Buletin Sistem Informasi dan Teknologi Islam
Vol 1, No 1, November 2020, pp. 266-269
ISSN: 2721-0901

Peningkatan Keamanan Data dengan Menggunakan *Equation* pada Metode *Playfair Cipher*

Rahmat Suriadi [a,1,*],Ramdan Satra [a,2],Farniwati Fattah [a,3]

[a] *Program Studi Teknik Informatika, Universitas Muslim Indonesia, Jalan Urip Sumoharjo KM.05, Makassar, 90231, Indonesia*
[1] *rahmatsuariadi99@gmail.com;* [2] *ramdan@umi.ac.id;* [3] *farniwati.fattah@umi.ac.id;*
**corresponding author*

INFORMASI ARTIKEL

Diterima : 05 – 10 – 2020
Direvisi : 20 – 11 – 2020
Diterbitkan : 30 – 11 – 2020

Kata Kunci:
Metode *Playfair Cipher*
Dekripsi
ASCII
Enkripsi
Equation

ABSTRAK

Internet merupakan suatu sistem jaringan komputer yang terhubung satu sama lain di seluruh dunia. Jaringan ini memungkinkan penggunanya saling bertukar informasi satu sama lain tanpa batas. Dunia berkembang kian cepat seiring majunya teknologi informasi. Komunikasi kini menjadi tidak terbatas. Dengan banyaknya kemudahan untuk melakukan pengaksesan informasi, adakalanya diperlukan pengamanan informasi tersebut. Pengamanan ini berfungsi menangani pencegahan atas sampainya informasi ketangan yang tidak berhak yang dapat menimbulkan kerugian bagi pemilik informasi. Komponen yang penting pada metode *playfair* adalah tabel *cipher* yang digunakan untuk melakukan enkripsi dan dekripsi tabel bawaan yang diperkenalkan oleh playfair adalah tabel yang berbentuk matrik berukuran (5×5) yang berisi huruf kapital dari A- Z dengan menghilangkan J. Metode *Playfair Cipher* menggunakan pembentukan tabel berdasarkan kunci yang diketahui. Hasil enkripsi dan dekripsi data menggunakan simbol ASCII terhadap teks berupa equation atau rumus matematika tidak tepat digunakan dikarenakan ada banyak simbol matematika yang tidak ada dalam simbol ASCII seperti simbol akar (√), integral (∫), dll.

I. Pendahuluan

Internet merupakan suatu sistem jaringan komputer yang terhubung satu sama lain di seluruh dunia. Jaringan ini memungkinkan penggunanya saling bertukar informasi satu sama lain tanpa batas. Dunia berkembang kian cepat seiring majunya teknologi informasi[1],[2]. Komunikasi kini menjadi tidak terbatas. Dengan banyaknya kemudahan untuk melakukan pengaksesan informasi, adakalanya diperlukan pengamanan informasi tersebut. Pengamanan ini berfungsi menangani pencegahan atas sampainya informasi ketangan yang tidak berhak yang dapat menimbulkan kerugian bagi pemilik informasi[3],[4],[5].

Kriptografi pada awalnya merupakan ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandingkannya kedalam bentuk yang tidak dapat dimengerti lagi maknanya. Kemudian seiring dengan berkembangnya kriptografi yaitu kriptografi tidak lagi sebatas mengenkripsikan pesan, tetapi juga memberikan aspek keamanan yang lain seperti serangan dari kriptanalisis. Karena itu pengertian dari kriptografi berubah menjadi ilmu sekaligus seni untuk menjaga keamanan pesan[6],[7],[8].

Komponen yang penting pada metode *playfair* adalah tabel *cipher* yang digunakan untuk melakukan enkripsi dan dekripsi tabel bawaan yang diperkenalkan oleh playfair adalah tabel yang berbentuk matrik berukuran (5×5) yang berisi huruf kapital dari A- Z dengan menghilangkan J. Tabel bawaan yang ada pada *playfair cipher* tidak dapat mengenkripsi *Plaintext* yang berisiangka (0-9) dan simbol-simbol[9],[10].

Tabel *playfair cipher* telah dimodifikasi dengan tabel yang berbentuk tabel berukuran (8×8) yang pernah diteliti oleh [11] (Susanti, 2019) yang dapat digunakan untuk melakukan enkripsi huruf, angka dan simbol. Akan tetapi pada *playfair* 8×8 ini belum bisa mengekripsi data berupa *equation*/persamaan.

Karena itu muncul suatu gagasan yang mengacu pada hal tersebut, yaitu untuk meninkatkan keamanan serta penggunaan kunci rahasia yang digunakan pada metode *Playfair Cipher* dengan menerapkam *equation*. Pada penelitian ini penulis mencoba membahas mengenai pengamanan data atau informasi dengan meningkatkan keamanan data dengan menerapkan *equation* pada metode *playfair cipher*.

II. Metode

Metode yang digunakan dalam pengembangan sistem pada penelitian ini adalah metode *waterfall* yang terdiri dari beberapa tahapan yaitu sebagai berikut.

A. Perancangan

Tahap perangcangan yaitu:

- Mengidentifikasi semua kebutuhan dalam pembuatan keamanan data dengan menerapkan *equation* pada metode *playfair cipher* yaitu *hardware*, *software* dan kebutuhan lainnya.
- Merancang *interface*.
- Merancang program yaitu *input*, proses dan *output*.

B. Playfair Cipher

Playfair Cipher merupakan *digraphs Cipher*, yang dimana setiap proses enkripsi dilakukan pada setiap dua huruf, berikut adalah Algoritma enkripsi dari *playfair cipher*:

- Jika dua huruf terdapat pada baris kunci yang sama maka tiap huruf diganti dengan huruf dikanannya.
- Jika dua huruf terdapat pada kolom kunci yang sama maka tiap huruf diganti dengan huruf dibawahnya.
- Jika dua huruf tidak pada baris yang sama atau kolom yang sama, maka huruf pertama diganti dengan huruf pada perpotongan huruf baris pertama dengan kolom huruf kedua. Huruf kedua diganti dengan huruf pada titik sudut keempat dari persegi panjang yang dibentuk dari 3 huruf yang digunakkan sampai sejauh ini.

C. Pembuatan

Pada tahap ini akan dilakukan pembetukan sistem keamanan data dengan menerapkan *equation* pada metode *playfair cipher*. Dengan menerapkan rancangan program yang telah dibuat dan mengimplementasikan kedalam *software* dan *hardware* yang telah disediakan.

D. Pengujian

Setelah tahapan perancangan dan pembuatan selesai, maka dilakukan pengujian dengan tujuan untuk mengetahui apakah sesuai dengan apa yang direncanakan. Apabilah masi ada kekurangan dan tidak sesuai dengan apa yang diharapkan maka perlu untuk diperbaiki kembali.

E. Analisis

Pada tahap ini dilakukan analisis data hasil pengujian yang bertujuan untuk mengetahui hasil dan kesimpulan dari beberapa pengujian yang telah dilakukan. Dari analisis ini akan diketahui kekurangan dan kelebihan.

III. Hasil dan Pembahasan

A. Pengujian Sistem berdasarkan Jumlah Karakter pada Plaintext bernilai Ganjil.

Pada proses enrkipsi dan dekripsi dengan kondisi jumlah *plaintext* dan *ciphertext* bernilai ganjil maka pada karakter terakhir dari *plaintext* akan ditambahkan simbol "X". Berikut hasil pengujian yang dilakukan dapat dilihat pada tabel 1.

Tabel 1. Pengujian Jumlah Karakter Ganjil

Enkripsi				
Pengujian	***Plaintext***	***Key***	***Hasil***	***Durasi(s)***
Jumlah karakter ganjil	$(10+4)+9=10+(4+9)$	PlayFairCipher	)21,8%*:@.1,%7*:(Y	0.011
Jumlah karakter genap	$30\times(9-2)=(30\times9)-(30\times2)$	PlayFairCipher	?$Ø)<*$*7.?$ƒ8*.$7)Ñ$*	0.050
Dekripsi				
Pengujian	***Ciphertext***	***Key***	***Hasil***	***Durasi(s)***
Jumlah karakter ganjil	)21,8%*:@.1,%7*:(Y	PlayFairCipher	$(10+4)+9=10+(4+9)$	0.012
Jumlah karakter genap	?$Ø)<*$*7.?$ƒ8*.$7)Ñ$*	PlayFairCipher	$30\times(9-2)=(30\times9)-(30\times2)$	0.020

Dari data tabel 1 dapat disimpulkan bahwa proses Enkripsi dikatakan berhasil karena hasil enkripsi yang kemudian didekripsi menggunakan *key* yang sama menghasilkan hasil dekripsi yang sama dengan *plaintext*.

B. Pengujian Sistem dengan Menggunakan Simbol Equation Umum

Pengujian sistem dengan menggunakan simbol *equation* dilakukan dengan *plaintext* dituliskan dalam format *equation* pada *Microsoft Word* kemudian disalin ke *Form Plaintext* di halaman Enkripsi. Beberapa penulisan dalam *equation* akan berubah yang kemudian teks tersebutlah yang akan dienkripsi. Setelah hasil dari proses enkripsi dilakukan, dilanjutkan dengan proses dekripsi. Hasil dari proses dekripsi ini, akan disalin ke format penulisan *equation* pada *Microsoft Word*. Jika penulisan hasil dekripsi dalam format *equation* dari *Microsoft Word* sama dengan *plaintext* sebelumnya, maka proses enkripsi dan dekripsi dikatakan berhasil.

Berikut pengujian sistem dengan menggunakan simbol *Equation* umum dapat dilihat pada tabel 2.

Tabel 2. Pengujian Jumlah Karakter Ganjil

Enkripsi				
Pengujian Rumus	***Plaintext***	***Key***	***Hasil***	***Durasi(s)***
Penjumlahan	$a + \mathrm{b} + \mathrm{c} + \mathrm{d} = \mathrm{abcd}$	PlayFairCipher	C&[1[2t3"VTx	0.007
Pengurangan	$(10 - 4) - 9 = 10 - (4 - 9)$	PlayFairCipher	)21.8%*<@.1.%7*<(Y	0.006
Perkalian	$(a + b) \times c = (a \times c) + (b \times c)$	PlayFairCipher	&F1[8¡^A&FºY*,1XºY(Y	0.016
Pembagian	$32 \div 4 = 8$	PlayFairCipher	A$¶6>9	0.008
Perpangkatan	$KPK: 2^3 \times 3^4 = 8 \times 81 = 648$	PlayFairCipher	BC[K.c8Ö=T5>I¡@)>759	0.010
Penarikan akar	$a^{\frac{1}{n}} = \sqrt[n]{a}$ a^(1/n)=√(n&a)	PlayFairCipher	eV)2*u.8*)g*i&	0.013
Pecahan	$\frac{1}{4} + \frac{2}{5} + \frac{5+8}{20} = \frac{13}{20}$ 1/4+2/5+(5+8)/20=13/20	PlayFairCipher	20:%$06>&7):*0$1@.>$$1	0.051
Integral	$\int f(x)dx = f(x) + c$	PlayFairCipher	h¿k%m2fd7e2k*,TY	0.047
Dekripsi				
Pengujian	***Ciphertext***	***Key***	***Hasil***	***Durasi(s)***
Penjumlahan	C&[1[2t3"VTx	PlayFairCipher	$a + \mathrm{b} + \mathrm{c} + \mathrm{d} = \mathrm{abcd}$	0.006
Pengurangan	)21.8%*<@.1.%7*<(Y	PlayFairCipher	$(10 - 4) - 9 = 10 - (4 - 9)$	0.007
Perkalian	&F1[8¡^A&FºY*,1XºY(Y	PlayFairCipher	$(a + b) \times c = (a \times c) + (b \times c)$	0.012
Pembagian	A$¶6>9	PlayFairCipher	$32 \div 4 = 8$	0.009
Perpangkatan	BC[K.c8Ö=T5>I¡@)>759	PlayFairCipher	$KPK: 2^3 \times 3^4 = 8 \times 81 = 648$ KPK:2^3×3^4=8×81=648	0.011
Penarikan akar	eV)2*u.8*)g*i&	PlayFairCipher	a^(1/n)=)(n&a)	0.010
Pecahan	20:%$06>&7):*0$1@.>$$1	PlayFairCipher	1/4+2/5+(5+8)/20=13/20	0.024
Integral	h¿k%m2fd7e2k*,TY	PlayFairCipher	P▒f(x)dx=f(x)+c	0.024

Berdasarkan hasil pengujian yang dapat dilihat pada tabel 2 dapat disimpulkan bahwa proses enkripsi untuk pengujian rumus penjumlahan, pengurangan, perkalian, pembagian, perpangkatan, dan pecahan berhasil karena hasil enkripsi yang kemudian didekripsi menggunakan *key* yang sama menghasilkan hasil dekripsi yang sama dengan *plaintext.* Hal ini juga dapat dilihat dari penulisan hasil dekripsi dan *plaintext* dalam format *equation* di *Microsoft Word.*

Sedangkan untuk proses enkripsi untuk pengujian penarikan akar dan integral tidak berhasil karena hasil enkripsi yang kemudian didekripsi menggunakan *key* yang sama menghasilkan hasil dekripsi yang berbeda dengan *plaintext.* Hal ini juga dapat dilihat dari penulisan hasil dekripsi dan *plaintext* dalam format *equation* di *Microsoft Word* tidak sama. Ini dikarenakan simbol akar (√) dan integral (∫) tidak ada dalam simbol ASCII, sehingga menyebabkan proses enkripsi dan dekripsi tidak berhasil.

Proses pengujian dari proses enkripsi dan dekripsi yang telah dilakukan dapat dilihat dari hasil percobaan bahwa lambat cepatnya proses enkripsi dan dekripsi itu dipengaruhi oleh panjang *key* lambat cepatnya proses enkripsi dan dekripsi itu dipengaruhi oleh panjang *key* yang digunakan, dimana semakin panjang *key* yang digunakan maka semakin lama waktu yang dibutuhkan untuk proses enkripsi dan dekripsi.

IV. Kesimpulan dan saran

Proses kriptografi menggunakan metode *playfair cipher* efektif dalam melakukan proses enkripsi dan dekripsi data teks. Proses enkripsi dan dekripsi data menggunakan simbol ASCII terhadap teks berupa *equation* atau rumus matematika tidak tepat digunakan dikarenakan ada banyak simbol matematika yang tidak ada dalam simbol ASCII seperti simbol akar (√), zigma (∑), integral (∫), dll. Proses enkripsi dam dekripsi masih berpeluang tidak berhasil dalam proses enkripsi dan dekripsinya jika dalam proses enkripsi melibatkan karakter "RS", "US", dan spasi. Ini dikarenakan implementasi enkripsi dan dekripsi dilakukan per karakter.

Daftar Pustaka

[1] P. S. Eka, "Implementasi Keamanan Data Menggunakan Algoritma Vernam Cipher Dan Playfair Cipher," *J. Pelita Inform.*, vol. 17, no. 4, pp. 430–435, 2018.

[2] R. C. N. Santi, "Implementasi Algoritma Enkripsi Playfair pada File Teks," *J. Teknol. Inf. Din.*, vol. XV, no. 1, pp. 27–33, 2010.
[3] D. P. O. Simamora, "Implementasi Algoritma RC4 dan Playfair Cipher untuk Menggunakan Data Teks," *J. Pelita Inform.*, vol. 16, no. 3, pp. 328–334, 2017.
[4] Y. K. B. Simbolon, "Perancangan Aplikasi Pengamanan File PDF Menggunakan Algoritma Playfair Cipher," *Majalah Ilmiah INTI*, vol. 14, no. 2, pp. 30–36, 2019.
[5] M. Q. Khairuzzaman, "Implementasi kriptografi kunci publik dengan algoritma rsa," in *Seminar Nasional Sistem Informatika*, 2019, no. 2, pp. 219–228.
[6] A. L. Noviani, I. D. Ayu, and E. Yuliani, "Perancangan Perangkat Lunak Kriptografi Menggunakan Gronsfeld Cipher , Vernam Cipher dan Ron Code 4 Stream Cipher," *J. ENTER*, vol. 2, no. 1, pp. 549–559, 2019.
[7] F. Azmi and R. Anugrahwati, "Analisis Matriks 5x7 Pada Kroptografi Playfair Cipher," *J. dan Penelit. Tek. Inform.*, vol. 1, no. 2, pp. 27–30, 2017.
[8] S. T. C. Kurniawan, D. Dedih, and S. Supriyadi, "Implementasi Kriptografi Algoritma Rivest Shamir Adleman dengan Playfair Cipher pada Pesan Teks Berbasis Android," *JOIN(Jurnal Online Inform.*, vol. 2, no. 2, p. 102, 2018.
[9] E. H. Nurkifli, "Modifikasi Algoritma Playfair Dan Menggabungkan Dengan Linear Feedback Shift Register (Lfsr)," *Semin. Nas. Teknol. Inf. dan Komun. 2014 (SENTIKA 2014)*, vol. 1, no. 1, pp. 366–371, 2014.
[10] A. Hariati, K. Hardiyanti, and W. E. Putri, "Kombinasi Algoritma Playfair Cipher Dengan Metode Zig-zag Dalam Penyandian Teks," *Publ. J. Penelit. Tek. Inform. Vol. 2 Nomor 2*, vol. 2, no. 2, pp. 13–17, 2018.
[11] D. Susanti, "Analisis Modifikasi Metode Playfiar Cipher Dalam Pengamanan Data," 2019.