BAB IV

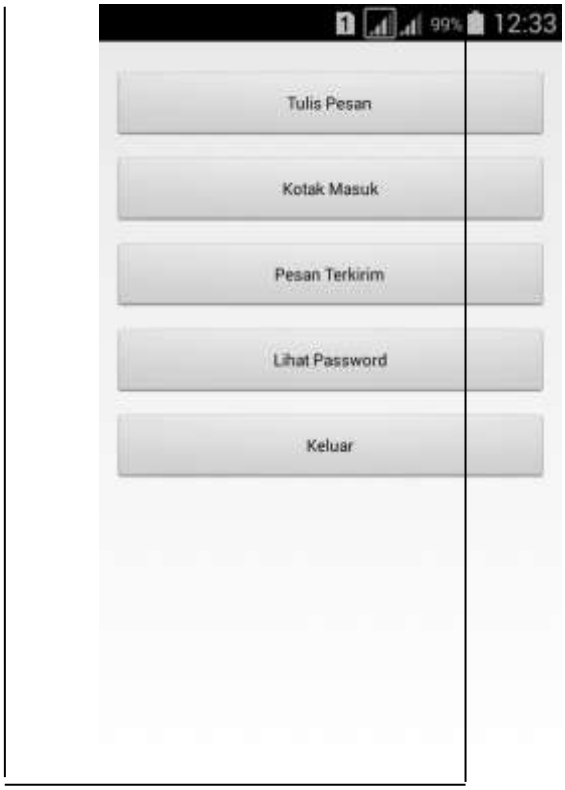
HASIL DAN UJI COBA

IV.1. Hasil

Pada tahapan ini penulis akan menjelaskan tentang hasil dan informasi-informasi kinerja yang diperoleh dari perangcangan pengamanan SMS yang telah dibuat. Pengamanan yang digunakan adalah algoritma kriptografi klasik *vigenere cipher* dan *one time pad* yaitu dengan cara mengenkripsi pesan SMS menggunakan salah satu algoritma tersebut. Dan untuk memudahkan pengguna penulis menggunakan beberapa *form, database* , dan beberapa jalan pintas yang disediakan aplikasi yang telah dirancang. Setelah melakukan pengujian aplikasi penulis memperoleh informasi-informasi baik tentang sistem aplikasi maupun tampilah aplikasi. Berikut beberapa penjelasan dan hasil tampilan aplikasi yang dibuat.

IV.1.1. Tampilan Menu Utama

Tampilan menu utama merupakan sebuah *interface* yang akan ditampilkan pertama kali saat aplikasi dijalankan. Pada perancangan ini, penulis membuat beberapa *Button* untuk melakukan *event* yang diinginkan pengguna. Untuk tampilan menu utama pada perancangan ini dapat dilihat pada gambar IV.1.



Gambar IV.1. Tampilan Menu Utama

1. *Button* tulis pesan,digunakan untuk menulis dan mengirim pesan SMS.
2. *Button* kotak masuk, digunakan untuk melihat pesan yang telah diterima.
3. *Button* pesan terkirim, digunakan untuk melihat pesan yang telah dikirim.
4. *Button* lihat *password*, digunakan untuk melihat kontak yang telah disimpan ke *database* dengan *password*.
5. *Button* keluar, digunakan untuk keluar dari aplikasi.

IV.1.2. Tampilan Tulis Pesan

Menu tulis pesan memiliki fungsi untuk mengirim pesan kepada nomor tujuan. Pada tampilan ini terdapat beberapa komponen, yaitu sebagai berikut:

1. *Text view* nama, yaitu sebuah tampilan untuk menampilkan informasi nama kontak.
2. *Edit text* nomor HP, yaitu sebuah *field* yang digunakan untuk nomor telepon.

3. *Image button* kontak, untuk memperoleh kontak dari kontak telepon atau SIM.
4. *Edit text password, field* untuk memasukkan *password*.
5. *Edit text* pesan, *field* untuk memasukkan pesan.
6. *Button* Enkripsi, tombol untuk mengenkripsi pesan.
7. *Edit text ciphertext*, yaitu sebuah tampilan untuk menampilkan hasil enkripsi.
8. *Button* simpan, untuk menyimpan informasi kontak ke dalam *database* .
9. *Button* kirim, tombol yang berfungsi untuk mengirim pesan ke nomor tujuan.

Adapan tampilan tulis pesan pada perancangan ini dapat dilihat pada gambar IV.2 berikut:

Gambar IV.2. Tampilan Menu Tulis Pesan

IV.1.3. Tampilan Kotak Masuk Dan Pesan Terkirim

Kotak masuk adalah tampilan informasi yang digunakan untuk melihat pesan yang diterima dari pengirim pesan. Sedangkan pesan terkirim adalah tampilan informasi yang

digunakan untuk melihat pesan yang telah terkirim ke nomor tujuan. Kotak masuk dan pesan terkirim memiliki komponen yang sama dapat dijelaskan sebagai berikut:

1. *Text view* informasi, digunakan untuk menampilkan label kotak masuk atau pesan terkirim.
2. *Text view* nama, digunakan untuk menampilkan nama pengirim pada kotak masuk dan nama penerima pada pesan terkirim.
3. *Text view* tanggal, digunakan untuk menampilkan tanggal pengiriman pada kotak masuk dan nama menerima pada pesan terkirim.
4. *Text view* ciphertext, digunakan untuk menampilkan pesan *ciphertext* baik pada kotak masuk maupun pesan terkirim.

Berikut tampilan kotak masuk dan pesan terkirim.

Gambar IV.3. Tampilan Menu Kotak Masuk

Gambar IV.4. Tampilan Menu Pesan Terkirim

IV.1.4. Tampilan Deskripsi Pesan

Tampilan deskripsi pesan adalah tampilan yang digunakan untuk mendeskripsi pesan yang terenkripsi pada kotak masuk. Berikut komponen yang terdapat pada tampilan deskripsi pesan:

1. *Text view* nama, yaitu sebuah tampilan untuk menampilkan informasi nama pengirim.

2. *Text view* nomor HP, yaitu sebuah tampilan yang digunakan untuk nomor telepon pengirim.
3. *Text view* tanggal, yaitu sebuah tampilan yang digunakan untuk tanggal pesan diterima.
4. *Text view ciphertext*, sebuah tampilan pesan *ciphertext* yang diterima.
5. *Edit text password*, field untuk menginput *password* deskripsi.
6. *Button* Deskripsi, tombol untuk mendeskripsi pesan.
7. *Text view plaintext* , sebuah tampilan pesan yang sudah dideskripsi.
8. *Button* hapus, sebuah tombol untuk menghapus pesan yang dibuka.

Tampilan Deskripsi Pesan dapat dilihat pada gambar IV.5:

Gambar IV.5. Tampilan Deskripsi Pesan

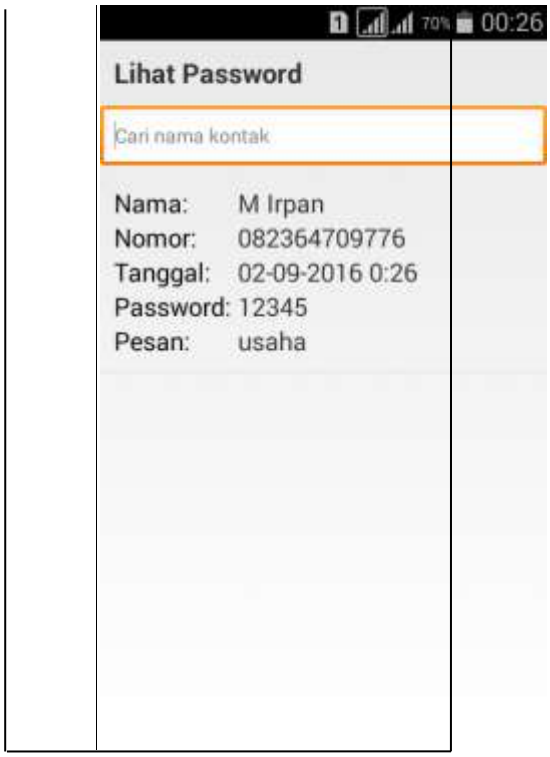
IV.1.5. Tampilan Lihat *Password*

Pada tampilan lihat *password*, komponennya hampir sama dengan kotak masuk, hanya saja ditambahkan satu *edit text*. Tampilan lihat *password* merupakan *interface* tentang informasi

kontak dimana terdapat tambahan *password* di dalamnya. Berikut komponen-komponen yang terdapat pada *interface* lihat *password*:

1. *Text view* lihat *password*, yaitu informasi menunjukkan bahwa kontak tersimpan sedang dibuka.
2. *Edit text search*, yaitu *field* yang berfungsi mencari kontak yang terdaftar melalui *filter* nama.
3. *List view* daftar kontak, adalah daftar kontak yang tersimpan. Dimana di dalamnya terdapat *text view* nama, nomor, *password*, dan pesan.

Adapun tampilan dari lihat *password* adalah sebagai berikut:



Gambar IV.6. Tampilan Menu Lihat *Password*

IV.2. Pembahasan

Pembahasan yang dimaksud pada tahapan ini adalah bagaimana proses enkripsi dan deskripsi dilakukan pada aplikasi pengamanan SMS yang telah dirancang oleh penulis.

IV.2.1. Pembahasan Enkripsi Pesan

Pada aplikasi ini penulis menggunakan dua metode kriptografi *vigenere cipher* dan *one time pad*. Dimana pesan *ciphertext* yang akan diperoleh yaitu dengan menggabungkan kedua algoritma tersebut.

1. Enkripsi *Vigenere Cipher*

Penulis menggunakan tambahan karakter pada perancangan ini agar pengguna lebih nyaman tanpa kekurangan enkripsi karakter. Berikut karakter yang dapat di enkripsi pada *vigenere cipher* dengan *index* yang dimulai dari 0:

Tabel IV.1. *Index* Alfabet *Vigenere Cipher*

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
V	W	X	Y	Z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41
q	r	s	t	u	v	w	x	y	z	1	2	3	4	5	6	7	8	9	0	~
42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62
!	@	#	$	%	^	&	*	(	)	_	+	{	}	\	|	:	;	“	‘	,
63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83
.	/																			
84	85	86																		

Untuk memperoleh *ciphertext* menggunakan rumus Ci = (Pi + Ki) mod 87.

Diketahui *plaintext* “usaha” dan *password* “12345” sehingga *index* yang didapat yaitu 46, 44, 26, 33, 26 untuk *plaintext* dan 52, 53, 54, 55, 56 untuk *password*, jadi *ciphertext* yang diperoleh adalah:

Plaintext	46	44	26	33	26
Password	52	53	54	55	56
Ciphertext	11	10	80	1	82

Ciphertext = LK;B'

2. Enkripsi *One time pad* (OTP)

Pada proses enkripsi *one time pad* kita hanya meng-XOR *plaintext* dengan sandi. Pertama ubah *plaintext* ke biner lalu lakukan perhitungan XOR dimana logika XOR 1 sama 1 menghasilkan 0, 1 sama 0 menghasilkan 1, 0 sama 0 menghasilkan 0.

Diketahui *plaintext* "LK;B"' dan *password* "12345" akan diperoleh bilangan biner 01001100, 01001011, 00111011, 01000010, 00100111 untuk *plaintext* dan 00110001, 00110010, 00110011, 00110100, 00110101 untuk *password* sehingga *plaintext* yang didapat:

Plaintext	01001100	01001011	00111011	01000010	00100111
Password	00110001	00110010	00110011	00110100	00110101
Ciphertext	01111101	01111001	00001000	01110110	00010010

Sehingga *ciphertext* yang diperoleh adalah "} – y – BS – v – DC2".

Gambar IV.7. Tampilan Enkripsi Pesan

IV.2.2. Pembahasan Deskripsi Pesan

Setelah dilakukan enkripsi *one time pad* pada enkripsi pesan, untuk mendeskripsi pesan harus dilakukan deskripsi *one time pad* terlebih dahulu kemudian deskripsi vigenere cipher, deskripsi *one time pad* dapat dijelaskan sebagai berikut.

1. Deskripsi *One Time Pad* (OTP)

Untuk memperoleh *plaintext* menggunakan rumus Pi = Ci XOR Ki, tidak jauh berbeda dengan rumus enkripsi pada XOR yaitu dengan mengubah letak Pi dan Ci. Diketahui *ciphertext* "} – y – BS – v – DC2" dan *password* "12345" akan diperoleh bilangan biner 01111101, 01111001, 00001000, 01110110, 00010010 untuk *plaintext* dan 00110001, 00110010, 00110011, 00110100, 00110101 untuk *password* sehingga *plaintext* yang didapat:

Ciphertext	01111101	01111001	00001000	01110110	00010010
Password	00110001	00110010	00110011	00110100	00110101
Plaintext	01001100	01001011	00111011	01000010	00100111

Sehingga *ciphertext* yang diperoleh adalah "LK;B"'.

2. Deskripsi *Vigenere Cipher*

Untuk memperoleh *plaintext* menggunakan rumus Pi = (Ci – Ki) mod 26, untuk Ci >= Ki dan Pi = (Ci - Ki) + 26, untuk Ci <= Ki. Diketahui *ciphertext* "LK;B"' dan *password* "12345" sehingga *index* yang didapat yaitu 11, 10, 80, 1, 82 untuk *ciphertext* dan 52, 53, 54, 55, 56 untuk *password*, jadi *plaintext* yang diperoleh adalah:

Ciphertext	11	10	80	1	82
Password	52	53	54	55	56
Plaintext	46	44	26	33	26

Plaintext = usaha

Untuk tampilan hasil deskripsi pada aplikasi pengamanan SMS dapat dilihat pada gambar IV.9.

Gambar IV.8. Tampilan Deskripsi Pesan

IV.3. Uji Coba

Pada tahapan ini penulis akan menjelaskan tentang pengujian sistem pada aplikasi pengamanan SMS menggunakan algoritma *vigenere cipher* dan *one time pad*, dimana akan di buat penjelasan dalam bentuk *blackbox*. *Blackbox* adalah suatu pengujian aplikasi dalam bentuk penjelasan fungsi komponen maupun spesifikasi pada aplikasi tersebut. Pada perancangan aplikasi pengamanan SMS ini punulis melakukan pengujian fungsi pada komponen dan kejadian apa yang akan diperoleh pada hasil pengujian. Berikut tabel hasil pengujian pada aplikasi pengamanan SMS.

Table IV.2. Tabel Pengujian Pengiriman Pesan

Deskripsi	Skenario Pengujian	Hasil yang diharapkan	Keterangan
Pengujian	Klik tombol	Mengenkripsi pesan dengan	Sesuai

Tombol Enkripsi	Enkripsi	*password* menggunakan penggabungan dua metode *vigenere cipher* dan *one time pad.*	
	Klik tombol Enkripsi tanpa menginput pesan dan *password*	Menampilkan notifikasi “pesan atau *password* belum diisi”.	Sesuai
Pengujian Tombol kirim pesan	Klik tombol kirim pesan	Mengirim pesan yang sudah dienkripsi dan menampilkan notifikasi apakah pesan sudah terkirim.	Sesuai
	Klik tombol kirim tanpa mengirim *form*	Menampilakan notifikasi *form* belum lengkap.	Sesuai
Pengujian Tampilan notifikasi	Notifikasi akan ditampilkan saat pesan telah terkirim	Menampilkan notifikasi pesan terkirim dan menyimpan pesan secara otomatis ke *database* “DbSMS”	Sesuai

IV.3.1. Spesifikasi Kebutuhan Aplikasi

Spesifikasi aplikasi adalah hal-hal yang berkaitan pada proses aplikasi dan rincian *platform* yang dibutuhkan pada aplikasi tersebut.

1. Sebuah laptop dengan spesifikasi sebagai berikut:
    a. Processor intel core i3
    b. Ram 2 gb
    c. Hardisk 500 gb
2. Spesifikasi perangkat lunak sebagai berikut:
    a. Android SDK
    b. Java Depelopment Kit (JDK)
    c. Eclipse
3. Pengujian sistem sebagai berikut:

a. Proses enkripsi *vigenere cipher* dan *one time pad*
b. Proses deskripsi *vigenere cipher* dan *one time pad*
c. Tampilan sistem
d. Fungsi tombol

IV.4. Kelebihan Dan Kekurangan Sistem

Setelah melakukan proses pengujian pada perancangan ini penulis menemukan beberapa kelebihan dan kekurangan. Berikut kelebihan dan kekurangan sistem pada aplikasi pengamanan SMS yang telah dirancang.

IV.4.1. Kelebihan Sistem

Adapun kelebihan dari aplikasi pengamanan SMS yang telah dirancang adalah sebagai berikut:

1. Tampilan aplikasi lebih menarik.
2. Pesan SMS yang dikirim lebih aman karena sudah dienkripsi menggunakan algoritma kriptografi.
3. Sistem keamanan yang digunakan yaitu mengenkripsi pesan SMS menggunakan dua metode, *vigenere cipher* dan *one time pad.*
4. Menggunakan *database* untuk penyimpan informasi sandi.
5. Penggunaan aplikasi yang mudah dan nyaman karena menggunakan beberapa *shortcut*, seperti buka kontak, simpan informasi kontak dan memasukkan sandi secara otomatis apabila membukan kontak yang sudah disimpan.

IV.4.2. Kekurangan Sistem

Berikut beberapa kekurangan dari aplikasi pengamanan SMS yang telah dirancang:

1. Masih menggunakan algoritma kriptografi klasik sehingga mudah dipecahkan oleh kriptanalis.
2. Terdapat beberapa karakter yang tidak bisa dienkripsi oleh *vigenere cipher*.
3. Tidak terdapat tombol hapus kontak yang sudah disimpan dalam *database* .