# BAB V PENGUJIAN

Rancangan yang telah diimplementasikan dalam bentuk nyata memerlukan suatu pengujian. Uji coba ini adalah untuk mengetahui hasil dari percobaan yang dilakukan sekaligus sebagai sarana pemunculan ide-ide bagi proses pengembangan I dalam L. selanjutnya. Pengujian yang dilakukan dalam bab ini adalah pengujian kebenaran perangkat lunak, antara lain :

- 1. Pengujian proses generate key
- Pengujian proses enkripsi. 2.
- 3. Pengujian proses dekripsi.
- 4. Analisis cipher citra dan plain citra.

#### 5.1 Lingkungan Pengujian

Lingkungan pengujian perangkat lunak ini, memiliki spesifikasi yang sama dengan lingkungan implementasi perangkat lunak yang telah dijelaskan pada sub bab 4.4.

#### 5.2 **Tujuan Pengujian**

Terdapat beberapa hal yang merupakan tujuan dari pengujian perangkat lunak dalam skripsi ini, yaitu:

- 1. Menguji kebenaran proses citra dapat di enkripsi dan dekripsi.
- 2. Menganalisa hasil *cipher* citra dan *plain* citra serta membandingkannya.

#### 5.3 **Data Pengujian**

Pada tabel 5.1 menunjukkan berkas citra yang digunakan untuk menguji perangkat lunak ini.

No.	Plain Citra	Citra Ukuran Kunci Publik Citra g		Ukuran	Dimensi	Format
1	baboon	192 KB	goldhill	65 KB	200 x 200	bmp
2	peppers	768 KB	boat	257 KB	500 x 500	bmp

Table 5.1 Berkas Citra Uji

# 5.4 Pelaksanaan dan Hasil Pengujian

Sub bab ini menjelaskan pelaksanaan dan hasil pengujian perangkat lunak dengan menggunakan data pengujian yang dijelaskan pada tabel 5.1.

# 5.4.1 Pengujian Proses Generate key

Tujuan dari pengujian ini untuk mendapatkan nilai p, r, g, dan z sebagai kunci untuk enkripsi dan dekripsi.

- a. Prosedur Pengujian
  - 1. Jalankan program seperti pada gambar 5.1.



Gambar 5.1 user interface program generate key

2. Tekan tombol *get prime* untuk mendapatkan bilangan prima dan nilai r (kunci privat) secara acak. Seperti pada gambar 5.2.

🖳 Generate Key ElGamal	
Generate Key	
p : get prime 16777153	
۲ : <b>13605324</b>	
g : Load Save	
7	
Z . Jave	
Generated	

Gambar 5.2 user interface mendapatkan bilangan prima dan nilai r

 Tekan tombol *load* untuk mendapatkan nilai-nilai intensitas citra g. Pada gambar 5.3 citra yang digunakan adalah citra *boat*.



Gambar 5.3 user interface mendapatkan nilai intensitas citra g

4. Selanjutnya tekan tombol *generate* untuk mendapatkan nilai-nilai z yang dihitung dengan persamaan  $z = g^r \mod p$  dan diubah menjadi citra. Seperti pada gambar 5.4.

As         Iso         Iso <thiso< th="">         Iso         <thiso< th=""> <thiso< th=""> <thiso< th=""></thiso<></thiso<></thiso<></thiso<>
r       : 13605324         g       : Load         Save       A6         A6       166         162       1933905       A6D691         A6       166         178388       150854       21         A7       167       9633759       92FDF       14         AA       170       13785799       D25AC7       21         A6       166       1378388       150854       21         A7       167       9633759       92FDF       14         AA       170       13785799       D25AC7       21         A5       166       1378388       150854       21         A9       169       4457339       440378       68         AA       170       13785789       D25AC7       21         A5       166       1378388       150854       21         A7       167       9633759       92FFDF       14         A7       167       9633759       92FFDF       14         A7       167       9633759       92FFDF       14         A9       169       4457339       440378       68         A7
g :         Load         Save           A6         166         1378388         150854         21           A6         166         1378388         150854         21           A7         167         9633759         92FDF         14           AA         170         1378388         150854         21           A6         166         1378388         150854         21           A7         167         9633759         92FDF         14           AA         170         13785799         D25AC7         21           A6         166         1378388         150854         21           A9         169         4457339         440378         68           AA         170         13785799         D25AC7         21           A5         166         1378388         150854         21           A7         167         9633759         92FDF         14           A7         167         9633759         92FDF         14           A9         169         4457339         440378         68           A7         167         9633759         92FDF         14           A9
A6         166         1378388         150854         21           A7         167         9633759         92FFDF         14           AA         170         13785799         D25AC7         21           A6         166         137338         150854         21           A7         167         9633759         92FFDF         14           AA         170         13785799         D25AC7         21           A6         166         1373388         150854         21           A9         169         4457339         440378         68           A6         166         1378388         150854         21           A7         167         9633759         92FFDF         14           A7         167         9633759         92FFDF         14           A7         167         9633759         92FFDF         14           A9         169         4457339         440378         68           A7         167         9633759         92FFDF         14           A9         169         4457339         440378         68           A7         167         9633759         92FFDF         <
A7         167         9633759         92FEDF         14           AA         170         13785799         D25AC7         21           A6         166         137338         150854         21           A9         169         4457339         40378         68           AA         170         13785799         D25AC7         21           A6         166         137338         150854         21           A7         167         9533759         D25AC7         21           A6         166         1378388         150854         21           A7         167         9533759         92FDF         14           A7         167         9633759         92FDF         14           A7         167         9633759         92FDF         14           A9         169         4457339         440378         68           A7         167         9633759         92FDF         14           A9         169         4457339         440378         68           A7         167         9633759         92FDF         14
AA         170         13785799         D25AC7         21           A6         166         1378388         150854         21           A9         169         4457339         44037B         68           AA         170         13785799         D25AC7         21           A6         166         1378388         150854         21           A7         166         1378388         150854         21           A7         167         9633759         92FDF         14           A7         167         9633759         92FDF         14           A9         169         4457339         44037B         68           A7         167         9633759         92FDF         14           A9         169         4457339         44037B         68           A7         167         9633759         92FDF         14
A6         166         1378388         150854         21           A9         169         4457339         440378         68           AA         170         13785799         D25AC7         21           A6         166         1378388         150854         21           AA         170         13785799         D25AC7         21           A6         166         1378388         150854         21           A7         167         9633759         92FDF         14           A7         167         9633759         92FDF         14           A9         169         4457339         440378         68           A7         167         9633759         92FDF         14           A7         167         9633759         92FDF         14
A9         169         4457339         440378         68           AA         170         13785799         D25AC7         21           A6         166         137838         150854         21           A7         167         9633759         92FDF         14
AA         170         13785799         D25AC7         21           A6         166         1378388         150854         21           A7         167         9633759         92FDF         14
A6         166         1378388         150854         21           A7         167         9633759         92FDF         14           A9         169         4457339         44037B         68           A7         167         9633759         92FDF         14
A7         167         9633759         92FFDF         14           A9         169         4457339         440378         68           A7         167         9633759         92FFDF         14
A7         167         9633759         92FFDF         14           A9         169         4457339         440378         68           A7         167         9633759         92FFDF         14           A9         169         4457339         440378         68           A7         167         9633759         92FFDF         14
Z         Save         A9         169         4457339         440378         68           A7         167         9633759         92FFDF         14
A7 167 9633759 92FFDF 14
A7 167 9633759 92FFDF 14
AA 170 13785799 D25AC7 21
A9 169 4457339 44037B 68
A7 167 9633759 92FFDF 14
A9 169 4457339 44037B 68
AA 170 13785799 D25AC7 21

Gambar 5.4 user interface mendapatkan nilai citra z

5. Simpan nilai p, r, dan citra z, serta melakukan percobaan dengan *load* citra *goldhill*. Seperti pada gambar 5.5.



Gambar 5.5 user interfacesave citra z

b. Hasil Pengujian

Dari percobaan diatas diperoleh hasil seperti pada tabel 5.2.

Tabel 5.2 Hasil Proses Generate Key

No.	Citra g	Ukuran	Citra z	Ukuran	Dimensi	Format
1	goldhill	65.0 KB		256 KB	200 x 200	bmp
2	boat	257 KB		1.00 MB	500 x 500	bmp

Dari hasil pengujian, Citra z yang dihasilkan ukurannya lebih besar dari citra g dan hasil citra z terlihat sedikit sama dengan citra g. Terbukti bahwa perangkat lunak yang sudah dibuat berhasil menjalankan proses *generate key* dengan baik.

### 5.4.2 Pengujian Proses Enkripsi

Tujuan dari pengujian ini untuk mendapatkan *cipher* citra a dan b dengan menggunakan bilangan prima dan kunci publik yaitu g dan z.

1. Prosedur PengujianJalankan program enkripsi. Seperti pada gambar 5.6.



Gambar 5.6 user interface program enkripsi

repository.ub.ac.id

2. Pilih *menu strip file* kemudian pilih pada *tool open* untuk memilih *plain* citra yang akan di enkripsi. Seperti pada gambar 5.7.



Gambar 5.7 user interface saat melakukan proses open plain citra

3. *Input* bilangan prima yang didapat dari *generate key*. Dan tekan tombol *Grayscalling* yang akan mengubah citra *true color* menjadi citra *grayscale*. Pada saat setelah *input* bilangan prima secara otomatis nilai k akan dipilih secara acak. Seperti pada gambar 5.8.

Encrypt ElGamal	
File	
Craycaling	p : 1577153 g : Load
Cipher A Cipher B	
Encrypt Process A Encrypt Process B	Z : Load
	k : 133

Gambar 5.8 *user interface* saat melakukan *input* bilangan prima dan proses *grayscalling* 

4. Tekan tombol *Load* citra kunci publik yaitu citra g dan z yang didapat dari proses *generate key*. seperti pada gambar 5.9



Gambar 5.9 user interface saat melakukan load citra g dan z

- 5. Kemudian tekan tombol Encrypt Process Adan Encrypt Process
- B. Seperti pada gambar 5.10. - 0 <u>- X</u> 🖳 Encrypt ElGama nput Key pixel baris pixel G р AG 16777153 162 A2 g Loa AG 166 166 AG A 167 170 166 169 170 166 167 167 167 AA AG Grayscalling A9 AA Cipher A Cipher B A6 A7 10 Ζ Load A A9 12 A7 13 167 170 169 167 A7 14 AA A9 15 16 A7 Encrypt Process A Encrypt Process B 169 A9 18 133 00:06.024 00:17.986 k

Gambar 5.10 user interface hasil Cipher Adan Cipher B

6. Setelah mendapatkan *cipher* citra Adan *cipher* citra B seperti pada gambar 5.10. Lakukan percobaan untuk *input plain* citra *baboon*, kunci citra g dan z. kemudian simpan masing-masing *cipher* citra pada *save toolmenu strip*. Seperti pada gambar 5.11.

	Input Key			atual bases	aburd balance
	🛃 Save an image		X	pixel bans	pixel Kolom
	Contraction in the American Allii Citra pape	- 512-512 × - 4a See	arch Lili Citra nannar 512-512	0	1
	S S S S S S S S S S S S S S S S S S S	• • • • • •	nen oji cura pepper 512x512 🎾	0	-
The service	Organize 🔻 New folder		E + 0	0	2
				0	3
			A REAL PROPERTY AND INCOME.	0	4
	Encrypt E			0	5
	Generate			0	6
caling	install			0	7
	Nilai_Inte hasil.bmp pep	bers512warna PlainCitra	Z 16285463 15838437 hmp	0	8
	Program	ionip (ojicon)ionip	130304571511p	0	9
- 6 m	👃 1. Gene			0	10
and the second	2. Encry			0	11
	📕 3. Decry 🗉		=	0	12
	📙 Uji Citra			0	12
and the second	Uji Citra Z 16777153			0	13
and the second	🔰 uji citra 5 👻 13605324.bmp		-	0	14
The second la second	File name			0	15
A CARLES AND A CARLES				0	16
Int Process A	Save as type: [Image Files(^.bmp)			0	17
ypt 1100665 /Y				0	18

Gambar 5.11 user interface saat melakukan save cipher citra A dan B

a. Hasil Pengujian

Dari percobaan diatas diperoleh hasil seperti pada tabel 5.3.

No.	Plain Citra	Cipher A	Ukuran	Cipher B	Ukuran	Dimensi
1.	baboon		256 KB		256 KB	200 x 200
2.	peppers		1.00 MB		1.00 MB	500 x 500

Tabel 5.3 Hasil Proses Enkripsi

Dari hasil uji tabel 3, hasil *cipher* citra mempunyai ukuran 2 kali dari *plain* citra. Dan untuk *cipher*A masih terlihat sedikit sama dengan citra z. sedangkan *cipher* B terlihat lebih acak.

# 5.4.3 Pengujian Proses Dekripsi

Tujuan dari pengujian ini untuk mendapatkan kembali *plain* citra *grayscale*.

a. Prosedur Pengujian

🖳 Decrypt Elgamal	NAME AND ADDRESS OF	No. 11 Margines Ministra	
File			
Cipher A	Cipher B		
p :	Plain Image		
r :			
Get Plainimage			
	Gambar 5.12 Use	r Interface Program dekr	ipsi
2. Pilit	n <i>menu tool strip</i> kem	udian pilih <i>load cipl</i>	her A dan load
cink	ar B Dilih cinhar cit	ra A dan B yang did	anat dari hasil
Cipi		Ta A dali D yang did	apat dari nash
pros	es enkripsi. Seperti p	ada gambar 5.13.	
Decrypt Elgamal			
le har A	Cipher P		
r []	Plain Image		
Get Plainimage			
Get Plainimage			

1. Jalankan program proses dekripsi. Seperti pada gambar 5.12.

Gambar 5.13 User Interface load cipher Adan cipher B

3. *Input* bilangan prima p dan nilai kunci privat r yang didapat dari proses *generate key*. Kemudian tekan tombol *Get Plainimage*. Seperti pada gambar 5.14.



Gambar 5.14 User Interface hasil proses dekripsi

4. Dari gambar 5.14 didapat hasil *plain* citra. Lakukan percobaan seperti diatas dengan menggunakan *cipher* citra A dan *cipher* citra B untuk *plain* citra *baboon*. Kemudian simpan dengan menggunakan *save menu tool strip* dan pilih *save plain image*. Seperti pada gambar 5.15.

ile	🖳 Save an image					×
Cipher A	🚱 🗢 📕 « Program ke	🕨 Uji Citra pepp	er 512x512 🔸	🕶 🍫 🛛 Search Uji	Citra pepper 512x512	9
	Organize 🔻 New folder				■ - (	0
	🍑 Generate 🔦	15838437.bmp	13605324.bmp	15838437 (ujiCorr).bmp	15838437.bmp	-
2 C	🍌 Nilai_Inte		I. Wal	11.1	Cha!	
	🍌 1. Gene					
1677715	3. Decry	B 16777153 13605324.bmp	boat.bmp	hasil.bmp	peppers512warna .bmp	E
: 1360532	🎉 Uji Citra	11.12				
Germanning	i uji citra 1 🔻		Land Street L	and a sec		-
	File name: Save as type: Image Fi	les(*.bmp)				÷
10:12. <mark>9</mark> 21	Alide Folders			Save	Cancel	

Gambar 5.15 User Interface save menu tool strip hasil proses dekripsi

repository.ub.ac.id

b. Hasil Pengujian

Dari percobaan diatas didapat hasil proses dekripsi. Seperti pada tabel 5.4.

No.	Plain Citra	Cipher A	Cipher B	Hasil <i>Plain</i> Citra	Ukuran Hasil <i>Plain</i> Citra	Dimensi
1.	baboon				256 KB	200 x 200
2.	peppers				1.00 MB	500 x 500

Tabel 5.4 Hasil Proses Dekripsi

Dari hasil uji tabel 4, terlihat hasil *plain* citra dapat ditemukan kembali. Dan ukuran hasil *plain* citra lebih besar dari ukuran *plain* citra awal.

# 5.4.4 Analisis hasil cipher citra dan plain citra

Pada bagian ini dilakukan 2 metode analisis, yaitu analisis korelasi dan analisis histogram.

### 5.4.4.1 Analisis Korelasi

Di dalam natural-*image*, *pixel-pixel* yang bertetangga memiliki hubungan linier yang kuat. Ini ditandai oleh koefisien korelasinya yang tinggi (mendekati +1 atau -1). Di dalam citra acak, korelasi antar *pixel* bertetangga tidak ada atau koefisien korelasinya mendekati nol. Enkripsi citra bertujuan membuat korelasi *pixel-pixel* yang bertetangga di dalam *cipher-image* menjadi lemah atau dengan kata lain membuat koefisien korelasinya mendekati nol. Untuk mengetahui korelasi *pixel-pixel* di

dalam plain-image maupun cipher-image, maka dihitung koefisien korelasi antara dua pixel bertetangga secara horizontal [f(i,j) dan f(i, j+1)], dua *pixel* bertetangga secara vertkal [f(i,j) dan f(i+1, j)], dan dua pixel bertetangga secara diagonal f(i,j) dan f(i+1, j+1)]. Dengan mengambil 1000 pasang *pixel* bertetangga pada setiap arah (vertikal, horizontal, dan diagonal), masing-masing pada citra plainimage cipher-image. kehilangan dan Tanpa generalisasi, analisis korelasi dilakukan pada citra grayscale saja. Dalam hal ini x dan y adalah nilai keabuan dari dua pixel bertetangga. [7] Berikut hasil perhitungan korelasi pada tabel 5.5.

Fabel 5.5	Perbandingan Koefisien Korelasi antara dua	pixel
	bertetangga	

Citra	Korelasi	Citra	Kore	lasi
baboon	Horizontal 0.54847 Vertikal 0.53330 Diagonal 0.39401	4 6 4 peppers	Horizontal Vertikal Diagonal	0.99338 0.262402 0.251838
cipher A	Horizontal 0.40565 Vertikal 0.31176 Diagonal 0.20686	2 6 2 <i>cipher</i> A	Horizontal Vertikal Diagonal	0.357317 0.248607 0.239924
cipher B	Horizontal 0.1317 Vertikal 0.1915 Diagonal 0.0276	74 18 32 <i>cipher</i> B	Horizontal Vertikal Diagonal	0.704049 0.051994 0.029243

Dari tabel 5.5 dapat dilihat bahwa koefisien *plain* citra lebih mendekati 1 daripada koefisien *cipher* citra, yang

mengindikasikan *plain* citra mempunyai korelasi yang lebih kuat dari pada *cipher* citra. Pada koefisien *cipher*A masih terlihat adanya sedikit korelasi. Sedangkan *cipher* B koefisien korelasi mendekati 0 yang berarti pixel-pixel yang bertetangga tidak lagi berkolerasi.

Untuk melihat lebih jelas korelasi antara pixel-pixel bertetangga, maka tabel 5.6 memperlihatkan distribusi korelasi pixel-pixel yang bertetangga. Pada *plain* citra dapat dilihat bahwa pixel-pixel yang bertetangga nilainilainya saling berkolerasi. Sedangkan pada *cipher* citra A dan B nilainya tersebar dan sedikit nilai yang saling berkolerasi.

 Tabel 5.6 Distribusi Korelasi Pixel-pixel Bertetangga Pada Plain Citra dan

 Cipher Citra dari Citra 'peppers'



### 5.4.4.2 Analisis Histogram

Di dalam bidang pengolahan citra histogram memperlihatkan distribusi nilai *pixel* di dalam sebuah citra. Histogram digunakan penyerang (*attacker*) untuk melakukan kriptanalisis dengan memanfaatkan frekuensi kemunculan *pixel* di dalam histogram. Penyerang berharap nilai *pixel* yang sering muncul di dalam *plain-image* berkorelasi dengan nilai *pixel* yang sering muncul di dalam *cipher-image*. Dengan menganalisis frekuensi kemunculan nilai *pixel*, penyerang mendeduksi kunci atau *pixel-pixel* di dalam *plain-image*.

Agar penyerang tidak dapat menggunakan histogram untuk melakukan analisis frekuensi, maka histogram *plainimage* dan histogram *cipherimage* seharusnya berbeda secara signifikan atau secara statistik tidak memiliki kemiripan. Oleh karena itu, histogram *cipher-image* seharusnya datar (*flat*) atau secara statistik memiliki distribusi (relatif) *uniform*. Distribusi yang (relatif) *uniform* pada *cipher-image* adalah sebuah indikasi bahwa algoritma enkripsi citra memiliki tingkat keamanan yang bagus. [7]

 Tabel 5.7 Histogram Citra 'peppers'



Pada tabel 5.7 memperlihatkan histogram pada *cipher* B terlihat datar (flat) atau terdistribusi uniform dan berbeda signifikan dengan histogram *plain* citra dan *cipher* A.