PERBANDINGAN *PLAYFAIR CIPHER* DENGAN *3D PLAYFAIR CIPHER* PADA PENGAMANAN CITRA

SKRIPSI

Oleh
Rika Ayu Sukmawati
NIM 151810101024

JURUSAN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS JEMBER
2019

PERBANDINGAN *PLAYFAIR CIPHER* DENGAN *3D PLAYFAIR CIPHER* PADA PENGAMANAN CITRA

SKRIPSI

Diajukan guna memenuhi tugas akhir dan memenuhi salah satu syarat untuk menyelesaikan Program Studi Matematika (S1) dan mencapai gelar Sarjana Sains

Oleh
Rika Ayu Sukmawati
NIM 151810101024

JURUSAN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS JEMBER
2019

PERSEMBAHAN

Skripsi ini saya persembahkan untuk:

1. Kedua Orang tua saya tercinta, Bapak saya Moh Ma'ruf, Mama saya Ernawati, adik-adik saya Ahmad Fiqih Firdaus dan M fathir Akbar, serta keluarga besar saya yang senantiasa memberi dukungan dan do'a;
2. Guru-guru dan dosen dari taman kanak-kanak hingga perguruan tinggi;
3. Almamater Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Jember, SMAN 4 Jember, SMPN 4 Jember, SDN Sumbersari 3 Jember, dan TK Dharma Indria II;
4. Hadi Sutrisno yang senantiasa menemani, memberi dukungan, dan do'a;
5. Sahabat saya Intan Puspa Dewi Agusti, Bunda (Izdihar Salsabila), Nirmalawati H, Yessica Afriane S, Nursiana Suci W, "Istri Sholeha" (Intan, Nadiya, Rivi, Mitha, Eris, dan Mela), Zhafir Zarfani P, dan Rulita Irma Ristamaya yang senantiasa selalu memberi dukungan dan do'a;
6. Seluruh teman-teman "SIGMA" 2015 dan "UKM SPORA" yang tidak dapat disebutkan satu per satu yang telah memberikan motivasi serta dukungannya selama ini.

MOTTO

Bermimpilah, tapi jangan terlelap. Bangun, lalu wujudkan!
(Rika Ayu Sukmawati)

Usaha tanpa do'a? Atau do'a tanpa usaha? Itu sama saja dengan bohong, karena mereka selalu berdampingan.
(Rika Ayu Sukmawati)

PERNYATAAN

Saya yang bertanda tangan di bawah ini:

Nama : Rika Ayu Sukmawati

NIM : 151810101024

menyatakan dengan sesungguhnya bahwa skripsi yang berjudul "Perbandingan *Playfair Cipher* dengan *3D Playfair Cipher* pada Pengamanan Citra" adalah benar-benar hasil karya sendiri, kecuali kutipan yang sudah saya sebutkan sumbernya, belum pernah diajukan pada institusi mana pun, dan bukan karya jiplakan. Saya bertanggung jawab atas keabsahan dan kebenaran isinya sesuai dengan sikap ilmiah yang harus dijunjung tinggi.

Demikian pernyataan ini saya buat dengan sebenarnya, tanpa ada tekanan dan paksaan dari pihak manapun serta bersedia mendapat sanksi akademik jika ternyata di kemudian hari pernyataan ini tidak benar.

Jember, April 2019

Yang menyatakan,

Rika Ayu Sukmawati

NIM 151810101024

SKRIPSI

PERBANDINGAN *PLAYFAIR CIPHER* DENGAN *3D PLAYFAIR CIPHER* PADA PENGAMANAN CITRA

Oleh:

Rika Ayu Sukmawati

NIM. 151810101024

Pembimbing

Dosen Pembimbing Utama : Abduh Riski, S.Si., M.Si.

Dosen Pembimbing Anggota : Ahmad Kamsyakawuni, S.Si., M.Kom.

PENGESAHAN

Skripsi berjudul "Perbandingan *Playfair Cipher* dengan *3D Playfair Cipher* pada Pengaman Citra" telah diuji dan disahkan pada:

hari, tanggal :

tempat : Fakultas Matematika dan Ilmu Pengetahuan Alam
Universitas Jember

Tim Penguji:

Ketua,	Anggota I,
Abduh Riski, S.Si., M.Si.	Ahmad Kamsyakawuni, S.Si., M.Kom.
NIP 199004062015041001	NIP 197211291998021001
Anggota II,	Anggota III,
Kiswara Agung Santoso, S.Si., M.Kom.	Kusbudiono, S.Si., M.Si.
NIP 197209071998031003	NIP 197704302005011001

Mengesahkan
Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam
Universitas Jember

Drs. Sujito., Ph.D.
NIP 196102041987111001

RINGKASAN

Perbandingan *Playfair Cipher* dengan *3D Playfair Cipher* pada Pengamanan Citra; Rika Ayu Sukmawati, 151810101024; 2019: 98 Halaman; Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Jember.

Zaman teknologi saat ini, perkembangan pengiriman pesan semakin canggih dengan munculnya banyaknya aplikasi yang mewadahi masyarakat agar lebih mudah mengirim pesan tetapi kecanggihan ini pula juga menyebabkan semakin mudahnya pihak ketiga mengakses atau menyabotase isi pesan tersebut, maka dibutuhkan suatu teknik yang dinamakan kriptografi untuk mengamankan isi pesan. Kriptografi merupakan suatu ilmu untuk melindungi atau menyembunyikan pesan agar aman dan tidak diketahui oleh pihak ketiga dengan cara mengubah isi pesan asli menjadi kode–kode yang sulit dimengerti maknanya.

Pada penelitian ini membahas tentang peningkatan keamanan pada penyandian citra menggunakan algoritma *Playfair Cipher* dan *3D Playfair Cipher*. Proses enkripsi menggunakan *Playfair Cipher* dan *3D Playfair Cipher* tediri dari tiga tahap yaitu mensubstitusikan kunci kedalam matriks kunci, membagi piksel citra menjadi digram untuk *Playfair Cipher* dan trigram untuk *3D Playfair Cipher* serta proses enkripsi itu sendiri. Hasil penyandian citra menggunakan *Playfair Cipher* dan *3D Playfair Cipher* terlihat acak. Proses dekripsi menggunakan *Playfair Cipher* dan *3D Playfair Cipher* berhasil mengembalikan *cipherimage* menjadi *plainimage*.

Berdasarkan data penelitian yang terdiri dari lima kunci dan sepuluh citra yang telah diuji, hasil dari analisis histogram menghasilkan histogram *3D Playfair* lebih merata dibandingkan histogram *Playfair Cipher*, terlihat juga dari perhitungan X^2 bahwa hasil yang diperoleh menggunakan *3D Playfair Cipher* lebih kecil dibandingkan hasil yang diperoleh menggunakan *Playfair Cipher*. Hasil perhitungan NPCR yang diperoleh menggunakan kunci KRITO adalah 97,62% hingga 99,56%, kunci Sigma15 adalah 97,61% hingga 99,49%, kunci

Himatika adalah 97,65% hingga 99,58%, kunci 1234567890 adalah 97,70% hingga 99,50%, dan kunci !@+$%*)#_(= adalah 97,69% hingga 99,55%. Hasil NPCR dari proses enkripsi berdasarkan 50 data yang telah didapat, 38 diantaranya menunjukkan bahwa *Playfair Cipher* lebih besar daripada *3D Playfair Cipher*, karena *pixel* pada citra mengalami perubahan setelah dilakukan proses enkripsi. Hasil perhitungan UACI yang diperoleh menggunakan kunci KRITO adalah 19,46% hingga 41,16%, kunci Sigma15 adalah 19,68% hingga 41,11%, kunci Himatika adalah 19,70% hingga 41,11%, kunci 1234567890 adalah 19,14% hingga 41,18%, dan kunci !@+$%*)#_(= adalah 19,19% hingga 41,21%. Hasil UACI dari proses enkripsi berdasarkan 50 data yang telah didapat, 36 diantaranya menunjukkan bahwa *3D Playfair Cipher* lebih besar daripada *Playfair Cipher*.

Secara visual hasil dari enkripsi *Playfair Cipher* dan *3D Playfair Cipher* terlihat acak dan rata. Hasil dari analisis histogram menghasilkan histogram *3D Playfair* lebih aman daripada *Playfair Cipher* karena histogram *3D Playfair* lebih merata dibandingkan histogram *Playfair Cipher*, terlihat juga dari perhitungan X^2 bahwa hasil yang diperoleh menggunakan *3D Playfair Cipher* lebih kecil dibandingkan hasil yang diperoleh menggunakan *Playfair Cipher*. Hasil dari NPCR menghasilkan *Playfair Cipher* lebih aman daripada *3D Playfair Cipher* karena nilai NPCR *Playfair Cipher* lebih besar daripada *3D Playfair Cipher* hal ini dikarenakan pixel pada citra mengalami perubahan setelah dilakukan proses enkripsi. Hasil dari UACI menghasilkan *3D Playfair Cipher* lebih aman daripada *Playfair Cipher* karna nilai UACI *3D Playfair Cipher* lebih besar daripada *Playfair Cipher*.

PRAKATA

Puji syukur ke hadirat Allah SWT. atas segala rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul "Perbandingan *Playfair Cipher* dengan *3D Playfair Cipher* pada Pengaman Citra". Skripsi ini disusun untuk memenuhi salah satu syarat menyelesaikan pendidikan strata satu (S1) pada Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Jember.

Penyusunan skripsi ini tidak lepas dari bantuan berbagai pihak. Oleh karena itu, penulis menyampaikan terima kasih kepada:

1. Abduh Riski S.Si., M.Si., dan Ahmad Kamsyakawuni, S.Si., M.Kom., selaku Dosen Pembimbing yang telah memberikan bimbingan dan bantuan dalam penyempurnaan skripsi ini;
2. Kiswara Agung Santoso, S.Si., M.Kom., dan Kusbudiono, S.Si., M.Si., selaku Dosen Penguji yang telah memberikan kritik dan saran yang membangun dalam penyempurnaan skripsi ini;
3. Dian Anggraeni, S.Si., M.Si., selaku selaku Dosen Pembimbing Akademik yang telah membimbing dalam pemilihan matakuliah;
4. Seluruh dosen dan staff Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Jember yang telah memberikan banyak ilmu dan pengalaman selama perkuliahan;
5. Seluruh kakak tingkat dan adik tingkat yang telah memberikan bantuan, dukungan dan pengalamannya selama perkuliahan;
6. Semua pihak yang tidak dapat disebutkan satu per satu.

Penulis menerima segala kritik dan saran yang bersifat membangun dari semua pihak demi kesempurnaan penulisan skripsi ini. Akhirnya penulis berharap, semoga skripsi ini dapat bermanfaat.

Jember, April 2019

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

BAB 1. PENDAHULUAN

1.1 Latar Belakang

Zaman teknologi saat ini, perkembangan pengiriman pesan semakin canggih. Hal ini didukung dengan munculnya banyaknya aplikasi yang mewadahi masyarakat agar lebih mudah mengirim pesan. Kecanggihan ini pula menyebabkan pengiriman pesan rentan terhadap pengaksesan pesan oleh pihak ketiga. Hal ini tentunya merugikan pengirim dan penerima, karena menyebabkan pesan yang ingin disampaikan oleh pengirim telah diubah isinya oleh pihak ketiga sehingga apa yang ingin disampaikan oleh pengirim tersampaikan dengan pesan yang berbeda.

Kriptografi (*cryptography*) merupakan ilmu dan seni untuk menjaga pesan agar aman. *Crypto* berarti *secret* yang artinya rahasia dan *graphy* berarti *writing* yang artinya tulisan. Kriptografi (*cryptography*) dapat diartikan sebagai tulisan atau pesan rahasia. Kriptografi muncul atas dasar untuk melindungi pesan dari penulis yang ditujukan kepada penerima agar tidak ada pihak ketiga untuk mengakses pesan yang dikirim dengan cara mengubah isi pesan asli menjadi kode-kode yang sulit dimengerti maknanya. Terdapat beberapa metode yang digunakan pada kriptografi, diantaranya adalah *Playfair Chiper* dan *3D Playfair Cipher*.

Playfair Cipher merupakan salah satu metode kriptografi yang proses enkripsi dan dekripsinya menggunakan tabel berukuran 5×5, dimana setiap bagian dalam tabel kunci mewakili huruf-huruf kapital dalam alfabet dengan menghilangkan huruf J tanpa perulangan yang akan digunakan sebagai acuan proses enkripsi dan dekripsi. *Playfair Cipher* mengenkripsi pasangan huruf (digram) melalui kunci yang telah dituliskan pada tabel. Singh (2015) mengembangkan *Playfair Cipher* menjadi *3D Playfair Cipher* untuk meningkatkan keamanan pesan teks. *3D Playfair Cipher* menggunakan kunci untuk melakukan proses enkripsi dan dekripsi, dimana kunci tersebut dituliskan pada empat tabel berukuran 4×4 yang mendukung 10 digit angka (0-9), 26 huruf (A-Z), dan 28 karakter khusus yang kemudian akan dijadikan acuan untuk proses

enkripsi dan dekripsi. *3D Playfair Cipher* bekerja dalam bentuk trigram sebagai proses enkripsi dan dekripsi.

Pada penelitian kali ini, penulis akan membandingkan *Playfair Cipher* dengan *3D Playfair Cipher* pada pengamanan citra menggunakan kunci berupa teks. Pada proses enkripsi dan dekripsi, kunci teks akan diubah ke dalam bentuk ASCII (*American Standard Code for Information Intercange*) dan kemudian dienkripsi dan didekripsi menggunakan *Playfair Cipher* dan *3D Playfair Cipher*.

1.2 Rumusan Masalah

Berdasarkan latar belakang, dapat dibuat rumusan masalah sebagai berikut:

a. Bagaimana proses enkripsi dan dekripsi citra secara matematis menggunakan *Playfair Cipher* dan *3D Playfair Cipher*?
b. Bagaimana hasil perbandingan tingkat keamanan citra terenkripsi menggunakan *Playfair Cipher* dan *3D Playfair Cipher*?

1.3 Tujuan Penelitian

Tujuan yang ingin dicapai dari penelitian ini adalah sebagai berikut:

a. Mengetahui proses enkripsi dan dekripsi citra secara matematis menggunakan *Playfair Cipher* dan *3D Playfair Cipher*.
b. Mengetahui hasil perbandingan tingkat keamanan citra terenkripsi menggunakan *Playfair Cipher* dan *3D Playfair Cipher*.

1.4 Manfaat Penelitian

Manfaat dari penelitian ini dapat diuraikan sebagai berikut:

a. Menambah pengetahuan dalam mengkaji permasalahan yang berkaitan dengan keilmuan lain seperti komputasi matematika, khususnya pesan yang berupa citra menggunakan *Playfair Cipher* dan *3D Playfair Cipher* yang dianalisis tingkat keamaannya menggunakan analisis histogram, NPCR, dan UACI dengan bantuan program MATLAB, serta permasalahan matematika dalam menyelesaikan masalah tersebut.

b. Memberikan motivasi penelitian lain untuk dapat melanjutkan tentang mengembangkan aplikasi keamanan citra dengan metode yang berbeda.
c. Memberikan motivasi penelitian lain untuk dapat melanjutkan tentang mengembangkan aplikasi keamanan citra menggunakan Playfair Cipher maupun 3D Playfair yang dimodifikasi dengan metode lainnya.

BAB 2. TINJAUAN PUSTAKA

2.1 Kriptografi

Kriptografi merupakan salah satu ilmu di bidang komputasi matematika yang mempelajari tentang bagaimana suatu pesan atau informasi agar tetap aman dan tidak dapat diketahui oleh pihak yang tidak berkepentingan. Menurut Santi (2010) terdapat beberapa aspek yang harus terpenuhi dalam keamanan informasi yaitu aspek kerahasiaan (*confidentiality*), integritas data (*data integrity*), otentifikasi (*authentication*), dan penyangkalan (*non repudiation*). Kriptografi (*cryptography*) merupakan ilmu dan seni untuk menjaga pesan agar aman. *Crypto* berarti *secret* yang artinya rahasia dan *graphy* berarti *writing* yang artinya tulisan. Kriptografi (*cryptography*) dapat diartikan sebagai tulisan atau pesan rahasia. Pesan yang dirahasiakan dinamakan *plaintext*, sedangkan pesan hasil penyandian disebut *ciphertext*. Proses penyandian *plaintext* menjadi *ciphertext* disebut enkripsi dan proses membalikkan *ciphertext* menjadi *plaintext* disebut dekripsi.

2.2 *Playfair Cipher*

Playfair Cipher adalah salah satu metode dari kriptografi yang menggunakan bentuk tabel berukuran 5×5 sebagai acuan untuk melakukan proses enkripsi dan dekripsi. *Playfair Cipher* hanya mengenkripsikan *plaintext* berupa huruf besar tanpa huruf J dan tidak berulang. *Playfair Cipher* menggunakan metode pasangan huruf (bigram) untuk mengenkripsikan dan mendekripsi melalui kunci yang telah diinputkan pada tabel.

Gambar 2.1 Proses enkripsi dan dekripsi pada *Playfair Cipher*

Nurkifli (2014) menuliskan beberapa aturan dan proses enkripsi maupun dekripsi pada *Playfair Cipher*. Berikut beberapa aturan yang perlu dipersiapkan sebelum dilakukannya enkripsi:

a. *Playfair Cipher* mengenkripsi *plaintext* berupa huruf besar selain huruf J. Spasi, karakter yang bukan huruf besar, dan huruf J harus dihilangkan dari *plaintext.*
b. Apabila terdapat huruf J pada *plaintext*, maka digantikan dengan huruf I.
c. *Plaintext* yang akan dienkripsi dituliskan dalam pasangan huruf (bigram).
d. Apabila ada huruf yang sama dalam pasangan huruf, maka disisipkan huruf X atau Z di tengahnya. Huruf yang disisipkan sebaiknya huruf X, karena kemungkinan terdapat huruf X yang sama dalam bigram sangat kecil.
e. Apabila jumlah huruf pada *plaintext* adalah ganjil, maka dipilih sebuah huruf sembarang untuk ditambahan di akhir *plaintext*.

Ilustrasi tabel yang akan dijadikan kunci untuk menyelesaikan proses enkripsi dan dekripsi pada *Playfair Cipher* seperti pada Tabel 2.1.

Tabel 2.1 Kunci pada *Playfair Cipher*

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

Setelah dilakukan aturan-aturan dan didapat rangkaian kunci pada *Playfair Cipher*, rangkaian kunci tersebut diperluas.

Berikut merupakan langkah-langkah enkripsi *Playfair Cipher*:

a. Apabila ada dua huruf terdapat pada baris kunci yang sama, maka setiap huruf diganti dengan huruf di kanannya.
b. Apabila ada dua huruf terdapat pada kolom kunci yang sama, maka setiap huruf diganti dengan huruf di bawahnya.

c. Apabila ada dua huruf tidak pada baris atau kolom yang sama, maka huruf pertama diganti dengan 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 huruf yang digunakan.

Berikut merupakan langkah-langkah dekripsi *Playfair Cipher*:

a. Apabila ada dua huruf terdapat pada baris kunci yang sama maka tiap huruf diganti dengan huruf di kirinya.

b. Apabila ada dua huruf terdapat pada kolom yang sama maka tiap huruf diganti dengan huruf di atasnya.

c. 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. Huruf kedua diganti dengan huruf pada titik sudut keempat dari persegi panjang yang dibentuk dari huruf yang digunakan.

Berikut contoh ilustrasi sederhana pada *Playfair Cipher* yang menggunakan tabel kunci sebagai acuan proses enkripsi dan dekripsi seperti pada Tabel 2.2:

Kunci : RXCNY

Tabel 2.2 Kunci pada ilustrasi *Playfair Cipher*

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

a. Enkripsi

Plaintext : HIMATIKA

Digraf : {HI}, {MA}, {TI}, dan {KA}

Enkripsi HI : IK

Enkripsi MA : TG

Enkripsi TI : VG

Enkripsi KA : GE

Ciphertext : IKTGVGGE

b. Dekripsi

Ciphertext : IKTGVGGE

Digraf : {IK}, {TG}, {VG}, dan {GE}

Enkripsi IK : HI

Enkripsi TG : MA

Enkripsi VG : TI

Enkripsi GE : KA

Plaintext : HIMATIKA

2.3 *3D Playfair Cipher*

Singh (2015) menuliskan sebuah jurnal yang isinya mengembangkan *Playfair Cipher* menjadi *3D Playfair Cipher*. *3D Playfair Cipher* dikembangkan melalui tabel yang semula berukuran 5×5 menjadi empat tabel berukuran 4×4 untuk menuliskan kunci sebagai acuan untuk menyelesaikan proses enkripsi dan dekripsi. Ilustrasi tabel yang akan dijadikan acuan untuk menyelesaikan proses enkripsi dan dekripsi pada *3D Playfair Cipher* seperti pada Tabel 2.3.

Tabel 2.3 Kunci pada *3D Playfair Cipher*

TINGKAT 1			
0	1	2	3
4	5	6	7
8	9	A	B
C	D	E	F

TINGKAT 2			
G	H	I	J
K	L	M	N
O	P	Q	R
S	T	U	V

TINGKAT 3			
W	X	Y	Z
!	“	=	$
%	&	‘	(
)	*	+	,

TINGKAT 4			
-	.	/	:
;	<	=	>
?	@	[	\
]	^	_	|

3D Playfair Cipher dikembangkan untuk mengenkripsi dan mendekripsikan 10 angka (0-9), 26 huruf besar alfabet (A-Z), dan 28 karakter khusus tanpa perulangan. *3D Playfair Cipher* menggunakan metode trigram untuk melakukan proses enkripsi dan dekripsi. *3D Playfair Cipher* sama seperti *Playfair Cipher* yang memiliki aturan yang perlu dipersiapkan terlebih dahulu sebelum dilakukan proses enkripsi dan dekripsi, aturan tersebut hanya menginputkan kunci rahasia pada tabel sesuai urutan pada ilustrasi Tabel 2.3 tanpa perulangan. Setelah didapatkan tabel kunci, selanjutnya akan dilakukan proses enkripsi dan dekripsi.

Proses enkripsi pada *3D Playfair Cipher* adalah *plaintext* akan dipecah menjadi trigram (pasangan yang tediri dari tiga huruf). Huruf tambahan X dan Z digunakan untuk memenuhi trigraph, X ditambahkan jika terdapat tersisa satu tempat kosong pada pesan, X dan Z ditambahkan jika terdapat dua tempat kosong. Contohnya LOLLIPOP akan dirubah menjadi {LOL}, {LIP}, {OPX}, dan GOODGRACES menjadi {GOO}, {DGR}, {ACE), {SXZ). Proses enkripsi dan dekripsi menggunakan model *circular,* dimana penggantian huruf dalam trigram akan diganti oleh pesan yang sehubungan dengan posisi huruf dalam trigram di baris, kolom, dan tingkat dengan cara melingkar. Ilustrasi tabel proses enkripsi seperti pada Tabel 2.4.

Tabel 2.4 Proses enkripsi pada *3D Playfair Cipher*

Trigraf *Plaintext*	Trigraf *Plaintext*			Trigraf *Ciphertext*
	Karakter 1	Karakter 2	Karakter 3	
Karakter 1	Baris	Kolom	Tingkat	Karakter 1
Karakter 2	Tingkat	Baris	Kolom	Karakter 2
Karakter 3	Kolom	Tingkat	Baris	Karakter 3

Proses dekripsi sama seperti proses enkripsi yaitu dengan model melingkar, akan tetapi hanya berbeda pada urutannya yaitu baris, tingkat, kolom dalam trigraf. Ilustrasi tabel proses dekripsi seperti pada Tabel 2.5.

Tabel 2.5 Proses dekripsi pada *3D Playfair Cipher*

Trigraf *Ciphertext*	Trigraf *Ciphertext*			Trigraf *Plaintext*
	Karakter 1	Karakter 2	Karakter 3	
Karakter 1	Baris	Tingkat	Kolom	Karakter 1
Karakter 2	Kolom	Baris	Tingkat	Karakter 2
Karakter 3	Tingkat	Kolom	Baris	Karakter 3

Proses dekripsi mendapatkan hasil yang berupa *plaintext*. Huruf penambah X dan Z pada hasil *plaintext* dihilangkan dari trigram.

Berikut contoh ilustrasi sederhana pada *3D Playfair Cipher* yang menggunakan tabel kunci sebagai acuan proses enkripsi dan dekripsi seperti pada Tabel 2.6:

Kunci : HIMATIKA JAYA menjadi HIMATKJY

Tabel 2.6 Kunci pada ilustrasi *3D Playfair Cipher*

TINGKAT 1			
H	I	M	A
T	K	J	Y
0	1	2	3
4	5	6	7

TINGKAT 2			
8	9	B	C
D	E	F	G
L	N	O	P
Q	R	S	U

TINGKAT 3			
V	W	X	Z
!	“	=	$
%	&	‘	(
)	*	+	,

TINGKAT 4			
-	.	/	:
;	<	=	>
?	@	[	\
]	^	_	|

a. Enkripsi

Plaintext : JEMBER

Trigraf : {JEM} dan {BER}

Tabel 2.7 Enkripsi *plaintext* dari JEM menggunakan *3D Playfair Cipher*

Trigraf *Plaintext*	Trigraf *Plaintext*			Trigraf *Ciphertext*
	J	E	M	
J	Baris	Kolom	Tingkat	K
E	Tingkat	Baris	Kolom	J
M	Kolom	Tingkat	Baris	B

Tabel 2.8 Enkripsi *plaintext* dari BER menggunakan *3D Playfair Cipher*

Trigraf *Plaintext*	Trigraf *Plaintext*			Trigraf *Ciphertext*
	B	E	R	
B	Baris	Kolom	Tingkat	9
E	Tingkat	Baris	Kolom	E
R	Kolom	Tingkat	Baris	S

Ciphertext : KJB9ES

b. Dekripsi

Kunci : HIMATIKA JAYA menjadi HIMATKJY

Ciphertext : KJB9ES

Trigraf : {KJB} dan {9ES}

Tabel 2.9 Dekripsi *ciphertext* dari KJB menggunakan *3D Playfair Cipher*

Trigraf *Ciphertext*	Trigraf *Ciphertext*			Trigraf *Plaintext*
	K	J	B	
K	Baris	Tingkat	Kolom	J
J	Kolom	Baris	Tingkat	E
B	Tingkat	Kolom	Baris	M

Tabel 2.10 Dekripsi *ciphertext* dari 9ES menggunakan *3D Playfair Cipher*

Trigraf *Ciphertext*	Trigraf *Ciphertext*			Trigraf *Plaintext*
	9	E	S	
9	Baris	Tingkat	Kolom	B
E	Kolom	Baris	Tingkat	E
S	Tingkat	Kolom	Baris	R

Plaintext : JEMBER

2.4 Citra

Citra adalah gambar (*image*) pada bidang dua dimensi. Citra adalah salah satu media yang memiliki peranan penting sebagai bentuk informasi visual. Citra dapat dilakukan proses komputasi pada program komputer apabila citra didigitalkan terlebih dahulu. Citra memiliki dua jenis yaitu citra *grayscale* dan citra RGB (citra warna atau *truecolor*).

Citra *grayscale* merupakan citra digital yang hanya memiliki satu nilai kanal pada setiap *pixel*-nya, artinya nilai *Red = Green = Blue*. Nilai-nilai tersebut digunakan untuk menunjukkan intensitas warna. Citra yang ditampilkan terdiri atas warna abu-abu, bervariasi pada warna hitam sebagai bagian intensitas terlemah dan putih sebagai intensitas terkuat (Sholehah, 2017).

Citra berwarna yaitu citra yang nilai *pixel*-nya merepresentasikan warna tertentu. Banyaknya warna yang mungkin digunakan bergantung kepada kedalaman *pixel* citra yang bersangkutan. Citra RGB direpresentasikan dalam beberapa kanal yang menyatakan komponen-komponen warna penyusun. Banyak kanal yang digunakan bergantung pada model warna yang digunakan pada citra tersebut (Muhendra, 2016).

2.5 ASCII

ASCII (*American Standard Code for Information Intercange*) merupakan standar internasional dalam kode huruf dan simbol yang bersifat universal. ASCII digunakan oleh komputer dan alat komunikasi lainnya untuk menunjukkan teks (Muhendra, 2016).

ASCII merupakan kode yang digunakan untuk merepresentasikan huruf, angka dan simbol. Jumlah ASCII adalah 250 kode. ASCII 0-127 merupakan kode untuk manipulasi teks, sedangkan ASCII 128-255 merupakan kode untuk manipulasi grafik.

2.6 Analisis Keamanan

2.6.1 Analisis Histogram

Teknik analisis histogram digunakan untuk melihat kesesuaian distribusi warna antara *plainimage* dengan *cipherimage*. Jika histogram *cipherimage* memiliki keragaman distribusi dan memiliki perbedaan yang signifikan dengan *plainimage*, maka dapat dikatakan *cipherimage* tidak memberikan petunjuk untuk melakukan *statistical attack* pada *cipherimage* yang dihasilkan.

Pengujian X^2 digunakan untuk menganalisis keseragaman histogram dari gambar yang terenkripsi. Persamaan nilai dari X^2 untuk gambar yang terenkripsi dari dimensi $m \times n$ seperti pada persamaan 2.1.

$$X^2 = \sum_{i=0}^{255} \frac{(v_i - v_0)^2}{v_0} \quad (2.1)$$

dimana v_i merupakan frekuensi yang diamati dari nilai *pixel* $i(0 \leq i \leq 255)$ dan v_0 merupakan frekuensi yang diharapkan dari sebuah nilai *pixel* i, jadi $v_0 = \frac{m \times n}{256}$, dimana m merupakan panjang citra dan n merupakan lebar citra . Semakin kecil hasil dari X^2 maka tingkat keseragaman dalam histogram semakin merata dan hasil dari pengenkripsian semakin baik (aman), sedangkan semakin besar hasil dari X^2 maka tingkat keseragaman dalam histogram semakin tidak merata dan hasil dari pengenkripsian tentunya semakin tidak baik (tidak aman) (Boriga dkk, 2014).

2.6.2 NPCR

NPCR (*Number of Pixel Change Rate*) adalah perbandingan *pixel gray* antara *plainimage* dengan *cipherimage*. Tujuan pengujian ini yaitu untuk menjamin bahwa pada setiap *pixel* terdapat perubahan elemen warna. NPCR dirumuskan dengan menggunakan persamaan 2.2.

$$\text{NPCR} = \left(\sum_{i=1}^{m}\sum_{j=1}^{n}\sum_{k=1}^{o} \frac{d_{i,j,k}}{T}\right) \times 100\% \quad (2.2)$$

Dengan persyaratan sebagai berikut :

$$d\,(i,j,\text{k}) = \begin{cases} 0, & jika\ C_1(i,j,k) = C_2(i,j,k) \\ 1, & jika\ C_1(i,j,k) \neq C_2(i,j,k) \end{cases}$$

Keterangan :

$d_{i,j,k}$: variabel untuk menghitung banyaknya perbedaan *pixel*

C_1 : *pixel plainimage*

C_2 : *pixel cipherimage*

i : baris

j : kolom

k : kanal

m, n, o : banyaknya dari baris, kolom, dan kanal

T : jumlah total *pixel*

Nilai *d*(*i*,*j*,*k*) adalah banyaknya perbedaan *pixel* yang dikalikan dengan nilai 100% setelah itu dibagi dengan lebar dan tinggi dari citra sampel. Kanal pada setiap jenis citra berbeda, diantaranya *Greyscale* yang memiliki 1 kanal, hitam putih memiliki 2 kanal, dan RGB memiliki 3 kanal. *Cipherimage* dapat dikatakan baik (aman) jika nilai pada indikator NPCR semakin besar (Boriga dkk, 2014).

2.6.3 UACI

UACI (*Unified Averaged Changed Intensity*) merupakan salah satu parameter yang digunakan untuk menganalisa perubahan satu *pixel* dalam *plainimage* yang menyebabkan perubahan besar pada *cipherimage*. UACI dirumuskan dengan menggunakan persamaan 2.3.

$$\text{UACI} = \left(\sum_{i=1}^{m}\sum_{j=1}^{n}\sum_{k=1}^{o}\frac{|C_1(i,j,k)-C_2(i,j,k)|}{F.T}\right)\times 100\% \quad (2.3)$$

Keterangan :

$C_1(i,j,k)$: *plainimage* 1

$C_2(i,j,k)$: *cipherimage* 2

i : baris

j : kolom

k : kanal

m, *n*, *o* : banyaknya dari baris, kolom, dan kanal

T : jumlah total *pixel*

F : nilai *pixel* terbesar pada citra sebesar 255

Cipherimage dapat dikatakan baik (aman) jika nilai pada indikator UACI semakin besar (Boriga dkk, 2014).

BAB 3. METODE PENELITIAN

3.1 Data Penelitian

Data yang digunakan dalam penelitian ini adalah data teks yang akan digunakan sebagai kunci (*key*) dan gambar (citra) yang akan digunakan sebagai *plainimage*. *Key* akan diubah ke dalam bentuk ASCII (*dec*). Kunci yang akan digunakan sebagai berikut:

a. KRIPTO
b. Sigma15
c. Himatika
d. 1234567890
e. !@+$%*)#_(=

Citra yang akan digunakan sebagai *plainimage* ditunjukkan pada Gambar 3.1 sampai Gambar 3.10 sebagai berikut:

Gambar 3.1 Citra Lena

Gambar 3.2 Citra Bunga

Gambar 3.3 Citra Borobudur

Gambar 3.4 Citra Bunga Kombaja

Gambar 3.5 Citra Macan Tutul

Gambar 3.6 Citra *Sunset*

Gambar 3.7 Citra Buah

Gambar 3.8 Citra Gapura

Gambar 3.9 Citra Bukit

Gambar 3.10 Citra Sayur

3.2 Langkah-langkah Penelitian

Langkah-langkah yang akan dilakukan pada penelitian ini, diuraikan sebagai berikut:

a. Studi Literatur

Tahap studi literatur dilakukan dengan mempelajari referensi yang berkaitan dengan kriptografi, *Playfair Cipher*, *3D Playfair Cipher*, citra, ASCII, dan juga mempelajari tentang analisis keamanan yang diantaranya yaitu analisis histogram, NPCR, dan UACI.

b. Proses Penelitian

1) Menginputkan kunci (*key*)

Kunci (*key*) yang berbentuk teks diubah ke dalam ASCII (*dec*). Kunci yang telah berbentuk *dec* diinputkan pada tabel berukuran 16×16 dan empat tabel berukuran 8×8.

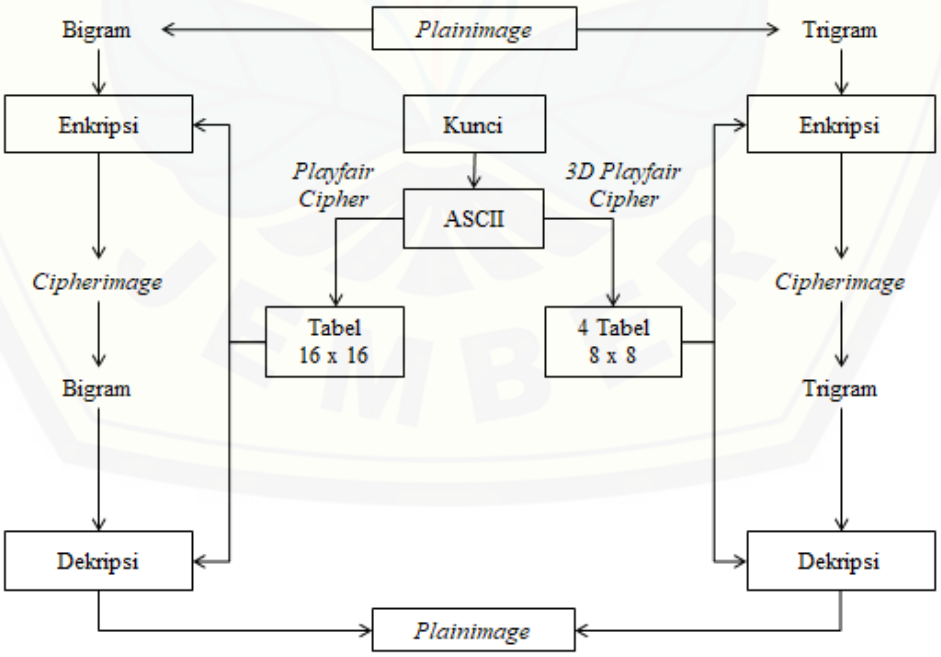
2) Enkripsi *plainimage* menggunakan *Playfair Cipher* dan *3D Playfair Cipher*

Plainimage berbentuk gambar dienkripsi menggunakan *Playfair Cipher* dan *3D Playfair Cipher* dengan metode bigram dan trigram menggunakan tabel sebagai acuan proses enkripsi.

3) Dekripsi *cipherimage* menggunakan *Playfair Cipher* dan *3D Playfair Cipher*

Cipherimage hasil dari proses enkripsi didekripsi menggunakan *Playfair Cipher* dan *3D playfair Cipher* dengan metode bigram dan trigram menggunakan tabel sebagai acuan proses dekripsi.

Langkah-langkah pada proses ini adalah sebagai berikut:



Gambar 3.11 Proses enkripsi dan dekripsi pada *Playfair Cipher* dan *3D Playfair Cipher*

c. Perancangan Program

Tahap perancangan program menggunakan *software* MatLab 2015b dan melakukan perancangan desain GUI (*Graphic User Interface*) seperti tata letak tombol-tombol untuk setiap proses yang dibutuhkan serta letak *properties* pendukung program lainnya.

d. Pembuatan Program

Tahap pembuatan program dilakukan berdasarkan konsep *Playfair Cipher* dan *3D Playfair Cipher* untuk proses enkripsi dan dekripsi kunci berupa teks dan *plainimage* berupa citra dengan metode bigram dan trigram.

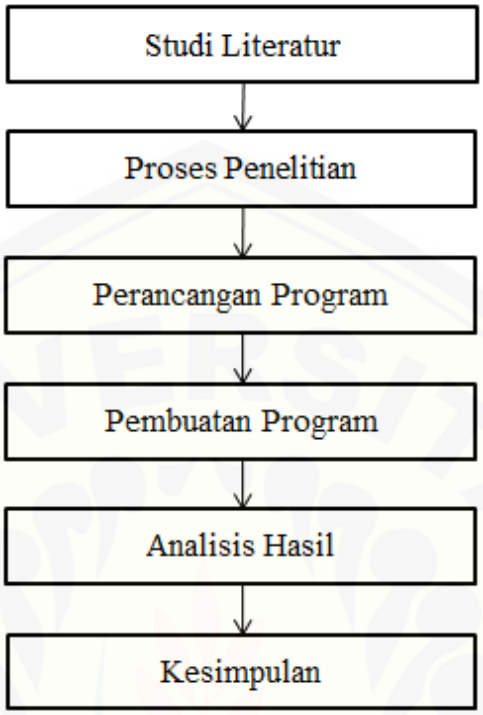
e. Analisis Keamanan Hasil

Tahap analisis keamanan hasil akan dilakukan beberapa skema enkripsi dan dekripsi dengan menggunakan kombinasi lima kunci dan sepuluh citra yang bervariasi, kemudian hasil akan dianalisis keamanaannya dengan analisis histogram, NPCR, dan UACI.

f. Kesimpulan

Tahap kesimpulan diambil kesimpulan dari penelitian yang dilakukan yaitu menganalisis hasil citra yang telah dienkripsi dan didekripsi menggunakan *Playfair Cipher* dan *3D Playfair Cipher*.

Berikut adalah diagram alur penelitian seperti pada Gambar 3.12:



Gambar 3.12 Diagram alur penelitian

BAB 5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan, didapat beberapa kesimpulan sebagai berikut:

a. Proses enkripsi menggunakan *Playfair Cipher* dan *3D Playfair Cipher* berhasil karena terlihat jelas bahwa *plainimage* dan *cipherimage* sangat berbeda secara visual. Begitu juga pada proses dekripsi menggunakan *Playfair Cipher* dan *3D Playfair Cipher* berhasil karena *cipherimage* kembali seperti *plainimage* semula.

b. Hasil perbandingan tingkat keamanan citra terenkripsi menggunakan Playfair Cipher dan 3D Playfair Cipher berdasar analisis histogram, NPCR, dan UACI adalah sebagai berikut:

   1) Berdasarkan hasil analisis histogram, tingkat keamanan citra terenkripsi menggunakan *3D Playfair Cipher* lebih aman daripada *Playfair Cipher*, hal ini dikarenakan perhitungan nilai X^2 *3D Playfair Cipher* lebih kecil daripada *Playfair Cipher* dan grafik histogram *3D Playfair Cipher* lebih merata daripada *Playfair Cipher* karena tidak ada *pixel* yang mendominasi.

   2) Berdasarkan hasil NPCR, tingkat keamanan citra terenkripsi menggunakan *Playfair Cipher* lebih aman daripada *3D Playfair Cipher*, hal ini dikarenakan nilai NPCR *Playfair Cipher* lebih besar daripada *3D Playfair Cipher*.

   3) Berdasarkan hasil UACI, tingkat keamanan citra terenkripsi menggunakan *3D Playfair Cipher* lebih aman daripada *Playfair Cipher*, hal ini dikarenakan nilai UACI *3D Playfair Cipher* lebih besar daripada *Playfair Cipher*.

5.2 Saran

Adapun saran yang perlu diperhatikan untuk penelitian selanjutnya adalah Peneliti selanjutnya dapat menerapkan algoritma *Playfair Cipher* atau *3D Playfair Cipher* yang dikombinasikan dengan algoritma kriptografi lainnya.

DAFTAR PUSTAKA

Boriga, R. E., A. C. Dăscălescu, dan A.V. Diaconu. 2014. A New Fast Image Encryption Scheme Based on 2D Chaotic Maps. *IAENG International Journal of Compuer Science* 41 (4).

Muhendra, A. Z. 2016. Implementasi Kriptografi Affine Cipher pada Citra Digital Hasil Steganografi Metode Parity Coding dengan Pseudo Random Number Generator (PRNG). *Skripsi*. Jember: Universitas Jember.

Nurkifli, E. H. 2014. Modifikasi Algoritma Playfair dan Menggabungkan dengan Linear Feedback Shift Register (LFSR). *SENTIKA 2014*. 366-371.

Santi, R. C. N. 2010. Implementasi Algoritma Enkripsi Playfair pada File Teks. *Jurnal Teknologi Informasi DINAMIK*. 15(1): 27-33.

Sholehah, D. P. T. 2017. Penerapan Algoritma DNA-Vigenere Cipher dengan Kunci Citra Grayscale pada Data Teks. *Skripsi*. Jember: Universitas Jember.

Singh, S., R. Jain, dan P. Deep. Agarwal. 2015. Developing Mobile Message Security Application Using 3D Playfair Cipher Algorithm. *ICACEA*. 838-841.

LAMPIRAN

LAMPIRAN A. ASCII

DEC	OCT	HEX	BIN	Symbol
0	000	00	00000000	NUL
1	001	01	00000001	SOH
2	002	02	00000010	STX
3	003	03	00000011	ETX
4	004	04	00000100	EOT
5	005	05	00000101	ENQ
6	006	06	00000110	ACK
7	007	07	00000111	BEL
8	010	08	00001000	BS
9	011	09	00001001	HT
10	012	0A	00001010	LF
11	013	0B	00001011	VT
12	014	0C	00001100	FF
13	015	0D	00001101	CR
14	016	0E	00001110	SO
15	017	0F	00001111	SI
16	020	10	00010000	DLE
17	021	11	00010001	DC1
18	022	12	00010010	DC2
19	023	13	00010011	DC3
20	024	14	00010100	DC4
21	025	15	00010101	NAK
22	026	16	00010110	SYN
23	027	17	00010111	ETB
24	030	18	00011000	CAN
25	031	19	00011001	EM
26	032	1A	00011010	SUB
27	033	1B	00011011	ESC
28	034	1C	00011100	FS
29	035	1D	00011101	GS
30	036	1E	00011110	RS
31	037	1F	00011111	US
32	040	20	00100000	
33	041	21	00100001	!
34	042	22	00100010	“
35	043	23	00100011	#
36	044	24	00100100	$
37	045	25	00100101	%
38	046	26	00100110	&
39	047	27	00100111	‘

DEC	OCT	HEX	BIN	Symbol
40	050	28	00101000	(
41	051	29	00101001	)
42	052	2A	00101010	*
43	053	2B	00101011	+
44	054	2C	00101100	,
45	055	2D	00101101	–
46	056	2E	00101110	.
47	057	2F	00101111	/
48	060	30	00110000	0
49	061	31	00110001	1
50	062	32	00110010	2
51	063	33	00110011	3
52	064	34	00110100	4
53	065	35	00110101	5
54	066	36	00110110	6
55	067	37	00110111	7
56	070	38	00111000	8
57	071	39	00111001	9
58	072	3A	00111010	:
59	073	3B	00111011	;
60	074	3C	00111100	<
61	075	3D	00111101	=
62	076	3E	00111110	>
63	077	3F	00111111	?
64	100	40	01000000	@
65	101	41	01000001	A
66	102	42	01000010	B
67	103	43	01000011	C
68	104	44	01000100	D
69	105	45	01000101	E
70	106	46	01000110	F
71	107	47	01000111	G
72	110	48	01001000	H
73	111	49	01001001	I
74	112	4A	01001010	J
75	113	4B	01001011	K
76	114	4C	01001100	L
77	115	4D	01001101	M
78	116	4E	01001110	N
79	117	4F	01001111	O
80	120	50	01010000	P
81	121	51	01010001	Q
82	122	52	01010010	R
83	123	53	01010011	S
84	124	54	01010100	T

DEC	OCT	HEX	BIN	Symbol
85	125	55	01010101	U
86	126	56	01010110	V
87	127	57	01010111	W
88	130	58	01011000	X
89	131	59	01011001	Y
90	132	5A	01011010	Z
91	133	5B	01011011	[
92	134	5C	01011100	\
93	135	5D	01011101	]
94	136	5E	01011110	^
95	137	5F	01011111	_
96	140	60	01100000	`
97	141	61	01100001	a
98	142	62	01100010	b
99	143	63	01100011	c
100	144	64	01100100	d
101	145	65	01100101	e
102	146	66	01100110	f
103	147	67	01100111	g
104	150	68	01101000	h
105	151	69	01101001	i
106	152	6A	01101010	j
107	153	6B	01101011	k
108	154	6C	01101100	l
109	155	6D	01101101	m
110	156	6E	01101110	n
111	157	6F	01101111	o
112	160	70	01110000	p
113	161	71	01110001	q
114	162	72	01110010	r
115	163	73	01110011	s
116	164	74	01110100	t
117	165	75	01110101	u
118	166	76	01110110	v
119	167	77	01110111	w
120	170	78	01111000	x
121	171	79	01111001	y
122	172	7A	01111010	z
123	173	7B	01111011	{
124	174	7C	01111100	|
125	175	7D	01111101	}
126	176	7E	01111110	~
127	177	7F	01111111	
128	200	80	10000000	€
129	201	81	10000001	

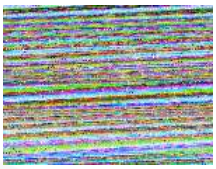
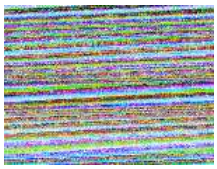
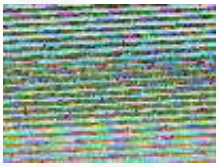
DEC	OCT	HEX	BIN	Symbol
130	202	82	10000010	‚
131	203	83	10000011	*ƒ*
132	204	84	10000100	„
133	205	85	10000101	…
134	206	86	10000110	†
135	207	87	10000111	‡
136	210	88	10001000	ˆ
137	211	89	10001001	‰
138	212	8A	10001010	Š
139	213	8B	10001011	‹
140	214	8C	10001100	Œ
141	215	8D	10001101	
142	216	8E	10001110	Ž
143	217	8F	10001111	
144	220	90	10010000	
145	221	91	10010001	‘
146	222	92	10010010	’
147	223	93	10010011	“
148	224	94	10010100	”
149	225	95	10010101	•
150	226	96	10010110	–
151	227	97	10010111	—
152	230	98	10011000	˜
153	231	99	10011001	™
154	232	9A	10011010	š
155	233	9B	10011011	›
156	234	9C	10011100	œ
157	235	9D	10011101	
158	236	9E	10011110	ž
159	237	9F	10011111	Ÿ
160	240	A0	10100000	
161	241	A1	10100001	¡
162	242	A2	10100010	¢
163	243	A3	10100011	£
164	244	A4	10100100	¤
165	245	A5	10100101	¥
166	246	A6	10100110	¦
167	247	A7	10100111	§
168	250	A8	10101000	¨
169	251	A9	10101001	©
170	252	AA	10101010	ª
171	253	AB	10101011	«
172	254	AC	10101100	¬
173	255	AD	10101101	
174	256	AE	10101110	®

DEC	OCT	HEX	BIN	Symbol
175	257	AF	10101111	¯
176	260	B0	10110000	°
177	261	B1	10110001	±
178	262	B2	10110010	²
179	263	B3	10110011	³
180	264	B4	10110100	´
181	265	B5	10110101	µ
182	266	B6	10110110	¶
183	267	B7	10110111	·
184	270	B8	10111000	¸
185	271	B9	10111001	¹
186	272	BA	10111010	º
187	273	BB	10111011	»
188	274	BC	10111100	¼
189	275	BD	10111101	½
190	276	BE	10111110	¾
191	277	BF	10111111	¿
192	300	C0	11000000	À
193	301	C1	11000001	Á
194	302	C2	11000010	Â
195	303	C3	11000011	Ã
196	304	C4	11000100	Ä
197	305	C5	11000101	Å
198	306	C6	11000110	Æ
199	307	C7	11000111	Ç
200	310	C8	11001000	È
201	311	C9	11001001	É
202	312	CA	11001010	Ê
203	313	CB	11001011	Ë
204	314	CC	11001100	Ì
205	315	CD	11001101	Í
206	316	CE	11001110	Î
207	317	CF	11001111	Ï
208	320	D0	11010000	Ð
209	321	D1	11010001	Ñ
210	322	D2	11010010	Ò
211	323	D3	11010011	Ó
212	324	D4	11010100	Ô
213	325	D5	11010101	Õ
214	326	D6	11010110	Ö
215	327	D7	11010111	×
216	330	D8	11011000	Ø
217	331	D9	11011001	Ù
218	332	DA	11011010	Ú
219	333	DB	11011011	Û

DEC	OCT	HEX	BIN	Symbol
220	334	DC	11011100	Ü
221	335	DD	11011101	Ý
222	336	DE	11011110	Þ
223	337	DF	11011111	ß
224	340	E0	11100000	À
225	341	E1	11100001	Á
226	342	E2	11100010	Â
227	343	E3	11100011	ã
228	344	E4	11100100	ä
229	345	E5	11100101	å
230	346	E6	11100110	æ
231	347	E7	11100111	ç
232	350	E8	11101000	è
233	351	E9	11101001	é
234	352	EA	11101010	ê
235	353	EB	11101011	ë
236	354	EC	11101100	ì
237	355	ED	11101101	í
238	356	EE	11101110	î
239	357	EF	11101111	ï
240	360	F0	11110000	ð
241	361	F1	11110001	ñ
242	362	F2	11110010	ò
243	363	F3	11110011	ó
244	364	F4	11110100	ô
245	365	F5	11110101	õ
246	366	F6	11110110	ö
247	367	F7	11110111	÷
248	370	F8	11111000	ø
249	371	F9	11111001	ù
250	372	FA	11111010	ú
251	373	FB	11111011	û
252	374	FC	11111100	ü
253	375	FD	11111101	ý
254	376	FE	11111110	þ
255	377	FF	11111111	ÿ

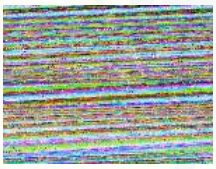
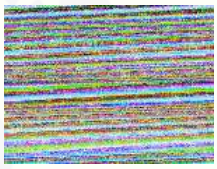
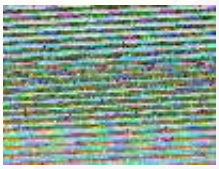
LAMPIRAN B. Hasil proses enkripsi pada program menggunakan kunci KRIPTO

No	*Plainimage*	*Playfair Cipher*	*3D Playfair Cipher*
1.			
2.			
3.			
4.			
5.			
6.			
7.			

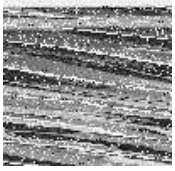
No	*Plainimage*	*Playfair Cipher*	*3D Playfair Cipher*
8.			
9.			
10.			

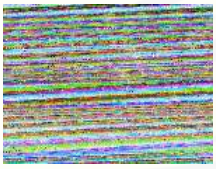
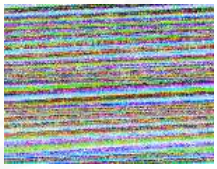
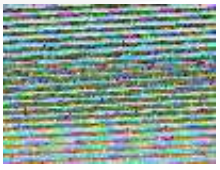
LAMPIRAN C. Hasil proses enkripsi pada program menggunakan kunci Sigma15

No	*Plainimage*	*Playfair Cipher*	*3D Playfair Cipher*
1.			
2.			
3.			
4.			

No	*Plainimage*	*Playfair Cipher*	*3D Playfair Cipher*
5.			
6.			
7.			
8.			
9.			
10.			

LAMPIRAN D. Hasil proses enkripsi pada program menggunakan kunci Himatika

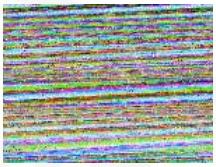
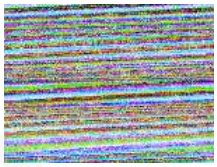
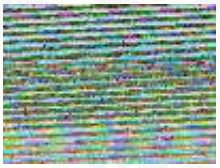
No	*Plainimage*	*Playfair Cipher*	*3D Playfair Cipher*
1.			

No	*Plainimage*	*Playfair Cipher*	*3D Playfair Cipher*
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			

No	*Plainimage*	*Playfair Cipher*	*3D Playfair Cipher*
10.			

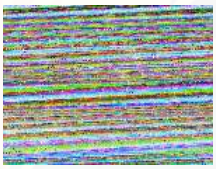
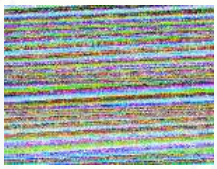
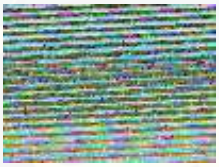
LAMPIRAN E. Hasil proses enkripsi pada program menggunakan kunci 1234567890

No	*Plainimage*	*Playfair Cipher*	*3D Playfair Cipher*
1.			
2.			
3.			
4.			
5.			
6.			

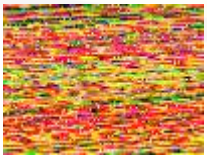
No	*Plainimage*	*Playfair Cipher*	*3D Playfair Cipher*
7.			
8.			
9.			
10.			

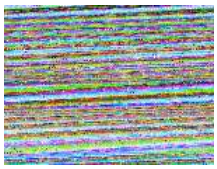
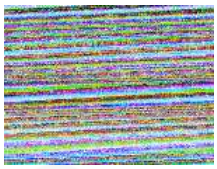
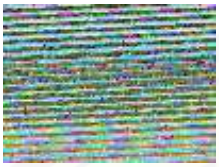
LAMPIRAN F. Hasil proses enkripsi pada program menggunakan kunci !@+$%*)#_(=

No	*Plainimage*	*Playfair Cipher*	*3D Playfair Cipher*
1.			
2.			
3.			

No	*Plainimage*	*Playfair Cipher*	*3D Playfair Cipher*
4.			
5.			
6.			
7.			
8.			
9.			
10.			

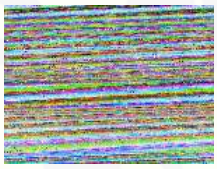
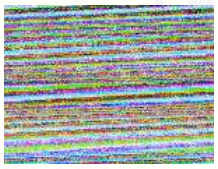
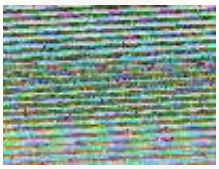
LAMPIRAN G. Hasil proses dekripsi pada program menggunakan kunci KRIPTO

No	*Playfair Cipher*	*3D Playfair Cipher*	*Cipherimage*
1.			
2.			
3.			
4.			
5.			
6.			
7.			

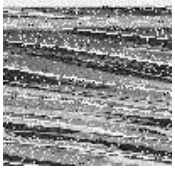
No	*Playfair Cipher*	*3D Playfair Cipher*	*Cipherimage*
8.			
9.			
10.			

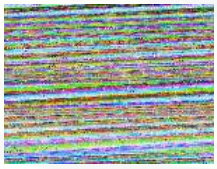
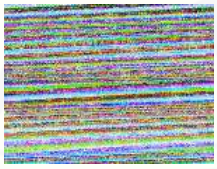
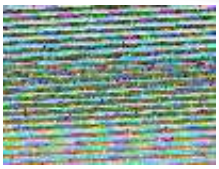
LAMPIRAN H. Hasil proses dekripsi pada program menggunakan kunci Sigma15

No	*Playfair Cipher*	*3D Playfair Cipher*	*Cipherimage*
1.			
2.			
3.			
4.			

No	*Playfair Cipher*	*3D Playfair Cipher*	*Cipherimage*
5.			
6.			
7.			
8.			
9.			
10.			

LAMPIRAN I. Hasil proses dekripsi pada program menggunakan kunci Himatika

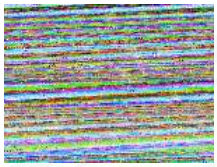
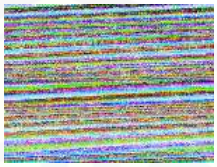
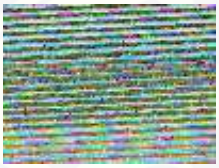
No	*Playfair Cipher*	*3D Playfair Cipher*	*Cipherimage*
1.			

No	*Playfair Cipher*	*3D Playfair Cipher*	*Cipherimage*
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			

No	*Playfair Cipher*	*3D Playfair Cipher*	*Cipherimage*
10.			

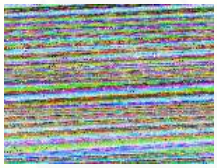
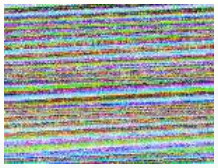
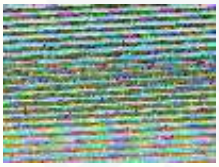
LAMPIRAN J. Hasil proses dekripsi pada program menggunakan kunci 1234567890

No	*Playfair Cipher*	*3D Playfair Cipher*	*Cipherimage*
1.			
2.			
3.			
4.			
5.			
6.			

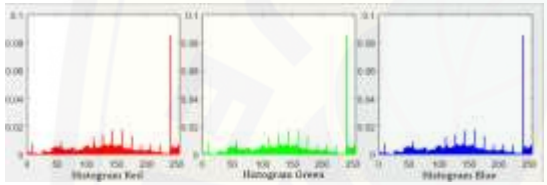
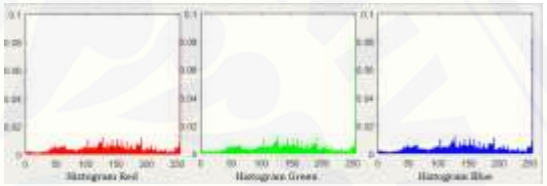
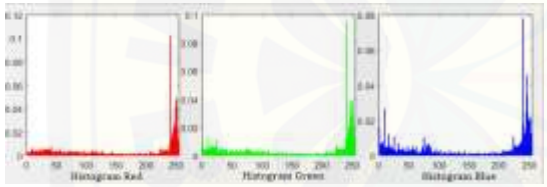
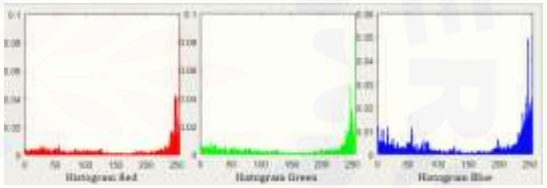
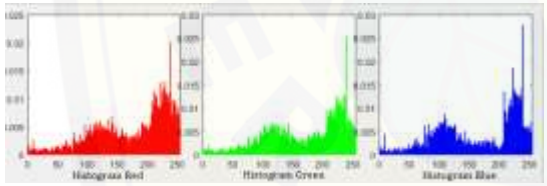
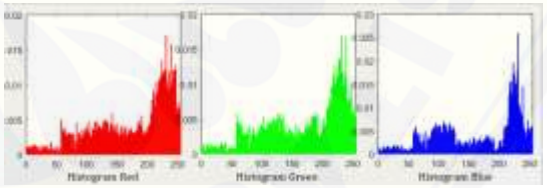
No	*Playfair Cipher*	*3D Playfair Cipher*	*Cipherimage*
7.			
8.			
9.			
10.			

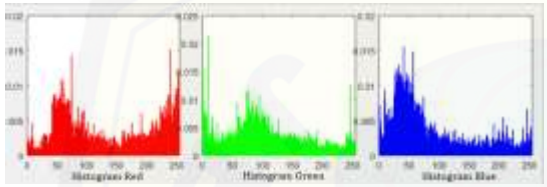
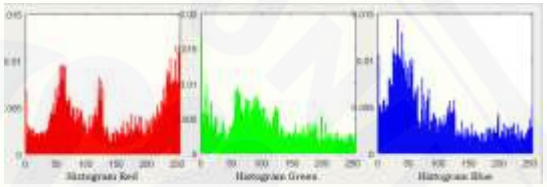
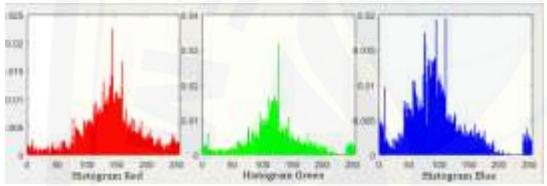
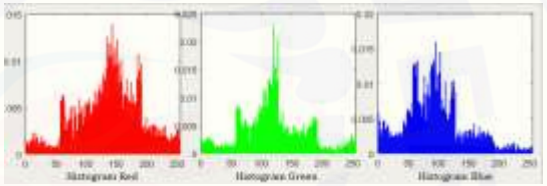
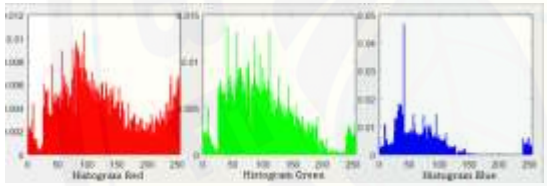
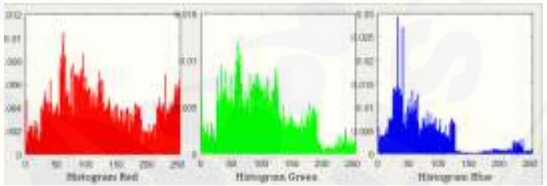
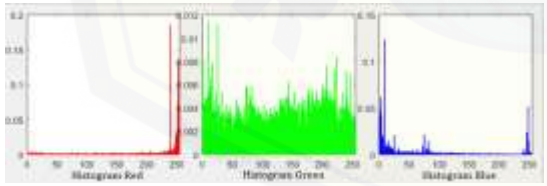
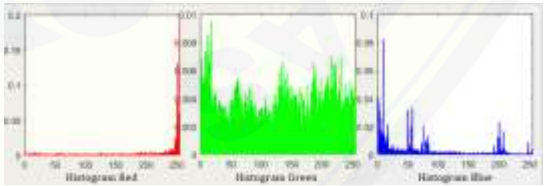
LAMPIRAN K. Hasil proses dekripsi pada program menggunakan kunci !@+$%*)#_(=

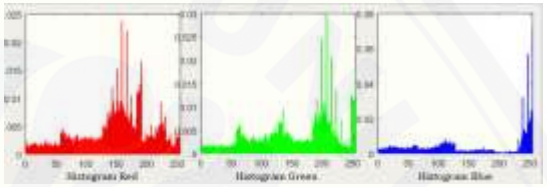
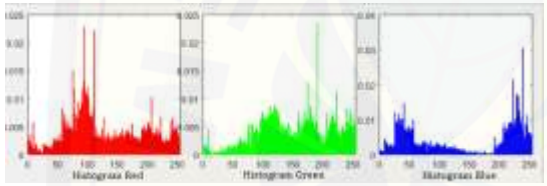
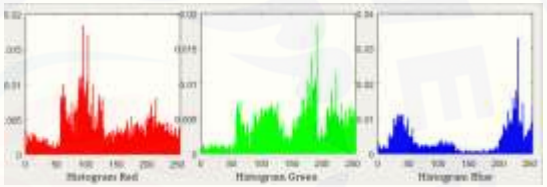
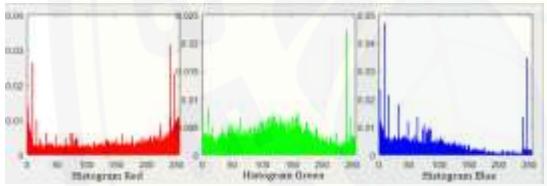
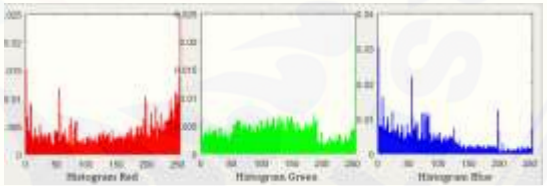
No	*Playfair Cipher*	*3D Playfair Cipher*	*Cipherimage*
1.			
2.			
3.			

No	*Playfair Cipher*	*3D Playfair Cipher*	*Cipherimage*
4.			
5.			
6.			
7.			
8.			
9.			
10.			

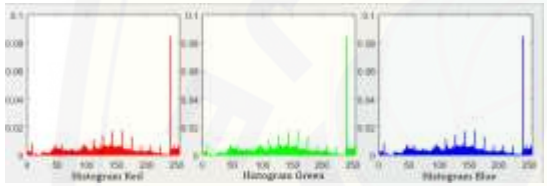
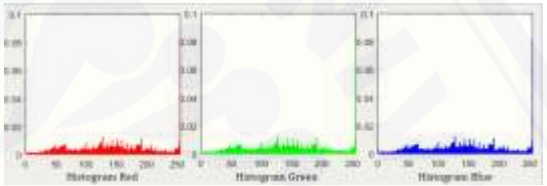
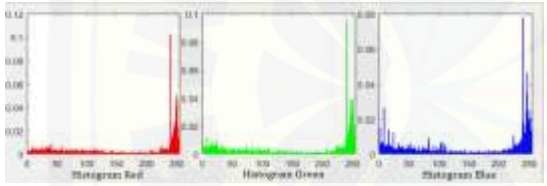
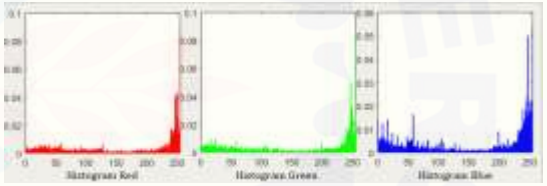
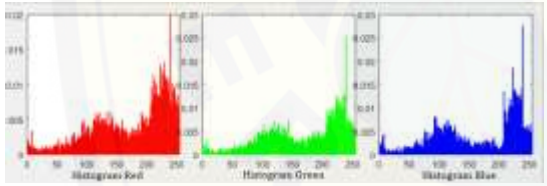
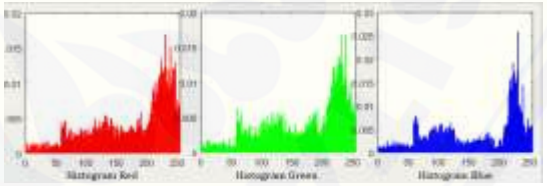
LAMPIRAN L. Hasil analisis histogram pada program menggunakan kunci KRIPTO

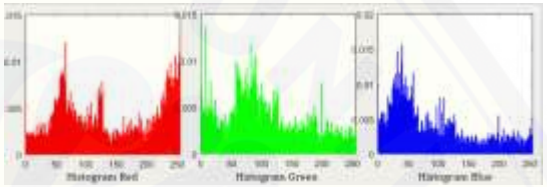
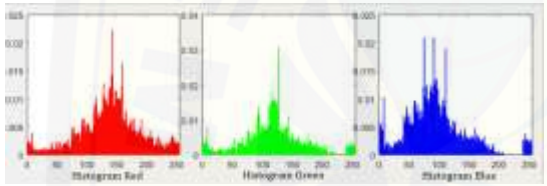
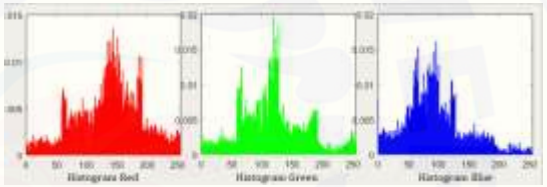
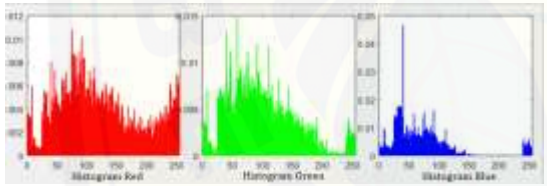
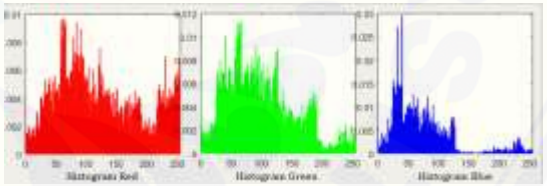
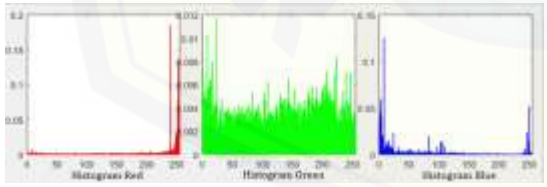
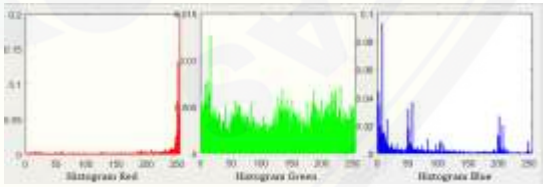
No	Data Penelitian	*Playfair Cipher*	*3D Playfair Cipher*	X^2
1.	Citra 1			*Playfair Cipher* = 20921,80 *3D Playfair Cipher* = 18000,33
2.	Citra 2			*Playfair Cipher* = 26762,26 *3D Playfair Cipher* = 20986,91
3.	Citra 3			*Playfair Cipher* = 4939,59 *3D Playfair Cipher* = 5089,55

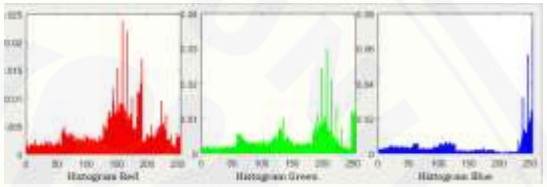
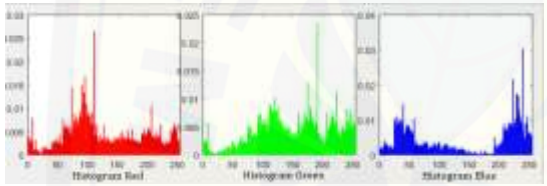
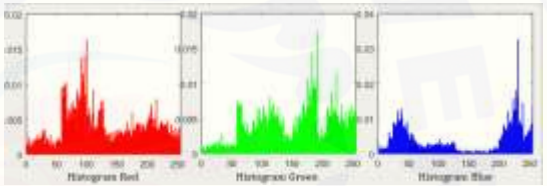
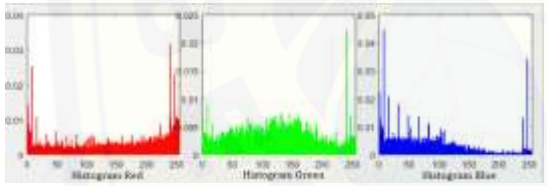
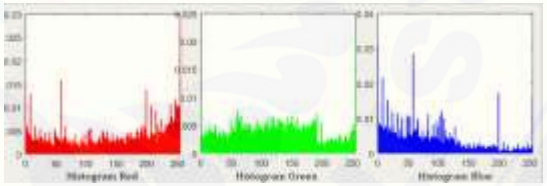
No	Data Penelitian	*Playfair Cipher*	*3D Playfair Cipher*	X^2
4.	Citra 4			*Playfair Cipher* = 3371,66 *3D Playfair Cipher* = 2565,86
5.	Citra 5			*Playfair Cipher* = 5878,87 *3D Playfair Cipher* = 4845,80
6.	Citra 6			*Playfair Cipher* = 4690,76 *3D Playfair Cipher* = 4063,86
7.	Citra 7			*Playfair Cipher* = 58273,60 *3D Playfair Cipher* = 50087,69

No	Data Penelitian	*Playfair Cipher*	*3D Playfair Cipher*	X^2
8.	Citra 8			*Playfair Cipher* = 30436,63 *3D Playfair Cipher* = 24944,18
9.	Citra 9			*Playfair Cipher* = 5290,62 *3D Playfair Cipher* = 4858,42
10.	Citra 10			*Playfair Cipher* = 5559,72 *3D Playfair Cipher* = 3539,01

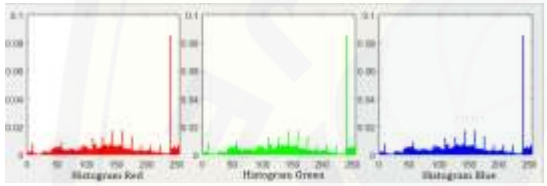
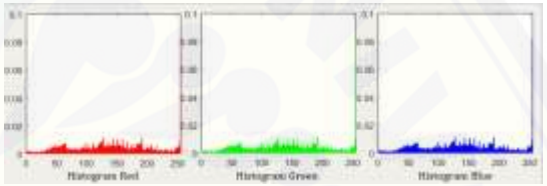
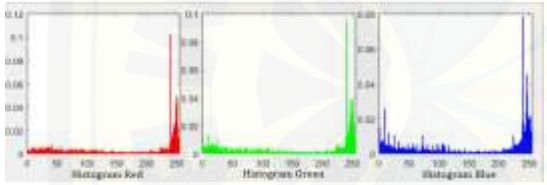
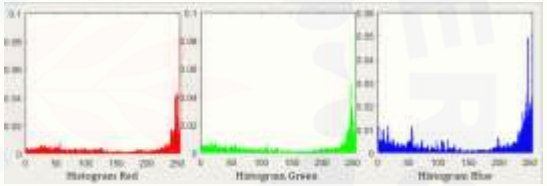
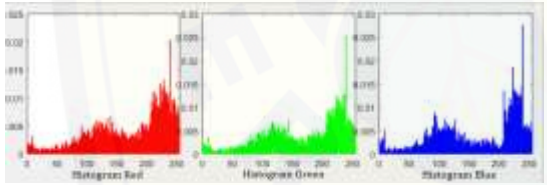
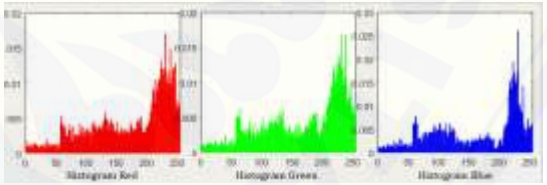
LAMPIRAN M. Hasil analisis histogram pada program menggunakan kunci Sigma15

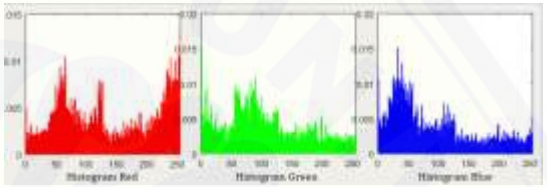
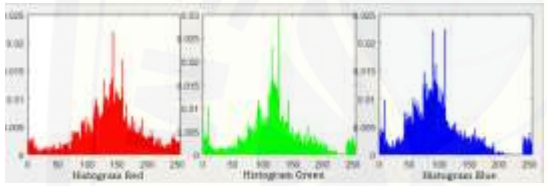
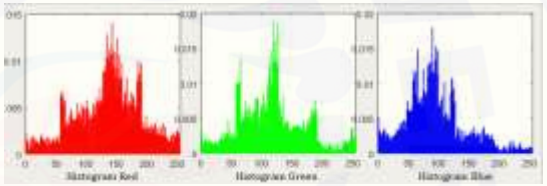
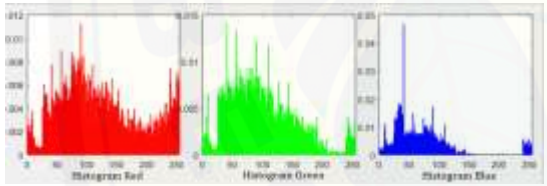
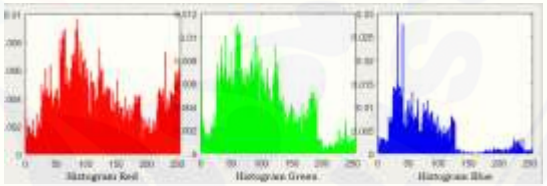
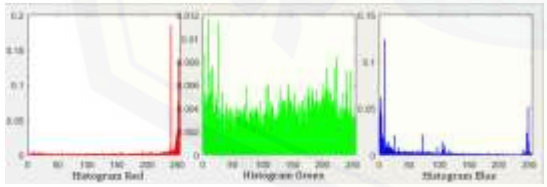
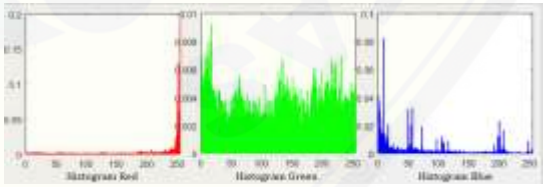
No	Data Penelitian	*Playfair Cipher*	*3D Playfair Cipher*	X^2
1.	Citra 1			*Playfair Cipher* = 20634,35 *3D Playfair Cipher* = 17847,71
2.	Citra 2			*Playfair Cipher* = 26736,80 *3D Playfair Cipher* = 21423,90
3.	Citra 3			*Playfair Cipher* = 4833,88 *3D Playfair Cipher* = 4990,31

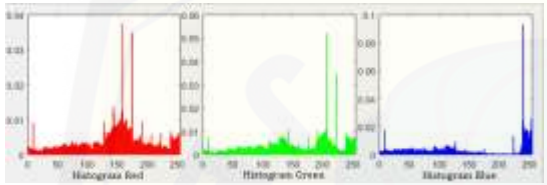
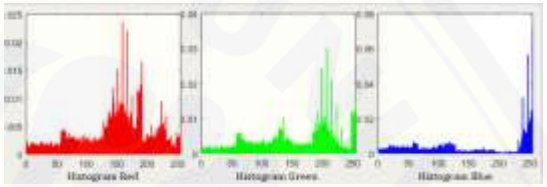
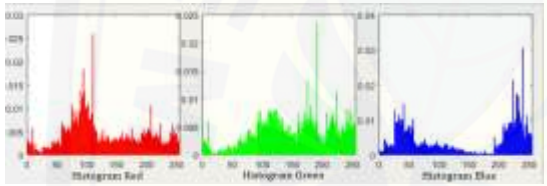
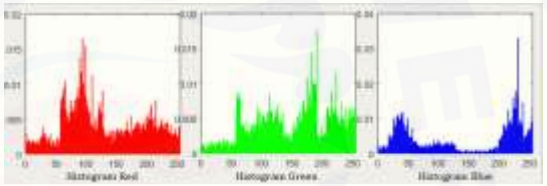
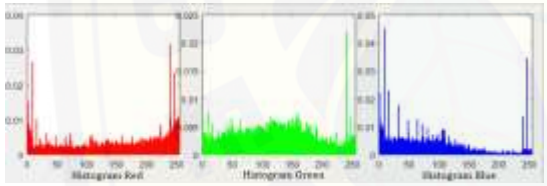
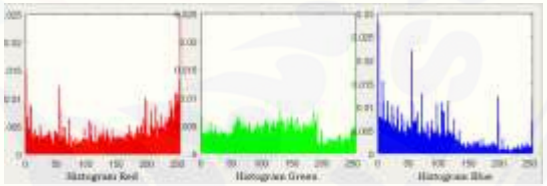
No	Data Penelitian	*Playfair Cipher*	*3D Playfair Cipher*	X^2
4.	Citra 4			*Playfair Cipher* = 3309,72 *3D Playfair Cipher* = 2630,94
5.	Citra 5			*Playfair Cipher* = 5743,97 *3D Playfair Cipher* = 4653,57
6.	Citra 6			*Playfair Cipher* = 4853,63 *3D Playfair Cipher* = 4327,41
7.	Citra 7			*Playfair Cipher* = 58093,72 *3D Playfair Cipher* = 51679,32

No	Data Penelitian	*Playfair Cipher*	*3D Playfair Cipher*	X^2
8.	Citra 8			*Playfair Cipher* = 30511,78 *3D Playfair Cipher* = 24928,69
9.	Citra 9			*Playfair Cipher* = 5196,05 *3D Playfair Cipher* = 4679,67
10.	Citra 10			*Playfair Cipher* = 5373,58 *3D Playfair Cipher* = 4081,85

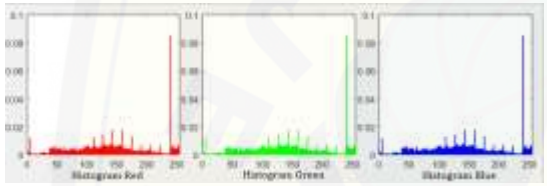
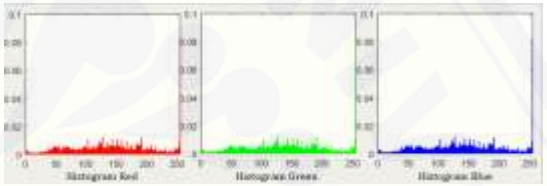
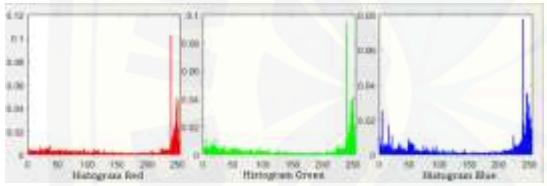
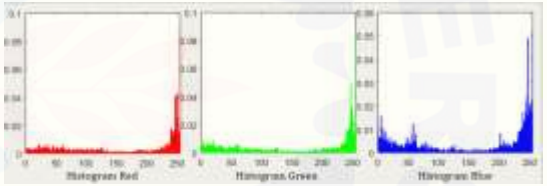
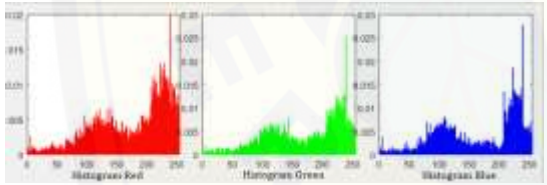
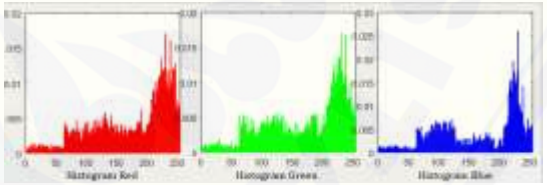
LAMPIRAN N. Hasil analisis histogram pada program menggunakan kunci Himatika

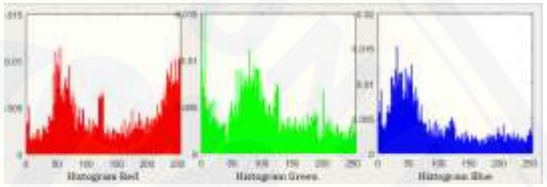
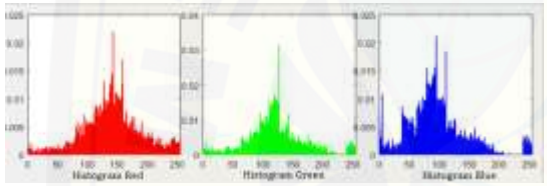
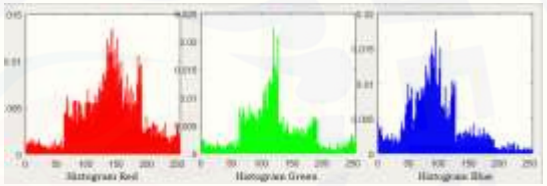
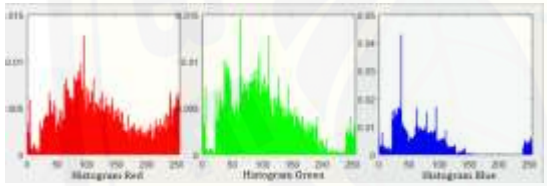
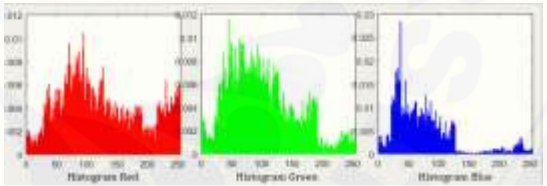
No	Data Penelitian	*Playfair Cipher*	*3D Playfair Cipher*	X^2
1.	Citra 1			*Playfair Cipher* = 20758,07 *3D Playfair Cipher* = 17842,69
2.	Citra 2			*Playfair Cipher* = 26700,52 *3D Playfair Cipher* = 20977,67
3.	Citra 3			*Playfair Cipher* = 4826,04 *3D Playfair Cipher* = 4973,26

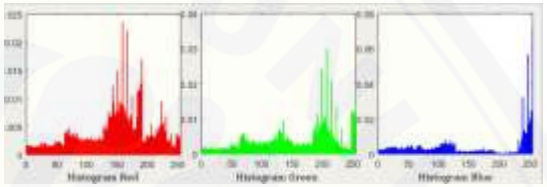
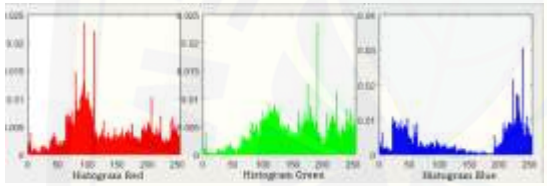
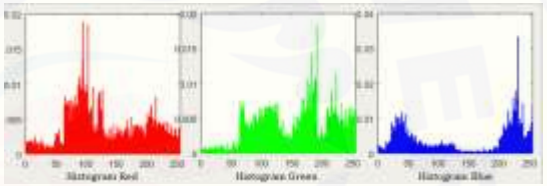
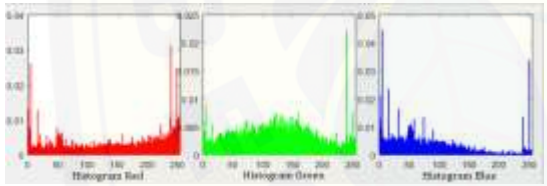
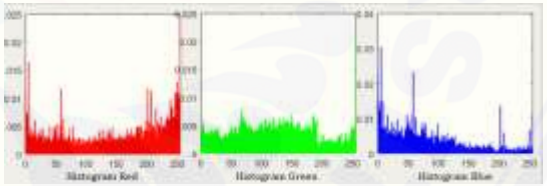
No	Data Penelitian	*Playfair Cipher*	*3D Playfair Cipher*	X^2
4.	Citra 4			*Playfair Cipher* = 3410,16 *3D Playfair Cipher* = 2538,20
5.	Citra 5			*Playfair Cipher* = 5736,83 *3D Playfair Cipher* = 4581,74
6.	Citra 6			*Playfair Cipher* = 4845,27 *3D Playfair Cipher* = 4269,59
7.	Citra 7			*Playfair Cipher* = 58244,04 *3D Playfair Cipher* = 49997,24

No	Data Penelitian	*Playfair Cipher*	*3D Playfair Cipher*	X^2
8.	Citra 8			*Playfair Cipher* = 30428,08 *3D Playfair Cipher* = 24899,60
9.	Citra 9			*Playfair Cipher* = 5227,92 *3D Playfair Cipher* = 4735,34
10.	Citra 10			*Playfair Cipher* = 5442,38 *3D Playfair Cipher* = 3454,44

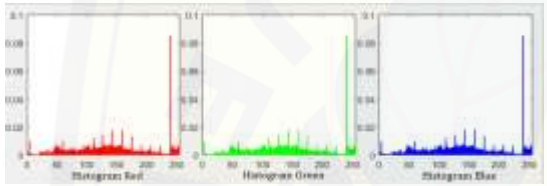
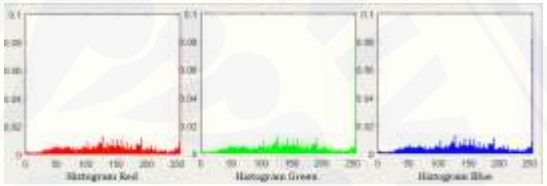
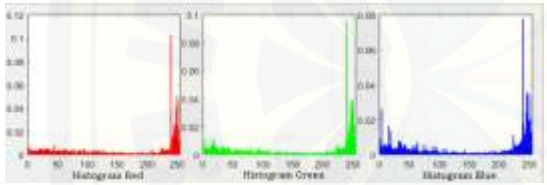
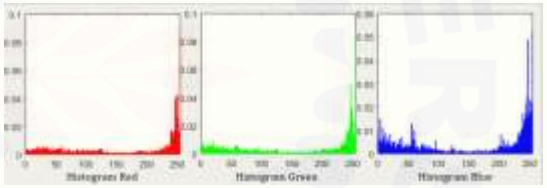
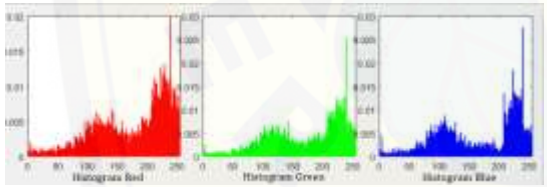
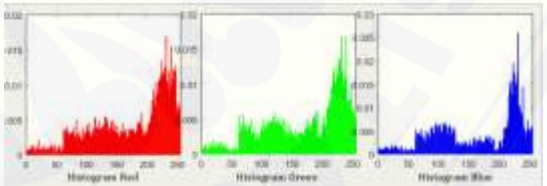
LAMPIRAN O. Hasil analisis histogram pada program menggunakan kunci 1234567890

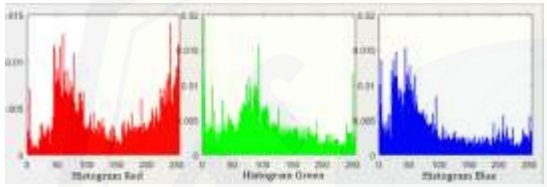
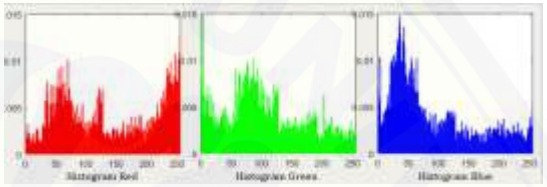
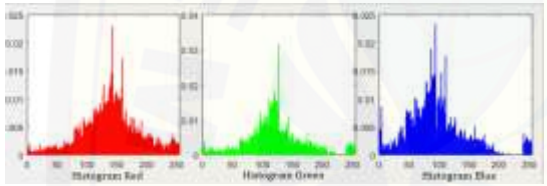
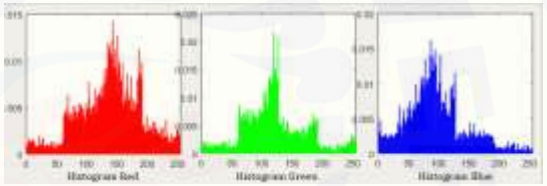
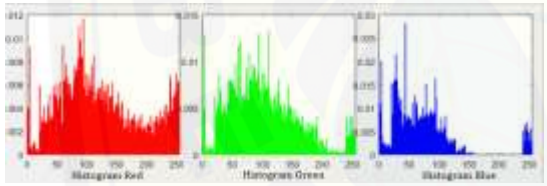
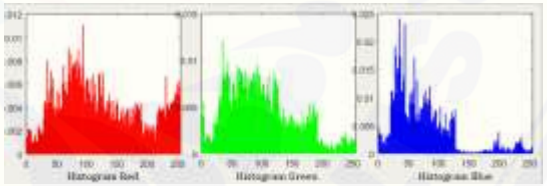
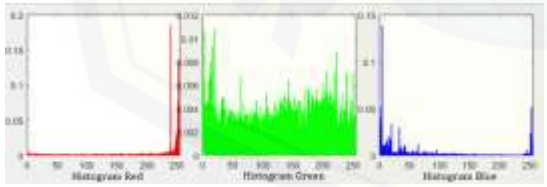
No	Data Penelitian	*Playfair Cipher*	*3D Playfair Cipher*	X^2
1.	Citra 1			*Playfair Cipher* = 20919,12 *3D Playfair Cipher* = 18149,01
2.	Citra 2			*Playfair Cipher* = 26538,79 *3D Playfair Cipher* = 21094,29
3.	Citra 3			*Playfair Cipher* = 4965,87 *3D Playfair Cipher* = 5154,24

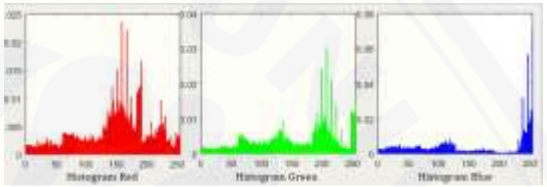
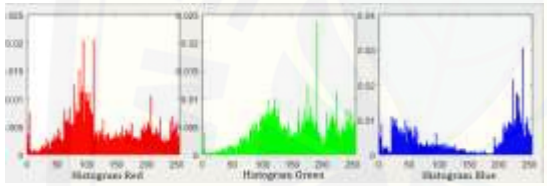
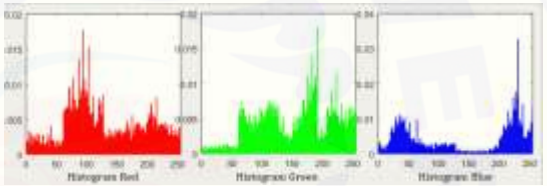
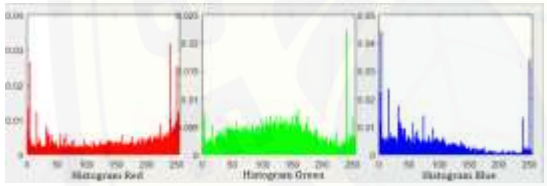
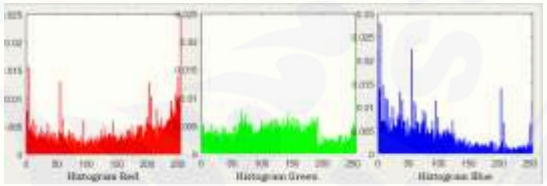
No	Data Penelitian	*Playfair Cipher*	*3D Playfair Cipher*	X^2
4.	Citra 4			*Playfair Cipher* = 3114,35 *3D Playfair Cipher* = 2814,86
5.	Citra 5			*Playfair Cipher* = 6021,99 *3D Playfair Cipher* = 5174,56
6.	Citra 6			*Playfair Cipher* = 4654,85 *3D Playfair Cipher* = 4235,93
7.	Citra 7			*Playfair Cipher* = 57755,68 *3D Playfair Cipher* = 51764,08

No	Data Penelitian	*Playfair Cipher*	*3D Playfair Cipher*	X^2
8.	Citra 8			*Playfair Cipher* = 30557,19 *3D Playfair Cipher* = 24985,76
9.	Citra 9			*Playfair Cipher* = 5213,09 *3D Playfair Cipher* = 5040,56
10.	Citra 10			*Playfair Cipher* = 5454,55 *3D Playfair Cipher* = 3707,12

LAMPIRAN P. Hasil analisis histogram pada program menggunakan kunci !@+$%*)#_(=

No	Data Penelitian	*Playfair Cipher*	*3D Playfair Cipher*	X^2
1.	Citra 1			*Playfair Cipher* = 21004,81 *3D Playfair Cipher* = 17927,10
2.	Citra 2			*Playfair Cipher* = 26621,35 *3D Playfair Cipher* = 21064,20
3.	Citra 3			*Playfair Cipher* = 4959,61 *3D Playfair Cipher* = 5113,62

No	Data Penelitian	*Playfair Cipher*	*3D Playfair Cipher*	X^2
4.	Citra 4			*Playfair Cipher* = 3257,99 *3D Playfair Cipher* = 2755,75
5.	Citra 5			*Playfair Cipher* = 6023,50 *3D Playfair Cipher* = 4978,41
6.	Citra 6			*Playfair Cipher* = 4200,79 *3D Playfair Cipher* = 4256,29
7.	Citra 7			*Playfair Cipher* = 59262,49 *3D Playfair Cipher* = 50816,76

No	Data Penelitian	*Playfair Cipher*	*3D Playfair Cipher*	X^2
8.	Citra 8			*Playfair Cipher* = 30527,89 *3D Playfair Cipher* = 25006,69
9.	Citra 9			*Playfair Cipher* = 4980,06 *3D Playfair Cipher* = 4738,54
10.	Citra 10			*Playfair Cipher* = 5475,72 *3D Playfair Cipher* = 3666,63

LAMPIRAN Q. Hasil NPCR pada program

No	Data Penelitian	Kunci	*Playfair Cipher*	*3D Playfair Cipher*
1.	Citra 1	KRIPTO	99,46%	97,62%
2.	Citra 2	KRIPTO	98,88%	98,67%
3.	Citra 3	KRIPTO	99,33%	99,18%
4.	Citra 4	KRIPTO	99,45%	99,45%
5.	Citra 5	KRIPTO	99,21%	99,26%
6.	Citra 6	KRIPTO	99,34%	99,23%
7.	Citra 7	KRIPTO	98,18%	97,70%
8.	Citra 8	KRIPTO	99,21%	99,24%
9.	Citra 9	KRIPTO	99,47%	99,39%
10.	Citra 10	KRIPTO	99,56%	99,53%
11.	Citra 1	Sigma15	99,49%	97,61%
12.	Citra 2	Sigma15	98,86%	98,63%
13.	Citra 3	Sigma15	99,38%	99,21%
14.	Citra 4	Sigma15	99,44%	99,38%
15.	Citra 5	Sigma15	99,25%	99,30%
16.	Citra 6	Sigma15	99,28%	99,28%
17.	Citra 7	Sigma15	98,18%	97,68%
18.	Citra 8	Sigma15	99,16%	99,22%
19.	Citra 9	Sigma15	99,48%	99,42%
20.	Citra 10	Sigma15	99,53%	99,39%
21.	Citra 1	Himatika	99,51%	97,65%
22.	Citra 2	Himatika	98,87%	98,67%
23.	Citra 3	Himatika	99,35%	99,19%
24.	Citra 4	Himatika	99,43%	99,41%
25.	Citra 5	Himatika	99,29%	99,30%
26.	Citra 6	Himatika	99,21%	99,18%
27.	Citra 7	Himatika	98,23%	97,72%

No	Data Penelitian	Kunci	*Playfair Cipher*	*3D Playfair Cipher*
28.	Citra 8	Himatika	99,21%	99,25%
29.	Citra 9	Himatika	99,47%	99,43%
30.	Citra 10	Himatika	99,58%	99,56%
31.	Citra 1	1234567890	99,49%	97,70%
32.	Citra 2	1234567890	98,90%	98,69%
33.	Citra 3	1234567890	99,31%	99,20%
34.	Citra 4	1234567890	99,46%	99,40%
35.	Citra 5	1234567890	99,23%	99,22%
36.	Citra 6	1234567890	99,28%	99,12%
37.	Citra 7	1234567890	98,15%	97,72%
38.	Citra 8	1234567890	99,20%	99,24%
39.	Citra 9	1234567890	99,40%	99,42%
40.	Citra 10	1234567890	99,50%	99,43%
41.	Citra 1	!@+$%*)#_(=	99,52%	97,69%
42.	Citra 2	!@+$%*)#_(=	98,85%	98,69%
43.	Citra 3	!@+$%*)#_(=	99,33%	99,17%
44.	Citra 4	!@+$%*)#_(=	99,49%	99,32%
45.	Citra 5	!@+$%*)#_(=	99,25%	99,28%
46.	Citra 6	!@+$%*)#_(=	99,27%	99,16%
47.	Citra 7	!@+$%*)#_(=	98,20%	97,74%
48.	Citra 8	!@+$%*)#_(=	99,18%	99,22%
49.	Citra 9	!@+$%*)#_(=	99,48%	99,40%
50.	Citra 10	!@+$%*)#_(=	99,55%	99,47%

LAMPIRAN R. Hasil UACI pada program

No	Data Penelitian	Kunci	*Playfair Cipher*	*3D Playfair Cipher*
1.	Citra 1	KRIPTO	26,92%	27,30%
2.	Citra 2	KRIPTO	41,16%	41,13%
3.	Citra 3	KRIPTO	25,10%	25,48%
4.	Citra 4	KRIPTO	29,13%	29,41%
5.	Citra 5	KRIPTO	19,46%	20,13%
6.	Citra 6	KRIPTO	21,31%	21,80%
7.	Citra 7	KRIPTO	30,19%	29,88%
8.	Citra 8	KRIPTO	31,25%	31,47%
9.	Citra 9	KRIPTO	31,60%	31,81%
10.	Citra 10	KRIPTO	32,61%	32,53%
11.	Citra 1	Sigma15	27,22%	27,51%
12.	Citra 2	Sigma15	41,11%	41,06%
13.	Citra 3	Sigma15	25,36%	25,74%
14.	Citra 4	Sigma15	29,14%	29,29%
15.	Citra 5	Sigma15	19,68%	20,31%
16.	Citra 6	Sigma15	21,31%	21,67%
17.	Citra 7	Sigma15	30,35%	29,90%
18.	Citra 8	Sigma15	31,32%	31,56%
19.	Citra 9	Sigma15	31,74%	31,98%
20.	Citra 10	Sigma15	32,60%	32,50%
21.	Citra 1	Himatika	27,28%	27,60%
22.	Citra 2	Himatika	41,11%	41,03%
23.	Citra 3	Himatika	25,49%	25,82%
24.	Citra 4	Himatika	29,08%	29,31%
25.	Citra 5	Himatika	19,70%	20,42%
26.	Citra 6	Himatika	21,24%	21,69%
27.	Citra 7	Himatika	30,30%	30,00%

No	Data Penelitian	Kunci	*Playfair Cipher*	*3D Playfair Cipher*
28.	Citra 8	Himatika	31,44%	31,62%
29.	Citra 9	Himatika	31,76%	32,07%
30.	Citra 10	Himatika	32,62%	32,55%
31.	Citra 1	1234567890	26,95%	27,16%
32.	Citra 2	1234567890	41,18%	41,17%
33.	Citra 3	1234567890	24,94%	25,28%
34.	Citra 4	1234567890	29,12%	29,14%
35.	Citra 5	1234567890	19,14%	19,67%
36.	Citra 6	1234567890	21,30%	21,35%
37.	Citra 7	1234567890	30,29%	29,94%
38.	Citra 8	1234567890	31,18%	31,35%
39.	Citra 9	1234567890	31,38%	31,52%
40.	Citra 10	1234567890	32,53%	32,55%
41.	Citra 1	!@+$%*)#_(=	26,90%	27,23%
42.	Citra 2	!@+$%*)#_(=	41,21%	41,15%
43.	Citra 3	!@+$%*)#_(=	25,01%	25,37%
44.	Citra 4	!@+$%*)#_(=	29,00%	29,16%
45.	Citra 5	!@+$%*)#_(=	19,19%	19,83%
46.	Citra 6	!@+$%*)#_(=	21,48%	21,44%
47.	Citra 7	!@+$%*)#_(=	30,26%	30,04%
48.	Citra 8	!@+$%*)#_(=	31,17%	31,40%
49.	Citra 9	!@+$%*)#_(=	31,52%	31,75%
50.	Citra 10	!@+$%*)#_(=	32,55%	32,55%

LAMPIRAN S. Skrip program enkripsi dan dekripsi pada MATLAB R2015b

a. Skrip program enkripsi menggunakan *Playfair Cipher*

```
function Chiper=en_2d(knci,A)
A=double(A);
[m,n]=size(A);
kunci=double(knci);
keyIn=0:255;
kunciIn=[kunci setxor(kunci,keyIn)];
k=0;
for i=1:16
    for j=1:16
        k=k+1;
         T(i,j)=kunciIn(k);
    end
end
A=A';
sisa=mod(m*n,2);
if sisa==0
    nn=A(1:m*n);
elseif sisa==1
   nn=[A(1:m*n) 255];
end
panjang=length(nn)/2;
awl=1;
ahr=2;
hh=0;
for j=1:panjang
    simpan=[];
    sb=[];
    sk=[];
    B=nn(awl:ahr);
    for i=1:2
        for z=1:2
            [R,C]=ambil_r_c(B(z),T);
            gabung=[R C];
            sb(z)=R;
            sk(z)=C;
            simpan(i,z)=posisi2d(i,z,gabung);
        end
        if sb(1)==sb(2) && sk(1)~=sk(2)
            if sk(1)==16 && sk(2)~=16
                simpan(i,1)=posisi2d(i,1,[sb(1) sk(2)+1]);
                simpan(i,2)=posisi2d(i,2,[sb(1) 1]);
            elseif sk(1)~=16 && sk(2)==16
                simpan(i,1)=posisi2d(i,1,[sb(1) 1]);
                simpan(i,2)=posisi2d(i,2,[sb(1) sk(1)+1]);
            elseif sk(1)==16 && sk(2)==16
                 simpan(i,1)=posisi2d(i,1,[sb(1) 1]);
                 simpan(i,2)=posisi2d(i,2,[sb(1) 1]);
            else
                simpan(i,1)=posisi2d(i,1,[sb(1) sk(2)+1]);
                simpan(i,2)=posisi2d(i,2,[sb(1) sk(1)+1]);
            end
```

```
            end
            if sk(1)==sk(2) && sb(1)~=sb(2)
                if sb(1)==16 && sb(2)~=16
                    simpan(i,1)=posisi2d(i,1,[1 sk(1)]);
                    simpan(i,2)=posisi2d(i,2,[sb(2)+1 sk(1)]);
                elseif sb(1)~=16 && sb(2)==16
                    simpan(i,1)=posisi2d(i,1,[sb(1)+1 sk(1)]);
                    simpan(i,2)=posisi2d(i,2,[1 sk(1)]);
                elseif sb(1)==16 && sb(2)==16
                     simpan(i,1)=posisi2d(i,1,[1 sk(1)]);
                     simpan(i,2)=posisi2d(i,2,[1 sk(1)]);
                else
                    simpan(i,1)=posisi2d(i,1,[sb(1)+1 sk(1)]);
                    simpan(i,2)=posisi2d(i,2,[sb(2)+1 sk(1)]);
                end
            end
            if sk(1)==sk(2) && sb(1)==sb(2)
                if sk(1)==16
                    simpan(i,1)=posisi2d(i,1,[sb(1) 1]);
                    simpan(i,2)=posisi2d(i,2,[sb(2) 1]);
                else
                    simpan(i,1)=posisi2d(i,1,[sb(1) sk(1)+1]);
                    simpan(i,2)=posisi2d(i,2,[sb(2) sk(1)+1]);
                end
            end
            hh=hh+1;
            cip(hh)=ambil_chip2d(i,simpan(i,:),T);
        end
        awl=ahr+1;
        ahr=awl+1;
    end
    [Chiper,sisa]=buat_matrik(m*n,cip,m,n);
```

b. Skrip program dekripsi menggunakan *Playfair Cipher*

```
function Chiper=de_2d(knci,A,rgb)
[m,n]=size(A);
A=double(A);
kunci=double(knci);
keyIn=0:255;
kunciIn=[kunci setxor(kunci,keyIn)];
k=0;
for i=1:16
    for j=1:16
        k=k+1;
         T(i,j)=kunciIn(k);
    end
end
A=A';
sisa=mod(m*n,2);
if sisa==0
    nn=A(1:m*n);
elseif sisa==1
   nn=[A(1:m*n) 255];
end
panjang=length(nn)/2;
```

```
awl=1;
ahr=2;
hh=0;
for j=1:panjang
    simpan=[];
    sb=[];
    sk=[];
    B=nn(awl:ahr);
    for i=1:2
        for z=1:2
            [R,C]=ambil_r_c(B(z),T);
            gabung=[R C];
            sb(z)=R;
            sk(z)=C;
            simpan(i,z)=posisi2d(i,z,gabung);
        end
        if sb(1)==sb(2) && sk(1)~=sk(2)
            if sk(1)==1 && sk(2)~=1
                simpan(i,1)=posisi2d(i,1,[sb(1) sk(2)-1]);
                simpan(i,2)=posisi2d(i,2,[sb(1) 16]);
            elseif sk(1)~=1 && sk(2)==1
                simpan(i,1)=posisi2d(i,1,[sb(1) 16]);
                simpan(i,2)=posisi2d(i,2,[sb(1) sk(1)-1]);
            elseif sk(1)==1 && sk(2)==1
                 simpan(i,1)=posisi2d(i,1,[sb(1) 16]);
                 simpan(i,2)=posisi2d(i,2,[sb(1) 16]);
            else
                simpan(i,1)=posisi2d(i,1,[sb(1) sk(2)-1]);
                simpan(i,2)=posisi2d(i,2,[sb(1) sk(1)-1]);
            end
        end
        if sk(1)==sk(2) && sb(1)~=sb(2)
            if sb(1)==1 && sb(2)~=1
                simpan(i,1)=posisi2d(i,1,[16 sk(1)]);
                simpan(i,2)=posisi2d(i,2,[sb(2)-1 sk(1)]);
            elseif sb(1)~=1 && sb(2)==1
                simpan(i,1)=posisi2d(i,1,[sb(1)-1 sk(1)]);
                simpan(i,2)=posisi2d(i,2,[16 sk(1)]);
            elseif sb(1)==1 && sb(2)==1
                 simpan(i,1)=posisi2d(i,1,[16 sk(1)]);
                 simpan(i,2)=posisi2d(i,2,[16 sk(1)]);
            else
                simpan(i,1)=posisi2d(i,1,[sb(1)-1 sk(1)]);
                simpan(i,2)=posisi2d(i,2,[sb(2)-1 sk(1)]);
            end
        end
        if sk(1)==sk(2) && sb(1)==sb(2)
            if sk(1)==1
                simpan(i,1)=posisi2d(i,1,[sb(1) 16]);
                simpan(i,2)=posisi2d(i,2,[sb(2) 16]);
            else
                simpan(i,1)=posisi2d(i,1,[sb(1) sk(1)-1]);
                simpan(i,2)=posisi2d(i,2,[sb(2) sk(1)-1]);
            end
        end
        hh=hh+1;
```

```
            cip(hh)=ambil_chip2d(i,simpan(i,:),T);
        end
        awl=ahr+1;
        ahr=awl+1;
    end
    [pl,sisa]=buat_matrik(m*n,cip,m,n);
    C=pl';
    if rgb==1
        sis=dlmread('2dsisa_selip.txt');
        uk=dlmread('2dbrkl.txt');
        ssa=dlmread('2dposisi_selip.txt');
        a=[C(1:m*n) sis];
    elseif rgb==2
        sis=dlmread('2dsisa_selip1.txt');
        uk=dlmread('2dbrkl1.txt');
        ssa=dlmread('2dposisi_selip1.txt');
        a=[C(1:m*n) sis];
    else
        sis=dlmread('2dsisa_selip2.txt');
        uk=dlmread('2dbrkl2.txt');
        ssa=dlmread('2dposisi_selip2.txt');
        a=[C(1:m*n) sis];
    end
    j=0;
    for i=1:length(a)
        if ismember(i,ssa)==0
            j=j+1;
            an(j)=a(i);
        end
    end
    Chiper=buat_matrik2(uk(1)*uk(2),an,uk(1),uk(2));
```

c. Skrip program enkripsi menggunakan *3D Playfair Cipher*

```
function Chiper=enk_plyfair3d(knci,A,a,b)
kunci=(knci);
[m, n]=size(A);

keyIn=0:255;
kunciIn=[kunci setxor(kunci,keyIn)];
k=0;
for i=1:4
    for j=1:8
        for z=1:8
            k=k+1;
            if i==1
                T1(j,z)=kunciIn(k);
            elseif i==2
                T2(j,z)=kunciIn(k);
            elseif i==3
                T3(j,z)=kunciIn(k);
            elseif i==4
                T4(j,z)=kunciIn(k);
            end
        end
```

```
    end
end
A=A';
sisa=mod(m*n,3);
if sisa==0
    nn=A(1:m*n);
elseif sisa==1
   nn=[A(1:m*n) 254 255];
else
   nn=[A(1:m*n) 255];
end
panjang=length(nn)/3;
awl=1;
ahr=3;
hh=0;
for j=1:panjang
    simpan=[];
    B=nn(awl:ahr);
    for i=1:3
        for z=1:3
            %AMBIL B K T
            a1=ismember(B(z),T1);
            b1=ismember(B(z),T2);
            c1=ismember(B(z),T3);
            if a1==1
                T=1;
                [R,C]=ambil_r_c(B(z),T1);
            elseif b1==1
                T=2;
                [R,C]=ambil_r_c(B(z),T2);
            elseif c1==1
                T=3;
                [R,C]=ambil_r_c(B(z),T3);
            else
                T=4;
                [R,C]=ambil_r_c(B(z),T4);
            end
            gabung=[R C T];
            simpan(i,z)=posisi3d(i,z,gabung);
        end
        hh=hh+1;
        cip(hh)=ambil_chip3d(i,simpan(i,:),T1,T2,T3,T4);
    end
    awl=ahr+1;
    ahr=awl+2;
end
cip=double(cip);
[Chiper,sisa]=buat_matrik(m*n,cip,m,n);
dlmwrite('sisa3d.txt', sisa, 'delimiter', '\t', ...
         'precision', 6)
```

d. Skrip program dekripsi menggunakan *3D Playfair Cipher*

```
function plain=de_plyfair3d(knci,A,rgb)
[m,n]=size(A);
A=double(A);
```

```
kunci=double(knci);
keyIn=0:255;
kunciIn=[kunci setxor(kunci,keyIn)];
k=0;
for i=1:4
    for j=1:8
        for z=1:8
            k=k+1;
            if i==1
                T1(j,z)=kunciIn(k);
            elseif i==2
                T2(j,z)=kunciIn(k);
            elseif i==3
                T3(j,z)=kunciIn(k);
            elseif i==4
                T4(j,z)=kunciIn(k);
            end
        end
    end
end
A=A';
sisa=mod(m*n,3);
if sisa==0
    nn=A(1:m*n);
else
    data=dlmread('sisa3d.txt');
    nn=[A(1:m*n) data(1:length(data))];
end
panjang=length(nn)/3;
awl=1;
ahr=3;
hh=0;
for j=1:panjang
    simpan=[];
    B=nn(awl:ahr);
    for i=1:3
        for z=1:3
            %AMBIL B T K
            a1=ismember(B(z),T1);
            b1=ismember(B(z),T2);
            c1=ismember(B(z),T3);
            if a1==1
                T=1;
                [R,C]=ambil_r_c(B(z),T1);
            elseif b1==1
                T=2;
                [R,C]=ambil_r_c(B(z),T2);
            elseif c1==1
                T=3;
                [R,C]=ambil_r_c(B(z),T3);
            else
                T=4;
                [R,C]=ambil_r_c(B(z),T4);
            end
            gabung=[R T C];
            simpan(i,z)=posisi3d(i,z,gabung);
```

```
            end
            hh=hh+1;
            cip(hh)=ambil_plain3d(i,simpan(i,:),T1,T2,T3,T4);
        end
        awl=ahr+1;
        ahr=awl+2;
end
pl=buat_matrik(length(nn),cip,m,n);
C=pl';
if rgb==1
        sis=dlmread('sisa_selip.txt');
        uk=dlmread('brkl.txt');
        ssa=dlmread('posisi_selip.txt');
        a=[C(1:m*n) sis];
elseif rgb==2
        sis=dlmread('sisa_selip1.txt');
        uk=dlmread('brkl1.txt');
        ssa=dlmread('posisi_selip1.txt');
        a=[C(1:m*n) sis];
else
        sis=dlmread('sisa_selip2.txt');
        uk=dlmread('brkl2.txt');
        ssa=dlmread('posisi_selip2.txt');
        a=[C(1:m*n) sis];
end
j=0;
for i=1:length(a)
        if ismember(i,ssa)==0
            j=j+1;
            an(j)=a(i);
        end
end
plain=buat_matrik2(uk(1)*uk(2),an,uk(1),uk(2));
```