

BAB IV

HASIL DAN UJI COBA

IV.1. Uji Coba

Proses uji coba dari aplikasi ini dengan melakukan pengujian langsung terhadap pesan yang akan dienkripsi maupun didekripsi.

Berikut adalah langkah-langkah yang dilakukan dalam proses pengujian aplikasi :

1. Melakukan instalasi *eclipse*.
2. Membuka aplikasi yang telah selesai dibuat dengan cara mengimport kedalam *workspace eclipse*.
3. Setelah proses import selesai dengan benar, langkah selanjutnya menginstal aplikasi *wifi adb* dari *playstore* ke *handphone android*.
4. Buka aplikasi *wifi adb* tersebut dan hubungkan dengan laptop atau komputer yang sudah terdapat program yang telah dibuat.
5. Lalu jalankan program aplikasi yang sudah dimasukkan tersebut.
6. Jika tidak terjadi kesalahan dalam aplikasi maka aplikasi tersebut akan berjalan sempurna dan terbuka jendela baru.

IV.2. Hasil

Berikut ini adalah hasil dan analisa hasil dari perancangan aplikasi enkripsi data pesan singkat dengan menggunakan algoritma ElGamal berbasis *android*. Pada pembuatan aplikasi ini penulis membuat keamanan sistem data SMS yang mana dalam program ini pesan yang akan dikirim terenkripsi dengan menggunakan algoritma yang sudah ditentukan.

Pada umumnya orang mengirim pesan tanpa menggunakan enkripsi, jadi pada pengiriman pesan bisa di hacker atau di seludupi orang yang tidak bertanggung jawab. Maka dari itu penulis membuat perancangan aplikasi enkripsi data pesan singkat dengan menggunakan algoritma ElGamal berbasis *android*, yang mana program ini dibuat dengan sebaik mungkin.

Dengan adanya program ini saya bisa lebih aman mengirim pesan yang rahasia kepada teman saya tanpa diketahui oleh orang lain. Aplikasi ini sangat mudah di pahami dan dipelajari dan aplikasi ini bisa dijalankan didalam *Smartphone*.

IV.2.1. Tampilan Layar

Pada bagian ini merupakan penjelasan dari hasil rancangan *interface* untuk administrator yang terdiri dari sebagai berikut :

1. *Interface Splash*

Adapun hasil dari rancangan *interface splash* dapat dilihat pada gambar IV.1 dibawah ini.



Gambar IV.1 Interface Splash

2. Interface Menu Utama

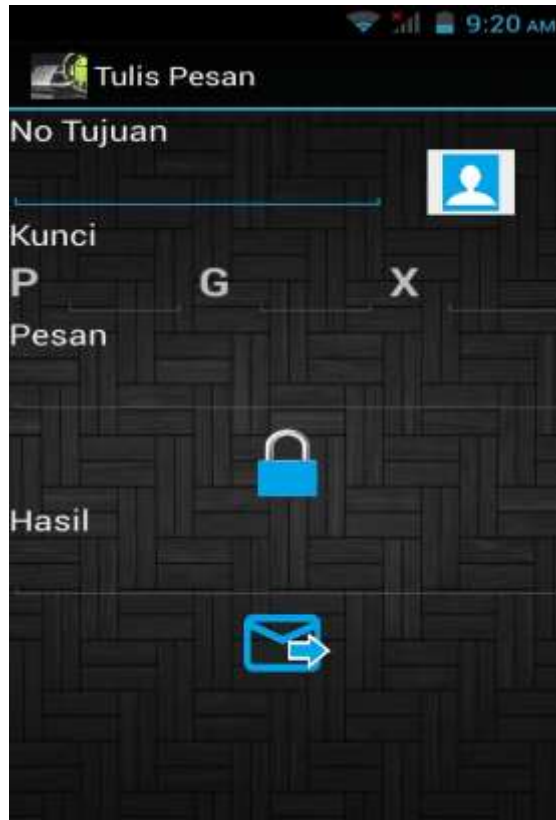
Pada *interface* menu ini menampilkan *form* yang disediakan untuk pengguna mengakses sistem atau untuk menjalankan aplikasi yang telah dirancang, dimana pada menu terdapat *form-form* yang mempunyai fungsi masing-masing. Adapun *interface menu* dapat dilihat pada gambar IV.2 berikut ini



Gambar IV.2. Interface Menu Utama

3. Interface Menu

Pada *interface* menu ini menampilkan *form* yang disediakan untuk pengguna menjalankan aplikasi pesan yang telah dirancang, dimana pada menu terdapat fungsi mengenkripsi pesan dan mengirim pesan. Adapun *interface* menu dapat dilihat pada gambar IV.3 berikut ini



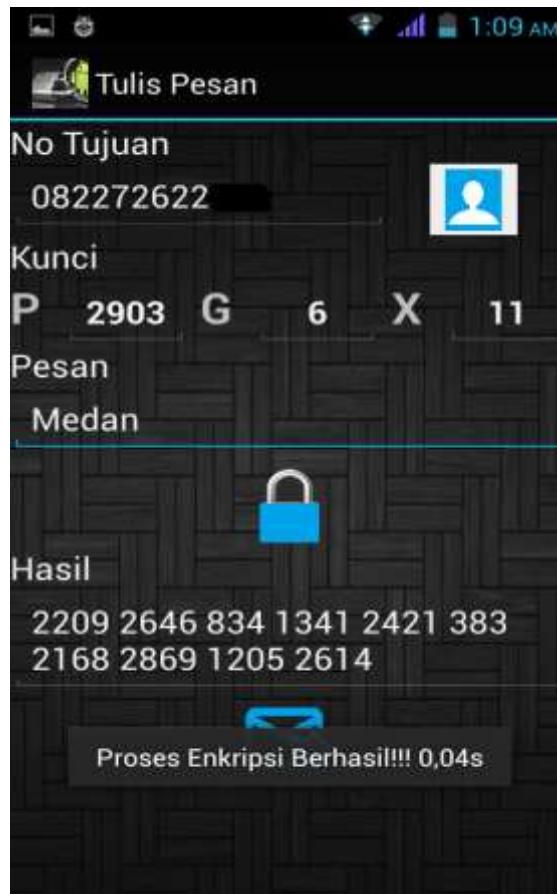
Gambar IV.3. Interface Menu Tulis Pesan

Pada desain *menu* tulis pesan di aplikasi untuk keamanan data pesan singat ini dapat dijelaskan sebagai berikut :

1. No tujuan, berfungsi untuk memasukkan no.
2. Kontak, berfungsi untuk mengambil no tujuan dari penyimpanan no.
3. Kunci p, g, berfungsi untuk menginputkan kunci publik untuk melakukan enkripsi pesan.
4. Kunci x, berfungsi untuk menginput kunci privat sebelum melakukan enkripsi pesan.
5. Pesan, berfungsi untuk memasukkan pesan yang akan di enkripsi.
6. Tombol enkripsi, berfungsi untuk memproses enkripsi pesan.
7. Hasil, berfungsi untuk menampilkan hasil proses dari enkripsi pesan.
8. Tombol kirim, berfungsi untuk mengirimkan pesan.

4. *Interface Form* Hasil Enkripsi

Interface ini merupakan *form* setelah proses enkripsi pesan berjalan lancar. Adapun *interface form* hasil enkripsi dapat dilihat pada gambar IV.4 berikut ini.



The screenshot shows a mobile application interface with a dark background and a woven texture. At the top, there is a status bar with icons for signal, battery, and time (1:09 AM). Below the status bar is a header with a small icon and the text "Tulis Pesan". The main form contains the following fields and data:

- No Tujuan**: 082272622, with a profile icon to the right.
- Kunci**: P 2903 G 6 X 11
- Pesan**: Medan
- Hasil**: 2209 2646 834 1341 2421 383
2168 2869 1205 2614

Below the "Hasil" field, there is a blue padlock icon and a message box that says "Proses Enkripsi Berhasil!!! 0,04s".

Gambar IV.4. *Interface Form* Hasil Enkripsi

5. *Interface Form* Hasil Dekripsi

Interface ini merupakan *form* setelah proses dekripsi pesan berjalan. Adapun *interface form* hasil dekripsi dapat dilihat pada gambar IV.5 berikut ini.



Gambar IV.5. *Interface Form* Hasil Dekripsi

6. *Interface Form About*

Pada *interface form about* terdapat keterangan dari aplikasi yang dibuat oleh perancang. Adapun *interface form about* dapat dilihat pada gambar IV.6 berikut ini.



Gambar IV.6. Interface Form About

VI.2.2. BlackBox

Pengujian *blackbox* (*blackbox testing*) adalah salah satu metode pengujian perangkat lunak yang berfokus pada sisi fungsionalitas. Tahap pengujian atau testing merupakan salah satu tahap yang harus ada dalam sebuah siklus pengembangan perangkat lunak (selain tahap perancangan atau desain). Berikut pengujian sistem dengan metode *blackbox testing* yang disajikan pada tabel pengujian *blackbox* seperti dibawah ini.

Tabel IV.1 Hasil Pengujian Black Box Aplikasi Enkripsi Teks Menggunakan Algoritma Elgamal

No	Form	Keterangan	Hasil
1	Masuk ke aplikasi ElGamal	Sistem akan membuka aplikasi menampilkan layar pembuka aplikasi dan menuju menu pilihan	Valid
2	Memilih menu tulis pesan	Akan membuka form tulis pesan	Valid
3	Klik tulis pesan, no. tujuan, masukan Key, enkripsi pesan dan kirim sms	Menghasilkan plainteks yang tersimpan di kotak masuk	Valid
4	Lanjut proses dekripsi dengan melihat kotak masuk dan masukan key klik hasil	Menghasilkan chiperteks yang telah di dekripsi	Valid
5	Melihat pesan terkirim	Akan tampil hasil yang telah di kirim	Valid
6	Memilih menu <i>about</i>	Akan tampil menu <i>About</i>	Valid

IV.2.3. *Hardware/Software Yang Dibutuhkan*

Untuk menjalankan program ini dibutuhkan perangkat keras (*hardware*) dan perangkat lunak (*software*) sebagai berikut :

a. Perangkat Keras (*Hardware*)

1. Prosesor *Intel Core i3* atau diatasnya.
2. RAM dengan kapasitas 2Gb
3. *Keyboard, Mouse*
4. *Android Mobile Phone*

b. Perangkat Lunak (*Software*)

1. *SDK Java* sebagai mesin aplikasi *Java* pada aplikasi desktop

2. Sistem operasi *android* pada *mobile phone*
3. *Wifi* ADB dari *playstore*

IV.3. Analisa Hasil

IV.3.1 Pasangan Kunci

Prosedur pembangkitan kunci sistem kriptografi elgamal adalah sebagai berikut :

1. Kunci publik pertama (p) merupakan bilangan prima lebih besar dari 255.
2. Kunci privat (x) didapat dengan cara menentukan secara acak dari bilangan 1 hingga $p - 2$.
3. Kunci publik kedua (g) merupakan bilangan yang dimulai dari 2,3,4,5 dan seterusnya hingga hasil perhitungan $g^{(p-1)/2} \bmod p$ tidak sama dengan 1.
4. Kunci publik ketiga (y) merupakan hasil perhitungan dengan rumus $y = g^x \bmod p$.

Tabel IV.2 Pasangan Kunci Sistem Kriptografi ElGamal

Kunci Publik P	Kunci Publik G	Kunci Privat X
2903	6	11
863	5	373
911	7	199
719	11	631
2909	7	13

IV.3.2. Hasil Uji Coba Enkripsi

Berikut ini adalah tabel hasil pengujian enkripsi pesan karakter dengan menggunakan kunci publik $P = 2903$, $G = 6$, dan kunci privat $X = 11$.

Tabel IV.3 Hasil Pengujian Enkripsi

No	Karakter	Desimal	k	$C1 = G^k \text{ Mod } P$	$C2 = Y^k \text{ m Mod } P$
1.	M	117	784	2209	2646
2.	e	116	2315	834	1341
3.	d	97	826	2421	383
4.	a	109	422	2168	2869
5.	n	97	2806	1205	2614

IV.3.3 Hasil Uji Coba Dekripsi

Berikut ini adalah tabel hasil pengujian dekripsi pesan karakter dengan menggunakan kunci publik $P = 2903$ kunci privat $X = 11$.

Tabel IV.4 Hasil Pengujian Dekripsi

No	C1	C2	$D = \{C1^{p-x-1} \cdot C2\} \text{ Mod } P$	Karakter
1.	2209	2646	77	M
2.	834	1341	101	e
3.	2421	383	100	d
4.	2168	2869	97	a
5.	1205	2614	110	n

IV.3.4. Kelebihan Dan Kekurangan

a) Kelebihan aplikasi yang dirancang adalah sebagai berikut :

1. Aplikasi dapat menjaga keamanan dan kerahasiaan pesan dari orang yang tidak bertanggung jawab.

2. Aplikasi ini bekerja dengan kombinasi dari tiga kunci publik dan satu kunci privat yang merupakan bilangan prima.
 3. Mempermudah *user* dalam mengamankan data.
 4. Mudah digunakan karena *user interface* yang sederhana
- b) Kekurangan aplikasi yang dirancang adalah sebagai berikut :
1. Tampilan dan *layout* dari aplikasi masih sederhana.
 2. Proses enkripsi hanya bisa dilakukan pada pesan karakter saja, tidak bisa *file* audio, gambar dan video.
 3. Biaya untuk kirim pesan yang telah di enkripsi menjadi *Chiphertext* akan lebih besar, karena panjang hasil enkripsi pesan menjadi dua kali lipat dari sebelumnya.
 4. Ketika mengenkripsi pesan dengan jumlah karakter yang terlalu panjang akan memakan waktu yang cukup lama.