JITEKH, Vol. 11, No. 1, Tahun 2023, 41-50

ISSN 2338-5677 Cetak
ISSN 2548-6646 Online

Optimasi Keamanan Hasil Enkripsi Algoritma Playfair Cipher ke dalam Kode Morse

Eko Prasetyo[1], Yessi Fitri Annisah Lubis[2]

[1,2]Program Studi Teknik Informatika, Fakultas Teknik dan Komputer, Universitas Harapan Medan, Medan, Indonesia
Email: [1]idsetyo31@gmail.com, [2]yessy.annisa@gmail.com

Abstrak

Meningkatkan keamanan kripto sistem merupakan tantangan yang menarik banyak pihak peneliti untuk mengusulkan dan mengembangkan kriptosistem baru untuk mencapai tujuan kriptografi. Selain menerapkan algoritma kriptografi yang baru, maka cara yang dapat dilakukan adalah dengan memodifikasi, menggabungkan algoritma atau bahkan dengan menambahkan metode lain guna meningkatkan algoritma kriptografi yang sudah ada. Playfair Cipher adalah salah satu algoritma kriptografi yang telah lama dikenal dan masih banyak dipakai dan dipelajari sampai saat ini. Untuk mengoptimasi atau memperkuat kerahasiaan data dari hasil enkripsi (ciphertext) menggunakan algoritma Playfair Cipher, maka akan dilakukan penelitian dengan menambahkan operasi reverse dan konversi kedalam kode morse. Penelitian ini menghasilkan sebuah aplikasi berbasis desktop yang dapat digunakan dalam mengoptimasi keamanan hasil enkripsi algoritma kriptografi Playfair Cipher. Darai hasil uji coba pada 10 sampel data menunjukkan bahwa frekuensi karakter hasil reverse dan enkripsi (ciphertext) mengalami perubahan nilai secara konstan seiring dengan penambahan jumlah karakter pada teks uji. Namun setelah dikonversi kedalam kode morse, maka tidak memperlihatkan adanya pola keterhubungan antara hasil konversi kode morse dengan plaintext. Hal ini membuktikan bahwa hasil enkripsi setelah dikonversi kedalam kode morse dapat meningkatkan (optimasi) keamanan dari algoritma Playfair Cipher, karena akan menghasilkan teks yang lebih acak serta tidak akan memperlihatkan pola-pola keterhubungan antara hasil konversi kedalam kode morse dengan teks asli (plaintext).

Kata Kunci : Optimasi, Kriptografi, Playfair Cipher, Reverse, Kode Morse

Abstract

Improving the security of cryptosystems is a challenge that attracts many researchers to propose and develop new cryptosystems to achieve cryptographic goals. In addition to implementing new cryptographic algorithms, the way that can be done is to modify, combine algorithms or even add other methods to improve existing cryptographic algorithms. Playfair Cipher is a cryptographic algorithm that has long been known and is still widely used and studied today. To optimize or strengthen the confidentiality of data from encryption (ciphertext) using the Playfair Cipher algorithm, research will be carried out by adding reverse operations and conversion into Morse code. This research produces a desktop-based application that can be used in optimizing the security of the encryption results of the Playfair Cipher cryptographic algorithm. From the test results on 10 data samples, it shows that the frequency of characters from the results of reverse and encryption (ciphertext) changes in value constantly along with the addition of the number of characters in the test text. However, after being converted into Morse code, it does not show any pattern of connection between the results of the Morse code conversion and plaintext. This proves that the encryption results after being converted into Morse code can increase (optimize) the security of the Playfair Cipher algorithm, because it will produce more random text and will not show patterns of connection between the results of the conversion into Morse code and the original text (plaintext).

Keyword: Optimizing, Cryptography, Playfair Cipher, Reverse, Morse Code.

1. PENDAHULUAN

Pesatnya kemajuan dalam bidang teknologi informasi dan komunikasi di era *modern* saat ini membawa perubahan yang besar, tidak hanya dalam hal kecepatan tetapi juga dalam hal kemudahan untuk mengakses informasi dan kemudahan untuk penyebarluasan informasi oleh masyarakat. Kemajuan dalam bidang teknologi informasi memberikan banyak keuntungan bagi kehidupan

ISSN 2338-5677 Cetak
ISSN 2548-6646 Online

ummat manusia, tetapi keuntungan yang ditawarkan juga menimbulkan kejahatan. Keamanan dan kerahasiaan sebuah informasi meruapakan hal yang sangat penting untuk dilakukan, terutama informasi sensitif atau pribadi yang hanya boleh diakses oleh pihak yang berhak saja, baik pada saat disimpan dalam media penyimpanan (*hard drive*) ataupun pada saat akan dikirimkan. Hal tersebut terlebih lagi jika pengirimannya dilakukan melalui jaringan publik, apabila informasi tersebut tidak diamankan terlebih dahulu maka sangat rentan disadap dan diketahui isi informasinya oleh pihak-pihak yang tidak memiliki wewenang. Salah satu cara yang dapat dilakukan untuk mengamankan informasi adalah dengan menggunakan teknik kriptografi.

Kriptografi merupakan salah satu ilmu pengkodean pesan yang digunakan untuk meningkatkan keamanan dalam pengiriman pesan atau komunikasi data. Kriptografi saat ini telah menjadi salah satu syarat penting dalam keamanan teknologi informasi dalam pengiriman pesan penting dan rahasia. Pengiriman pesan penting dan rahasia sangat rentan terhadap serangan yang dilakukan oleh pihak ketiga, seperti penyadapan, pemutusan komunikasi, dan pengubahan pesan yang dikirim. Tujuan dari kriptografi adalah untuk membuat informasi baik berupa teks, ataupun yang lainnya dapat dilindungi privasi atau kerahasiannya pada saat dibagikan sehingga sampai ke tujuan yang dimaksud dalam satu saluran yang sama[1]–[3]. Adanya kriptografi juga menjamin bukan hanya keamanan atas informasi yang dilindungi atau disembunyikan dari entitas tidak berkepentingan, melainkan juga menjaga otentifikasi daripada pengguna dalam hal ini pengirim dan penerima atas informasi tersebut [2].

Meningkatkan keamanan kripto sistem merupakan tantangan yang menarik banyak pihak peneliti untuk mengusulkan dan mengembangkan kriptosistem baru untuk mencapai tujuan kriptografi. Selain menerapkan algoritma kriptografi yang baru, maka cara yang dapat dilakukan adalah dengan memodifikasi, menggabungkan algoritma atau bahkan dengan menambahkan metode lain guna meningkatkan algoritma kriptografi yang sudah ada. *Playfair Cipher* adalah salah satu algoritma kriptografi yang telah lama dikenal dan masih banyak dipakai dan dipelajari sampai saat ini. Untuk mengoptimasi atau memperkuat kerahasiaan data dari hasil enkripsi (*ciphertext*) menggunakan algoritma *Playfair Cipher*, maka akan dilakukan penelitian dengan menambahkan operasi *reverse* dan konversi ke dalam kode *morse*. Tahapan penyandian yang dilakukan melalui proses *reverse*, enkripsi, dan konversi kode *morse* bertujuan untuk menghasilkan teks (*ciphertext*) yang benar-benar acak serta tidak memperlihatkan pola-pola keterhubungannya dengan teks asli (*plaintext*), sehingga dapat meningkatkan kerahasiaan hasil enkripsi algoritma *Playfair Cipher* serta mempersulit pihak-pihak yang tidak berwenang yang berusaha untuk memecahkan dan mengetahui makna asli dari teks yang bersifat rahasia.

Algoritma *Playfair Cipher* mempunyai sifat penyandian yang lemah jika penerapannya dilakukan secara individu. Penggunaan *ciphertext* tunggal yang secara komparatif lemah karena hanya menggunakan satu algoritma kriptografi. Modifikasi dari algoritma *Caesar Cipher* ke dalam bentuk sandi *morse* dapat dilakukan untuk tujuan meningkatkan keamanan dari suatu pesan teks, sehingga sulit untuk dipecahkan oleh pihak-pihak yang tidak bertanggung jawab [3]. Selain itu, modifikasi algoritma LCG (*Linear Congruential Generator*) dan konversi kode *morse* juga dapat membantu untuk proses kriptografi yang membuat hasil enkripsi pesan cukup susah untuk dibaca karena dalam proses enkripsi pesan tiap-tiap karakter *plaintext* akan dikonversikan dengan tanda titik (.) dan tanda kurang (-) pada *ciphertext*-ny [4].

Berdasarkan permasalahan yang telah telah diuraikan serta penjelasan dari hasil penelitian terdahulu, maka pembaruan yang dilakukan dalam penelitian ini adalah terletak pada konsep dan algoritma yang digunakan. Tujuan dari penelitian ini adalah menggabungkan algoritma kriptografi *Playfair Cipher* ke dalam kode *morse* yang bertujuan untuk mendapatkan hasil enkripsi (*ciphertext*) yang lebih kuat dan tidak mudah untuk dipecahkan serta membangun sebuah aplikasi dengan menerapkan algoritma kriptografi *Playfair Cipher* ke dalam kode *morse* guna mengoptimasi keamanan hasil enkripsi.

ISSN 2338-5677 Cetak
ISSN 2548-6646 Online

2. METODE PENELITIAN

Playfair Cipher merupakan salah satu algoritma kriptografi klasik [4], sebagai salah satu kriptosistem simetris populer yang ditemukan oleh Sir Charles Wheatstone dan Baron Lyon Playfair pada tahun 1854 [5]. Algoritma *Playfair Cipher* digunakan oleh tentara Inggris pada Perang Boer (Perang Dunia I) [6]. Algoritma kriptografi ini mengenkripsi pasangan huruf, bukan huruf tunggal seperti pada algoritma kriptografi klasik lainnya. Tujuan utamanya adalah untuk mempersulit analisis frekuensi dengan menyetarakan jumlah frekuensi kemunculan huruf-huruf di dalam *ciphertext* [4].

Playfair Cipher menggunakan 25 huruf kapital dengan ketentuan huruf I = J. Kata kunci untuk pengkodean dipilih, dan matriks 5 x 5 dibangun dengan menempatkan kata kunci tanpa huruf duplikat dari kiri ke kanan dan dari atas ke bawah[1], [7]. *Playfair Cipher* menggunakan kunci dalam tabel berukuran $5x5$ yang berisi 25 huruf *alphabet* [8] yang disusun dalam bentuk bujur sangkar sebagai tabel acuan dalam melakukan proses enkripsi dan dekripsi. Kunci ini mengandung seluruh huruf di dalam *alphabe*t kecuali huruf "J" yang dileburkan dengan huruf "I" [4]. Tujuannya adalah untuk membuat analisa frekuensi menjadi sangat sulit, sebab frekuensi kemunculan karakter-karakter di dalam *ciphertext* menjadi datar [9] sehingga tidak memperlihatkan pola-pola keterhubungannya antara teks asli (*plaintext*) dengan hasil enkripsi (*ciphertext*).

Playfair Cipher merupakan suatu algoritma kriptografi klasik yang termasuk ke dalam *polyalphabetic cipher*, dimana *plaintext* diubah menjadi bentuk poligram dan proses enkripsi dekripsi dilakukan untuk poligram tersebut [10]. Pada algoritma *Playfair Cipher* dibutuhkan dua huruf yang berpasangan (*digram*) dalam mengenkripsi dan mendekripsi pesan [8]. Algoritma *Playfair Cipher* bekerja dengan tiga tahap utama yaitu membuat bujursangkar/matriks kunci, proses mengatur pesan, proses enkripsi/dekripsi [11]. Beberapa aturan pada algoritma *Playfair Cipher* [8], yaitu sebagai berikut:

1. *Playfair Cipher* mengenkripsi *plaintext* berupa huruf besar selain huruf J. Spasi, karakter yang bukan huruf besar, dan huruf J harus dihilangkan dari *plaintext*.
2. Apabila terdapat huruf J pada *plaintext*, maka digantikan dengan huruf I.
3. *Plaintext* yang akan dienkripsi dituliskan dalam pasangan huruf (*bigram*).
4. Apabila ada huruf yang sama dalam pasangan huruf, maka disisipkan huruf X atau Z di tengahnya. Huruf yang disisipkan sebaiknya huruf X, karena kemungkinan terdapat huruf X yang sama dalam *bigram* sangat kecil.
5. Apabila jumlah huruf pada *plaintext* adalah ganjil, maka dipilih sebuah huruf sembarang untuk ditambahan di akhir *plaintext*.

Proses pembentukkan kunci pada algoritma *Playfair Cipher* hampir mirip dengan algoritma kriptografi *Vigenere Cipher*, tetapi pada *Playfair Cipher* memiliki teknik pemetaan yang lebih sulit jika dibandingkan dengan *Vigenere Cipher*. Adapun tahapan enkripsi dalam pembentukkan kunci pada *Playfair Cipher* [1] adalah sebagai berikut:

1. Susun huruf ke dalam bentuk matriks n×n dengan menghilangkan huruf yang sama atau berulang dari abjad kunci, dan tambahkan huruf yang belum ada.
2. Koreksi apabila terdapat dua huruf yang sama pada baris kunci, maka tiap huruf diganti dengan huruf di kanannya.
3. Apabila terdapat dua haruf pada kolom kunci yang sama, maka huruf tersebut harus diganti dengan huruf di bawahnya.
4. Apabila pada baris atau kolom tidak terdapat dua huruf tidak yang sama, maka huruf pertama harus diganti dengan huruf pada perpotongan baris huruf pertama dengan kolom huruf kedua. Selanjutnya, huruf kedua diganti dengan huruf pada titik sudut ke empat dari matriks persegi tersebut yang dibentuk dari 3 huruf.

Langkah-langkah enkripsi algoritma *Playfair Cipher* [8], yaitu sebagai berikut:

1. Apabila ada dua huruf terdapat pada baris kunci yang sama, maka setiap huruf diganti dengan huruf di kanannya.

ISSN 2338-5677 Cetak
ISSN 2548-6646 Online

2. Apabila ada dua huruf terdapat pada kolom kunci yang sama, maka setiap huruf diganti dengan huruf di bawahnya.
3. Apabila ada dua huruf tidak pada baris atau kolom yang sama, maka huruf pertama diganti dengan dengan huruf pada perpotongan baris huruf pertama dengan kolom huruf kedua. Huruf kedua diganti dengan huruf pada titik sudut ke empat dari persegi panjang yang dibentuk dari huruf yang digunakan.

Langkah-langkah dekripsi algoritma *Playfair Cipher* [8], yaitu sebagai berikut:

1. Apabila ada dua huruf terdapat pada baris kunci yang sama maka tiap huruf diganti dengan huruf di kirinya.
2. Apabila ada dua huruf terdapat pada kolom yang sama maka tiap huruf diganti dengan huruf diatasnya.
3. Jika dua huruf tidak pada baris yang sama atau kolom yang sama, maka huruf pertama diganti dengan huruf pada perpotongan baris huruf pertama dengan kolom huruf kedua. Huruf kedua diganti dengan huruf pada titik sudut keempat dari persegi panjang yang dibentuk dari huruf yang digunakan.

Algoritma *Playfair Cipher* merupakan salah satu algoritma kriptografi klasik yang mudah tertebak karena terdapat korespondensi satu-satu antara *plaintext* dengan *ciphertext*. Algoritma *Playfair Cipher* masih rentan terhadap serangan, karena sandi *Playfair Cipher* dapat dipecahkan dengan menggunakan teknik analisis frekuensi pasangan huruf [9]. Enkripsi menggunakan *Playfair Cipher* sulit untuk dikriptanalisis secara manual. Akan tetapi dapat dipecahkan dengan melakukan indentifikasi informasi jumlah frekuensi kemunculan *bigram* (pasangan huruf *alphabet*) [12].

Meningkatkan keamanan kripto sistem merupakan tantangan yang menarik banyak pihak peneliti untuk mengusulkan dan mengembangkan kriptosistem baru untuk mencapai tujuan ini. *Playfair Cipher* adalah salah satu algoritma kriptografi yang telah lama dikenal dan masih banyak dipakai dan dipelajari sampai saat ini[13]. Untuk mengoptimasi atau memperkuat kerahasiaan data dari hasil enkripsi (*ciphertext*) menggunakan algoritma *Playfair Cipher*, maka akan dilakukan penelitian dengan menambahkan operasi *reverse* dan konversi kedalam kode *morse*. Proses penyandian yang dilakukan dengan tahapan proses *reverse*, enkripsi, dan konversi kode *morse* bertujuan untuk menghasilkan teks yang benar-benar acak serta tidak memperlihatkan pola-pola keterhubungannya dengan teks asli, sehingga dapat meningkatkan kerahasiaan hasil enkripsi.

algoritma *Playfair Cipher* serta mempersulit pihak-pihak yang tidak berwenang yang berusaha untuk memecahkan dan mengetahui makna asli dari teks yang bersifat rahasia[14].

Optimasi Keamanan Kriptografi

Keamanan terhadap informasi data merupakan suatu proses untuk melindungi data dari perusakan atau penyalahgunaan yang dilakukan oleh pihak yang tidak bertanggung jawab. Kriptografi merupakan cara yang tepat untuk melakukan pengamanan terhadap informasi data, yang dimana enkripsi dan dekripsi menjadi fungsi dasar dari kriptografi. Pengamanan terhadap suatu data semakin hari juga semakin berkembang, hal ini dikarenakan banyak algoritma kriptografi telah dapat dipecahkan oleh piranti lunak yang memang dibuat untuk memecahkan algoritma-algoritma kriptografi. Selain menerapkan algoritma kriptografi yang baru, biasanya banyak peneliti memodifikasi suatu algoritma kriptografi, akan tetapi hal ini bukanlah suatu pekerjaan yang mudah [2]

Dalam penelitian yang dilakukan oleh [15], hasil penelitian menunjukkan bahwa penambahan operasi *bitswap* dan transposisi acak mampu meningkatkan kinerja algoritma *Vigenere Cipher* dalam enkripsi citra. Pengembangan dengan mengkombinasikan teknik kriptografi *Caesar Cipher* dengan algoritma kompresi *Stout Codes* [2]. Hasil penelitian ini menyimpulkan bahwa kombinasi dari *Caesar Cipher* dan algoritma *Stout Codes* dapat meningkatkan keamanan data. Hasil *ciphertext* dari *Caesar Cipher* yang telah dikompresi terlihat seperti hasil enkripsi dari algoritma kriptografi *modern*, sehingga dapat menjadi solusi untuk mengamankan data yang penting.

ISSN 2338-5677 Cetak
ISSN 2548-6646 Online

Kode Morse

Kode *morse* adalah metode mentransmisi informasi teks dalam urutan nada *on-off*, cahaya, atau klik yang bisa langsung dimengerti oleh pendengar atau pengamat berpengalaman tanpa alat khusus. Kode *morse* dinamai berdasarkan penemu telegraf, Samuel F. B. Morse.[16]. Kode *morse* internasional akan menyandikan huruf latin dasar, beberapa huruf latin spesial, angka *Arabic*, dan *prosigns* yang memiliki standarisasi deretan *signal* pendek dan panjang yang dinamai sebagai titik dan garis (*dots and dashes*). Setiap simbol pada kode *morse* akan menggambarkan sebuah huruf karakter (teks atau angka) atau *prosigns*. Jangka waktu lamanya suatu *signal* panjang yang berbentuk *dashes*/garis merupakan tiga kalinya dari jangka waktu *dots*/titik. Jarak antar *dashes*/*dots* adalah satu garis [17].

Penerapan Algoritma Playfair Cipher

Berikut ini akan dicontohkan proses enkripsi dan dekripsi algoritma *Playfair Cipher* dengan menggunakan kunci berukuran $5x5$ yang berisi 25 huruf *alphabet*. Misalkan kunci yang dipilih adalah 'TEKNIKINFORMATIKA". Kemudian dilakukan proses enkripsi, adalah sebagi berikut:

1. Cek huruf yang sama pada kunci dan jika terdapat huruf "J" maka diganti dengan huruf "I". Sehingga, diperoleh kunci "TEKNIFORMA" dan tambahkan dengan huruf abjad untuk sisanya yang tidak terdapat pada kunci tadi.

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

Selanjutnya *plaintext* yang akan diamankan adalah "KRIPTOGRAFI". *Plaintext* tersebut dibentuk berpasangan, yaitu:

KR IP TO GR AF IZ

Untuk karakter "KR", maka hasil enkripsinya yaitu:

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

Dua huruf *plaintext* tersebut tidak satu baris tetapi satu kolom, maka huruf "R" turun 1 tingkat ke bawah menjadi "D", dan "K" turun ke bawah menjadi huruf "R", karena "R" disebut pembanding "K", sehingga *ciphertext* dari "KR" adalah "RD". Untuk karakter "IP", maka hasil enkripsinya yaitu:

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

Sama seperti *plaintext* sebelumnya, maka *ciphertext* dari "IP" adalah "EU".
Untuk karakter "TO", maka hasil enkripsinya yaitu:

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

Sama seperti *plaintext* sebelumnya, maka *ciphertext* dari "TO" adalah "EF".

Untuk karakter "GR", maka hasil enkripsinya yaitu:

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

Sama seperti *plaintext* sebelumnya, maka *ciphertext* dari "GR" adalah "DM".
Untuk karakter "AF", maka hasil enkripsinya yaitu:

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

Sama seperti *plaintext* sebelumnya, maka *ciphertext* dari "AF" adalah "FO".
Untuk karakter "IZ", maka hasil enkripsinya yaitu:

ISSN 2338-5677 Cetak
ISSN 2548-6646 Online

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

Sama seperti *plaintext* sebelumnya, maka *ciphertext* dari "IZ" adalah "TV".

Dari proses enkripsi di atas maka diperoleh *ciphertext* dari *plaintext* "KR IP TO GR AF IZ" adalah "RD EU EF DM FO TV".

Ciphertext	T	A	F	M	C	M	E	L	K	A	I	X
Kode Morse	-	.-	..-.	--	-.-.	--	.	.-..	-.-	.-	..	-..-

Dari proses *reverse*, enkripsi, dan konversi kode *morse* di atas maka diperoleh hasil perbandingan antara *plaintext*, hasil *reverse*, hasil enkrips, dan hasil konversi kedalam kode *morse* seperti disajikan pada tabel 1.

Tabel 1. Hasil Enkripsi

Plaintext	K	R	I	P	T	O	G	R	A	F	I	
Reverse	I	F	A	R	G	O	T	P	I	R	K	
Ciphertext	T	A	F	M	C	M	E	L	K	A	I	X
Kode Morse	-	.-	..-.	--	-.-.	--	.	.-..	-.-	.-	..	-..-

2. Untuk mengembalikan *ciphertext* ke bentuk *plaintext* dilakukan dengan proses dekripsi, adalah sebagai berikut:

Untuk karakter "RD", maka hasil dekripsinya yaitu:

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

Maka, *plaintext* dari "RD" adalah "KR".
Untuk karakter "TU", maka hasil dekripsinya yaitu:

T	E	K	N	I
F	O	R	M	A
B	C	D	G	H
L	P	Q	S	U

Berdasarkan proses enkripsi dengan menggunakan kunci algoritma *Playfair Cipher*, maka diperoleh *ciphertext* yaitu TAFMCMELKAIX. Hasil enkripsi (*ciphertext*) kemudian akan dikonversi kedalam kode *morse*, sehingga diperoleh hasilnya yaitu:

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

Maka, *plaintext* dari "EF" adalah "TO".

Untuk karakter "DM", maka hasil dekripsinya yaitu:

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

Maka, *plaintext* dari "TU" adalah "IP".

Untuk karakter "EF", maka hasil dekripsinya yaitu:

Maka, *plaintext* dari "DM" adalah "GR".
Untuk karakter "FO", maka hasil dekripsinya yaitu:

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

Maka, *plaintext* dari "FO" adalah "AF".
Untuk karakter "TV", maka hasil dekripsinya yaitu:

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

Maka, *plaintext* dari "TV" adalah "IZ".

Berdasarkan proses dekripsi dengan menggunakan kunci algoritma *Playfair Cipher*, maka diperoleh

ISSN 2338-5677 Cetak
ISSN 2548-6646 Online

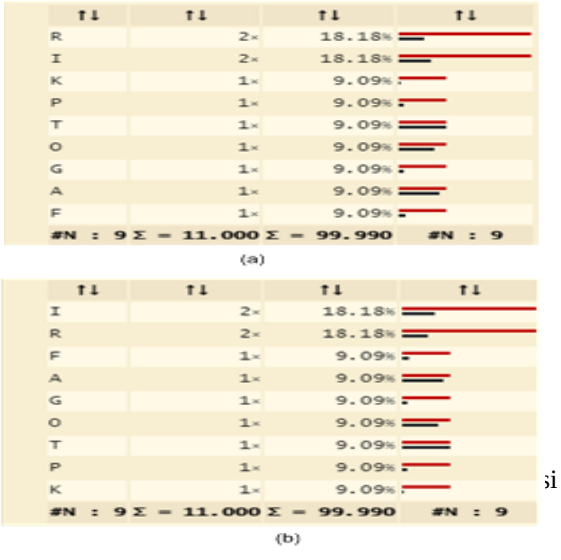
plaintext yaitu IFARGOTPIRKZ. Dari hasil enkripsi ini kemudian akan dihilangkan karakter "Z" yang merupakan karakter tambahan pada proses enkripsi sebelumnya, sehingga hasil akhir dari proses dekripsi yaitu IFARGOTPIRK. Hasil dekripsi kemudian akan dilakukan proses *reverse* untuk mengembalikan sususan asli dari *plaintext* sebelumnya, sehingga diperoleh hasil *reverse* yaitu:

Plaintext	I	F	A	R	G	O	T	P	I	R	K
Reverse	K	R	I	P	T	O	G	R	A	F	I

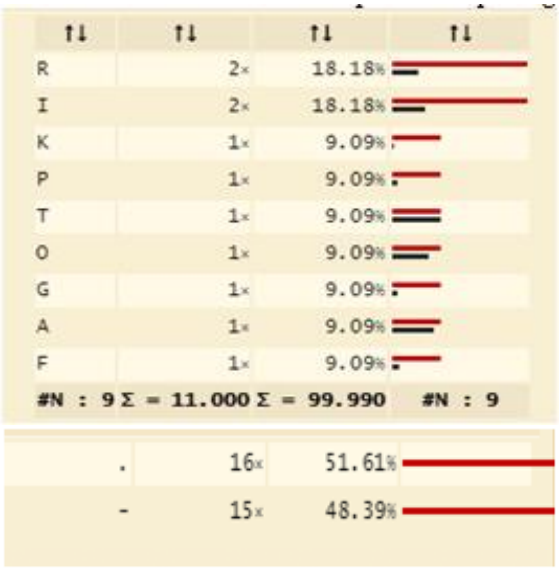
Berdasarkan hasil akhir dari proses *reverse* maka diperoleh kembali pesan aslinya yang sama persis dengan pesan asli sebelum di enkripsi yaitu KRIPTOGRAFI.

3. HASIL DAN PEMBAHASAN

Pengujian dengan teknik frekuensi dilakukan untuk membuktikan keamanan sistem yang ditinjau dari frekuensi pengulangan karakter pada hasil enkripsi (*ciphertext*) yang kerap muncul. Pengujian dilakukan dengan memanfaatkan *tools* yang diakses secara *online* dari *https://www.dcode.fr/frequency-analysis*. Adapun hasil pengujian keamanan sistem yang ditinjau dari frekuensi pengulangan karakter pada hasil enkripsi (*ciphertext*) dapat disajikan pada gambar 1.



Gambar 1. Hasil Pengujian Analisis Frekuensi Karakter (a) Plaintext (b) Ciphertext



Gambar 2. Hasil Pengujian Analisis Frekuensi Plaintext Kode Morse

Adapun hasil perbandingan analisis frekuensi pada sampel data dengan jumlah karakter 160 sampai 760 dapat disajikan pada tabel 2.

Tabel 2. Perbandingan Hasil Analisis Frekuensi Tertinggi

Panjang Karakter	Kunci	Frekuensi Tertinggi (Plaintext)			Frekuensi Tertinggi (Ciphertext)		
		Karakter	Frekuensi	Persentase	Karakter	Frekuensi	Persentase
160	Unhammedan	A	23	16,67%	E	11	7,97%
360	Unhammedan	A	53	17,21%	B	29	9,42%
510	Unhammedan	A	76	17,47%	R	47	10,78
645	Unhammedan	A	102	18,51%	R	64	11,59%
760	Unhammedan	A	128	19,78%	R	79	12,19%

Hasil Pengujian Waktu Eksekusi Enkripsi dan Deskripsi

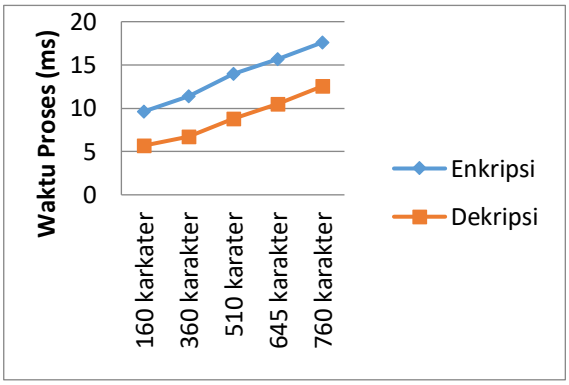
Pengujian waktu eksekusi (*running time*) dilakukan untuk mengetahui kinerja tingkat kecepatan dalam waktu enkripsi dan dekripsi dalam satuan waktu ms (*millisecond*). Pengujian dilakukan terhadap lima file uji dengan jumlah karakter 160 sampai 760 karakter. Adapun hasil pengujian waktu eksekusi enkripsi dan dekripsi dapat disajikan pada tabel 3.

ISSN 2338-5677 Cetak
ISSN 2548-6646 Online

Tabel 3. Hasil Uji Coba Pengujian Waktu Eksekusi Enkripsi dan Dekripsi

No.	Panjang Karakter	Kunci	Waktu Enkripsi (ms)	Waktu Dekripsi (ms)
1.	160	unharmedan	9,6175	5,6818
2.	360	unharmedan	11,3562	6,7389
3.	510	unharmedan	13,939	8,8193
4.	645	unharmedan	15,6901	10,4554
5.	760	unharmedan	17,5914	12,5363
Rata-rata			13,6388	8.8463

Hasil uji coba pengujian pada tabel 3 didapatkan rata-rata kecepatan proses enkripsi yaitu 13,6388 ms (*millisecond*). Sedangkan rata-rata kecepatan proses dekripsi yaitu 8.8463 ms (*millisecond*). Data yang sudah diperoleh dari hasil pengujian proses enkripsi dan dekripsi pada tabel 3 dapat digambarkan dalam bentuk grafik untuk mengetahui perbandingan antara jumlah karakter dengan waktu proses eksekusi (running time) enkripsi dan dekripsi seperti pada gambar 3.



Gambar 3. Perbandingan Waktu Proses Enkripsi dan Dekripsi

Dapat disimpulkan dari grafik pada gambar 3 bahwa banyaknya jumlah karakter yang dienkripsi dan dekripsi berbanding lurus dengan besarnya waktu yang dibutuhkan untuk melakukan proses eksekusi (*running time*). Artinya semakin panjang karakter yang digunakan maka akan semakin lama juga waktu yang dibutuhkan untuk melakukan proses enkripsi dan dekripsi.

4. KESIMPULAN

Kesimpulan yang dapat diambil setelah melakukan implementasi dan pengujian sistem optimasi keamanan hasil enkripsi algoritma *Playfair Cipher* kedalam kode *morse* adalah sebagai berikut:

1. Hasil enkripsi algoritma kriptografi *Playfair Cipher* dapat ditingkatkan (optimasi) dengan menambahkan operasi *reverse* pada *plaintext* sebelum di enkripsi, lalu dilakukan konversi pada *ciphertext* kedalam kode *morse* untuk menghasilkan teks yang lebih acak serta tidak akan memperlihatkan pola-pola keterhubungan antara hasil konversi *ciphertext* kedalam kode *morse* dengan teks asli (*plaintext*).
2. Penelitian ini menghasilkan sebuah aplikasi berbasis *desktop* yang dapat digunakan dalam mengoptimasi keamanan hasil enkripsi algoritma kriptografi *Playfair Cipher*. Darai hasil uji coba pada 10 sampel data menunjukkan bahwa frekuensi karakter hasil *reverse* dan enkripsi (*ciphertext*) mengalami perubahan nilai secara konstan seiring dengan penambahan jumlah karakter pada teks uji. Namun setelah dikonversi kedalam kode *morse*, maka tidak memperlihatkan adanya pola keterhubungan antara hasil konversi kode *morse* dengan *plaintext*. Hal ini membuktikan bahwa hasil enkripsi setelah dikonversi kedalam kode *morse* dapat meningkatkan (optimasi) keamanan dari algoritma *Playfair Cipher*, karena akan menghasilkan teks yang lebih acak serta tidak akan memperlihatkan pola-pola keterhubungan antara hasil konversi kedalam kode morse dengan teks asli (*plaintext*).

5. DAFTAR PUSTAKA

[1] F. Azmi and R. Anugrahwaty, "Analisis Matriks 5x7 Pada Kriptografi Playfair Cipher," *J. Penelit. Tek. Inform.*, vol. 1, no. 2, pp. 27–30, 2017, [Online]. Available: https://jurnal.polgan.ac.id/index.php/sinkron/article/view/32

[2] M. Mesran and S. D. Nasution, "Peningkatan Keamanan Kriptografi Caesar Cipher dengan Menerapkan Algoritma Kompresi

ISSN 2338-5677 Cetak
ISSN 2548-6646 Online

Stout Codes," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 6, pp. 7–12, 2020, doi: 10.29207/resti.v4i6.2730.

[3] I. Darmayanti, D. N. Astrida, and D. Ariyus, "Penerapan Keamanan Pesan Teks Menggunakan Modifikasi Algoritma Caisar Chiper Kedalam Bentuk Sandi Morse," *J. Ilm. IT CIDA*, vol. 4, no. 1, pp. 39–47, 2018, doi: 10.55635/jic.v4i1.78.

[4] S. D. Surbakti, "Implementasi Algoritma Playfair Cipher pada Penyandian Data," *J. Tek. Inform. Unika St. Thomas*, vol. 4, no. 2, pp. 166–123, 2019, doi: 10.17605/jti.v4i2.42.

[5] M. S. Yousif, R. K. Salih, and N. M. G. Alsaidi, "A New Modified Playfair Cipher," *AIP Conf. Proc.*, vol. 2086, no. April, pp. 2–6, 2019, doi: 10.1063/1.5095132.

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

[7] M. Syahrizal, M. Murdani, S. D. Nasution, M. Mesran, R. Rahim, and A. P. U. Siahaan, "Modified Playfair Cipher Using Random Key Linear Congruent Method," *J. Online Jar. COT POLIPD*, vol. 8, no. 1, pp. 45–49, 2017, [Online]. Available: https://www.geocities.ws/apacc/paper8_syarizalscience_irstc_vol9.pdf

[8] R. A. Sukmawati, A. Riski, and A. Kamsyakawuni, "Perbandingan Playfair Cipher Dengan 3D Playfair Cipher Pada Pengamanan Citra," *Maj. Ilm. Mat. dan Stat.*, vol. 21, no. 1, pp. 15–24, 2021, doi: 10.19184/mims.v21i1.23116.

[9] A. Hariati, K. Hardiyanti, and W. E. Putri, "Kombinasi Algoritma Playfair Cipher Dengan Metode Zig-zag Dalam Penyandian Teks," *Sink. (Publikasi J. Penelit. Tek. Inform.*, vol. 2, no. 2, pp. 13–17, 2018, [Online]. Available: https://jurnal.polgan.ac.id/index.php/sinkron/index

[10] Y. Permanasari and E. Harahap, "Kriptografi Polyalphabetic," *J. Mat.*, vol. 17, no. 1, pp. 31–34, 2018, doi: 10.29313/jmtm.v17i1.4065.

[11] R. K. Hondro, "Modifikasi Platform Kunci Algoritma Playfair Untuk Meningkatkan Nilai Confusion Pada Ciphertext," *J. Comput. Syst. Informatics*, vol. 1, no. 2, pp. 76–82, 2020, [Online]. Available: https://ejurnal.seminar-id.com/index.php/josyc/article/view/102

[12] S. Murdowo, "Manual Perhitungan Menggunakan Kriptografi Klasik Playfair Chiper," *J. INFOKAM*, vol. XVI, no. 19, 2020, doi: https://doi.org/10.53845/infokam.v16i1.217.

[13] M. Z. Siambaton and A. Muhazir, "Modifikasi Algoritma Playfair Cipher Dengan Pengurutan Array Pada Matriks," *J. Ilmu Komput. dan Inform.*, vol. 2, no. 1, pp. 66–71, 2018.

[14] A. Ridho, C. Mutia, and A. P. Sinaga, "Analisis Enkripsi dan Dekripsi Cipher Teks Menggunakan Kombinasi Gronsfeld Cipher Dengan Reverse Cipher," *J. Tek. Inform. Kaputama*, vol. 6, no. 1, 2022, [Online]. Available: https://jurnal.kaputama.ac.id/index.php/JTIK/article/view/689

[15] L. Andriani, Rihartanto, and A. B. W. Putra, "Optimasi Vigenere Cipher Menggunakan Bitswap dan Transposisi Acak pada Citra RGB," *Techno.Com*, vol. 19, no. 2, pp. 168–177, 2020, doi: 10.33633/tc.v19i2.3322.

[16] A. Wijaya, E. Kwok, and H. Agung, "Aplikasi Morse Code Translator Metode Klasifikasi Euclidean Distance dengan Algoritma Ocrchie untuk Menerjemahkan Kode Morse," *KALBISCIENTIA J. Sains dan Teknol.*, vol. 5, no. 1, pp. 30–34, 2018, [Online]. Available: http://research.kalbis.ac.id/Research/Files/A

ISSN 2338-5677 Cetak
ISSN 2548-6646 Online

rticle/Full/5GJT98A5SN6NP8S131Z5HQAM3.pdf

[17] D. N. Triwibowo, Purwono, I. A. Ashari, A. S. Sandi, and Y. F. Rahman, "Enkripsi Pesan Menggunakan Algoritma Linear Congruential Generator (LCG) dan Konversi Kode Morse," *Bul. Ilm. Sarj. Tek. Elektro*, vol. 3, no. 3, pp. 194–201, 2022, doi: 10.12928/biste.v3i3.5546.