Modifikasi Playfair Chiper Dengan Kombinasi Bifid, Caesar, dan Transpositional Chiper

Indra Mukmin
Jurusan Teknik Informatika ITB, Jalan Ganesha 10 Bandung 40132, email: if16082@students.if.itb.ac.id

Abstraksi

Perkembangan teknologi dirasakan telah memberikan manfaat besar dalam menunjang kehidupan manusia hingga saat ini. Dapat kita katakan, media komunikasi berperan besar dalam proses interaksi masyarakat di berbagai belahan dunia. Piranti elektronik dan sarana penunjangnya semisal komputer dan jaringan internetnya membuat proses pertukaran data menjadi lebih mudah, efektif, dan efisien. Akan tetapi, peningkatan kualitas komunikasi ini juga diiringi dengan meningkatnya kejahatan yang berkaitan dengan pencurian maupun manipulasi informasi secara tidak sah oleh pihak yang tidak bertanggung jawab. Disinilah peran kriptografi muncul yaitu sebagai jawaban atas permasalahan mengenai penyandian maupun penjagaan kerahasiaan isi pesan. Kriptografi telah dikenal sejak ribuan tahun yang lalu. Algoritma kriptografi sendiri hingga saat ini ada banyak jenisya. Salah satunya adalah Playfair Chiper yang dapat digolongkan sebagai algoritma penyandian kriptografi klasik (definisi klasik mengacu pada masa sebelum ditemukannya komputer). Playfair Chiper ini sendiri termasuk sebagai chiper substitusi poligram.

Playfair Chiper merupakan algoritma penyandian dengan kunci kriptografinya berupa 25 huruf yang disusun dalam bujur sangkar 5x5 dengan menghilangkan huruf J dari abjad. Setiap elemen bujursangkar berisi huruf yang berbeda satu sama lain.

Sekarang ini sudah terdapat banyak sekali aplikasi komputer sebagai simulator yang dapat memecahkan chiperteks yang disandi dengan Playfair Chiper dalam waktu yang relatif singkat. Oleh sebab itu, penulis ingin mencoba sedikit memodifikasi algoritma Playfair Chiper ini dengan menambahkan beberapa prosedur pada algoritma enkripsi dan dekripsi plainteksnya. Tambahan prosedur ini sendiri merupakan kombinasi dari prosedur pada Bifid Chiper (mirip dengan Playfair Chiper tanpa adanya tambahan baris dan kolom pada bujur sangkar kunci), Caesar Chiper untuk pergeseran huruf plainteks yang akan dienkripsi, serta Chiper transposisi untuk melakukan pertukaran posisi cipherteks sebelum akhirnya dienkripsi dengan Playfair Cipher yang menjadi algoritma dasarnya. Dengan adanya modifikasi ini, diharapkan bahwa bila terdapat suatu chiperteks yang harus didekripsi, program – program pendekripsi chiperteks biasa tidak dapat menemukan plainteks yang diinginkan dan hanya orang – orang yang mengetahui mekanisme modifikasi Playfair Chiper ini saja yang dapat menemukan plainteks yang benar.

Kata Kunci

Playfair Cipher, Bifid Cipher, Caesar Cipher,kriptografi, enkripsi, dekripsi

1. PENDAHULUAN

Kriptografi telah dipergunakan sejak ribuan tahun lalu. Kita tidak dapat memungkiri bahwa kriptografi telah memberikan manfaat besar bagi kehidupan manusia khususnya dalam masalah penyandian dan kerahasiaan pesan. Sebelum ditemukannya komputer, metode kriptografi masih berbasiskan penyandian pada mode karakter dengan hanya menggunakan kertas dan pena. Kriptografi pada masa tersebut dapat digolongkan sebagai kriptografi klasik. Algoritma kriptografi klasik dapat digolongkan menjadi:

a. *Cipher* Subsitusi (*substitution chiper*)
Metode yang digunakan adalah dengan mengganti (menyulih atau mensubstitusi) setiap karakter dengan karakter lain dalam susunan abjad (alfabet).

b. *Cipher* Transposisi (*transposition cipher*)
Metode yang digunakan adalah melakukan transposisi terhadap rangkaian karakter di dalam teks.

Terdapat sejumlah algoritma yang tercatat dalam sejarah kriptografi yang tergolong ke dalam algoritma kriptografi klasik. Salah satunya adalah *Playfair Cipher*.

2. PLAYFAIR CIPHER

Playfair Cipher termasuk ke dalam *polygram cipher*, yaitu blok karakter disubstitusi dengan blok cipherteks. Misalnya ABA diganti MID, ABB dengan JJS, dan lain – lain. Metode ini ditemukan oleh Sir Charles Wheatstone dan Baron Lyon Playfair pada tahun 1854. *Playfair Cipher* digunakan oleh tentara Inggris pada Perang Boer (Perang Dunia I).

Algoritma ini menggunakan kunci sebanyak 25 buah huruf yang disusun dalam bujursangkar 5x5 dengan menghilangkan huruf J dari abjad. Setiap elemen bujur sangkar terdiri atas huruf yang berbeda satu sama lain. Misalkan contoh kunci : INDRA MUKMIN. Buang semua huruf J dan huruf berulang sehingga menjadi INDRAMUK. Kemudian distribusikan kunci tersebut ke dalam bujur sangkar. Isi elemen bujursangkar yang masih kosong dengan huruf lain sisanya.

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

Berdasarkan gambar di atas, dapat kita lihat bahwa kemungkinan kunci yang ada adalah sebanyak 25! = 15.511.210.043.330.985.984.000.000 buah

a. Proses Enkripsi *Playfair Cipher*

Untuk kunci yang telah dibangun, tambahkan baris dan kolom baru dengan aturan:

- Baris ke-6 = baris ke-1
- Kolom ke-6 = kolom ke-1

Untuk kunci di atas, bentuk kunci yang sudah diperluasnya adalah sebagai berikut:

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

Selanjutnya, pesan yang akan dienkripsi diatur terlebih dahulu sebagai berikut:

1. Ganti huruf J (bila ada) dengan huruf I
2. Tulis pesan dalam pasangan huruf (*bigram*)
3. Bila terdapat pasangan huruf yang sama, sisipkan Z di tengah keduanya sehingga *bigram* tidak menjadi pasangan huruf yang berulang.
4. Jika jumlah huruf ganjil, tambahkan huruf Z di akhir

Contoh plainteks : BAD DOCTORS

Tidak terdapat huruf J, maka plainteks dapat langsung dituliskan dalam pasangan huruf sebagai berikut:

BA DZ DO CT OR SZ

Algoritma enkripsinya (dengan menggunakan kunci yang sudah diperluas) adalah sebagai berikut:

1. Bila kedua huruf terdapat pada baris kunci yang sama, kedua huruf tersebut diganti dengan huruf di sebelah kanannya.
2. Bila kedua huruf terletak pada kolom yang kunci yang sama, kedua huruf tersebut diganti dengan huruf di sebelah bawahnya.
3. Bila kedua huruf tidak terletak pada baris dan kolom yang sama, huruf pertama diganti dengan huruf pada perpotongan antara baris huruf pertama dengan kolom huruf kedua. Sedangkan huruf kedua diganti dengan huruf pada titik sudut keempat dari persegi panjang yang dibentuk oleh 3 huruf yang digunakan sampai sejauh ini.

Untuk plainteks di atas, hasil enkripsinya adalah sebagai berikut:

CR AX IQ LZ SI TY

Enkripsi DZ menjadi AX dapat ditunjukkan sebagai berikut:

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

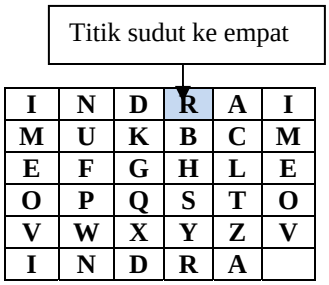
I	**N**	**D**	**R**	**A**	**I**
M	**U**	**K**	**B**	**C**	**M**
E	**F**	**G**	**H**	**L**	**E**
O	**P**	**Q**	**S**	**T**	**O**
V	**W**	**X**	**Y**	**Z**	**V**
I	**N**	**D**	**R**	**A**	

Titik sudut ke empat

b. Proses Dekripsi *Playfair Cipher*

Algoritma dekripsi *Playfair Cipher* memiliki langkah yang sama dengan algoritma enkripsinya. Hanya saja, *bigram* yang dimasukkan adalah cipherteks yang akan digunakan untuk mencari plainteks yang berkorespondensi. Contoh, *bigram* SI yang akan kembali menghasilkan *bigram* OR pada plainteks.

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



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

3. BIFID CIPHER

Bifid Cipher ditemukan oleh Felix Delastelle pada tahun 1901. Algoritma ini mirip dengan *Playfair Cipher* dalam hal pengunaan kunci yang dibangun dengan bentuk bujur sangkar 5x5. Perbedaannya adalah tidak adanya perluasan kunci pada bujur sangkar serta adanya prinsip *difussion* pada proses enkripsinya. Untuk mempermudah, kita gunakan contoh bujursangkar kunci sebelumnya.

	1	**2**	**3**	**4**	**5**
1	**I**	**N**	**D**	**R**	**A**
2	**M**	**U**	**K**	**B**	**C**
3	**E**	**F**	**G**	**H**	**L**
4	**O**	**P**	**Q**	**S**	**T**
5	**V**	**W**	**X**	**Y**	**Z**

a. **Proses Enkripsi**

Pertama, kita identifikasikan koordinat tiap huruf berdasarkan baris dan kolom. Huruf J yang ada pada plainteks kita ubah menjadi huruf I. Kita gunakan kembali plainteks sebelumnya.

Plainteks	:	**B**	**A**	**D**	**D**	**O**	**C**	**T**	**O**	**R**	**S**
Baris	:	**2**	**1**	**1**	**1**	**4**	**2**	**4**	**4**	**1**	**4**
Kolom	:	**4**	**5**	**3**	**3**	**1**	**5**	**5**	**1**	**4**	**4**

Setelah koordinat masing – masing karakter pada plainteks ditemukan, maka proses enkripsi dilakukan dengan melakukan pengacakan terhadap koordinat posisi di atas menjadi koordinat posisi baru dengan aturan tertentu. Sebagai contoh, aturan yang kita gunakan yaitu *konkatenasi seluruh koordinat baris mulai dari karakter pertama hingga karakter terakhir yang selanjutnya dikonkatenasi kembali dengan koordinat kolom yang juga diperlakukan sama seperti koordinat baris*. Selanjutnya kita akan mendapatkan barisan angka berikut:

2 1 1 1 4 2 4 4 1 4 4 5 3 3 1 5 5 1 4 4

Barisan angka di atas kemudian dapat kita pisahkan menjadi *bigram – bigram* yang akan menjadi koordinat untuk karakter – karakter baru

21 11 42 44 14 45 33 15 51 44

Keterangan : 21 berarti baris ke-2 dan kolom ke-1

Berdasarkan barisan koordinat di atas, akhirnya kita dapat menemukan cipherteksnya yaitu

Baris	:	**2**	**1**	**4**	**4**	**1**	**4**	**3**	**1**	**5**	**4**
Kolom	:	**1**	**1**	**2**	**4**	**4**	**5**	**3**	**5**	**1**	**4**
Cipherteks	:	**M**	**I**	**P**	**S**	**R**	**T**	**G**	**A**	**V**	**S**

Melalui *Bifid Cipher*, dari plainteks “BAD DOCTORS” kita peroleh cipherteks “MIPSRTGAVS”

b. **Proses Dekripsi**

Proses dekripsi merupakan kebalikan dari proses enkripsi dengan urutan mulai dari belakang secara sekuensial.

4. CAESAR CIPHER

Merupakan salah satu *cipher* substitusi yang mula – mula digunakan oleh kaisar Romawi, Julius Caesar untuk menyandikan pesan yang dikirim kepada para gubernurnya. *Caesar Cipher* diimplementasikan dengan *Caesar Wheel*.
Algoritma ini bekerja dengan cara menggantikan setiap karakter dengan karakter lain susunan abjad. Misal dengan kunci pergeseran 3 (k = 3), diperoleh tabel substitusi sebagai berikut:

Pi	A	B	C	D	E	F	G	H	I	J	K	L	M
Ci	D	E	F	G	H	I	J	K	L	M	N	O	P

Pi	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ci	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Berdasarkan tabel substitusi di atas, dari plainteks **BAD DOCTORS** akan kita peroleh cipherteks **EDG GRFWRV**

Fungsi enkripsinya dapat dituliskan sebagai berikut:

$$E(Pi) = (Pi + k) \bmod 26$$

Dan fungsi dekripsinya yaitu

$$D(Ci) = (Ci - k) \bmod 26$$

Sebagai catatan, angka 26 di atas menyatakan jumlah karakter yang terdapat dalam alfabet romawi. Apabila karakter yang kita gunakan adalah ASCII, maka angka yang dipakai adalah 256

5. CIPHER TRANSPOSISI

Pada cipher transposisi, plainteks yang digunakan tetap sama, namun urutannya diubah. Dengan kata lain, algoritma ini melakukan proses transposisi terhadap rangkaian karakter di dalam teks.

Nama lain untuk metode ini adalah permutasi karena proses transposisi yang kita lakukan terhadap tiap karakter sama dengan mempermutasikan karakter – karakter tersebut.

Misalkan terdapat plainteks

BAD DOCTORS IS MY FAVOURITE NOVEL

Untuk mengenkripsi pesan tersebut, plainteks ditulis secara horizontal dengan lebar kolom tetap, misal selebar 7 karakter (kunci $k = 7$) yaitu

B A D D O C T
O R S I S M Y
F A V O U R I
T E N O V E L

Sehingga akan kita peroleh cipherteks **BOFTARAEDSVNDIOOOSUVCMRETYIL**

Untuk proses dekripsi, kita membagi cipherteks ke dalam kolom – kolom selebar = panjang cipherteks / kunci. Untuk contoh di atas, lebar kolom = 28 / 7 = 4

B O F T
A R A E
D S V N
D I O O
O S U V
C M R E
T Y I L

Dengan pembacaan per kolom, akan kita peroleh kembali plainteks yang diinginkan yaitu **BADDOCTORSISMY FAVOURITENOVEL**

6. MODIFIKASI PLAYFAIR CIPHER DENGAN CAESAR, BIFID, DAN CIPHER TRANS POSISI

Modifikasi yang dilakukan terhadap algoritma *Playfair Cipher* adalah dengan meningkatkan kompleksitas algoritma proses enkripsi dan dekripsinya dengan cara penambahan operasi pada tiap proses. Proses enkripsi dan dekripsi algoritma *Playfair Cipher* yang telah dimodifikasi ini dapat dijabarkan sebagai berikut:

a. Proses Enkripsi

Proses enkripsi *Playfair Cipher* modifikasi ini terdiri atas urutan – urutan langkah sebagai berikut:

- Hitung panjang kunci yang dimasukkan tanpa memasukkan spasi ke dalam hitungan. Misal pada contoh sebelumnya, kunci **INDRA MUKMIN** memiliki panjang kunci angka = 11
- Pertama, terapkan proses enkripsi *Caesar Cipher* terhadap plainteks dengan kunci = kunci angka (dalam hal ini 11). Sebagai contoh, kita gunakan plainteks yang sebelumnya **BAD DOCTORS**

$$E(Pi) = (Pi + 11) \bmod 26$$

Dalam hal ini, tabel substitusi yang diperoleh adalah sebagai berikut:

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

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

Berdasarkan tabel substitusi di atas, akan kita peroleh cipherteks C1 **MLOOZNEZCD**

- Selanjutnya cipherteks C1 yang kita peroleh di atas kita kenakan dengan proses enkripsi *Bifid Cipher*. Berikut kunci bujur sangkar yang kita peroleh dari kunci **INDRA MUKMIN** yang telah kita proses.

	1	2	3	4	5
1	I	N	D	R	A
2	M	U	K	B	C
3	E	F	G	H	L
4	O	P	Q	S	T
5	V	W	X	Y	Z

- Dengan kunci bujur sangkar di atas, kita lakukan enkripsi dengan metode *Bifid Cipher* beserta aturannya yang telah kita tentukan. Untuk algoritma modifikasi ini, aturan yang kita terapkan adalah "*Untuk setiap pasangan bigram, pertukarkan posisi koordinat huruf pertama dan kedua dengan aturan baris huruf pertama bertukar posisi dengan kolom huruf kedua, dan kolom huruf pertama bertukar posisi dengan baris huruf kedua*"

Cipherteks : **ML OZ OZ NE ZC DZ**
Baris : **2 3 4 5 4 5 1 3 5 2 1 5**
Kolom : **1 5 1 5 1 5 2 1 5 5 3 5**

Menjadi
Baris : **5 1 1 4 3 4 4 1 3 3 1 4**
Kolom : **3 2 4 4 1 4 1 1 3 1 4 3**

Selanjutnya, gabungkan koordinat baris diikuti dengan koordinat kolom sehingga menjadi **5114344133143244 14113143**. Selanjutnya pisahkan angka – angka tersebut ke dalam *bigram – bigram* dimana angka pertama menyatakan baris dan angka kedua menyatakan kolom.

51 14 34 41 33 14 32 44 14 11 31 43

Sehingga akan kita peroleh cipher C2 yaitu **VRHOGRFSRIEQ**

- Langkah berikutnya adalah melakukan proses trans posisi terhadap C2. Caranya adalah dengan membagi C2 ke dalam deretan baris memanjang ke bawah dengan panjang kolom adalah
  - Sama dengan kunci angka, jika kunci angka (jumlah huruf kunci yang dimasukkan tanpa

memasukkan spasi dalam hitungan) adalah satu digit
- Sama dengan jumlah digit pertama + digit kedua kunci angka, jika kunci angka adalah dua digit

Untuk contoh kita, kunci angka = 11 sehingga panjang kolom = 1 + 1 = 2. Maka proses transposisinya adalah

V	**R**
H	**O**
G	**R**
F	**S**
R	**I**
E	**Q**

Dengan cara pembacaan per kolom, kita peroleh C3 = **VHGFRERORSIQ**

- Selanjutnya proses terakhir adalah melakukan operasi enkripsi *Playfair Cipher* terhadap C3 dengan menggunakan kunci bujursangkar yang telah diperluas

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

- Dengan menerapkan aturan *Playfair Cipher*, kita pisahkan C3 **VHGFRERORSIQ** menjadi *bigram – bigram.*

Plainteks : **VH GF RE RO RS I Q**
Cipherteks : **YE HG IH I S BY DO**

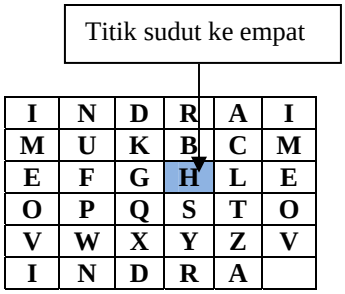
- Akhirnya setelah melalui rangkaian proses enkripsi yang telah dimodifikasi, kita peroleh cipherteks akhir C4 yaitu **YEHGIHISBYDO**

b. Proses Dekripsi

Proses dekripsi ini merupakan rangkaian kebalikan dari proses enkripsi. Langkah – langkah dekripsi dimulai dari akhir proses enkripsi yang sekuensial maju hingga ke proses pertama. Sebagai contoh, kita lakukan proses dekripsi terhadap cipherteks C4 yang telah kita peroleh pada penjelasan sebelumnya.

- Pertama, lakukan proses dekripsi terhadap cipherteks C4 dengan menggunakan algoritma *Playfair Cipher*. Aturan yang diberlakukan sama seperti proses enkripsinya sehingga dari cipherteks C4 **YEHGIHISBYDO** akan diperoleh cipherteks C3 **VHGFRERORSIQ**. Berikut contoh ilustrasinya: **YE → VH**

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



- Selanjutnya, terhadap C3 **VHGFRERORSIQ** kita kenakan proses transposisi dengan cara membagi C3 ke dalam baris – baris dengan panjang kolom adalah
  - Sama dengan (jumlah karakter C3) / (kunci angka), bila kunci angka adalah satu digit
  - Sama dengan (jumlah karakter C3) / (digit pertama kunci angka + digit kedua kunci angka), bila kunci angka adalah dua digit
- Untuk contoh ini, panjang C3 = 12 dan kunci angka = 11 (2 digit) sehingga panjang kolom = 12 / (1 + 1) = 6

V	**H**	**G**	**F**	**R**	**E**
R	**O**	**R**	**S**	**I**	**Q**

- Dengan cara pembacaan per kolom, akan kita peroleh cipherteks C2 **VRHOGRFSRIEQ**
- Selanjutnya kita proses **VRHOGRFSRIEQ** dengan cara membagi cipherteks tersebut menjadi *bigram – bigram.* Lalu dengan menggunakan kunci bujursangkar (yang belum diperluas) yang telah diberi nomor, kita tentukan koordinat masing – masing karakter.

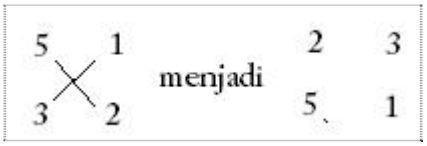
	1	**2**	**3**	**4**	**5**
1	**I**	**N**	**D**	**R**	**A**
2	**M**	**U**	**K**	**B**	**C**
3	**E**	**F**	**G**	**H**	**L**
4	**O**	**P**	**Q**	**S**	**T**
5	**V**	**W**	**X**	**Y**	**Z**

Cipherteks C2: **VR HO GR FS RI EQ**
Baris : **5 1 3 4 3 1 34 11 3 4**
Kolom : **1 4 4 1 3 4 24 41 1 3**

- Setelah mendapatkan deretan koordinat baris dan kolom seperti di atas, konkatenasi keduanya dengan aturan, isi deretan dengan angka pertama baris, diikuti angka pertama kolom, lalu diikuti angka kedua baris, lalu angka kedua kolom, begitu seterusnya hingga angka terakhir baris dan angka terakhir kolom. Selanjutnya akan kita peroleh deretan angka **511434413314 324414113143**
- Selanjutnya bagi deretan angka tersebut menjadi sama panjang dan atur menjadi dua baris dalam deretan *bigram - bigram*

51 14 34 41 33 14 (menunjukkan baris)
32 44 14 11 31 43 (menunjukkan kolom)

- Dari deretan baris dan kolom diatas, lakukan pertukaran dengan aturan sama seperti aturan pada proses enkripsi yaitu *Untuk setiap pasangan bigram, pertukarkan posisi koordinat huruf pertama dan kedua dengan aturan baris huruf pertama bertukar posisi dengan kolom huruf kedua, dan kolom huruf pertama bertukar posisi dengan baris huruf kedua*"
  Contoh :



  Sehingga akan kita peroleh

  Baris : **2 3 4 5 4 5 1 3 5 2 1 5**
  Kolom : **1 5 1 5 1 5 2 1 5 5 3 5**

  Dengan menggunakan baris dan kolom di atas sebagai koordinat pada kunci bujur sangkar yang telah diperluas, dapat kita temukan cipherteks C1

  Baris : **2 3 4 5 4 5 1 3 5 2 1 5**
  Kolom : **1 5 1 5 1 5 2 1 5 5 3 5**
  Cipherteks : **ML OZ OZ NE ZC DZ**

- Selanjutnya, sebagai proses terakhir, kita lakukan dekripsi terhadap cipher C1 yang telah kita temukan **MLOZOZNEZCDZ** dengan menggunakan *Caesar Cipher*. Fungsi dekripsinya

$$D(Pi) = (Pi - k) \bmod 26$$

  Dimana k = 11 (panjang kunci yang dimasukkan) sehingga akan kita peroleh plainteks **BADODOCTORSN**
- Plainteks yang telah kita temukan di atas belum murni karena masih terdapat karakter – karakter tambahan akibat proses enkripsi dengan *Bifid* maupun *Playfair Cipher*. Oleh sebab itu, harus kita teliti sekali lagi plainteks yang telah kita temukan dan membuang karakter – karakter yang tidak diperlukan sehingga dihasilkan sebuah plainteks yang memiliki makna. Untuk **BADODOCTORSN**, setelah membuang O (karakter ketiga) dan N (karakter terakhir), kita temukan plainteks BAD DOCTORS.

7. PERBANDINGAN KOMPLEKSITAS ALGORITMA YANG BELUM DAN SUDAH DIMODIFIKASI

Berdasarkan hasil penjabaran di atas, dapat kita lihat bahwa untuk proses kriptanalisis dengan metode *bruteforce* pada algoritma *Playfair Cipher* murni, kriptanalis harus mencoba kunci sebanyak 25! (faktorial dari 25). Sedangkan untuk algoritma yang telah dimodikasi, untuk cipherteks yang sama, maka kriptanalis harus mencoba 25! kali untuk menemukan cipherteks yang benar sebagai masukan bagi proses transposisi. Setelah itu, kriptanalis masih harus mencoba untuk menemukan cipherteks yang benar bagi proses – proses selanjutnya. Dapat kita lihat bahwa algoritma modifikasi ini membuat proses kriptanalisis menjadi lebih lama.

8. PENGUJIAN DAN ANALISIS

a. Pengujian

Pengujian dilakukan dengan memasukkan plainteks yang berbeda – beda dan membuat tabel perbandingan hasil enkripsi dan dekripsinya antara algoritma *Playfair Cipher* murni dengan *Playfair Cipher* modifikasi. Kunci yang digunakan adalah PLAYFAIR CIPHER. Kunci angka adalah 14 (panjang kunci masukan). Dengan menghilangkan spasi dan huruf J, serta huruf yang berulang hanya ditulis satu kali, diperoleh kunci yang akan dimasukkan ke dalam kunci bujur sangkar.

PLAYFIRCHE

	1	2	3	4	5	
1	P	L	A	Y	F	P
2	I	R	C	H	E	I
3	B	D	G	K	M	B
4	N	O	Q	S	T	N
5	U	V	W	X	Z	U
	P	L	A	Y	F	

Ket : pemberian angka di atas adalah untuk proses pada langkah yang menggunakan *Bifid Cipher*

Data penunjang:

Tabel substitusi *Caesar Cipher* dengan k = 14

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

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

Berikut tabel hasil pengujian untuk beberapa plainteks :

No	Plainteks	Cipherteks dengan *Playfair Cipher*	
		Murni	Modifikasi
1	INDRA MUKMIN	BUODFG XBBETU	PWVWGZ ORSPDA
2	JANGAN MARAH!!!	CPQBPQ GFCLEX	RXUIZ FAVHGIT
3	KKKK KKKK	MXMXMX MXMXMX MXMX	ZUZVVZ ZVZUZV ZVVZVUVU
4	VAS BUNGA	JOGPIBUO	CPLGFNRN

Berikut merupakan tabel plainteks hasil dekripsinya :

No	Plainteks	Plainteks hasil dekripsi dengan *Playfair Cipher*	
		Murni	**Modifikasi**
1	INDRA MUKMIN	INDRA MUKMINZ	INDRA MUKMINL
2	JANGAN MARAH!!!	IANGAN MARAHZ	JANGAN MARAHL
3	KKKK KKKK	KZKZKZKZ KZKZKZKZ	ELZLEL KLBLTL KLTLZLLL
4	VAS BUNGA	VAS BUNGA	UAS BUNGA

b. Analisis

Analisis yang dilakukan disini adalah membandingkan plainteks asli dengan plainteks hasil dekripsi menggunakan algoritma *Playfair Cipher* murni dan *Playfair Cipher* yang telah dimodifikasi.

1. **Pengujian I**

   Dari tabel di atas, dapat kita simpulkan bahwa plainteks hasil dekripsi di atas nyaris sama dengan plainteks asli, kecuali adanya karakter tambahan di akhir kalimat. Hal ini disebabkan oleh jumlah huruf plainteks yang ganjil sehingga pada saat diproses, ada penambahan karakter Z pada saat pembentukan *bigram*. Pada algoritma modifikasi, karakter terakhir bukan Z melainkan L karena proses terakhir dekripsi adalah dengan *Caesar Cipher* sehingga huruf Z yang ada pada cipher sebelumnya, ikut mengalami proses sehingga juga mengalami perubahan (dapat dilihat pada tabel substitusi)

2. **Pengujian II**

   Berdasarkan hasil pengujian, dapat kita lihat bahwa kedua algoritma *Playfair*, baik yang murni maupun yang merupakan hasil modifikasi memberikan hasil plainteks yang nyaris sama dengan aslinya (kecuali adanya tambahan karakter pada akhir kalimat. Penjelasan lihat pada pembahasan hasil pengujian I). akan tetapi, dapat kita lihat bahwa plainteks hasil dekripsi kedua algoritma tidak mengandung karakter tanda seru !. Karakter ! ini menjadi hilang akibat keterbatasan kedua algoritma yang hanya dapat memproses masukan hanya berupa karakter alfabet standar. Namun demikian, algoritma hasil modifikasi memberikan hasil yang lebih akurat, yaitu diperolehnya kembali kata JANGAN pada algoritma hasil modifikasi, berbeda dengan algoritma murni yang memberikan hasil IANGAN. Hal ini dikarenakan, pada algoritma *Playfair* murni, pada saat pemrosesan, setiap huruf J yang ditemui, akan diganti menjadi huruf I. Akan tetapi, pada algoritma hasil modifikasi, proses yang pertama dilakukan adalah mensubstitusi plainteks terlebih dahulu sehingga pada hasil enkripsinya, huruf J telah digantikan oleh huruf substitusinya. Oleh sebab itu, pada saat proses dekripsi, huruf J dapat diperoleh kembali.

3. **Pengujian III**

   Untuk pengujian III, algoritma modifikasi memberikan plainteks hasil yang jauh lebih buruk dibanding *Playfair Cipher* murni. Hal ini disebabkan karena adanya proses transposisi dengan pembagian kolom sesuai kunci angka. Apabila kunci angka ini tidak tepat sebagai panjang kolom, hasil dekripsinya menjadi tidak bagus, sekalipun apabila dilihat dari hasil enkripsi, kesan yang diperoleh adalah "masukan bukan huruf berulang". Melihat fakta ini, algoritma modifikasi mungkin tidak cocok digunakan untuk enkripsi plainteks berupa repetisi huruf yang sama.

4. **Pengujian IV**

   Berdasarkan hasil pengujian, dapat kita lihat bahwa untuk pengujian ini, algoritma *Playfair Cipher* murni memberikan plainteks yang jauh lebih benar. Hal ini dapat terjadi karena adanya proses enkripsi *Caesar Cipher* terlebih dahulu yang dilakukan pada algoritma modifikasi. Pada tabel substitusi di atas, huruf V akan digantikan oleh huruf J. akibatnya, untuk proses selanjutnya, huruf J ini akan digantikan oleh huruf I karena setelah proses enkripsi oleh *Caesar Cipher*, proses berikutnya dilanjutkan dengan enkripsi *Bifid Cipher* yang memiliki aturan sama seperti *Playfair Cipher* yaitu mengganti semua huruf J dengan huruf I. Akibatnya, untuk langkah terakhir pada proses dekripsi (dekripsi dengan *Caesar Cipher*), cipherteks tidak lagi mengandung huruf J karena telah digantikan oleh I sebagai hasil pemrosesan oleh dekripsi dengan *Bifid Cipher*. Oleh sebab itu, untuk kasus ini, plainteks yang didapatkan bukan lagi mengandung huruf V (pada kata VAS) yang sebelumnya berasosiasi dengan huruf J pada tabel substitusi di atas, namun digantikan oleh huruf I yang berasosiasi dengan huruf U pada tabel substitusi (sehingga kata yang diperoleh menjadi UAS)

Selain keunggulan dari segi perbandingan plainteks hasil dekripsi pada kebanyakan kasus secara umum, dari segi keamanan pun, algoritma *Playfair Cipher* modifikasi ini jauh lebih baik karena prosesnya yang lebih rumit disebabkan oleh adanya prosedur tambahan pada proses enkripsi dan dekripsi. Hal ini tentunya akan lebih mempersulit kriptanalis untuk memecahkan cipherteks hasil enkripsi.

9. KESIMPULAN DAN SARAN

Kriptografi berperan penting dalam penyandian dan menjaga kerahasiaan pesan sehingga hanya orang yang berhak saja yang dapat membaca pesan tersebut. Sekarang ini, kriptografi telah digunakan secara luas dengan proses penyandian yang telah menggunakan algoritma – algoritma

yang lebih modern dan berbasis komputer sehingga kompleksitas jauh lebih tinggi. Namun demikian, kita tidak tidak dapat menampik kehadiran algoritma kriptografi klasik yang beberapa ide dasarnya masih digunakan hingga saat ini.

Playfair Cipher merupakan salah satu dari algoritma kriptografi klasik yang dapat kita gunakan untuk menyandikan pesan. Begitu pula untuk algoritma *Playfair* modifikasi yang telah kita bahas sebelumnya. Dari sisi sekuritas, algoritma hasil modifikasi di atas memberikan tingkat keamanan yang lebih baik karena adanya tambahan beberapa prosedur yang menggabungkan teknik *Caesar* dan *Bifid Cipher* serta cipher transposisi sehingga proses kriptanalisis menjadi lebih rumit.

Masih terdapat beberapa kelemahan dalam algoritma modifikasi khususnya belum adanya penanganan otomatis untuk mengolah plainteks hasil dekripsi menjadi plainteks yang persis sama dengan plainteks asli, dengan kondisi adanya karakter selain alfabet maupun beberapa karakter sama yang berdampingan yang “terkena masalah” apabila juga berdampingan pada saat berbentuk *bigram*. Akan tetapi, selain dari kondisi di atas, plainteks hasil dekripsi harusnya memberikan hasil yang sama, persis seperti plainteks awal. Selain itu, pada beberapa kasus, plainteks hasil dekripsi algoritma modifikasi memberikan hasil yang lebih baik dibandingkan dengan hasil dari algoritma *Playfair Cipher* murni.

Berdasarkan kesimpulan di atas, penulis ingin memberikan beberapa saran pengembangan bagi mereka yang ingin menggunakan algorima ini antara lain:

- Adanya prosedur penyimpanan karakter selain alfabet pada cipherteks sehingga plainteks yang dihasilkan menjadi sama persis
- Adanya prosedur penyimpanan indeks karakter I yang merupakan substitusi dari karakter J (pada saat pemrosesan dengan *Bifid* maupun metode *Playfair* pada akhir proses enkripsi) sehingga dapat mengurangi waktu bagi penerima pesan untuk meneliti plainteks hasil dekripsi yang diterima (sebagai akibat harus menentukan karakter I yang mana saja yang harus diubah agar plainteksnya menjadi bermakna)
- Meningkatkan kompleksitas algoritma modifikasi yang sudah ada. Prosedur yang dapat dilakukan misalnya dengan melakukan transposisi berulang - ulang sebanyak kunci angka dengan posisi karakter pada kubus bujursangkar adalah : posisi sekarang + 1 langkah mod 25 dan lain sebagainya.

Daftar Pustaka

[1] Munir, Rinaldi, Diktat Kuliah IF5054 Kriptografi, Institut Teknologi Bandung 2006
[2] http://rumkin.com/tools/cipher/bifid.php
[3] http://trumpetpower.com/Papers/Crypto/ Playfair
[4] http://www.simonsingh.net/The_Black_Chamber/Playfaircipher.htm
[5] http://www.bryson.ltd.uk/cgi-bin/*Playfair*
[6] http://www.purplehell.com/riddletools/bifid.htm