Playfair Cipher untuk Kriptografi ASCII menggunakan Matriks 9x10

Arley Japardi[1], Ezra Louis Frasetyo[2], Adrian Sahertian[3], Chaerul Umam[4], Gustina Alfa Trisnapradika[5]
[1,2,3,4,5]Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro, Semarang

Artikel Info

Kata kunci:

Kriptografi
Playfair Cipher
ASCII
Tabel

ABSTRAK

Algoritma Playfair Cipher telah lama dikenal sebagai metode pengamanan informasi dengan mengenkripsi teks biasa menjadi teks sandi menggunakan tabel 5x5. Dalam pengembangan lebih lanjut, kami memodifikasi struktur tabel Playfair menjadi 9x10 untuk meningkatkan kapasitas penyandian hingga 90 karakter ASCII *printable*. Perubahan ini memungkinkan penggunaan karakter yang lebih luas dalam proses enkripsi, mencakup seluruh rentang karakter ASCII yang dapat dicetak. Kami menjelaskan langkah-langkah modifikasi tabel Playfair, termasuk pembentukan tabel, pengkodean teks masukan, dan dekripsi teks keluaran. Hasil eksperimen menunjukkan bahwa modifikasi ini memungkinkan penggunaan lebih banyak karakter tanpa mengorbankan keamanan. Hasil rata - rata Character Error Rate 20% yang berarti hasil dari Plaintext dengan hasil dari Dekripsi terdapat perbedaan huruf – huruf. Dengan demikian, algoritma Playfair Cipher yang dimodifikasi ini dapat diimplementasikan dengan efektif untuk mengamankan komunikasi yang melibatkan teks berbasis ASCII printable.

Penulis Korespondensi :

Chaerul Umam,
Program Studi Teknik Informatika
Fakultas Ilmu Komputer
Universitas Dian Nuswantoro, Semarang, 50131
Email: chaerul@dsn.dinus.ac.id

1. PENDAHULUAN

Enkripsi adalah proses mengubah data menjadi format yang mudah dikenal atau dibaca tanpa memiliki kunci enkripsi yang tepat. tujuan dari Enkripsi data digunakan untuk melindungi informasi agar mudah dibaca oleh pihak pihak yang tidak memiliki hak. Sedangkan Dekripsi adalah proses mengembalikan kata acak atau bentuk dari enkripsi menjadi kata- kata yang dapat dibaca. Kriptografi telah menjadi aspek penting dalam menjaga keamanan informasi di era digital ini. Salah satu teknik kriptografi yang telah ditemukan dan digunakan sejak awal abad ke-20 adalah Playfair Cipher. Playfair Cipher merupakan metode substitusi yang melibatkan penggunaan matriks 5x5 untuk mengenkripsi dan mendekripsi teks. Kelebihan utama dari Playfair Cipher terletak pada kemampuannya mengatasi kelemahan metode substitusi biasa, dimana huruf-huruf yang sering muncul dapat lebih mudah ditembakkan. Dengan menggunakan tabel matriks 5x5, Playfair Cipher memberikan tingkat keamanan yang lebih tinggi dalam menyandikan pesan.

Dalam perkembangan zaman, kebutuhan akan keamanan data semakin kompleks, termasuk ketika hendak mengamankan teks dalam bentuk ASCII. ASCII (American Standard Code for Information

Interchange) adalah sistem pengkodean karakter yang luas digunakan dalam dunia komputasi. Penggunaan Playfair Cipher dalam lingkup ASCII memungkinkan pengamanan data dalam konteks digital tanpa mengorbankan fleksibilitas dan keamanan.

Dalam kriptografi modern, penggunaan Playfair Cipher dengan memanfaatkan tabel matriks 9x10 memberikan pengalaman dalam pengamanan data. Tabel matriks 9x10 ini mencangkup 90 karakter ASCII yang dapat dicetak (printable), memberikan kapasitas lebih besar untuk menyandikan teks dalam format yang lebih luas. Dengan memperluas ukuran matriks, kita dapat memasukkan lebih banyak karakter ASCII ke dalam tabel dan meningkatkan kompleksitas penyandian. Penerapan Playfair Cipher dalam tabel matriks 9x10, yang mencakup seluruh karakter ASCII. Hal ini menjadikan Playfair Cipher sebagai pilihan yang menarik dalam keamanan data digital yang terus berkembang dengan kemampuannya mengatasi tantangan kompleksitas dan kapasitas karakter dalam bentuk tabel 9x10. Kemudian untuk menguji algoritma ini, akan diterapkan tiga pengujian untuk kriptografi yakni Character Error Rate, Bit Error Rate, dan Avalanche Effect. Character Error Rate merupakan sebuah metrik yang digunakan untuk mengukur tingkat kesalahan karakter dalam pemrosesan kalimat. CER selalu digunakan untuk mengukur seringnya karakter yang dihasilkan berbeda dari karakter yang seharusnya. Kelebihan. Bit Error Rate digunakan untuk seberapa seringnya terjadi kesalahan bit selama proses enkripsi ataupun dekripsi. BER berbeda dari CER yang mengukur bukan berdasar pada bit melainkan berdasarkan karakter. Hal inilah BER dapat memberikan gambaran tentang seberapa andal suatu metode enkripsi atau protokol keamanan dalam mengatasi gangguan atau kesalahan selama pengiriman data terenkripsi. Hal Ini membantu pengembang mengevaluasi keandalan protokol keamanan. Dan juga dari performa yang dioptimalkan, dapat mengidentifikasi area-area di mana performa kriptografi dapat dioptimalkan untuk mengurangi kesalahan transmisi. Keterbatasan dari BER dan menjadi Kekurangan BER adalah tidak menjamin keamanan yang dijaga, dan kesalahan dalam bit yang tidak memberikan keamanan informasi. Syarat jika BER ini digunakan atau dipakai adalah Data referensi (Plainteks dan Kunci) yang harus benar dalam membandingkan data yang diterima dan Sistem dari Transmisi perlu adanya pengukuran.

2. METODE

2.1 Penelitian Terkait

Pemakaian Playfair Cipher dalam matriks 8x8 dipakai oleh Dhiman Departemen Ilmu dan Teknik Komputer dari Institut Teknologi Nasional Hamirpur, India. Dalam penelitian ini memiliki latar belakang masalah yaitu dari keamanan pesan yang akan ditransfer yang dapat memainkan peran yang sangat penting. Strategi seperti Enkripsi/Dekripsi, Tanda Tangan Digital, Steganografi., telah dikembangkan untuk memastikan keamanan, privasi, dan kerahasiaan pesan-pesan ini. Tabelnya playfair cipher dengan matriks 8x8 seperti berikut.

TABLE I
LIST OF CHARACTERS USED IN EXTENDED PLAYFAIR CIPHER

A	B	C	D	E	F	G	H
I	J	K	L	M	N	O	P
Q	R	S	T	U	V	W	X
Y	Z	0	1	2	3	4	5
6	7	8	9	!	@	#	$
%	^	&	*	(	)	_	+
=	{	}	[	]	|	\	:
;	”	’	<	>	.	/	?

Gambar 1. Visualisasi karakter Playfair Cipher menggunakan tabel 8x8

Pemakaian matriks 6x6 yang digunakan oleh Anirban Bhowmick Student – B.Tech Dept of CSE-MIT, Manipal. Dalam penelitian ini melalukan pengujian cara memperkuat keamaan data dengan enkripsi. dengan cara menggabungkan teknik enkripsi biasa yaitu playfair dan transposisi myszkowsku ganda. Dengan

menggunakan algoritma ini membuat informasi tidak mudah dilacak atau terbaca. Dengan menggunakan algoritma ini jauh lebih aman daripada menggunakan playfair biasa.

2.1 Playfair Chiper

Playfair Cipher adalah metode enkripsi yang menggunakan matriks persegi panjang (biasanya 5x5) yang diisi dengan huruf-huruf alfabet unik, tanpa mengulang, sebagai kunci untuk mengenkripsi pasangan huruf. Berikut adalah langkah-langkah dan aturan untuk Playfair Cipher.

1. Pembuatan Tabel Kunci

Algoritma Playfair Cipher biasanya menggunakan tabel kunci 5x5 dengan 25 karakter, yaitu huruf A sampai dengan Z kecuali huruf J seperti contoh sebagai berikut :

Tabel 1. Tabel Kunci Playfair Cipher dengan matriks 5x5

A	B	C	D	E
F	G	H	I/J	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

2. Pembuatan Pasangan Huruf:
   - Pisahkan teks yang akan dienkripsi menjadi pasangan huruf.
   - Jika ada huruf yang berulang dalam satu pasangan, sisipkan huruf 'X' di antaranya.
   - Contoh: "HELLO" menjadi "HE LX LO"
3. Penggantian Huruf 'I' dan 'J':
   - Dalam matriks kunci, 'I' dan 'J' sering dianggap setara dan dapat saling menggantikan.
   - Contoh: "IJ" dianggap sebagai satu huruf.
4. Pengisian Matriks Kunci:
   - Matriks kunci diisi dari kiri ke kanan, berdasarkan kunci.
   - Jika terdapat huruf berulang pada kunci maka huruf tersebut cukup ditulis satu kali saja.
5. Enkripsi:
   - Untuk setiap pasangan huruf:
     - ❖ Jika keduanya berada pada baris yang sama, ganti setiap huruf dengan huruf sebelahnya.
     - ❖ Jika keduanya berada pada kolom yang sama, ganti setiap huruf dengan huruf bawahnya.
     - ❖ Jika keduanya berada di baris yang berbeda dan kolom yang berbeda, ganti huruf pertama dengan huruf pada kolom yang sama dengan huruf kedua dan sebaliknya.

6. Dekripsi:

Proses dekripsi mirip dengan enkripsi, tetapi sebaliknya.

Aturan untuk Playfair Cipher untuk ASCII tidak berbeda jauh dari Playfair Cipher biasa.

Berdasarkan aturan Playfair Cipher diatas, dapat dilakukan modifikasi sebagai berikut agar algoritma dapat digunakan untuk enkripsi karakter-karakter ASCII yang dapat dicetak (printable).

1. Pembuatan Tabel Matriks 10x9:

Pada Algoritma Playfair yang sudah dimodifikasi untuk ASCII, tabel kunci berbentuk matriks 10x9 yang mencakup huruf kapital A-Z, a-z, 0-9, serta simbol-simbol seperti : ! @ # $ % ^ & * ( ) - _ = + { } | : ; ' " , . < > / ? dan *spasi*.

Tabel 2. Tabel Kunci Playfair Cipher untuk ASCII dengan matriks 10x9

A	B	C	D	E	F	G	H	I	J
K	L	M	N	O	P	Q	R	S	T
U	V	W	X	Y	Z	a	b	c	d
e	f	g	h	i	j	k	l	m	n
o	p	q	r	s	t	u	v	w	x
y	z	0	1	2	3	4	5	6	7
8	9	!	@	#	$	%	^	&	*
(	)	-	_	=	+	{	}	|	;
:	‘	“	,	.	<	>	/	?	(spasi)

2. Pembuatan Pasangan Huruf:
   - Pisahkan teks yang akan dienkripsi menjadi pasangan huruf.
   - Jika ada huruf yang berulang dalam satu pasangan, sisipkan huruf 'X' di antaranya.
   - Contoh: "HELLO" menjadi "HE LX LO"
3. Pengisian Matriks Kunci:
   - Matriks kunci diisi dari kiri ke kanan, berdasarkan kunci.
   - Jika terdapat huruf berulang pada kunci maka huruf tersebut cukup ditulis satu kali saja.
4. Enkripsi:
   - Untuk setiap pasangan huruf:
     - ❖ Jika keduanya berada pada baris yang sama, ganti setiap huruf dengan huruf sebelahnya.
     - ❖ Jika keduanya berada pada kolom yang sama, ganti setiap huruf dengan huruf bawahnya.
     - ❖ Jika keduanya berada di baris yang berbeda dan kolom yang berbeda, ganti huruf pertama dengan huruf pada kolom yang sama dengan huruf kedua dan sebaliknya.
5. Dekripsi:
   - Proses dekripsi mirip dengan enkripsi, tetapi sebaliknya.

Dengan menggunakan matriks kunci yang lebih besar, penggunaan karakter ASCII yang lebih beragam dapat meningkatkan keamanan enkripsi. Proses enkripsi pada algoritma ini tetap mengikuti prinsip Playfair Cipher, di mana pasangan huruf dalam teks plainteks digantikan berdasarkan aturan tertentu dalam matriks kunci. Dengan demikian, implementasi ini menggabungkan keunikan Playfair Cipher dengan karakteristik khusus ASCII, menjadikannya lebih kokoh dalam mengamankan data.

2.1 Character Error Rate (CER)

Character Error Rate (CER) merupakan suatu metode evaluasi yang digunakan untuk mengukur tingkat keakuratan hasil enkripsi dengan cara membandingkan karakter asli plaintext (huruf, angka, simbol) dengan hasil enkripsi, dimana persentase yang lebih rendah berarti tingkat yang lebih tinggi. dari hasil enkripsi. akurasi, sedangkan persentase yang lebih tinggi berarti tingkat kesalahan yang lebih tinggi dalam proses enkripsi. Berikut Rumus dari CER :

$$Character\ Error\ Rate\ = \frac{Total\ Character\ Dikirim}{Jumlah\ Character\ Salah}\ x\ 100\% \quad (1)$$

2.2 Bit Error Rate (BER)

Bit Error Rate (BER) merupakan metode evaluasi yang mengukur keakuratan hasil enkripsi dibandingkan dengan hasil enkripsi setiap bit plaintext aslinya. Jika tingkat kesalahan semakin rendah maka menunjukkan semakin tinggi tingkat hasil enkripsi semakin baik menunjukkan keakuratan proses enkripsi. Bit Error Rate digunakan untuk seberapa seringnya terjadi kesalahan bit selama proses enkripsi ataupun dekripsi. BER berbeda dari CER yang mengukur bukan berdasar pada bit melainkan berdasarkan karakter. Hal inilah BER dapat memberikan gambaran tentang seberapa andal suatu metode enkripsi atau protokol keamanan dalam mengatasi gangguan atau kesalahan selama pengiriman data terenkripsi. Hal Ini membantu pengembang mengevaluasi keandalan protokol keamanan. Dan juga dari performa yang dioptimalkan, dapat mengidentifikasi area-area di mana performa kriptografi dapat dioptimalkan untuk mengurangi kesalahan transmisi. Keterbatasan dari BER dan menjadi Kekurangan BER adalah tidak menjamin keamanan yang dijaga, dan kesalahan dalam bit yang tidak memberikan keamanan informasi. Syarat jika BER ini digunakan atau dipakai adalah Data referensi (Plainteks dan Kunci) yang harus benar dalam membandingkan data yang diterima dan Sistem dari Transmisi perlu adanya pengukuran. Berikut Rumus yang digunakan oleh BER :

$$Bit\ Error\ Rate\ = \frac{Total\ Bit\ Dikirm}{Jumlah\ Bit\ Salah}\ x\ 100\% \quad (2)$$

2.3 Avalanche Effect (AE)

Avalanche Effect merupakan konsep kriptografi yang merujuk pada sifat algoritma enkripsi dimana perubahan input akan berpengaruh besar pada output. sehingga meningkatkan tingkat keamanan data yang dienkripsi. Kelebihan Avalanche Effect dalam keamanan yaitu menjadi kunci dari enkripsi yang baik karena sulit bagi penyerang untuk menganalisis pola atau hubungan antara input dan output, dan meningkatkan kompleksitas serangan dengan menerapkan Avalanche Effect. Namun, kekurangan yang didapati dari Avalanche Effect terjadi dari kinerjanya yang implementasinya bisa menjadi mahal karena dapat membutuhkan lebih banyak sumber daya komputasi. Berikut Rumus yang digunakan oleh AE :

$$Avalanche\ Effect\ =\ \frac{Jumlah\ Perubahan\ Bit}{Jumlah\ Seluruh\ Bit\ Keseluruhan}\ x\ 100\% \quad (3)$$

3. PEMBAHASAN HASIL

Dari penjelasan metode pengujian, diperoleh hasil yang sesuai dengan tahapan-tahapan yang telah dijelaskan sebelumnya. Oleh karena itu, berikut disajikan alur atau flowchart dari proses Playfair Cipher ASCII dengan Tabel Matriks 9x10, di mana terjadi proses pembentukan output. Pada penginputan plainteks dalam sebuah Tabel Kunci 9x10, teks akan terintegrasi sesuai jumlah huruf dan kotak di awal. Gambaran seperti berikut.

Plainteks : wiuetesdalkgafdgxcnvWEQOISDALKGLADSXMCV52275&^^(*@&!)(#
Key : UDINUSsetia

Hal ini bertujuan untuk mengintegrasikan Plainteks dan Key secara acak dengan rumus yang tersistem dan juga bertujuan supaya output yang dihasilkan sesuai dengan berjalannya sistem sehingga berhasil seperti pada Tabel 3. Pada Tabel 3, terdapat Key-nya di baris dan kolom pertama dengan dilanjutkan dengan cara horizontal ke kanan. Nantinya proses ini akan dijalankan dan menghasilkan output. Output yang pertama akan diintegrasikan atau diproses dengan cara mengenkripsi dari plainteks dengan Key teks. dan Output yang kedua akan diintegrasikan dengan plainteks dari output pertama untuk dikembalikan dengan yang plainteks seperti pada Gambar 2.

Dari Metode Pengujian yang telah di uji mendapatkan hasil dari percobaan diatas. Pertama, untuk proses enkripsi mendapatkan hasil sebagai berikut.

Enkripsi : 6K4HitNgLxlhSlfholowQJRPNsUBALHABUiRPAW46R3y6^&W8]8#*@-)&R

Setelah Melakukan proses tersebut, hasil dari enkripsi tadi akan diintegrasikan atau diproses kembali bersama key dan akan diproses dengan cara dekripsi sehingga menghasilkan hasil output kedua sebagai berikut.

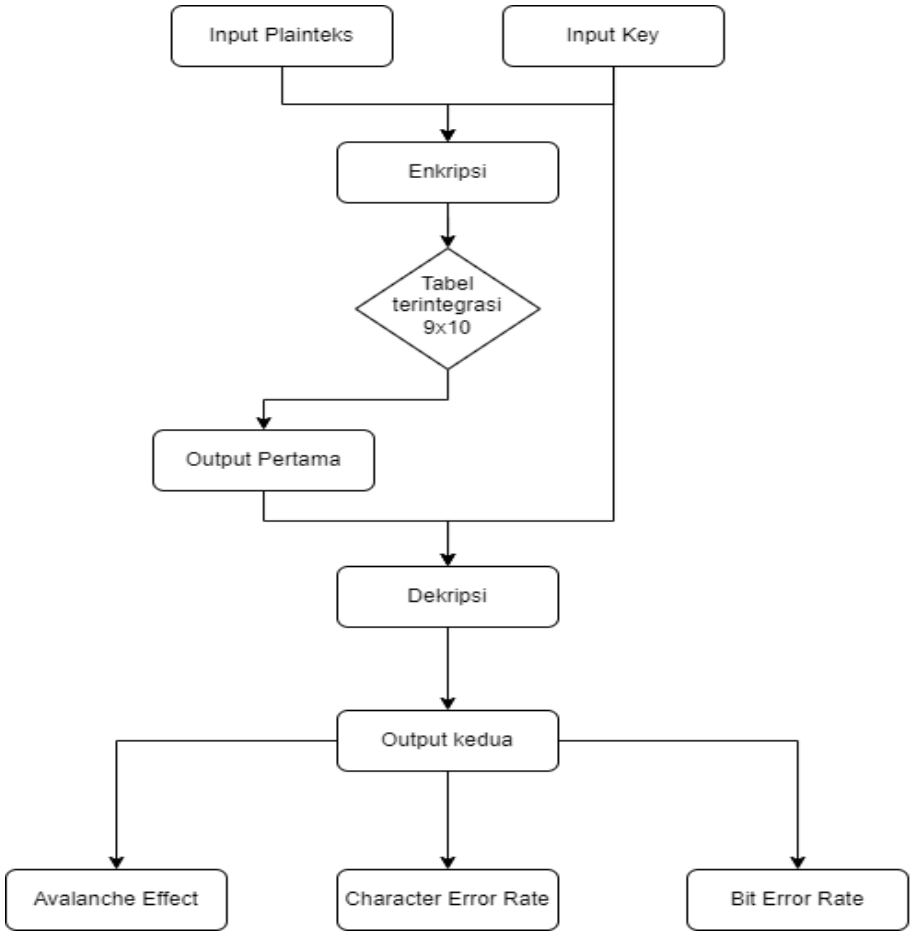
Dekripsi : wiuetesdalkgafdgxcnvWEQOISDALKGLADSXMCV52X275&^X^(*@&!)(#X

Melalui hasil output Dekripsi ini telah membalikkan kembali Plainteks Awal yang secara hampir semua dikembalikan.

Dekripsi : wiuetesdalkgafdgxcnvWEQOISDALKGLADSXMCV52X275&^X^(*@&!)(#X

Plainteks : wiuetesdalkgafdgxcnvWEQOISDALKGLADSXMCV52275&^^(*@&!)(#

Hal ini berbeda dikarenakan panjang dari Dekripsi dan Plainteks, sehingga mendapatkan kesalahan/Error. Maka dari itu, dari proses yang ada perlu namanya perhitungan kesalahan/Error dalam mengenkripsikan dan mendekripsikan sebuah plainteks dan key, yaitu Avalanche Effect, Character Error Rate, dan Bit Error Rate.



Gambar 2. Flowchart Playfair Cipher ASCII dengan Tabel Matriks 9x10

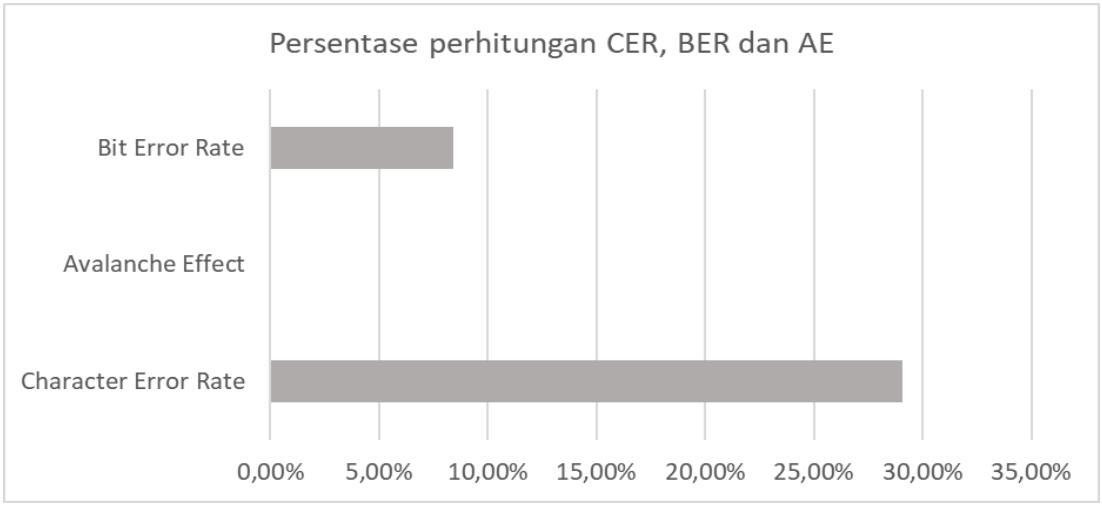
Dari Hasil Dekripsi yang telah teroutputkan oleh proses, maka akan menghasilkan Avalanche Effect, Character Error Rate, dan Bit Error Rate, namun memiliki syarat. Setelah melakukan Dekripsi dan juga perhitungan CER, BER dan AE mendapat hasil persentase sebagai berikut :

Character Error Rate (CER): 29.09%
Bit Error Rate (BER): 8.41%
Avalanche Effect (AE): 0.00%

Tabel 3. Tabel Kunci 9x10 sesuai Plainteks dan Key

U	D	I	N	S	s	e	t	i	a
A	B	C	E	F	G	H	J	K	L
M	O	P	Q	R	T	V	W	X	Y
Z	b	c	d	f	g	h	j	k	l
m	n	o	p	q	r	u	v	w	x
y	z	0	1	2	3	4	5	6	7
8	9	!	@	#	$	%	^	&	*
(	)	-	_	=	+	{	}	|	;
:	‘	“	,	.	<	>	/	?	(spasi)

Pada tabel 3 di atas menunjukkan tabel kunci dengan ukuran 9x10 disesuaikan dengan petak dari Plaintext serta Kunci (*Key*) yang ada pada percobaan sebelumnya. Dalam hal ini, dimulai dari menambahkan huruf – huruf yang ada pada kunci, menambahkan huruf – huruf alfabeth kecuali yang ada pada kunci sebelumnya kemudian menambahkan karakter – karakter yang tertera pada tabel sehingga nampak pada tabel 3 tersebut. Tabel ini nantinya akan digunakan untuk mengenkripsi dari plaintext.



Gambar 3. Prosentase perhitungan CER, BER, dan AE

Setelah melakukan proses enkripsi, maka perlu pengukuran yang nanti digunakan untuk mengukur hasil perolehan yang dicapai. Adapun alat ukur yang kita gunakan antara lain Bit Error Rate (BER), Avalenche Effect (AE) dan Character Error Rate (CER). Gambar 3 merupakan prosentase perhitungan BER, AE dan CER yang menunjukkan bahwa tingkat eror dalam penelitian ini sangat rendah. Berdasarkan dari hal

tersebut menunjukkan bahwa penerapan algoritma dalam penelitian ini sangat baik dengan ditunjukkan dari nilai error yang rendah.

Tabel 4. Hasil Pengujian

No	Plaintext	Key	Avalanche Effect	Bit Error Rate	Character Error Rate
1	ABCDEFGHIJKLMNOPQRST	ZYXWVUTSRQPONMLKJI	100.00%	0.00%	0.00%
2	aoefhanwlrwajtr2awtwgaebv	awe24q4r3tqa	100.00%	0.00%	4.00%
3	e2qtw;h.][413tyhsswr145656uyju	fdgawfwrq5234tryh	100.00%	13.33%	50.00%
4	e12455ygCDNHT	SWR1	100.00%	23.08%	69.23%
5	fwarRRq13ip'/;	warR1['uy	0.00%	19.64%	78.57%
6	dfgerufnABTDYGF2365":>:{>'/>	BUkantaHuN2045	100.00%	0.00%	0.00%
7	jlanvdgsBUFYCVR94287$#%$	JugaUI459?)	100.00%	0.00%	0.00%
8	UBTKuybds76*&^364jdfdsgbkjdrUVWY	ubeg8743YV	96.88%	0.00%	0.00%
9	reygbuvyudsg765432847&^%	hybdg6332%^$	95.83%	0.00%	0.00%
10	cfDVcetv63326%$#@!	GHASvfh1!	94.44%	0.00%	0.00%

Hasil Enkripsi dan Dekripsi dari Data diatas:

Tabel 5. Visualisasi Enkripsi dan Dekripsi

No	Plaintext	Key	Enkripsi	Dekripsi
1	ABCDEFGHIJKLMNOPQRST	ZYXWVUTSRQPONMLKJI	BPDEFGHaAIJKLMNOZQRS	ABCDEFGHIJKLMNOPQRST
2	aoefhanwlrwajtr2awtwgaebv	awe24q4r3tqa	3htXuBirn4ewpe34weAeVAqXxW	aoefhanwlrwajtr2awtwgaebvX
3	e2qtw;h.][413tyhsswr145656uyju	fdgawfwrq5234tryh	ngdCd"C'{]DpdFhA1Rxd5zDf127vAe1S	e2qtw;h.][413tyhsXswr145656uyjuX
4	e12455ygCDNHT	SWR1	gW352a6zj1NaTe	e1245X5ygCDNHT
5	fwarRRq13ip'/;	warR1['uy	WyrRaZAkuzjqA.|Y	fwarRXRq13ip'/;X
6	dfgerufnABTDYGF2365":>:{>'/>	BUkantaHuN2045	eVqVp2Z20aPIeAIu67C:'/>-/"|/	dfgerufnABTDYGF2365":>:{>'/>
7	jlanvdgsBUFYCVR94287$#%$	JugaUI459?)	kmIlzYJvDgBdKOT4?z!8%$^%	jlanvdgsBUFYCVR94287$#%$
8	UBTKuybds76*&^364jdfdsgbkjdrUVWY	ubeg8743YV	WAKL8t4WoV96*&u^upfhip8elkhpiuhb	UBTKuybds76*&^364jdfdsgbkjdrUVWY
9	reygbuvyudsg765432847&^%	hybdg6332%^$	1Tb6dtsg8Cvy!b752%958*h^	reygbuvyudsg765432847&^%
10	cfDVcetv63326%$#@!	GHASvfh1!	eSKPdgp!w4433*%$&S	cfDVcetv63326%$#@!

4. KESIMPULAN

Dari Pembahasan Hasil yang dapat dari percobaan tersebut diperoleh dapat mengambil kesimpulan bahwa Hasil dari Enkripsi dan Dekripsi mendapatkan Hasil rata - rata Character Error Rate 20% yang berarti hasil dari Plaintext dengan hasil dari Dekripsi terdapat perbedaan huruf - huruf. Hasil persentase Bit Error Rate Jumlah bit yang mengalami ketidakcocokan pada total bit yang sudah ditransmisikan atau disimpan.

Dari pembahasan tambahan, dapat disimpulkan bahwa Bit Error Rate dan Character Error Rate menunjukkan tingkat kesalahan yang hampir merata, sebagaimana juga terjadi pada Avalanche Effect. Kesalahan tersebut dapat terjadi karena Key dan plainteks memiliki beragam input, termasuk simbol, angka, huruf kapital, dan huruf kecil. Perpaduan ini menciptakan kompleksitas pada tingkat enkripsi yang dapat menghasilkan kesalahan dalam pengenkripsian dan pendeskripsian data. Oleh karena itu, pemahaman yang

mendalam terhadap karakteristik Bit Error Rate, Character Error Rate, dan Avalanche Effect menjadi krusial dalam meningkatkan keamanan dan kehandalan sistem kriptografi.

Kekurangan dari program tersebut kunci yang digunakan hanya berdasarkan text, jika kunci tersebut pendek mudah sekali ditebak. kelebihan playfair cipher pada saat melakukan enkripsi data, data tersebut tidak mudah ditebak dan teks yang sudah dilakukan enkripsi lebih aman. Saran dari penelitian ini untuk melakukan enkripsi text dilakukan secara dua kali, agar data yang sudah di enkripsi tidak mudah terbaca

REFERENCES

[1] Ibrahim, D., Ahmed, K., Abdallah, M., & Ali, A. A. (2022, Juni 8). A New Chaotic-Based RGB Image Encryption Technique Using a Nonlinear Rotational 16 × 16 DNA Playfair Matrix. *6*(2), 27.

[2] Nadeem, M., Arshad, A., Riaz, S., Zahra, S. W., Dutta, A. K., Moteri, M. A., & Almotairi, S. (2022, Oktober 26). An Efficient Technique to Prevent Data Misuse with Matrix Cipher Encryption Algorithms. *74*(2), 22. 10.32604/cmc.2023.032882

[3] Zhang, Q. (2021). An Overview and Analysis of Hybrid Encryption: The Combination of Symmetric Encryption and Asymmetric Encryption. (2), 7. 10.1109/CDS52072.2021.00111

[4] Putri, A. D., Rachmawati, D., & Herriyance. (2018). Analisis Dan Implementasi Algoritma Kriptografi Playfair Chiper Dan Algoritma Kompresi Run Length Encoding Dalam Pengamanan Dan Kompresi Data Teks. *1*(1), 10. 10.32734/st.v1i1.191

[5] Dian Susanti. (2020, Maret). Analisis Modifikasi Metode Playfair Cipher Dalam Pengamanan Data Teks. *1*(1), 8.

[6] Pristiwanto, Sunandar, H., & Nadeak, B. (2020, September). Analysis and Implementation of PlayFair Chipper Algorithm in Text Data Encoding Process. *10*(2), 5.

[7] Chowdhary, C. L., Patel, P. V., Kathrotia, K. J., Attique, M., Perumal, K., & Ijaz, M. F. (2020, September 10). Analytical Study of Hybrid Techniques for Image Encryption and Decryption. (20), 18.

[8] Abd, A. J., & Al-Janabi, S. T. F. (2019). Classification and Identification of Classical Cipher Type Using Artificial Neural Networks. *14*(11), 14.

[9] Zeebaree, S. R. M. (2020, Mei). DES encryption and decryption algorithm implementation based on FPGA. *18*(2). 10.11591/ijeecs.v18.i2.pp774-781

[10] Rahouma, K. H., AbdelGhany, F. M., Mahdy, L. N., & Hassan, Y. B. E. (2020, Januari). Design and Implementation of a New DNA Based Stream Cipher Algorithm using Python. *44*(1).

[11] Sharma, A., Gupta, N., Thakur, A., Guleri, K., & Dhiman, M. (2023, Oktober 30). Enhancing Communication Using 8 × 8 Extended Playfair Cipher and Steganography. 7.

[12] Yazdeen, A. A., Zeebaree, S. R. M., Sadeeq, M. A. M., Kak, S. F., Ahmed, O. M., & Zebari, R. R. (2021, Maret 15). FPGA Implementations for Data Encryption and Decryption via Concurrent and Parallel Computation: A Review. 9. 10.48161/issn.2709-8206

[13] Salih, R. K., & Yousif, M. S. (2021, November). Hybrid encryption using playfair and RSA cryptosystems. 12(2), 6. 10.22075/IJNAA.2021.5379

[14] Perdana, G. A., Carudin, & Mayasari, R. (2021, Februari). Implementasi Algoritma Kriptografi Playfair Cipher untuk Mengamankan Data Aset (Studi Kasus: PT Adyawinsa Stamping Industries). 7(2), 6.

[15] Hermansa, Umar, R., & Yudhana, A. (2020, Juni 20). Implementasi Algoritma Playfair Cipher dan Least Significant Bit pada Citra Digital. 4(3), 8.

[16] Sinaga, I. P. (2021, Desember). Implementasi Kriptografi Hybrid Algoritma Elgamal Dan Double Playfair Cipher Dalam Pengamanan File Jpeg Berbasis Dekstop. 1(2), 67-74.

[17] B., M. B. A. M., Salim, Y., & Sugiarti. (2022, Februari). Implementasi Metode Kriptografi Menggunakan Cipher Subtitusi dan Cipher Transposisi pada Data Teks. 3(1), 42-51.

[18] Manliclic, G. M. M., Lamac, K. A. R., Regala, R. C., Blanco, M. C. R., & Dioses, R. M. (2023). Improving the Extended 10x10 Polybius Square Key Matrix for Playfair, Bifid, and Polybius Cipher. 4(7), 290-295.

[19] Winarko, E. (2019). Modification of Playfair Chiper to Strengthen Playfair Chiper Algorith with 2 Key Layer Matrix (KLM) Method. 5(3), 602-619.

[20] Oladipupo, E. T., & Abikoye, O. C. (2022, Maret). Modified Playfair cryptosystem for improved data security. 3(1), 51-64. 10.11591/csit.v3i1.pp51-64

[21] Prasetyo, E., & Lubis, Y. F. A. (2023). Optimasi Keamanan Hasil Enkripsi Algoritma Playfair Cipher ke dalam Kode Morse. 11(1), 41-50.

[22] Priyatna, B., & Hananto, A. L. (2020, Juli). Password Data Authentication Using a Combination of MD5 and Playfair Cipher Matrix 13x13. 1(2), 33-36.

[23] Pujeri, U., & Pujeri, R. (2020, January). Symmetric Encryption Algorithm using ASCII Values. 8(5), 2355-2359.

[24] Dash, S., Mondal, J., Bhattacharyya, A., & Swain2, D. (2023, Desember 11). VTE- An Advanced Playfair Encryption Method. 2981(1), 020038-1 - 020038-4.

[25] Mohamed, K., Mohammed Pauzi, M. N., Hj Mohd Ali, F. H., & Ariffin, S. (2022). Analyse On Avalanche Effect in Cryptography Algorithm. In H. H. Kamaruddin, T. D. N. M. Kamaruddin, T. D. N. S. Yaacob, M. A. M. Kamal, & K. F. Ne'matullah (Eds.), Reimagining Resilient Sustainability: An Integrated Effort in Research, Practices & Education, vol 3. European Proceedings of Multidisciplinary Sciences (pp. 610-618). European Publisher. https://doi.org/10.15405/epms.2022.10.57