Penerapan Kombinasi Bifid Cipher dan Algoritma Playfair pada Proses Enkripsi

Anggi shena permata (13505117)

Departemen Teknik Informatika
Institut Teknologi Bandung
Jl. Ganesha 10 Bandung 40132

E-mail : if15117@students.if.itb.ac.id[1]

Abstraksi

Sejalan dengan pesatnya perkembangan dunia teknologi saat ini , keamanan pada lalu lintas data merupakan hal yang krusial bagi setiap pihak yang terlibat. Semakin hari semakin banyak data-data yang mengalir dan tidak semua pihak / orang berhak untuk mengetahui data-data tersebut. Oleh karena itu, pengembangan terhadap sistem keamanan panyimpanan dan lalu lintas data sangat diperlukan sebagai langkah dalam mengatasi permasalah yang telah dikemukakan diatas. Salah satu cara yang dapat diterapkan sebagai pemenuhan kebutuhan tersebut adalah dengan mengaplikasikan algoritma kriptogafi. Seperti kita ketahui, kriptografi merupakan salah satu metode penyandian pesan sedemikian rupa sehingga pesan tersebut tidak lagi dapat dikenali dan dimengerti oleh pihak-pihak yang tidak berhak mengetahui pesan tersebut. PlayFair merupakan salah satu metode penyandian kriptogafi klasik yang termasuk dalam jenis polygram cipher (salah satu tipe dari cipher subtitusi). Untuk selanjutnya, penulis akan menggabungkan pemikiran pada algoritma playfair cipher ini dengan dua metode lain yang juga merupakan polygram cipher yaitu bifid cipher yang kelak akan digunakan dalam pengenkripsian data.

Kata kunci

Playfair cipher , Bifid cipher , kriptografi , plainteks, cipherteks, enkripsi, dekripsi .

1. PENDAHULUAN

Seperti telah dijelaskan sebelumnya, tidak dapat dipungkiri bahwa kriptografi yang merupakan ilmu yang digunakan untuk menyembunyikan atau merubah suatu pesan kedalam bentuk yang tidak dapat dimengerti sangatlah diperlukan dalam kehidupan sehari-hari seperti beberapa teknik yang biasa digunakan untuk menjaga kerahasian suatu pesan agar tidak jatuh ketangan pihak yang tidak berhak. Sebelum ditemukannya teknik-teknik penyandian dengan kompleksitas yang cukup tinggi untuk mempersulit kriptanasis melakukan pemecahan pesan yang disandikan, kriptografi klasik yang biasa dilakukan hanya dengan menggunakan alat bantu kertas dan pena merupakan dasar dari algoritma-algoritma tersebut. Dalam hal ini, mempelajari dan mengembangkan metode algoritma klasik sangatlah bermanfaat dalam mengembangkan pemahaman kita akan konsep dasar kriptografi dan potensi-potensi kelemahan sistem cipher. Selain itu, pemaduan algoritma yang dilakukan penulis juga memberikan ide bagi pembaca untuk dapat melakukan kriptografi sederhana dengan tingkat kerumitan yang cukup.

Algoritma pada kriptografi klasik dapat dibagi menjadi dua kategori yaitu :

- ***Cipher Subtitusi***
  Teknik penyandian yang dilakukan dengan mengganti setiap karakter dengan karakter lain dalam susunan alfabet

- ***Cipher Transposisi***
  Teknik penyandian yang dilakukan dengan mempermutasikan karakter-karakter dalam plainteks

Dalam hal ini, kedua metode / algoritma yang akan digabungkan / dikombonasikan merupakan jenis algoritma yang termasuk dalam *polygram cipher* yang merupakan salah satu tipe dari cipher subtitusi .

1.1. PLAYFAIR CIPHER

Playfair cipher ditemukan oleh Sir Charles Wheatstone dan Baron Lyon Playfair pada tahun 1854 dan merupakan algoritma penyandian pesan yang sering digunakan dalam perang boer (perang dunia I). pada algoritma ini, kunci yang digunakan merupakan 25 huruf alfabet yang disusun secara acak kedalam sebuah bujur sangkar

yang dibuat berukuran 5 X 5 dengan menghilangkan huruf **J .** setiap sel pada bujur sangkar diisi dengan huruf yang berbeda secara acak, namun untuk mempermudah mengingat kunci, biasanya digunakan kunci berupa kata ataupun kalimat yang membentuk sebuah arti yang kemudian dihilangkan huruf-huruf berulangnya dan kemudian diisikan pada sel-sel bujur sangkar secara berurut dari kiri ke kanan, dari atas kebawah. Jika panjang kunci tidak mencapai 25 huruf, maka sel pada bujur sangkar yang tersisa akan diisi dengan huruf-huruf sisa pada alfabet yang belum tertulis secara berurut.

Misalkan kunci yang digunakan adalah

" Jalan ganesha sepuluh"

Maka dengan menghilangkan huruf-huruf berulang, kalimat tersebut akan menjadi

"a l n g e s h p u l"

Dengan memasukan huruf-huruf tersebut kedalam sel-sel bujur sangkar dan mengisi sel-sel yang belum terisi dengan huruf-huruf alfabet yang belum tertulis terkecuali hujur ***J*** maka akan diperoleh kunci yang akan digunakan dalam malakukan penyandian dengan menggunakan algoritma playfair adalah sebagai berikut

a	**l**	**n**	**g**	**E**
s	**h**	**p**	**u**	**B**
c	**d**	**f**	**i**	**K**
m	**o**	**q**	**r**	**T**
v	**w**	**x**	**y**	**Z**

Kemudian proses enkripsi akan diperluas dengan menambahkan kolom ke -6 yang akan diisi dengan huruf-huruf serupa dengan kolom pertama dan baris ke -6 yang akan diisi sesuai dengan huruf-huruf pada baris pertama. Kini papan kunci adalah sebagai berikut

a	**l**	**n**	**g**	**e**	**a**
s	**h**	**p**	**u**	**b**	**s**
c	**d**	**f**	**i**	**k**	**c**
m	**o**	**q**	**r**	**T**	**m**
v	**w**	**x**	**y**	**Z**	**v**
a	**l**	**n**	**g**	**e**	

Proses Enkripsi

Plainteks yang diberikan akan diatur terlebih dahulu sebagai berikut

1. Ganti huruf J dengan huruf I
2. Kelompokan karakter pesan menjadi bigram (dua-dua)
3. Jika ada pasangan huruf yang sama maka sisipka Z ditengahnya
4. Jika jumlah karakter pada plainteks ganjil maka tambahkan Z diakhir

Sebagai contoh, misalkan plainteks adalah

"good brooms "

Maka akan diproses berdasarkan ketentuan diatas menjadi

G O O D B R O Z O M S Z

Algoritma enkripsi adalah sebagai berikut

- Jika dua huruf terdapat pada papan kunci yang sama maka tiap huruf diganti dengan huruf yang ada di sebelah kanannya
- Jika dua huruf terdapat dalam kolom yang sama, maka tiap huruf diganti dengan huruf yang ada dibawahnya
- jika tidak terletak pada baris dan kolom yang sama maka, tiap huruf diganti dengan huruf pada sel perpotongan baris huruf tersebut dan kolom huruf lainnya

sebagai contoh, pada plaiteks diatas dengan papan kunci yang telah diperluas, maka diperoleh hasil enkripsi dari **G O** adalah **L R** yang digambarkan sebagai berikut

a	**l**	**n**	**g**	**e**	**a**
s	**h**	**p**	**u**	**b**	**s**
c	**d**	**f**	**i**	**k**	**c**
m	**O**	**q**	**r**	**T**	**m**
v	**w**	**x**	**y**	**Z**	**v**
a	**l**	**n**	**g**	**e**	

Berdasarkan algoritma diatas maka plainteks akan dienkripsikan menjadi

"LRWOUTTWQOBV"

Proses Dekripsi

Proses dekripsi yang dilakukan merupakan kebalikan dari proses enkripsi. Proses ini dilakukan secara sekuensial dari urutan terbelakang proses enkripsi.

1.2. BIFID CIPHER

Bifid cipher pertama kali ditemukan oleh Felix Delastelle pada tahun 1901 yang sampai saat ini mesih berperan sebagai salah satu algoritma penyandian sederhana yang biasa dilakukan hanya dengan menggunakan pensil dan kertas yang cukup aman karena prinsip diffusion yang terkandung didalamnya.

Algoritma ini merupakan salah satu algoritma yang juga menggunakan prinsip dasar playfair cipher dimana pesan akan dienkripsikan dengan mengacak posisi baris dan kolom huruf pada pesan yang sesuai dengan papan kunci yang juga berbentuk bujur sangkar 5 X 5 sama seperti yang diterapkan pada playfair cipher hanya saja tidak ada perluasan papan kunci yang dilakukan pada bifid cipher ini. Dengan contoh kasus yang sama dengan yang telah dipakai sebelumnya, papan kunci yang akan digunakan pada penyandian pesan dengan algoritma bifid ini dapat digambarkan sebagai berikut

	1	2	3	4	5
1	a	l	n	G	e
2	s	h	p	U	b
3	c	d	f	I	k
4	m	o	q	R	T
5	v	w	x	Y	Z

Proses Enkripsi

Awal proses enkripsi dilakukan dengan mengidentifikasi posisi tiap huruf berdasarkan baris dan kolomnya. Sama seperti aturan pada playfair, huruf ***J*** pada plainteks terlebih dahulu diubah menjadi huruf ***I*** . Untuk contoh kasus dengan plainteks **"good brooms"** akan diperoleh hasil identifikasi sebagai berikut

Plainteks : **g o o d b r o o m s**
Baris : **1 4 4 3 2 4 4 4 4 2**
Kolom : **4 2 2 2 5 4 2 2 1 1**

Kemudian plainteks tersebut akan dienkripsikan dengan mengacak kordinat posisi dan menjadikannya kordinat posisi yang baru dengan aturan tertentu. Dalam hal ini aturan yang digunakan adalah dengan menjadikan kordinat baris dan kolom menjadi satu baris karakter angka dan kemudian membuatnya menjadi bigram (dipisahkan dua-dua) untuk dijadikan kordinat baru yang isi sel nya merupakan hasil enkripsi yang dilakukan. Proses enkripsi secara sistematis akan diperlihatkan sebagai berikut

Kordianat baris dan kolom dijadikan satu baris karakter angka

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

Kemudian pisahkan menjadi bigram yang akan membentuk kordinat baru baris dan kolom

14 43 24 44 42 42 22 54 22 11

Maka cipherteks adalah isi dari sel dengan kordinat baru yang terbentuk

Baris : **1 4 2 4 4 4 2 5 2 1**
Kolom : **4 3 4 4 2 2 2 4 2 1**
Cipherteks : **g q u r o o h y h a**

Maka hasil enkripsi dengan menggunakan metode bifid cipher adalah sebagai berikut

Plainteks : **g o o d b r o o m s**
Cipherteks : **g q u r o o h y h a**

Proses Dekripsi

Proses dekripsi yang dilakukan merupakan kebalikan dari proses enkripsi. Proses ini dilakukan secara sekuensial dari urutan terbelakang proses enkripsi.

2. PENERAPAN BIFID CIPHER PADA METODE PLAYFAIR

Berdasarkan pengetahuan tentang beberapa prinsip dasar kriptografi klasik dan metode-metode yang diperoleh dan telah digambarkan secara garis besar pada bagian diatas, penulis berusaha mengembangkan algoritma baru dengan meningkatkan tingkat kompleksitas algoritma-algoritma sebelumnya dengan jalan mengkombinasikan kedua algoritma yang telah dijelaskan diatas yaitu dengan menyisipkan beberapa prinsip bifid cipher kedalam penyandian pesan yang menggunakan algoritma metode Playfair. Pada dasarnya kedua algoritma tersebut tidaklah jauh berbeda kerena menggunakan jenis papan kunci yang cendrung mirip hanya saja pada playfair cipher, kordinat baris dan kolom tidaklah terlalu diperlukan. Pada algoritma baru ini, penulis akan menggabungkan penggunaan prinsip bigram pada playfair dengan metode pangacakan kordinat pada bifid serta tidak menghilangkan unsur keaslian dari metode playfair itu sendiri.

2.1. PROSES ENKRIPSI

1. Pada bagian awal proses enkripsi, tidak berbeda dengan playfair, kali ini plainteks akan dikelompokan menjadi bigram dipadukan dengan ciri khas metode bifid dimana kordinat posisi huruf pada papan bujur sangkar akan diidentifikasi. Dalam penggambaran metode ini, akan digunakan contoh kasus (plainteks dan papan kunci) yang serupa dengan yang sebelumnya. Berikut merupakan penggambaran tahap awal dar proses enkripsi.

   Papan kunci :

	1	2	3	4	5
1	a	l	n	G	E
2	s	h	p	U	B
3	c	d	f	I	K
4	m	o	q	R	T
5	v	w	x	Y	Z

Plainteks : **g o o d b r o z o m s z**
Baris : **1 4 4 3 2 4 4 5 4 4 2 5**
Kolom : **4 2 2 2 5 4 2 5 2 1 1 5**

2. Selanjutnya kordinat untuk tiap bigram akan dipertukarkan dengan aturan kordinat baris suatu huruf akan menjadi kordinat kolom huruf lainnya dan kordinat kolom suatu huruf akan menjadi kordinat baris hufur lainnya. Kemudian kordinat baru tersebut akam membentuk kordinat bigram untuk huruf baru yang akan menjadi cipherteks sementara.

Baris : **2 4 2 2 4 5 5 2 1 2 5 1**
Kolom : **4 1 3 4 4 2 5 4 4 4 5 2**
C1 : **u m p u r w z u g u z l**

3. Selanjutnya, dengan papan kunci yang telah diperluas cipherteks sementara (c1) diatas akan dienkripsi dengan prinsip dasar playfair cipher sebagai berikut

   Papan kunci :

a	l	n	g	e	A
s	h	p	u	b	S
c	d	f	i	k	C
m	o	q	r	T	M
v	w	x	y	Z	V
a	l	n	g	e	

plainteks : **u m p u r w z u g u z l**

C2 : **s r u b o y b y u i w e**

4. Dengan menggunakan prinsip bifid, cipherteks sementara (C2) tersebut akan diidentifikasi kordinatnya sebagai berikut

C2 : **s r u b o y b y u i w e**
Baris : **2 4 2 2 4 5 2 5 2 3 5 1**
Kolom : **1 4 4 5 2 4 5 4 4 4 2 5**

5. Proses kahir dari algoritma ini adalah dengan menerapkan cara kerja mendasar dari bifid cipher yaitu dengan mentranposisikan kordinat huruf menjadi kordinat yang baru sebagai berikut

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

Baris : **2 2 4 2 2 5 1 4 2 5 4 2**
Kolom : **4 2 5 5 3 1 4 5 4 4 4 5**
cipherteks : **u h t w p v g t u y r b**

maka diperolehlah hasil akhir dari proses enkripsi yang dilakukan.

Plainteks : **g o o d b r o o m s**

Cipherteks : **u h t w p v g t u y r b**

2.2. PROSES DEKRIPSI

1. Cipherteks dikelompokan menjadi bigram untuk kemudian diidentifikasi kordinatnya berdasarkan prinsip bifid.

cipherteks : **u h t w p v g t u y r b**
Baris : **2 2 4 2 2 5 1 4 2 5 4 2**
Kolom : **4 2 5 5 3 1 4 5 4 4 4 5**

2. Kordinat tiap huruf (baris,kolom) di buat menjadi satu baris dan bagi menjadi 2 bagian sama panjang.

u h t w p v g t u y r b
242245252351 144524544425

3. Pindahkan posisi deretan angka yang berada disebelah kanan ke bawah deretan angkat disebelah kiri dan sejajarkan sehingga deret angka pada bagian atas merupakan kordinat baris huruf dan deret angka bagian bawah merupakan kordinat kolom huruf hasil dekripsi sementara.

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

D1 : **s r u b o y b y u i w e**

4. Dekripsikan D1 dengan prinsip dasar playfair menggunakan papan kunci yang diberikan.

a	**l**	**n**	**g**	**e**	**A**
s	**h**	**p**	**u**	**b**	**S**
c	**d**	**f**	**i**	**k**	**C**
m	**o**	**q**	**r**	**T**	**M**
v	**w**	**x**	**y**	**Z**	**V**
a	**l**	**n**	**g**	**e**	

cipherteks : **s r u b o y b y u i w e**

D2 : **u m p u r w z u g u z l**

5. Selanjutnya identifikasi kordinat tiap bigram kemudian pada tiap bigram, pertukarkan kordinat baris suatu huruf menjadi kordinat kolom huruf lainnya dan kordinat kolom suatu huruf menjadi kordinat baris huruf lainnya.

D2 : **u m p u r w z u g u z l**
Baris : **2 4 2 2 4 5 5 2 1 2 5 1**
Kolom : **4 1 3 4 4 2 5 4 4 4 5 2**

Dilanjutkan dengan melakukan pertukaran.

Baris : **1 4 4 3 2 4 4 5 4 4 2 5**
Kolom : **4 2 2 2 5 4 2 5 2 1 1 5**
Plainteks : **g o o d b r o z o m s z**

Proses akhir yang dilakukan adalah mengidentifikasi ketepatan makna peletakan huruf ***Z*** dan ***I.*** Karena pada proses enkripsi huruf J akan diganti menjadi huruf I dan bigram yang mengandung huruf yang sama akan disisipi huruf Z serta pada akhir kalimat akan ditambahkan huruf Z jika tidak membentuk bigram (bersisa satu huruf terakhir).

Berdasarkan hasil identifikasi , terlihat bahwa letak huruf **Z** tidaklah tepat karena menyebabkan plainteks menjadi tidak berarti. Oleh karena itu, huruf z akan dihilangkan sehingga diperoleh hasil akhir adalah

" Good brooms"

maka diperolehlah hasil akhir dari proses enkripsi yang dilakukan.

Cipherteks : **u h t w p v g t u y r b**

Plainteks : **g o o d b r o o m s**

3. ANALISIS DAN HASIL UJI

Dengan menggunakan papan kunci yang sama , berikut akan diberikan beberapa hasil uji enkripsi untuk beberapa jenis plainteks yang berbeda dan algoritma yang berbeda pula.

Diketahu papan kunci adalah

A	**l**	**n**	**g**	**e**	**a**
S	**h**	**p**	**u**	**b**	**s**
C	**d**	**f**	**i**	**k**	**c**
m	**o**	**q**	**r**	**T**	**m**
V	**w**	**x**	**y**	**Z**	**v**
A	**l**	**n**	**g**	**e**	

Data uji adalah sebagai brikut

No.	*Plainteks*	*Playfair*	*Bifid*	*kombinasi*
1	**Good brooms**	**lrwouttwq obu**	**gquroo hyha**	**uhtwpvgt uyrb**
2	**Enigma cipher**	**agruvsdk upgt**	**Acmfh gxragd y**	**Arawitmu bfhg**
3	**Cannon**	**msexlqex**	**Camaf p**	**Axpxuege**
4	**Lollipop**	**hwewgdh qbx**	**Gadoh hqp**	**hwopxwe nub**
5	**Fffff**	**Kxkxkxkx kx**	**fffff**	**Xkxkxkx kxk**
6	**Qqqq**	**txtxtxtx**	**rrff**	**xxxxtttt**
7	**Bsssbbs**	**shbvhssh**	**hhhbae v**	**svlshbhh**

Ket hasil uji

1. Pada pengujian data pertama penulis menyimpulkan bahwa panyandian dengan mengkombinasikan kedua algoritma playfair dan bifid memperoleh hasil yang lebih baik kerena lebih teracaknya karakter cipherteks yang dibentuk dari plainteks yang memiliki beberapa pengulangan huruf berdampingan yang juga tampak pada hasil penyandian dengan metode playfair ataupun bifid.
2. Pada pengujian kedua, plainteks yang digunakan tidak mengandung terlalu banyak huruf berulang bahkan tidak ada yang berdampingan sehingga pemanfaatan pengkombinasian algoritma tidak tampak terlalu jelas karena cipherteks yang dihasilkan dengan menggunakan ketiga metode panyandian tersebut sama baiknyas.
3. Pada pengujian data ketiga, terlihat bahwa penyandian dengan metode bifid kurang baik karena terdapat kunci lemah yang mengakibatkan hasil penyandian serupa dengan plainteks, terlihat dengan tidak

berubahnya dua karakter pertama pada plainteks yaitu karakter C dan A walaupun proses penyandian telah dilakukan. Penggunaan metode playfair ataupun kombinasi menghasilkan cipherteks yang cukup baik dan tidak jauh berbeda tingkat keberhasilannya.

4. Pengujian data kelima dilakukan pada plainteks terdiri dari lima karakter huruf yang sama yang memiliki kordinat baris dan kolom yang sama juga yaitu f → (3, 3). Penyandian dengan bifid sama sekali tidak berpengaruh karena pengacakan kordinat huruf tidak menghasilkan kordinat yang berbeda dengan kordinat plainteks. Dilain sisi, panyandiaan dengan menggunakan metode playfair dan kombinasi juga tidak membuahkan hasil yang cukup baik karena pola kesamaan huruf sanga terlihat jelas walaupun ukurannya tidak lagi sama.
5. Pengujian data keenam dilakukan pada plainteks yang terdiri dari 4 karakter huruf yang sama namun dengan kordinat baris dan kolom yang berbeda untuk tiap hurufnya yaitu q → (4, 3). Pada kasus ini terlihat bahwa hasil penyandian dengan menggunakan algoritma playfair sangatlah menunjukan pola plainteks yang tersimpan sedangkan pada bifid dapat sedikit mengecoh kriptananis dengan perbedaan pola yang dihasilkan dan metode kombinasi juga menunjukan pola yang cukup jelas untuk dapat ditelusuri.
6. Berdasarkan pengujian data terakhir, penulis berpendapat bahwa metode pengkombinasian dapat berperan cukup baik dalam melakukan enkripsi plainteks walapun masih terdapat dua karakter h yang berdampingan yang mencirikan pola karakter sama yang berdampingan pada palinteks yang tesimpan . pada playfair masih terdapat pola pengulangan huruf s yang sama dengan yang terdapat pada plainteks walaupun posisinya berbeda, sedangkan metode bifid yang dilakukan mengakibatkan kunci lemah yang menghasilkan hasil enkripsi yang sama pada karakter ke-4 plainteks.

4. KESIMPULAN

Kriptografi merupakan ilmu sangat dibutuhkan dalam meningkatkan keamanan lalu lintas data agar data tidak jatuh kesembarang pihak yang tidak berwenang. Berbagai teknik kriptografi modern telah diterapkan dan masih terus berkembang sampai saat ini namun, tidak dapat dipungkiri bahwa teknik panyandian pada kriptogafi klasik merupakan prinsip dasar yang ditanamkan dan menjadi pedoman teknik panyandian lain yang ada dimasa sekarang.

Berdasarkan hasil ananlis yang telah dilakukan penulis dengan melakukan perbandingan antara algoritma baru yang dirancang yang merupakan penggabungan metode bifid kedalam proses enkripsi pesan dengan prinsip playfair cipher dan metode dasarnya sendiri yaitu playfai cipher dan bifid cipher, penulis menyimpulkan bahwa algoritma yang dirancang sudah dapat berperan dengan baik bahkan dibandingkan dengan betode penyusunnya yang bekerja sendiri tanpa penggabungan. Hanya saja pada beberapa kasus tertentu seperti yang telah penulis lakukan pada pengujian plainteks ffff, algoritma ini begitu juga dengan algoritma dasarnya yang bekerja sendiri memang belum dapat membuahkan hasil yang baik yang juga menjadikan hal tersebut sebagai kelemahan dari metode yang dirancang ini dan Untuk kedepanya diharapkan menjadi salah satu bahan evaluasi untuk merancang algoritma baru yang dapat menangani permasalahan ini .

DAFTAR REFERENSI

[1] Munir, Rinaldi, *Kriptografi*, Institut Teknologi Bandung, 2006.

[2] http://www.answers.com/topic/hill-cipher Tanggal akses 5 januari 2009

[3] http://rumkin.com/tools/cipher/bifid.php Tanggal akses 5 januari 2009

[4] http://www.purplehell.com/riddletools/bifid.htm Tanggal akses 5 januari 2009

[5] http://trumpetpower.com/Papers/Crypto/Playfair Tanggal akses 5 januari 2009

[6] http://www.bryson.ltd.uk/cgi-bin/playfair Tanggal akses 5 januari 2009