintext	Jumlah Bit Berbeda	Panjang Bit Kunci	Avalanche Effect (%)
1	80	21	64	26,25
2	80	28	64	35,00
3	80	28	64	35,00

4	160	44	64	27,50
5	160	44	64	27,50
6	160	51	64	31,87
7	288	80	64	27,77
8	288	88	64	30,55
9	288	103	64	35,76
10	80	25	128	31,25
11	80	24	128	30,00
12	80	25	128	31,25
13	160	48	128	30,00
14	160	52	128	32,50
15	160	52	128	32,50
16	288	105	128	36,45
17	288	104	128	36,11
18	288	105	128	36,45
19	80	29	256	36,25
20	80	25	256	31,25
21	80	31	256	38,75
22	160	50	256	31,25
23	160	45	256	28
24	160	50	256	31,25
25	288	100	256	35
26	288	96	256	33
27	288	98	256	34

Tabel 2 Avalanche Effect **Electronic** Code Book

Data ke-	Jumlah Bit Plaintext	Jumlah Bit Berbeda	Panjang Bit Kunci	Avalanche Effect (%)
1	80	40	64	50,00
2	80	40	64	50,00
3	80	38	64	47,50
4	160	89	64	58,55
5	160	81	64	53,28
6	160	79	64	51,97
7	288	151	64	53,92
8	288	135	64	48,21
9	288	135	64	48,21
10	80	42	128	52,50
11	80	36	128	45,00
12	80	40	128	50,00
13	160	84	128	55,26
14	160	82	128	53,95
15	160	78	128	51,32
16	288	144	128	51,43
17	288	142	128	50,71
18	288	126	128	45,00
19	80	36	256	45
20	80	42	256	52,5
21	80	38	256	47,5

22	160	79	256	52
23	160	81	256	53
24	160	75	256	49
25	288	136	256	49
26	288	152	256	54
27	288	122	256	44

Tabel 3 Avalanche Effect Gabungan Playfair Cipher dan Electronic Code Book

Data ke-	Jumlah Bit Plaintext	Jumlah Bit Berbeda	Panjang Bit Kunci	Avalanche Effect (%)
1	80	41	64	51,24
2	80	38	64	47,50
3	80	41	64	51,24
4	160	91	64	56,87
5	160	79	64	49,37
6	160	90	64	56,25
7	288	149	64	51,73
8	288	143	64	49,65
9	288	144	64	50,00
10	80	47	128	58,75
11	80	36	128	45
12	80	49	128	61
13	160	79	128	49
14	160	77	128	48
15	160	79	128	49
16	288	134	128	47
17	288	131	128	45
18	288	134	128	47
19	80	41	256	51
20	80	47	256	58,75
21	80	41	256	51
22	160	76	256	47,5
23	160	81	256	51
24	160	80	256	50
25	288	139	256	48
26	288	139	256	48
27	288	141	256	49

Hasil Tabel 1,2,dan 3 didapati bahwa Playfair Cipher menunjukkan bahwa pada kunci 64 bit, rata-rata Avalanche Effectnya sekitar 30,8%, sementara pada kunci 128-bit, efek Avalanche meningkat menjadi sekitar 32,94%. Pada kunci 256-bit, rata-rata Avalanche Effect mencapai sekitar 33,22%. Selain itu, rata-rata dari kunci dengan panjang 64, 128, dan 256 bit adalah 32,32. ECB menunjukkan bahwa pada kunci 64-bit, rata-rata Avalanche Effectnya sekitar 51,06%, sedangkan pada kunci 128-bit, efek Avalanche sedikit lebih rendah, sekitar 50,71%. Pada kunci 256-bit, rata-rata Avalanche Effect adalah sekitar 49,95%. Tidak secara konsisten, panjang kunci mempengaruhi rata-rata Avalanche Effect pada ECB. Rata-rata dari kunci dengan panjang 64, 128, dan 256 bit adalah 50,47.

Gabungan Playfair Cipher dan ECB menunjukkan bahwa pada kunci 64-bit, rata-rata Avalanche Effectnya sekitar 51,04%, sedangkan pada kunci 128-bit, efek Avalanche sedikit lebih

rendah, yaitu sekitar 50,55%. Pada kunci 256-bit, rata-rata Avalanche Effect adalah sekitar 50,63%. Rata-rata dari kunci dengan panjang 64, 128, dan 256 bit adalah 50,70. Pada kunci 256-bit dan gabungan terdapat kecenderungan untuk mencapai rata-rata Avalanche Effect yang lebih tinggi.

KESIMPULAN

Berdasarkan penelitian dan pengujian yang telah dilakukan, dapat diambil beberapa kesimpulan bahwa bahwa rata-rata hasil pengujian Avalanche Effect yang dilakukan oleh peneliti adalah 32,32% untuk metode Playfair 9x9, 50,47 %untuk metode ECB dan 50,70 untuk gabungan keduanya. Dapat dilihat bahwa ada keselarasan dari kenaikan jumlah bit yang berbeda dengan persentase Avalanche Effect yang menunjukkan bahwa pada setiap panjang bit baris data maka ada batas persentase Avalanche Effect yang akan didapatkan. Dengan persentase Avalanche Effect paling tinggi yaitu 58,75% dan persentase paling rendah yaitu 26,25%.

DAFTAR PUSTAKA

[1] D. Susanti, "Analisis Modifikasi Metode Playfair Cipher Dalam Pengamanan Data Teks," *Indones. J. Data Sci.*, vol. 1, no. 1, pp. 11–18, Mar. 2020, doi: 10.33096/ijodas.v1i1.4.

[2] Ananda, "Kombinasi Algoritma Playfair Cipher Dengan Metode Zig-zag Dalam Penyandian Teks," INA-Rxiv, preprint, May 2018. doi: 10.31227/osf.io/7r4gk.

[3] A. Mufid, "TEKNIK ENKRIPSI DAN DESKRIPSI MENGGUNAKAN ALGORITHMA ELECTRONIC CODE BOOK (ECB)".

[4] R. Bauer, T. Glenn, S. Monteith, P. C. Whybrow, and M. Bauer, "Survey of psychiatrist use of digital technology in clinical practice," *Int. J. Bipolar Disord.*, vol. 8, no. 1, p. 29, Dec. 2020, doi: 10.1186/s40345-020-00194-1.

[5] M. Z. Siambaton and A. Muhazir, "MODIFIKASI ALGORITMA PLAYFAIR CIPHER DENGAN PENGURUTAN ARRAY PADA MATRIKS," vol. 02, 2018.

[6] W. Ariandi, S. Widyastuti, dan L. Haris, "Implementasi Block Cipher Electronic Codebook (ECB) untuk Pengamanan Data Pegawai," *Jurnal Ilmiah Intech: Information Technology Journal of UMUS*, vol. 2, no. 02, pp. 65-74, Nov. 2020.

[7] M. Z. Siambaton and A. Muhazir, "MODIFIKASI ALGORITMA PLAYFAIR CIPHER DENGAN PENGURUTAN ARRAY PADA MATRIKS," 2018.