STUDI PERBANDINGAN *PLAYFAIR CIPHER* DENGAN PAPAN KUNCI BUJURSANGKAR DAN PAPAN KUNCI KUBUS

Nicolas Andres – NIM : 13504109

Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if14109@students.if.itb.ac.id

Abstrak

Makalah ini membahas tentang studi dan implementasi *Playfair Cipher* untuk menyandikan data teks. *Playfair Cipher* merupakan salah satu algoritma kriptografi klasik yang menggunakan kunci simetri. Pada awal ditemukannya oleh Sir Charles Wheatstone dan Baron Lyon Playfair, algoritma ini menggunakan papan kunci berbentuk bujursangkar berukuran 5x5 dalam melakukan enkripsi dan dekripsi. Proses enkripsi dan dekripsi dilakukan dengan dengan mengelompokan huruf-huruf secara bigram.

Dengan menggunakan papan kunci berbentuk kubus, kita dapat mengenkripsi plainteks (data teks asli yang akan dienkripsi) dan mendekripsi cipherteks (data teks yang telah dienkripsi) dengan mengelompokkannya secara bigram tanpa harus menghilangkan huruf J dari plainteks. Kubus tersebut terdiri dari 27 bagian (berukuran 3x3x3) dimana setiap bagian mewakili sebuah huruf alfabet (26 karakter) dan sebuah karakter tambahan contohnya karakter titik. Proses enkripsi dan dekripsi pada papan kunci kubus dilakukan seperti pada *Playfair Cipher* dengan papan kunci bujursangkar tapi dilakukan sedikit modifikasi.

Sebuah perangkat lunak *Playfair Cipher* sederhana dibangun untuk mengimplementasi *Playfair Cipher* dengan papan kunci bujursangkar dan kubus. Papan kunci dibangkitkan secara acak oleh perangkat lunak sehingga setiap proses penyandian (enkripsi dan dekripsi) dapat menggunakan kunci yang berbeda-beda. Perangkat lunak ini digunakan juga untuk membuktikan kebenaran hasil enkripsi dan dekripsi dari *Playfair Cipher* dengan papan kunci kubus. Perangkat lunak *Playfair Cipher* dikembangkan dengan menggunakan bahasa C++ dan berbasis *console* dalam lingkungan pengembangan *Windows*.

Perangkat lunak *Playfair Cipher* tersebut digunakan membandingkan kelebihan dan kekurangan masing-masing papan kunci. Hasil analisis menunjukkan bahwa papan kunci berbentuk kubus dapat menjadi alternatif dari algoritma *Playfair Cipher* karena tidak ada karakter yang dihilangkan dari plainteks (yaitu karakter J) sehingga kriptanalis sulit menduga apakah cipherteks yang ada merupakan hasil enkripsi algoritma *Playfair Cipher* atau bukan. Selain itu, jumlah karakter pada papan kunci berbentuk kubus dapat mempersulit penemuan kunci meskipun hanya berbeda dua karakter.

Kata kunci: *Playfair Cipher*, papan kunci, bujursangkar, kubus, enkripsi, dekripsi.

1. Pendahuluan

Penemuan algoritma kriptografi klasik tidak dapat dilupakan begitu saja. Algoritma tersebut merupakan dasar dari algoritma kriptografi modern dan ditemukan sebelum adanya komputer. Para penemunya telah memikirkan tentang keamanan data rahasia yang akan dikirimkan atau disimpan, khusunya data teks. Data tersebut dapat berupa pesan rahasia mengenai strategi perang yang banyak dilakukan pada saat perang zaman dahulu. Kerahasian data tersebut harus tetap dijaga selama pengiriman tanpa diketahui oleh siapapun dan sampai pada tujuan. Untuk memenuhi hal tersebut, dilakukan proses enkripsi dan dekripsi terhadap data teks yang dikirimkan. Enkripsi dilakukan pada saat pengiriman dengan cara mengubah data teks asli menjadi data teks yang tidak dapat dimengerti (rahasia) sedangkan dekripsi dilakukan pada saat penerimaan dengan cara mengubah data rahasia menjadi data asli. Data yang dikirimkan tidak dapat diketahui dan dimengerti oleh pihak yang tidak berkepentingan jika tidak mengetahui kunci untuk mendekripsi data rahasia tersebut. Kunci

rashasia ini hanya diketahui oleh pihak yang berhak mengetahui data rahasia.

Dalam melakukan penyandian terhadap data teks yang akan dikirim, dapat digunakan algoritma kriptografi klasik yang telah dikenal dalam bidang kriptografi dan sangat mudah dipelajari. Algoritma kriptografi (*cipher*) klasik dapat dibagi menhadi dua kategori, yaitu [1]:

1. *Cipher* Substitusi
   Algoritma ini adalah algoritma kriptografi yang mula-mula digunakan oleh kaisar Romawi, Julius Caesar, untuk menyandikan pesan yang ia kirim kepada gubernurnya. Proses penyandian dilakukan dengan mengganti (mensubstitusi) setiap karakter dengan karakter lain dalam susunan abjad (alfabet).
2. *Cipher* Transposisi
   Algoritma ini melakukan *transpose* (permutasi) terhadap rangkaian karakter di dalam teks dengan mengubah urutannya. Dengan kata lain, jumlah masing karakter pada data teks asli akan sama dengan jumlah masing-masing karakter pada data teks hasil permutasi.

Salah satu jenis Cipher Substitusi yang akan dibahas dalam makalah ini adalah algoritma *Playfair Cipher*. Algoritma ini mensubstitusi karakter-karakter pada data asli dengan menggunakan sebuah papan kunci yang dirahasiakan. Dengan papan kunci ini, proses enkripsi dan dekripsi dilakukan.

Pada tahun 1854, seorang ilmuwan, berkebangsaan Inggris, bernama Sir Charles Wheatstone menemukan algoritma kriptografi *Playfair Cipher*. Akan tetapi, temannya yang bernama Baron Lyon Playfair berhasil membujuk pemerintah Inggris menggunakan algoritma tersebut secara resmi. Oleh karena itu, nama Playfair menjadi nama dari algoritma *Playfair Cipher* yang dikenal sebagai salah satu algoritma klasik dan bukan Wheatstone. *Playfair Cipher* digunakan oleh tentara Inggris pada perang Boer (Perang Dunia I).

2. *Playfair Cipher* dengan Papan Kunci Bujursangkar

Pada awal penemuannya tahun 1854, *Playfair Cipher* menggunakan papan kunci yang berbentuk bujursangkar dalam melakukan penyandian. Papan kunci ini berukuran 5x5, dimana setiap bagian dalam papn kunci mewakili huruf-huruf dalam alfabet (abjad) dengan menghilangkan huruf J dari abjad. Setiap elemen bujursangkar berisi huruf yang berbeda satu sama lain.
Contoh kunci:

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

Dari papan kunci tersebut, jumlah kemungkinan kunci adalah
25!=15.511.210.043.330.985.984.000.000

Susunan kunci di dalam bujursangkar diperluas dengan menambahkan kolom keenam dan baris keenam.

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

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

Penambahan susunan kunci pada kolom keeenam dan baris keenam dimaksudkan untuk mempermudah dalam melakukan proses penyandian.

Papan kunci dapat diibentuk dari sebuah kalimat yang mudah diingat, misalnya:

KRIPTOGRAFI IS AN ART

Buang huruf yang berulang dan huruf J jika ada:

KRIPTOGAFSN

Lalu tambahakn huruf-huruf yang belum ada (kecuali J):

KRIPTOGAFSNBCDEHLMQUVWXYZ

Masukkan huruf-huruf tersebut dalam papan kunci bujursangkar:

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

Papan kunci yang berbeda dalam setiap kali proses penyandian (enkripsi dan dekripsi) dapat meningkatkan keamanan dari pesan yang akan enkripsi (dirahasiakan). Akan tetapi, pihak yang akan mengirim pesan (enkripsi) dan pihak yang menenrima pesan (dekripsi) harus mempunyai papan kunci yang sama.

Kunci yang dibangkitkan dari kalimat yang mudah diingat dapat menjadi sebuah solusi dalam melakukan proses penyandian. Kalimat tersebut dapat digunakan oleh pihak yang melakukan enkripsi dan dekripsi dimana kedua belah pihak saling mengetahui kalimat yang digunakan untuk membangkitkan kunci.

2.1 Proses Enkripsi

Enkripsi merupakan sebuah proses dimana data teks asli diubah menjadi data teks rahasia. Sebelum melakukan enkripsi, pesan yang akan dienkripsi (plainteks) diatur terlebih dahulu sebagai berikut:

1. Semua spasi dan karakter yang bukan alfabet harus dihilangkan dari plainteks (jika ada).
2. Jika ada huruf J pada palinteks maka ganti huruf tersebut dengan huruf I.
3. Pesan yang akan dienkripsi ditulis dalam pasangan huruf (*bigram*).
4. Jika ada huruf yang sama dalam pasangan huruf, maka sisipkan huruf X atau Z di tengahnya. Huruf yang disisipkan sebaiknya huruf X karena sangat kecil kemungkinan terdapat huruf X yang sama dalam *bigram*, tidak seperti huruf Z, contohnya dalam kata FUZZY.
5. Jika jumlah huruf pada plainteks adalah ganjil maka pilih sebuah huruf tambahan yang dipilih oleh orang yang mengenkripsi dan tambahkan di akhir plainteks. Huruf tambahan dapat dipilih sembarang misalnya huruf Z atau X.

Contoh plainteks:
IT IS FULL MOON! MEET ME AT HAMMERSMITH BRIDGE TONIGHT

→ Hilangkan semua karakter yang bukan alfabet.
→ Tidak ada huruf J, maka langsung tulis pesan dalam pasangan huruf.
→ Jika ada huruf yang sama pasangan huruf (*bigram*), maka tambahkan huruf X ditengahnya.

Plainteks yang telah dilakukan pengaturan:
IT IS FU LX LM OX ON ME ET ME AT HA MX ME RS MI TH BR ID GE TO NI GH TX

Algoritma enkripsi untuk setiap *bigram* adalah sebagai berikut:

1. Jika ada dua huruf terdapat pada baris kunci yang sama maka tiap huruf diganti dengan huruf di kanannya (pada kunci yang telah diperluas).
2. Jika ada dua huruf terdapat pada kolom yang sama maka tiap huruf diganti dengan huruf di bawahnya (pada kunci yang telah diperluas).
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.
4. Huruf kedua diganti dengan huruf pada titik sudut keempat dari persegi panjang yang dibentuk dari 3 huruf yang digunakan sampai sejauh ini.

Contoh kunci (yang sudah diperluas) ditulis kembali sebagai berikut:

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

Plainteks (dalam pasangan huruf):
IT IS FU LX LM OX ON ME ET ME AT
HA MX ME RS MI TH BR ID GE TO NI
GH TX

Cipherteks:
DM GZ BZ PY KV TR MR OI DO OI MA
QO TN OI YF ZM OP FX GW ED AT IM
EL BD

Enkripsi IS menjadi GZ ditunjukkan pada papan kunci di bawah ini:

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

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

2.2 Proses Dekripsi

Proses dekripsi sangat mirip dengan proses enkripsi dan lebih mudah dilakukan. Untuk melakukan proses dekripsi, cipherteks dikelompokan terlebih dahulu dalam pasangan huruf (*bigram*) seperti pada saat enkripsi. Kemudian, terapkan algoritma dekripsi yang merupakan kebalikan dari algoritma enkripsi untuk setiap *bigram* tersebut.

Algoritma dekripsi adalah sebagai berikut:

1. Jika ada dua huruf terdapat pada baris kunci yang sama maka tiap huruf diganti dengan huruf di kirinya (pada kunci yang telah diperluas).
2. Jika ada dua huruf terdapat pada kolom kunci yang sama maka tiap huruf diganti dengan huruf di diatasnya (pada kunci yang telah diperluas).
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.
4. Huruf kedua diganti dengan huruf pada perpotongan baris huruf kedua dengan kolom huruf pertama.

Setelah menerapkan algoritma dekripsi pada cipherteks, huruf-huruf dapat dapat memiliki arti dengan menambahakan spasi diantara kata-kata yang mungkin. Jika terdapat huruf yang berada diantara dua huruf yang sama (tidak sesuai pada tempatnya) maka huruf tersebut dapat dihilangkan untuk dapat membaca pesan yang telah didekripsi dengan baik.

Contoh cipherteks yang telah dikelompokkan dalam pasangan huruf.

DM GZ BZ PY KV TR MR OI DO OI MA
QO TN OI YF ZM OP FX GW ED AT IM
EL BD

↑
Contoh *bigram* yang didekripsi

Papan kunci yang digunakan untuk mendekripsi pesan diatas (telah diperluas).

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

Plainteks setelah diterapkan algoritma dekripsi dengan menggunakan papan kunci bujursangkar yang telah diperluas.

IT IS FU LX LM OX ON ME ET ME AT
HA MX ME RS MI TH BR ID GE TO NI
GH TX

Dekripsi ED menjadi GE ditunjukkan pada papan kunci di bawah ini:

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

Pesan dapat dibaca dengan menambahkan spasi dan menghilangkan huruf-huruf tambahan yang tidak berguna.

IT IS FULL MOON MEET ME AT HAMMERSMTH BRIDGE TONIGHT

3. *Playfair Cipher* dengan Papan Kunci Kubus

Pada *Playfair Cipher* dengan papan kunci yang berbentuk kubus, proses penyandian dilakukan mirip dengan *Playfair Cipher* dengan papan kunci bujursangkar tapi dilakukan sedikit perubahan dalam menggunakan papan kunci. Proses penyandian dilakukan dengan mensubstitusi huruf-huruf pada plainteks dengan huruf-huruf yang terdapat pada papan kunci. Huruf pada papan kunci menentukan pesan yang terbentuk pada cipherteks.

Perbedaan utama dua buah *Playfair Cipher* tersebur adalah papan kunci dengan bentuk yang berbeda dan masing-masing memiliki jumlah bagian yang berbeda pula. Pada papan kunci yang berbentuk bujursangkar, jumlah bagian adalah 25, sedangkan pada papan kunci kubus, jumlah bagian adalah 27. Selain itu, pada saat pengaturan plainteks, huruf J tidak dihilangkan ataupun diganti dengan huruf lain.

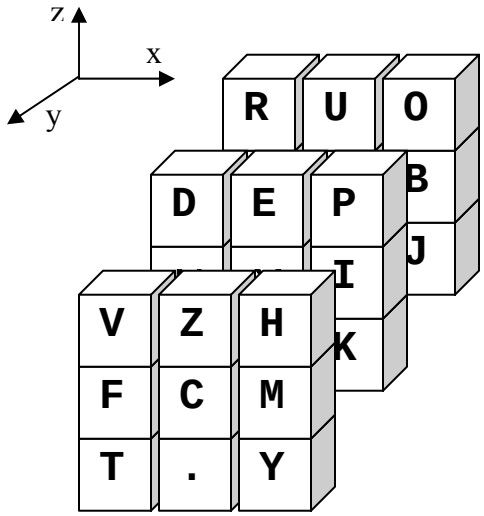
Papan kunci kubus dibentuk dari sebuah kubus yang berukuran 3x3x3. Setiap bagian kubus mewakili huruf-huruf pada alfabet yang berbeda satu sama lain dan sebuah karakter tambahan yaitu karakter titik. Huruf dan karakter ini digunakan dalam melakukan proses enkripsi dan dekripsi.

Pemilihan karakter tambahan berupa titik karena dapat mengelabui pihak yang ingin mengetahui pesan yang telah dienkripsi. Pesan yang mengandung titik tersebut menjadi lebih sulit diterka isinya karena pesan ini akan menyerupai pesan biasa yang ditulis pada umumnya dan biasanya titik digunakan sebagai sebuah gelar seseorang atau akhir dari kalimat, meskipun pesan tersebut tidak memiliki arti. Karakter titik dalam pesan tersebut sebenarnya mewakili sebuah karakter dari plainteks tapi karakter tersebut dapat dikira sebagai karakter tambahan yang tidak memiliki arti.

Untuk lebih memahami papan kunci kubus, papan kunci tersebut dapat dibayangkan sebagai sebuah kubus yang digambarkan dalam sebuah ruang vektor. Kubus memiliki sumbu x, y, dan z. Sumbu z dapat disebut sebagai seumbu yang menyatakan lapisan-lapisan dari huruf-huruf dalam kubus.

Contoh kunci :

Susunan kunci dalam bentuk kubus.



Susunan kunci bila dituliskan setiap lapisan (berdasarkan sumbu z) dari papan kunci berbentuk kubus diatas adalah sebagai berikut:

Lapisan pertama:

G	S	J
W	A	K
T	.	Y

Lapisan kedua:

L	Q	B
N	X	I
F	C	M

Lapisan ketiga:

R	U	O
D	E	P
V	Z	H

Jumlah kemungkinan kunci pada papan kunci berbentuk kubus:
27!=10.888.869.450.418.352.160.768.000.000

Susunan kunci di dalam kubus diperluas dengan menambahkan lapisan huruf-huruf baru pada setiap sumbu.

Lapisan pertama:

G	S	J	G
W	A	K	W
T	.	Y	T
G	S	J	

Lapisan kedua:

L	Q	B	L
N	X	I	N
F	C	M	F
L	Q	B	

Lapisan ketiga:

R	U	O	R
D	E	P	D

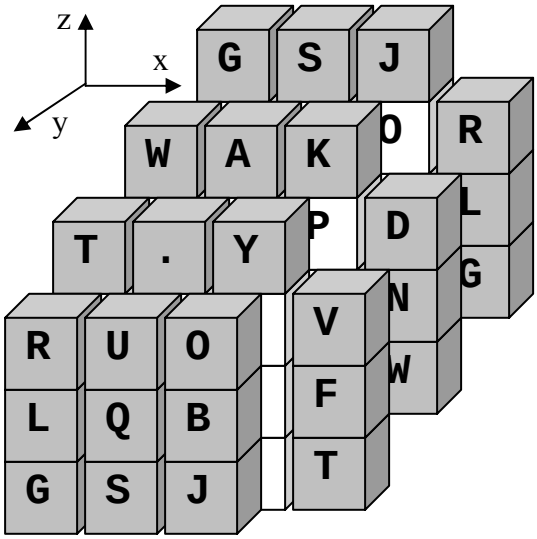
V	Z	H	V
R	U	O	

Lapisan keempat (lapisan tambahan=lapisan pertama sebelum penambahan):

G	S	J	
W	A	K	
T	.	Y	

Penambahan huruf-huruf dalam setiap sumbu (bagian yang diberi warna abu-abu), dilakukan untuk memudahkan dalam proses penyandian.

Susunan setiap lapisan dalam bentuk kubus.



Keterangan:
Bagian-bagian kubus yang diberi warna abu-abu adalah bagian yang ditambahkan pada papan kunci kubus tersebut.

3.1 Proses Enkripsi

Pada *Playfair Cipher* dengan papan kunci berbentuk kubus, proses enkripsi dilakukan dengan mengatur terlebih dahulu pesan yang akan dienkripsi, seperti pada *Playfair Cipher* dengan papan kunci berbentuk bujursangkar.

Pesan yang akan dienkripsi diatur sebagai berikut:

1. Semua spasi dan karakter yang bukan alfabet harus dihilangkan dari plainteks (jika ada).
2. Tulis pesan yang akan dienkripsi dalam pasangan huruf (*bigram*).
3. Jika ada huruf yang sama dalam pasangan huruf, maka sisipkan huruf X di tengahnya.
4. Jika jumlah huruf pada plainteks adalah ganjil maka tambahkan sebuah huruf tambahan X di akhir plainteks.

Contoh plainteks:
IT IS FULL MOON! MEET ME AT HAMMERSMITH BRIDGE TONIGHT

→ Hilangkan semua karakter yang bukan alfabet.
→ Jika ada huruf yang sama pasangan huruf (*bigram*), maka tambahkan huruf X ditengahnya.

Plainteks yang telah dilakukan pengaturan:
IT IS FU LX LM OX ON ME ET ME AT HA MX ME RS MI TH BR ID GE TO NI GH TX

Setelah dilakukan pengaturan, algoritma enkripsi diterapkan pada pesan yang telah diatur tersebut. Algoritma enkripsi untuk papan kunci berbentuk kubus adalah sebagai berikut:

1. Jika ada dua huruf berada pada sumbu x dan sumbu y yang sama maka setiap huruf diganti dengan huruf di atasnya (huruf yang sejajar dengan sumbu z).
2. Jika ada dua huruf berada pada sumbu x dan sumbu z yang sama maka setiap huruf diganti dengan huruf di depannya (huruf yang sejajar dengan sumbu y).
3. Jika dua huruf berada pada sumbu y dan sumbu z yang sama maka setiap huruf diganti dengan huruf di kanannya (huruf yang sejajar dengan sumbu x).
4. Jika ada dua huruf hanya berada pada sumbu x yang sama maka huruf pertama diganti dengan huruf pada perpotongan huruf yang sejajar sumbu y dari huruf pertama dengan huruf yang sejajar dengan sumbu z dari huruf kedua. Huruf kedua diganti dengan perpotongan huruf yang sejajar sumbu y dari huruf kedua dengan huruf yang sejajar sumbu z dari huruf pertama.
5. Jika ada dua huruf hanya berada pada sumbu y yang sama maka huruf pertama diganti dengan huruf pada perpotongan huruf yang sejajar sumbu x dari huruf pertama dengan huruf yang sejajar dengan sumbu z dari huruf kedua. Huruf kedua diganti dengan perpotongan huruf yang sejajar sumbu x dari huruf kedua dengan huruf yang sejajar sumbu z dari huruf pertama.
6. Jika ada dua huruf hanya berada pada sumbu z yang sama maka huruf pertama diganti dengan huruf pada perpotongan huruf yang sejajar sumbu x dari huruf pertama dengan huruf yang sejajar dengan sumbu y dari huruf kedua. Huruf kedua diganti dengan perpotongan huruf yang sejajar sumbu x dari huruf kedua dengan huruf yang sejajar sumbu y dari huruf pertama.
7. Jika ada dua huruf tidak berada pada sumbu yang sama (x, y, dan z) maka huruf pertama diganti dengan huruf pada perpotongan huruf yang sejajar sumbu x dari huruf pertama dengan huruf yang sejajar dengan sumbu y dari huruf kedua tapi huruf hasil perpotongan tersebut berada pada sumbu z yang sama dengan huruf kedua. Huruf kedua diganti dengan perpotongan huruf yang sejajar sumbu x dari huruf kedua dengan huruf yang sejajar sumbu y dari huruf pertama tapi berada pada sumbu z yang sama dengan huruf pertama.

Contoh kunci berbentuk kubus yang telah diperluas ditulis kembali sebagai berikut:

Lapisan pertama:

G	S	J	G
W	A	K	W
T	.	Y	T
G	S	J	

Lapisan kedua:

L	Q	B	L
N	X	I	N
F	C	M	F
L	Q	B	

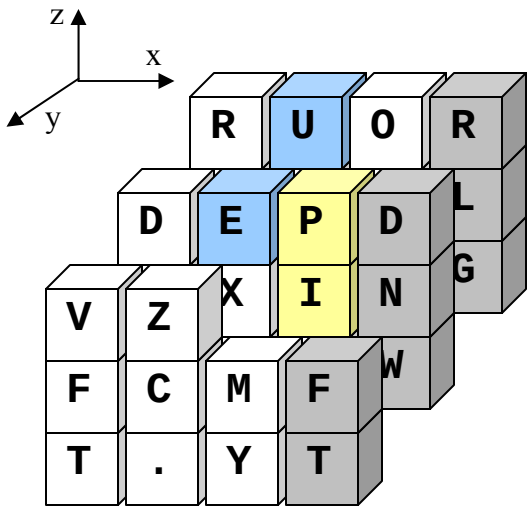
Lapisan ketiga:

R	U	O	R
D	E	P	D
V	Z	H	V
R	U	O	

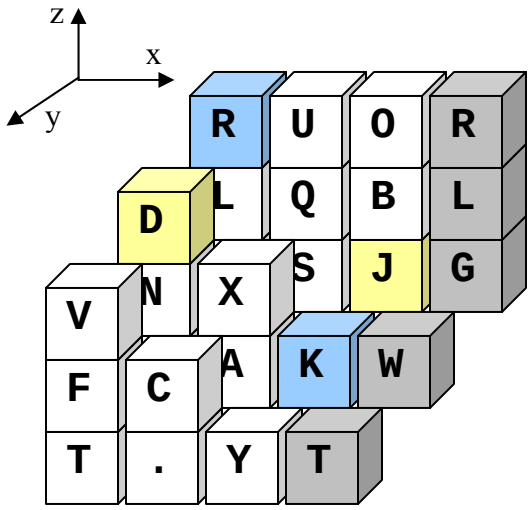
Lapisan keempat (lapisan tambahan=lapisan pertama sebelum penambahan):

G	S	J	
W	A	K	
T	.	Y	

Contoh *bigram* yang berada pada sumbu `x` dan sumbu `z` yang sama adalah `UE`. *Bigram* yang berada pada sumbu `x` dan `y` yang sama adalah `PI`. *Bigram* tersebut digambarkan dalam kubus (yang telah diperluas) sebagai berikut:



Contoh enkripsi *bigram* `RK` menjadi `JD` yang menggunakan aturan algoritma enkripsi yang ketujuh (tidak berada pada sumbu yang sama satupun). Enkripsi tersebut dapat diilustrasikan dalam kubus sebagai berikut:



Keterangan :
Huruf-huruf yang berwarna biru adalah pasangan huruf yang akan dienkripsi (plainteks) dan huruf-huruf yang berwarna kuning adalah pasangan huruf hasil enkripsi (cipherteks).

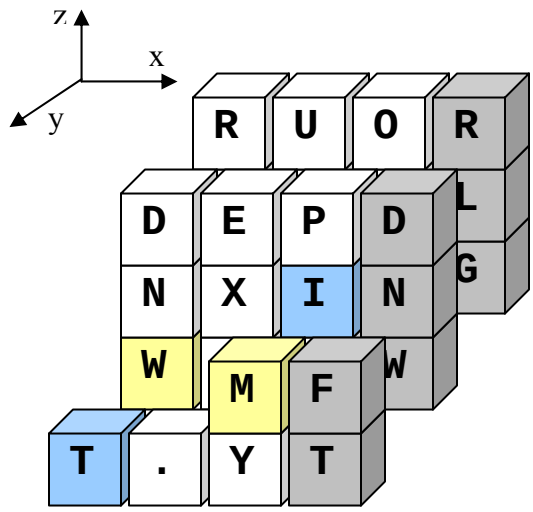
Contoh plainteks (dalam pasangan huruf) yang telah diatur terlebih dahulu:

```
IT IS FU LX LM OX ON ME ET ME AT
HA MX ME RS MI TH BR ID GE TO NI
GH TX
```

Cipherteks hasil enkripsi plainteks diatas:

```
WM AB ZL QN BF QP LP ZI WZ ZI W.
.P CI ZI UG BM YV LO NP UW HG XN
OT CW
```

Enkripsi `IT` menjadi `WM` ditunjukkan pada papan kunci berbentuk kubus di bawah ini:



Jika enkripsi `IT` menjadi `WM` ditunjukkan dengan menggunakan papan kunci berbentuk kubus yang ditulis setiap lapisannya adalah sebagai berikut:

Lapisan pertama:

G	S	J	G
W	A	K	W
T	.	Y	T
G	S	J	

Lapisan kedua:

L	Q	B	L
N	X	I	N
F	C	M	F
L	Q	B	

Lapisan ketiga:

R	U	O	R
D	E	P	D
V	Z	H	V
R	U	O	

Lapisan keempat (lapisan tambahan=lapisan pertama sebelum penambahan):

G	S	J	
W	A	K	
T	.	Y	

3.2 Proses Dekripsi

Pada proses dekripsi dengan *Playfair Cipher*, cipherteks dikelompokan dahulu dalam pasangan huruf (*bigram*) seperti pada saat proses enkripsi. Selanjutnya, algoritma dekripsi diterapkan pada hasil pengelompokan huruf tersebut. Algoritma dekripsi mempunyai aturan yang mirip dengan algoritma enkripsi namun dengan beberapa perbedaan. Dapat dikatakan bahwa algoritma dekripsi merupakan algoritma kebalikan dari algoritma enkripsi dan penyandian kembali data teks yang telah dienkripsi menjadi data teks asli.

Untuk melakukan proses dekripsi dengan baik, kunci yang sebelumnya digunakan pada saat proses enkripsi digunakan kembali dalam proses ini. Jika papan kunci yang digunakan berbeda maka hasil dekripsi tidak akan sama dengan arsip asal sebelum dienkripsi.

Algoritma dekripsi selengkapnya untuk *Playfair Cipher* dengan papan kunci berbentuk kubus adalah sebagai berikut:

1. Jika ada dua huruf berada pada sumbu `x` dan sumbu `y` yang sama maka setiap

huruf diganti dengan huruf di bawahnya (huruf yang sejajar dengan sumbu z).

2. Jika ada dua huruf berada pada sumbu x dan sumbu z yang sama maka setiap huruf diganti dengan huruf di belakangnya (huruf yang sejajar dengan sumbu y).
3. Jika dua huruf berada pada sumbu y dan sumbu z yang sama maka setiap huruf diganti dengan huruf di kirinya (huruf yang sejajar dengan sumbu x).
4. Jika ada dua huruf hanya berada pada sumbu x yang sama maka huruf pertama diganti dengan huruf pada perpotongan huruf yang sejajar sumbu y dari huruf pertama dengan huruf yang sejajar dengan sumbu z dari huruf kedua. Huruf kedua diganti dengan perpotongan huruf yang sejajar sumbu y dari huruf kedua dengan huruf yang sejajar sumbu z dari huruf pertama.
5. Jika ada dua huruf hanya berada pada sumbu y yang sama maka huruf pertama diganti dengan huruf pada perpotongan huruf yang sejajar sumbu x dari huruf pertama dengan huruf yang sejajar dengan sumbu z dari huruf kedua. Huruf kedua diganti dengan perpotongan huruf yang sejajar sumbu x dari huruf kedua dengan huruf yang sejajar sumbu z dari huruf pertama.
6. Jika ada dua huruf hanya berada pada sumbu z yang sama maka huruf pertama diganti dengan huruf pada perpotongan huruf yang sejajar sumbu x dari huruf pertama dengan huruf yang sejajar dengan sumbu y dari huruf kedua. Huruf kedua diganti dengan perpotongan huruf yang sejajar sumbu x dari huruf kedua dengan huruf yang sejajar sumbu y dari huruf pertama.
7. Jika ada dua huruf tidak berada pada sumbu yang sama (x, y, dan z) maka huruf pertama diganti dengan huruf pada perpotongan huruf yang sejajar sumbu x dari huruf pertama dengan huruf yang sejajar dengan sumbu y dari huruf kedua tapi huruf hasil perpotongan tersebut berada pada sumbu z yang sama dengan huruf kedua. Huruf kedua diganti dengan perpotongan huruf yang sejajar sumbu x dari huruf kedua dengan huruf yang sejajar sumbu y dari huruf pertama tapi berada pada sumbu z yang sama dengan huruf pertama.

Penerapan algoritma dekripsi pada cipherteks akan mengubah pesan yang semula tidak memiliki arti menjadi sebuah pesan yang memiliki arti. Pesan yang telah didekripsi tidak dapat langsung menjadi data teks asli karena ada kemungkinan penambahan huruf tambahan diantara dua buah huruf yang sama.

Berikut contoh cipheteks yang akan didekripsi:

```
YVKUD.DSLEMWZIDXMDURIFDX.FLP.WNX
G.ZPSK.DMDVGESBF.XPMXDUOFWMBZXSN
AQGQMISDBDUAWXKRD.XEKENOXMW.BPFN
SEXFZPVG.P.WUDXDXZAQA.JVHGUOIDUR
LGI.GABDCWZWXNFWZPSK.DDORJSDCIBM
LWSNLWESUW
```

Untuk memudahkan dalam menganalisis hasil dekripsi dari cipherteks diatas, cipherteks dikelompokan dalam pasangan huruf. Hasil pengelompokan dapat dilihat sebagai berikut:

```
YV KU D. DS LE MW ZI DX MD UR IF
DX .F LP .W NX G. ZP SK .D MD VG
ES BF .X PM XD UO FW MB ZX SN AQ
GQ MI SD BD UA WX KR D. XE KE NO
XM W. BP FN SE XF ZP VG .P .W UD
XD XZ AQ A. JV HG UO ID UR LG I.
GA BD CW ZW XN FW ZP SK .D DO RJ
SD CI BM LW SN LW ES UW
```

Papan kunci yang digunakan untuk melakukan dekripsi terhadap cipherteks (dituliskan dalam bentuk lapisan-lapisan untuk memudahkan dalam memahami proses dekripsi dan telah diperluas). Lapisan-lapisan ini disusun dari lapisan paling bawah sampai paling atas dalam kubus.

Lapisan pertama:

G	S	J	G
W	A	K	W
T	.	Y	T
G	S	J	

Lapisan kedua:

L	Q	B	L
N	X	I	N
F	C	M	F
L	Q	B	

Lapisan ketiga:

R	U	O	R
D	E	P	D
V	Z	H	V
R	U	O	

Lapisan keempat (lapisan tambahan=lapisan pertama sebelum penambahan):

G	S	J	
W	A	K	
T	.	Y	

Keterangan:
Kotak yang berwarna kuning pada tabel adalah pasangan huruf dalam cipherteks dan kotak berwarna biru adalah pasangan huruf dalam plainteks.

Plainteks hasil dekripsi dengan menggunakan papan kunci kubus yang telah diperluas diperlihatkan di bawah ini (dikelompokan dalam pasangan huruf untuk melihat pasangan huruf hasil dekripsi dengan pasangan huruf yang berpadanan pada cipherteks).

TH EJ AV AR UN TI ME EN VI RO NM
EN TC ON TA IN ST HE JA VA VI RT
UA LM AC HI NE RU NT IM EC LA SX
SL IB RA RI ES AN DJ AV AX AP PL
IC AT IO NL AU NC HE RT HA TA RE
NE CE SX SA RY TO RU NP RO GR AM
SW RI TX TE NI NT HE JA VA PR OG
RA MX MI NG LA NG UA GE

Dekripsi pasangan huruf cipherteks YV menjadi pasangan huruf plainteks TH diperlihatkan pada papan kunci. Pasangan huruf YV berada pada sumbu y yang sama. Oleh karena itu, pasangan huruf tersebut menggunakan aturan kelima algoritma dekripsi. Hasil dekripsi dari pasangan huruf YV adalah TH.

Pesan hasil dekripsi dari cipherteks dapat dibaca dengan menghilangkan huruf tambahan dan memberi spasi diantara kata-kata yang mungkin sehingga pesan tersebut memiliki arti seperti sebelum dienrkipsi. Berikut pesan yang telah memiliki arti.

THE JAVA RUNTIME ENVIRONMENT CONTAINS THE JAVA VIRTUAL MACHINE RUNTIME CLASS LIBRARIES AND JAVA APPLICATION LAUNCHER THAT ARE NECESSARY TO RUN PROGRAMS WRITTEN IN THE JAVA PROGRAMMING LANGUAGE

Papan kunci yang telah digunakan untuk melakukan enkripsi dan dekripsi dapat diubah atau dibuat yang baru. Hal ini dilakukan untuk menghindari diketahuinya papan kunci oleh pihak yang tidak berhak.

4. Pengujian

Proses pengujian dilakukan terhadap *Playfair Cipher* dengan papan kunci bujursangkar dan kubus. Masing-masing papan kunci akan diuji dengan kasus uji yang sama.

Pengujian dilakukan dengan memanfaatkan perangkat lunak yang telah dibuat. Perangkat lunak ini dibangun dengan bahasa pemrograman C++ dan menggunakan *console* sebagai antarmuka. Perangkat lunak tersebut dapat diunduh di
http://students.if.itb.ac.id/~if14109/kriptografi.

Perangkat lunak berupa sebuah *executable file* yang hanya dapat dijalankan di lingkungan sistem operasi Windows. Untuk medapatkan *source code* program, Anda dapat mengirimkan *email* yang tertera pada awal makalah ini.

Untuk melakukan pengujian dengan perangkat lunak ini, arsip yang akan dienkripsi maupun didekripsi harus diberi nama "`fin.txt`". Arsip hasil enkripsi maupun dekripsi diberi nama "`fout.txt`". Selain itu, papan kunci berbentuk

bujursangkar disimpan dalam arsip `squarekey.txt` dan papan kunci kubus disimpan dalam arsip `cubekey.txt`.

4.1 Perancangan Kasus Uji Pengujian Perangkat Lunak *Playfair Cipher*

Berdasarkan teknik pengujian yang telah dijelaskan, maka dirancang kasus-kasus uji sebagai berikut:

1. Kasus uji 1
   Kasus uji 1 bertujuan untuk menguji kebenaran proses enkripsi dan dekripsi dengan menggunakan algoritma kriptografi *Playfair Cipher* dengan papan kunci bujursangkar.
2. Kasus uji 2
   Kasus uji 2 bertujuan untuk menguji kebenaran proses enkripsi dan dekripsi dengan menggunakan algoritma kriptografi *Playfair Cipher* dengan papan kunci berbentuk kubus.
3. Kasus uji 3
   Kasus uji 3 bertujuan untuk menguji kebenaran proses enkripsi dan dekripsi dengan menggunakan algoritma kriptografi *Playfair Cipher* dengan papan kunci berbentuk bujursangkar dan arsip asal mengandung sebuah *bigram* dengan huruf yang sama.
4. Kasus uji 4
   Kasus uji 4 bertujuan untuk menguji kebenaran proses enkripsi dan dekripsi dengan menggunakan algoritma kriptografi *Playfair Cipher* dengan papan kunci berbentuk kubus dan arsip asal mengandung sebuah *bigram* dengan huruf yang sama.
5. Kasus uji 5
   Kasus uji 5 bertujuan untuk menguji kebenaran proses enkripsi dan dekripsi dengan menggunakan algoritma kriptografi *Playfair Cipher* dengan papan kunci berbentuk bujursangkar dan arsip asal mengandung beberapa *bigram* dengan huruf yang sama. *Bigram-bigram* tersebut terletak bersebelahan atau berdekatan.
6. Kasus uji 6
   Kasus uji 6 bertujuan untuk menguji kebenaran proses enkripsi dan dekripsi dengan menggunakan algoritma kriptografi *Playfair Cipher* dengan papan kunci berbentuk kubus dan arsip asal mengandung *bigram* dengan huruf yang sama. *Bigram-bigram* tersebut terletak bersebelahan atau berdekatan.
7. Kasus uji 7
   Kasus uji 7 bertujuan untuk menguji kebenaran proses enkripsi dan dekripsi beserta lama waktu proses enkripsi dan dekripsi dengan menggunakan algoritma kriptografi *Playfair Cipher* dengan papan kunci berbentuk bujursangkar dan jumlah karakter pada arsip berjumlah ganjil.
8. Kasus uji 8
   Kasus uji 8 bertujuan untuk menguji kebenaran proses enkripsi dan dekripsi beserta lama waktu proses enkripsi dan dekripsi dengan menggunakan algoritma kriptografi *Playfair Cipher* dengan papan kunci berbentuk kubus dan jumlah karakter pada arsip berjumlah ganjil.
9. Kasus uji 9
   Kasus uji 9 bertujuan untuk menguji kebenaran proses enkripsi dan dekripsi beserta lama waktu proses enkripsi dan dekripsi dengan menggunakan algoritma kriptografi *Playfair Cipher* dengan papan kunci berbentuk bujursangkar dan jumlah karakter pada arsip berjumlah genap.
10. Kasus uji 10
    Kasus uji 10 bertujuan untuk menguji kebenaran proses enkripsi dan dekripsi beserta lama waktu proses enkripsi dan dekripsi dengan menggunakan algoritma kriptografi *Playfair Cipher* dengan papan kunci berbentuk kubus dan jumlah karakter pada arsip berjumlah genap.

4.2 Proses Pengujian Perangkat Lunak *Playfair Cipher*

Proses pengujian dengan perangkat lunak *Playfair Cipher* dilakukan dengan memilih menu yang tersedia. Menu enkripsi dan dekripsi yang tersedia dapat dipilih dengan memasukkan nomor menu sesuai dengan yang ditampilkan. Dalam menu juga terdapat pembangkitan papan kunci yang dilakukan secara acak untuk masing-masing papan kunci.

Dalam proses pengujian kali ini, papan kunci berbentuk bujursangkar yang digunakan adalah sebagai berikut (telah diperluas).

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

Papan kunci berbentuk kubus yang digunakan dalam proses pengujian adalah sebagai berikut (dalam bentuk lapisan-lapisan dan telah diperluas).

Lapisan pertama:

U	P	M	U
K	.	S	K
Y	J	Q	Y
U	P	M	

Lapisan kedua:

L	R	G	L
A	T	W	A
E	N	X	E
L	R	G	

Lapisan ketiga:

Z	B	H	Z
C	O	D	C
I	V	F	I
Z	B	H	

Lapisan keempat (lapisan tambahan=lapisan pertama sebelum penambahan):

U	P	M	
K	.	S	
Y	J	Q	

Kedua papan kunci diatas digunakan dalam setiap proses pengujian. Hal ini dilakukan untuk mempermudah proses pengujian karena jika papan kunci yang digunakan berbeda akan menghasilkan hasil yang tidak sama dengan isi arsip asal.

Pada kasus uji 5 dan 6, arsip asal yang mempunyai beberapa *bigram* dengan huruf yang sama dan terletak bersebelahan dicontohkan sebagai berikut.

```
CONGRESS SHALL MAKE NO LAW
RESPECTING AN ESTABLISHMENT OF
RELIGION
```

Jika dikelompokkan dalam pasangan huruf (*bigram*) maka didapatkan beberapa *bigram* yang mempunyai huruf yang sama.

```
CO NG RE SS SH AL LM AK EN OL AW
RE SP EC TI NG AN ES TA BL IS HM
EN TO FR EL IG IO N
```

Pada pesan terseut, dapat dilihat bahwa *bigram* SS dan SH mempunyai huruf yang sama dari keduanya yaitu huruf S. Huruf tersebut dapat menyebabkan penambahan huruf-huruf yang telah dijelaskan diatas mengenai pengaturan sebelum dilakukan proses enkripsi.

4.3 Evaluasi Hasil Pengujian Perangkat Lunak *Playfair Cipher*

Dari hasil pengujian kasus uji 1 dan 2, dapat diketahui bahwa perangkat lunak *Playfair Cipher* telah melakukan proses enkripsi dan dekripsi algoritma kriptografi *Playfair Cipher* dengan papan kunci berbentuk kubus dan bujursangkar dengan benar. Proses enkripsi dengan menggunakan papan kunci akan menyandikan arsip teks asal. Proses dekripsi dengan menggunakan papan kunci yang sama dengan papan kunci yang digunakan dalam proses enkripsi akan mengembalikan isi arsip menjadi isi arsip asal. Sedangkan, kesalahan

penggunaan papan kunci akan mengakibatkan isi arsip hasil dekripsi tidak sama dengan arsip asal. Kasus uji 1 dan 2 juga menunjukkan bahwa wakktu enkripsi dan dekripsi algoritma kriptografi *Playfair Cipher* relarif sama baik dengan papan kunci berbentuk bujursangkar mapupun kubus.

Selain itu, proses enkripsi dan dekripsi dengan menggunakan algoritma *Playfair Cipher* hanya dapat dilakukan terhadap arsip yang berupa teks alfabet. Jika terdapat karakter selain alfabet maka karakter tersebut diabaikan sehingga tidak terdapat pada arsip hasil enkripsi. Karakter berupa angka dapat dituliskan dalam sebuah kalimat untuk menghindari penghilangan saat proses enkripsi.

Dari hasil pengujian kasus uji 3 dan 4, diketahui bahwa *bigram* dengan huruf yang sama dapat dienkripsi dan didekripsi dengan baik. Pada saat enkripsi terjadi penambahan huruf diantara huruf yang sama sehingga proses enkripsi dapat dilakukan. Arsip hasil proses dekripsi mengandung huruf tambahan yang tidak berguna dan dapat dihilangkan.

Dari hasil pengujian kasus uji 5 dan 6, dapat diketahui bahwa proses enkripsi dan dekripsi dengan papan kunci bujursangkar maupun kubus, dapat menyandikan pesan yang mengandung beberapa *bigram* dengan huruf yang sama dan terletak bersebelahan. Arsip hasil dekripsi dari arsip yang telah dienkripsi dapat dikembalikan mejadi arsip semula (asal) dengan menghilanngkan huruf yang ditambahkan pada saat proses enkripsi.

Dari hasil pengujian kasus uji 7 dan 8, dapat diketahui bahwa arsip asal yang jumlah karakternya ganjil dapat dienkripsi dengan menambahkan huruf tambahan di akhir arsip. Penambahan ini dimaksudkan untuk membuat huruf-huruf dalam arsip awal menjadi pasangan huruf (*bigram*).

Dari hasil pengujian kasus uji 9 dan 10, dapat diketahui bahwa arsip asal yang telah berjumlah genap tidak perlu ditambahkan huruf tambahan di akhir arsip untuk dapat dienkripsi. Arsip tersebut dapat dengan mudah dienkripsi maupun di dekripsi karena tidak ada huruf tambahan.

Secara keseluruhan, pengujian terhadap algoritma *Playfair Cipher* baik dengan papan kunci berbentuk bujursangkar maupun kubus dapat memberikan informasi bahwa algoritma ini dapat merahasiakan pesan dan mengembalikan isi pesan tersebut. Untuk melakukan proses penyandian, papan kunci yang digunakan harus sama jika ingin mendapatkan isi pesan sebelum dienkripsi. Akan tetapi, algoritma ini hanya dapat melakukan enkripsi terhadap pesan yang berupa teks alfabet.

Dalam melakukan proses enkripsi dan dekripsi, digunakan papan kunci yang sama baik untuk papan kunci berbentuk bujursangkar maupun berbentuk kubus. Jika papan kunci yang digunakan berbeda maka pesan hasil dekripsi tidak sama dengan pesan asal.

5. Kesimpulan

Berdasarkan hasil pengujian dan analisis terhadap studi perbandingan *Playfair Cipher* dengan papan kunci bujursangkar dan kubus, dapat diambil beberapa kesimpulan sebagai berikut:

1. *Playfair Cipher* dengan papan kunci berbentuk bujuesangkar maupun kubus dapat menyandikan pesan sehingga hanya pihak yang berhak saja yang dapat melihat isi pesan.
2. *Playfair Cipher* dengan menggunakan papan kunci berbentuk kubus adalah solusi yang lebih baik daripada papan kunci bujursangkar dalam mengatasi masalah keamanan dan kerahasian data teks.
3. Pada algoritma kriptografi *Playfair Cipher* terdapat kelemahan dalam pendistribusian kunci antara pengirim pesan dan penerima pesan karena algoritma ini menggunkan kunci simetri dalam proses penyandian (enkripsi dan dekripsi).
4. Papan kunci kubus memiliki tingkat keamanan yang lebih tinggi daripada papan kunci bujursangkar karena jumlah kemungkinan kunci yang lebih besar daripada papan kunci bujursangkar.
5. Pada papan kunci berbentuk kubus, proses enkripsi dan dekripsi menjadi lebih sulit dipahami daripada papan kunci berbentuk bujursangkar.
6. Proses penyandian dengan papan kunci kubus dapat divariasikan dengan mengubah algoritma enkripsi dan dekripsi. Contohnya penentuan huruf

pertama dan kedua dalam papan kunci kubus yang dapat berbeda-beda.

7. Kelemahan pada papan kunci bujursangkar yaitu penghilangan huruf J dari plainteks dapat diatasi pada papan kunci berbentuk kubus.
8. Proses enkripsi dan dekripsi pada kedua papan kunci harus dilakuakan dengan menggunakan papan kunci yang sama untuk mendapatkan isi arsip yang asal.
9. Arsip hasil proses enkripsi dapat memiliki ukuran yang lebih besar daripada arsip asal karena ada kemungkinan huruf yang sama dalam sebuah *bigram* dan jumlah huruf yang ganjil dalam arsip asal. Hal ini dapat menyebabkan adanya penambahan huruf untuk dapat melakukan proses enkripsi.
10. Papan kunci yang berbeda akan mengasilkan arsip enkripsi yang berbeda pula.
11. *Playfair Cipher* hanya dapat digunakan untuk mengenkripsi dan mendekripsi data yang berupa teks alfabet sehingga jika terdapat karakter selain alfabet maka akan diabaikan (tidak terdapat pada arsip hasil enkripsi maupun arsip hasil dekripsi). Karakter yang diabaikan dapat dihindari dengan menuliskannya dalam bentuk teks alfabet.
12. *Playfair Cipher* merupakan salah satu tipe dari *cipher* substitusi yaitu setiap huruf dalam plainteks diganti dengan huruf yang berada dalam papan kunci.
13. *Playfair Cipher* dapat digunakan untuk memahami inti dari sebuah proses enkripsi dan dekripsi dalam bidang kriptografi.

6. Saran

Beberapa saran terhadap studi perbandingan *Playfair Cipher* dengan papan kunci bujursangkar dan kubus.

1. Sebuah papan kunci yang digunakan dalam proses penyandian sebaiknya tidak digunakan lebih dari sekali. Hal ini untuk mengurangi kemungkinan papan kunci telah dipecahkan oleh orang yang tidak berkepentingan.
2. Penggunaan *Playfair Cipher* pada data yang tidak terlalu penting masih dapat ditolerir. Contohnya surat menyurat antara teman.
3. *Playfair Cipher* sebaiknya tidak digunakan lagi pada saat ini karena tingkat keamanannya sudah tidak dapat lagi menjamin kerahasian data teks yang dikirim apalagi jika data tersebut adalah data penting yang tidak boleh diketahui oleh pihak lain.
4. *Playfair Cipher* dapat dikembangkan lebih lanjut dengan tidak menggunakan pengelompokan huruf secara *bigram* melainkan *trigram* atau yang lain.

DAFTAR PUSTAKA

[1] Munir, Rinaldi. (2004). Bahan Kuliah IF5054 Kriptografi. Departemen Teknik Informatika, Institut Teknologi Bandung.

[2] Rhew, Benjamin (2003) Crytanalyzing the Playfair Cipher Using Evolutionary Algorithms. *http://web.umr.edu/~tauritzd/courses/ec/fs2003/project/Rhew.pdf*. Tanggal akses: 25 September 2006 pukul 15.00.

[3] Goren, Ben (2004) The Playfair Cipher. *http://www.trumpetpower.com/Papers/Crypto/Playfair*. Tanggal akses: 25 September 2006 pukul 15.00.

[4] Playfair Cipher Information *http://andersonclassroom.tripod.com/playfaircipherinformation.pdf*. Tanggal akses: 25 September 2006 pukul 15.00.

[5] Chapter 2 - Classical Encryption Techniques *http://mail.leader.edu.tw/~reinhard/is_ppts/ch02.pdf*. Tanggal akses: 25 September 2006 pukul 15.00.

[6] Playfair Cipher *http://www.simonsingh.net/The_Black_Chamber/playfaircipher.htm*. Tanggal akses: 25 September 2006 pukul 15.00.

[6] Wikipedia - Playfair Cipher *http://en.wikipedia.org/wiki/Playfair_cipher*. Tanggal akses: 25 September 2006 pukul 15.00.

[7] Cryptography - Slides provided by prof. Csilla Farkas, University of South Carolina *http://www.dti.unimi.it/~decapita/Didattica/SS/lect1b.pdf*. Tanggal akses: 25 September 2006 pukul 15.00.

[8] Playfair Cipher: Information From Answers.com *http://www.answers.com/topic/playfair-cipher*. Tanggal akses: 11 Oktober 2006 pukul 10.00.

[9] Cryptography/Playfair cipher – Wikibooks, collection of open-context textbooks *http://en.wikibooks.org/wiki/Cryptography/Playfair_cipher*. Tanggal akses: 11 Oktober 2006 pukul 10.00.