

# Modifikasi Playfair Cipher dengan Pembalikan Pesan

Desfrianta Salmon Barus (13508107)

Program Studi Teknik Informatika

Sekolah Teknik Elektro dan Informatika

Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia

If18107@itb.ac.id;salmonbarus@gmail.com

**Abstraksi—** Playfair Cipher adalah teknik pengenkripsian pesan dengan menggunakan enkripsi pasangan huruf. Teknik ini populer dan banyak digunakan sejak dulu. Teknik Playfair Cipher ini menggunakan kunci tertentu untuk memodifikasi pemetaan urutan kata untuk pembuatan cipherteks.

Dengan metode Playfair Cipher pesan dapat dienkripsi menjadi cipherteks dengan kunci tertentu. Namun metode ini masih mudah ditebak dengan memeriksa pola teks yang sering muncul dengan menggunakan teknik analisis frekuensi pasangan huruf.

Untuk menambah keamanan dari teknik ini, salah satu metode yang dapat digunakan adalah dengan membalikkan pesan. Pesan yang dibalikkan kemudian akan dienkripsi sehingga diperoleh enkripsi yang susah ditebak. Pola penulisan yang biasanya muncul juga dapat dihindari sehingga kunci semakin sulit untuk ditebak.

**Indexs—**Playfair cipher, enkripsi, kunci, cipherteks.

## I. PENDAHULUAN

Kriptografi adalah suatu ilmu, seni, atau teknik yang digunakan untuk menjaga keamanan dari sebuah pesan. Dalam menjaga keamanan pesan tersebut suatu pesan disandikan dengan menggunakan suatu metode kriptografi tertentu yang memiliki kunci tertentu yang dapat mengenkripsi suatu pesan menjadi sebuah cipherteks dan kunci tertentu yang dapat mendekripsi suatu pesan kembali menjadi suatu teks yang sama seperti awalnya sebelum dienkripsi. Dalam pengembangannya dari waktu ke waktu banyak metode yang digunakan sebagai teknik kriptografi, dan seiring bertambah pesatnya teknologi, teknik-teknik kriptografi pun berkembang secara pesat dari waktu- ke waktu.

Salah satu metode yang sering dipakai pada masa awal tahun sembilanpuluh-an adalah teknik playfair cipher, teknik ini sering digunakan selama masa perang dunia pertama dan kedua untuk mengenkripsikan pesan-pesan berisi taktis perang. Teknik ini dipilih karena teknik ini dapat digunakan dengan cepat dan tidak memerlukan peralatan khusus dalam penggunaannya.

Playfair cipher adalah salah satu teknik enkripsi pesan secara simetris yang dilakukan manual dan tergolong sebagai salah satu teknik kriptografi klasik. Skema playfair cipher ini ditemukan pada tahun 1854 oleh Charles Wheatstone namun skema ini memakai nama

Lord Playfair karena Lord Playfair lah yang mempromosikan penggunaan penggunaan playfair cipher ini.

Dalam penggunaannya teknik playfair cipher pasangan huruf digunakan untuk melakukan enkripsi pesan, sehingga membuat analisis frekuensi menjadi sulit karena frekuensi dari kemunculan huruf-huruf di dalam sebuah cipherteks menjadi datar.

Kunci dalam teknik kriptografi playfair cipher ini terdiri dari 25 huruf (huruf j dihilangkan, dan dalam pesan asli digantikan dengan huruf i) yang disusun dalam sebuah bujursangkar 5x5. Dengan suatu kata kunci tertentu yang akan menentukan susunan dari bujursangkar kunci ini.

Seperti yang pernah disebutkan sebelumnya dengan penggunaan algoritma playfair cipher ini pemecahan dengan melakukan analisis frekuensi relatif akan semakin sulit karena kemunculan dari huruf dalam suatu cipherteks menjadi *flat*, namun kunci tersebut masih dapat dipecahkan dan pemecahan dengan analisis frekuensi pasangan huruf. Untuk menambah tingkat kesulitan dari pemecahan algoritma ini salah satu teknik yang dapat digunakan adalah dengan membalikkan pesan sehingga dapat mengacaukan analisis frekuensi pasangan huruf yang dilakukan terhadap cipherteks tersebut. Dengan teknik pembalikan pesan ini diharapkan analisis frekuensi pasangan huruf yang sebelumnya dapat digunakan untuk memecahkan pesan menjadi semakin sulit bahkan tidak mungkin digunakan untuk memecahkan pesan bila pesan tersebut disadap.

## II. DASAR TEORI

Teknik Playfair Cipher menggunakan tabel 5x5 yang terdiri dari 25 huruf dan mengandung kata kunci atau frasa tertentu.

Dalam pembuatan kuncinya ada langkah-langkah tertentu yang harus diikuti. Langkah-langkah tersebut antara lain:

1. Pada tabel dilakukan pengisian diawali dengan mengisi kata kunci, dengan menggunakan satu huruf hanya dimunculkan hanya sekali sajadapa tabel (tidak ada pengulangan, misalnya: pewarnaan menjadi pewarn).
2. Tabel yang masih kosong diisi dengan huruf-huruf yang belum dimasukkan berdasarkan urutan abjad

a-z.

- Untuk menyesuaikan jumlah tabel satu huruf dapat dihilangkan dengan menghapus "Q" atau mengganti huruf "I" dengan huruf "J" atau huruf lain berdasarkan kesepakatan.
- Urutan penulisan kunci dapat dilakukan bervariasi boleh dari kiri ke kanan ataupun spiral mengikuti bentuk tabel sehingga kunci yang dihasilkan dapat bervariasi.

Sebagai contoh misalnya diberikan suatu kata kunci "Cahaya matahari", dengan mengikuti urutan langkah-langkah diatas maka akan diperoleh tabel kunci sebagai berikut ini:

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

Setelah kunci diperoleh maka untuk pesan yang akan dienkripsi dilakukan modifikasi pesan sehingga memudahkan dalam melakukan pengenkripsian. Langkah-langkah yang perlu dilakukan antara lain:

- Ganti huruf J (bila ada) dengan I (jika metode ini yang digunakan)
- Tulis pesan dalam pasangan huruf (bigram).
- Jangan sampai ada pasangan huruf yang sama. Jika ada, sisipkan Z ditengahnya
- Jika jumlah huruf ganjil, tambahkan huruf tertentu di akhir pesan.

Untuk melakukan enkripsi langkah-langkah algoritma yang perlu diikuti antara lain adalah:

- Bila dua huruf yang berpasangan terdapat pada baris kunci yang sama maka setiap huruf digantikan dengan huruf di kanannya.
- Bila dua huruf yang berpasangan terdapat pada kolom kunci yang sama maka tiap huruf diganti dengan huruf di bawahnya.
- Bila dua huruf yang berpasangan tidak pada baris yang sama atau kolom yang sama, maka huruf pertama diganti dengan huruf pada perpotongan baris huruf pertama dengan kolom huruf kedua. Huruf kedua diganti dengan huruf pada titik sudut keempat dari persegi panjang yang dibentuk dari 3 huruf yang digunakan sampai sejauh ini.

Sebagai contoh pembuatan pengenkripsian

(berdasarkan referensi [2]) :

Plainteks: GOOD BROOMS SWEEP CLEAN  
 → Tidak ada huruf J, maka langsung tulis pesan dalam pasangan huruf:  
GO OD BR OZ OM SZ SW EZ EP CL EA NZ

Kunci (yang sudah diperluas) ditulis kembali sebagai berikut:

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

Plainteks (dalam pasangan huruf):

GO OD BR OZ OM SZ SW EZ EP CL EA NZ

Cipherteks:

**FP UT EC UW PO DV TV BV CM BG CS DY**

Enkripsi OD menjadi **UT** ditunjukkan pada bujursangkar di bawah ini:

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

titik sudut  
ke-4  
↓

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

Berdasarkan contoh diatas kita dapat melihat tahap-tahap pengenkripsian dalam playfair cipher, dan dapat terlihat juga kenapa algoritma ini dapat mudah dipecahkan dengan menggunakan analisis frekuensi pasangan huruf. Dengan penyesuaian antara frekuensi pasangan huruf yang sering keluar dalam suatu bahasa dengan pasangan huruf yang sering keluar dalam hasil enkripsi, kemungkinan besar suatu cipherteks yang dienkripsi dengan menggunakan metode playfair cipher dapat dipecahkan dengan benar.

Untuk menghindari pemecahan dengan frekuensi pasangan huruf salah satu metode yang cukup mudah dilakukan adalah dengan membalik pesan, Penyadap yang tidak mengetahui informasi bahwa cipherteks yang diperoleh adalah cipherteks yang terbalik tentu saja tidak akan dapat memecahkan cipherteks tersebut dengan benar. Dan kemungkinan besar tidak akan memperoleh solusi yang benar dari cipherteks tersebut.

### III. STUDI KASUS PENDEKRIPSAN PLAYFAIR CIPHER

#### A. Pemecahan Dengan Metode Pasangan Huruf

Playfair cipher dapat dipecahkan dengan menggunakan metode pengecekan frekuensi pasangan huruf, metode ini akan menyesuaikan pasangan huruf yang sering keluar pada suatu bahasa dengan pasangan huruf yang sering keluar pada chiperteks. Sebagai contoh, berikut ini adalah contoh permasalahan dan pemecahan dengan menggunakan playfair cipher dengan metode pengecekan pasangan huruf.

Chipertext :

OR HY EK RK RU PH BO OW IH KR YK FW EK OI  
NR KR YK FW EK AF AXAT VA KU GX OW YH VM  
EI FL HT QT XG AB LO LZ RH EK KU AE MF QH AI  
EK HY KY QE OW IH KR UG FT ZN AI ZS FC LO TL  
PH TF BL LZ RH EK RQ QR RH OL CI ZS XL OF VD  
RE IK KR HR QK OD VK RO CI EK RH RQ LO OD  
VK KZ LI OL NR RL KI EK HU XZ KE AF XK SI LI

OW VC KU QE FW OR HY EK HU XZ KE MW AZ EK  
HY FW TB KU GX ZS VL LS DS HY EK HU XZ KE  
FL FU CI EK HY FW TB KU GX KR WL SD UH IC  
XZ KE OW IH KR HR AF UK PH OZ BZ OW IH KR  
HR AF AG AT OZ BZ EK RY FT OK FL FU CI ZS XL  
OF VD RE IK KR HR QK OW KY MU BO KQ RE QR  
YK ON KR AF ER KA NI UK MU WF ER AF ER WM  
TA RA OR RH OU ZS FV LF RE KR YK YG OW UK  
OW XL QE FW OR HY EK RQ OR RH OQ YH HE KR  
YK YG OW UK MW AZ EK RQ OR RH SW LZ TY RO  
CI ZN AF XG OU ZS VL LS DS HY EK KY KY MU  
BO KU EX OW IH KR HR AF UK PH OZ BZ OW IH  
KR HR AF AG AT OZ BZ EK KU HQ IO XI FL FU CI  
ZS XL OF VD RE IK KR AF ER EA CI RH EK KU EX  
QK MS EK RH HY NI IS QT VU LW RU CI UH HI EF  
MK UA CI UM YG RU WF CI ZN AF XG OU ZS VL  
LS DS HY EK HY EF MK UA CI SL CI OW IH KR MS  
EK RH HY AF ER KA KR WL SD UH XL RU OL CI  
ZS XL FA EK OR ZN AF XK SI LI EK TQ ZS XL OF  
VD RE IK KR SL CI ME LI LQ HP KP RE OR ZI BO  
KY HY QK FW ZO ZM SL ON OL CI EH KY KU IO  
EK HU OW IH RL KN RU WM EA ZN NF EK UK YK  
XY OZ RO BD NL HF ZO ZK IN KR FT ML TF UA  
XB ZO XL OW XY RN LO GX IN KR SL CI ME LI LQ  
HY PH PK RO NZ IO VU OW KO QK FW ZO KX KY  
HY LW DB AT XY BZ NI EK TY HT ZO XL OW IH  
HR YK XS RU TF BZ MW OY RN ZN KL KY HY ZO  
ZN LW DB AT XY BZ NI EK TY HT ZO XL OW XV  
LI OL NR RL NZ RN LO ZS IS FL CI EK RH RQ LO  
HP TQ ZO MS CI EK RH RQ LO ZA TW ZO ZK KR  
EK FT XI FL FU CI ZS XL OF VD RE IK KR HR QK  
OD VK KO ZO EK KY KY MU BO TU IR KR XB IE  
UO QE FW OR RE KR FL FD TA ZR KR OZ VK RO  
CI UH KI EK RP UK HM RU XG OX ZB OK AZ FW  
BX RU OU BO OW XI FL XU OW XF RU KA OW VD  
RE IK KR GW HU XZ KE OX ON KR YK YG OW UK  
AI EK KU EX NI ZX PH OD VK NI ON KR YK FW  
EK OW XY RN LO GX SZ LI RF YH RN SZ HR OR  
OD VK KO EK KP HR OR RH OD VK KI NI ZS PH  
TW EK HY UF OW IH KR UH XG UK HA XZ KE IK  
SZ LZ RH ON KR OZ VK EK RU SO AZ LF RE KR  
OK FW XK LI UK KI EK RP ZO EK KY KY MU BO  
TU IR KR XB IE SZ DZ HU XZ KE IO EK KY RU.

Langkah-langkah yang dilakukan untuk memecahkan pesan:

Dari proses penerjemahan pasangan bigram ditemukan pasangan:

KR=49,  
EK=45,  
RH=24,  
OW=24,  
KK=23,  
CI=20,  
KY=17,  
LO=17,  
LH=17,

HY=17,  
 ZO=16,  
 HR=16,  
 OZ=15,  
 ZS=14

Berdasarkan analisis frekuensi pasangan kata diperoleh pasangan paling sering keluar adalah th dan he, jadi kemungkinan terbesar adalah KR adalah HE dan EK adalah TH. Dari dua translasi tersebut kemungkinan besar bahwa E,K,T,H,R ada pada satu kolom ERHKT.

Karena kemungkinan sebagian besar huruf yang mengikuti HE adalah T, karena pasangan huruf terbanyak mengikuti KR adalah IH, IK, IN, OK, ON, ZK, jadi kemungkinan huruf IOZN berada pada kolom yang sama dengan T sehingga pada kolom tersebut kemungkinan adalah:

TNOIZ sehingga kemungkinan bila dipetakan adalah

E	R	H	K	T
				N
				O
				I
				Z

Hasil dari pengimplementasian pemetaan di atas diperoleh EK OR menjadi TH \*T, kemungkinan besar O adalah A, dan bila itu benar diperoleh kemungkinan untuk membentuk water dalam teks digunakan.

E	R	H	K	T
Q	W			N
	A			O
				I
				Z

Dengan mencoba beberapa kemungkinan pembentukan kata diperoleh translasi beberapa bagian berikut :

E	R	H	K	T
Q	W			N
U	A			O
Y				I
P		V	G	Z

Setelah diimplementasi lebih lanjut dengan kemungkinan berbagai kata yang ada dengan berbagai kemungkinan bahasa Inggris di peroleh :

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

Setelah di dekripsi maka diperoleh cipherteks:

“genesis the begin xning in the begin xning x god created the heavens and the earth now the earth was form less x sand empty darknes x was over the surface of the dex epan d the spirit of god was hovering over the waters and gods said let x there be light and there was light gods saw that x the light was go x od and these separated the light from the darknes x god cal x led the light day and the darknes x she cal x led night and there was evening and there was morning the first day and gods said let x there be an expanse between the water to separate water from waters o god made the expanse and separated the water under the expanse from the water above it and it was x so god cal x led the expanse sky and there was evening and there was morning the second x day and gods said let x the water under the sky be gathered to x one place and let dry ground ap x pear and it was x so god cal x led the dry ground land and the ga thered waters she cal x led seas and gods saw that it was go x od then gods said let x the land produce vegetation sex ed bearing plants and trees on the land that bear fruit with sex ed in it ac x cording to their various kinds and it was x so the land produced vegetation plants bearing sex ed ac x cording to their kinds and trees bearing fruit with sex ed in it ac x cording to their kinds and gods saw that it was go x od and there was evening and there was morning the third x day and gods said let x there be lights in the expanse of the sky to separate the day from the night and let x them serve as x sign stom ark seasons and x days and years and let x them be lights in the expanse of the sky to give light on the earth and it was x so god made tw o great lights the greater light x to govern the day and the lesser light x to govern the night the also made the stars god set x them in the expanse of the sky to give light on the x ea”.

Dari contoh pemecahan di atas dapat dilihat betapa playfair cipher dapat dengan mudah dipecahkan dengan menggunakan pengecekan frekuensi pasangan huruf. Untuk mengatasi ini kita dapat memodifikasi pesan ataupun cipherteks sehingga penyadap yang tidak memiliki informasi bahwa pesan dibalik tidak dapat memecahkan pesan tersebut dengan pengecekan frekuensi pasangan huruf.

## B. Modifikasi Pembalikan Pesan pada Playfair Cipher

Dengan membalikkan pesan maka akan diperoleh cipherteks yang terbalik sebagai berikut:

UR YK KE OI EK ZX UH ZD ZS EI BX RK RI UT  
OB UM YK YK KE OZ PR KE IK KU IL KX WF KO  
RK ER FL ZA OS UR KE KV ZO RK NO HR ZL ZS KI  
EK ZX AH KU GX HU RK HI WO FU YH KE WT HP  
SZ IN IK KV DO HR RO RH PK KE OK KV DO RO  
RH ZS NR HY FR IL ZS XG OL NR YX WO KE WF  
KY RK NO IN KV DO HP XZ IN XE UK KE IA KU  
WO GY KY RK NO XO EK ZX UH WG RK KI ER DV  
WO AK UR FX WO UX LF IX WO OB UO UR XB WF  
ZA KO BZ XO GX UR MH KU PR KE IK HU IC OR  
KV ZO RK RZ AT DF LF RK ER RO WF EQ OU EI  
BX RK RI UT OB UM YK YK KE OZ OK KV DO KQ  
RH RK KI ER DV FO LX SZ IC UF LF IX TF KE RK  
KZ OZ WT AZ OL QR HR KE IC SM OZ QT PH OL  
QR HR KE IC LF SI SZ OL NR ZN LR RN LO IL VX  
WO LX OZ TH YT KE IN ZB YX TA BD WL NZ OZ  
YH YK LK NZ NR YO WM ZB FT UR SX KY RH HI  
WO LX OZ TH YT KE IN ZB YX TA BD WL YH YK  
XK OZ WF KQ OK WO UV OI ZN OR KP HP YH QL  
IL EM IC LS RK NI XG OL NR YX WO LX OZ BX AU  
FT LM TF RK NI KZ OZ FH LN DB OR ZO YX KY  
KU KE FN NZ AE MW UR NK LR HI WO UH KE OI  
UK YK HE IC LO NO LS MZ OZ WF KQ YH YK OB  
IZ RO ER PK PH QL IL EM IC LS RK KI ER DV FO  
LX SZ QT KE IL IS KX FA NZ RO KE AF LX SZ IC  
LO UR LX HU DS LW RK AK RE FA YH HR KE SM  
RK HI WO IC LS IC AU KM FE YH KE YH SD SL LV  
SZ UO GX FA NZ IC FW UR GY MU IC AU KM FE  
IH HU IC UR WL UV TQ SI IN YH HR KE SM KQ XE  
UK KE HR IC AE RE FA RK KI ER DV FO LX SZ IC  
UF LF IX OI QH UK KE ZB ZO TA GA FA RH RK HI  
WO ZB ZO HP KU FA RH RK HI WO XE UK OB UM  
YK YK KE YH SD SL LV SZ UO GX FA NZ IC OR YT  
ZL WS HR RO QR KE ZA WM KU WO GY KY RK EH  
HY QO HR RO QR KE YH RO WF EQ LX WO KU  
WO GY KY RK ER FL VF SZ UO HR RO AR AT MW  
RE FA RE FW UM KU IN AK RE FA RK NO KY RQ  
ER QK OB UM YK WO KQ RH RK KI ER DV FO LX  
SZ IC UF LF KO TF YR KE ZB ZO TA GA FA RH RK  
HI WO ZB ZO HP KU FA RH RK HI WO EK ZX CI  
HU DS LW RK XG UK BT WF YH KE IC UF LF EK  
ZX UH KE YH SD SL LV SZ XG UK BT WF YH KE  
ZA WM EK ZX UH KE YH RO WF EQ UK CV WO IL  
IS KX FA EK ZX UH KE IK LR RN LO IL ZK KV DO  
OL QR HR KE IC OR KV DO KQ RH RK KI ER DV  
FO LX SZ IC LO HR RQ QR KE HR ZL LB FT HP LT  
OL CF SZ IA NZ TF GU RK HI WO EQ YK YH KE IA  
HQ FM EA UK KE HR ZL OL BA GX TQ TH LF IE  
MV HY WO XG UK AV TA XA FA KE WF KY RK  
RN IO KE WF KY RK HI WO OB HP UR KR KE YH  
RO RH LV SZ GK OZ BI OZ PK QK KE OZ ZB ZO IB  
XZ KQ RK KO XO TQ KP.

Bila pesan dibalikkan seperti diatas maka bila seseorang mencoba untuk melakukan enkripsi dengan menggunakan metode analisis frekuensi pasangan huruf akan memperoleh hasil sebagai berikut ini:

Frekuensi huruf terbanyak yang diperoleh adalah:

RK=49,  
KE=45,  
HR=24,  
WO=24,  
KK=23,  
IC=20,  
YK=17,  
OL=17,  
HL=17,  
YY=17,  
OZ=16,  
RH=16,  
ZO=15,  
SZ=14.

Bila dilakukan analisis dari hasil diatas dan bila disesuaikan dengan frekuensi kemunculan pasangan huruf bahasa inggris dimana pasangan paling sering keluar adalah th dan he, yang kemungkinan terbesar RK adalah HE dan KE adalah TH. Namun bila dilakukan pemetaan tidak akan diperoleh hasil yang tepat karena itu harus dicoba kemungkinan lain bahwa saja salah satu dari pasangan huruf tersebut dicoba dipasangkan ke pasangan huruf yang lain yang mungkin.

Dari contoh pemasangan ini saja sudah diperoleh hasil yang berbeda jauh dengan kunci awal yang seharusnya menjadi kunci dari cipherteks tersebut. Bila proses enkripsi dilanjutkan, pasti akan diperoleh kunci yang menyimpang dari hasil awal, dan dengan demikian hasil dekripsi pesan yang diperoleh tidak akan berhasil didapatkan. Dengan pembuktian ini, terlihatlah pengaruh dari pembalikan pesan terhadap hasil dekripsi dari suatu chiperteks dengan metode playfair cipher.

Pesan yang terbalik, akan menghasilkan cipherteks yang terbalik juga, sehingga bila seseorang ingin memecahkan pesan tersebut dengan metode analisis frekuensi pasangan huruf, orang tersebut akan mengalami kesulitan yang jauh lebih besar dan seringkali tidak ada solusi yang benar

## IV. KESIMPULAN

Dengan pemaparan yang telah dilakukan pada bagian-bagian sebelumnya, maka dapat ditarik kesimpulan mengenai teknik playfair cipher khususnya dengan modifikasi pembalikan pesan yaitu:

1. Tingkat keamanan metode penggunaan playfair cipher dengan modifikasi pembalikan pesan dapat menjadi lebih baik daripada teknik playfair cipher biasa, dan teknik yang sangat mudah untuk diterapkan ini dapat menutupi

kelemahan dari playfair cipher yaitu dapat dipecahkan dengan teknik analisis frekuensi pasangan huruf.

2. Banyak metode lain yang dapat digunakan untuk memberikan variasi pada metode playfair cipher sehingga keamanan teknik ini meningkat dan karena mudahnya penggunaan dari teknik playfair cipher ini tidak heran teknik ini sangat populer digunakan untuk mengenkripsi pesan-pesan penting.

## V. UCAPAN TERIMA KASIH

Melalui bagian ini penulis ingin mengucapkan terima kasih kepada Tuhan YME atas segala berkat yang diberikan sehingga karya tulis ini dapat diselesaikan, kepada dosen Kriptografi pak Rinaldi Munir atas bimbingannya dalam semester ini, kepada orangtua dan sahabat penulis yang telah banyak mendukung penulis dalam berbagai hal.

## DAFTAR PUSTAKA

- [1] Bishop, David, Introduction to Cryptography with Java Applet, Jones and Bartlett's Publisher, 2003.
- [2] Slide perkuliahan IF3058 Kriptografi, Algoritma Kriptografi Klasik (Bagian 3)

## PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 23 Maret 2011

ttd



Desfrianta Salmon Barus  
13508107