

BAB IV

HASIL DAN PEMBAHASAN

IV.1. Hasil

Hasil yang disajikan oleh sistem berdasarkan Perancangan Keamanan Data SMS Dengan Menggunakan Kriptografi Vigenere Cipher Berbasis Android adalah berupa sistem yang menghasilkan informasi-informasi penyampaian data berupa aplikasi vigenere seperti yang telah dirancang, form-form yang berfungsi sebagai media pengolahan data riwayat pesan agar menjadi lebih mudah dan cepat dalam penyebaran informasi dan dilakukan pengujian terhadap sistem untuk mengetahui tingkat keamanan dari sistem yang dirancang. Adapun pembahasan hasil yang disajikan adalah tampilan hasil sistem seperti berikut :

IV.1.1. Tampilan Hasil

Berikut ini dijelaskan tentang tampilan hasil dari Perancangan Keamanan Data SMS Dengan Menggunakan Kriptografi Vigenere Cipher Berbasis Android dapat dilihat sebagai berikut :

1. Tampilan Menu Awal Aplikasi Vigenere

Halaman utama merupakan halaman yang akan ditampilkan ketika pertama kali perangkat lunak dijalankan. Halaman utama ini berfungsi untuk menampilkan menu-menu utama yang terdapat pada aplikasi sms. Pada halaman utama ini terdapat tombol untuk membuka dan menampilkan halaman pesan baru.

Adapun tampilan menu awal aplikasi vigenere terlihat seperti pada gambar

IV.1 berikut :



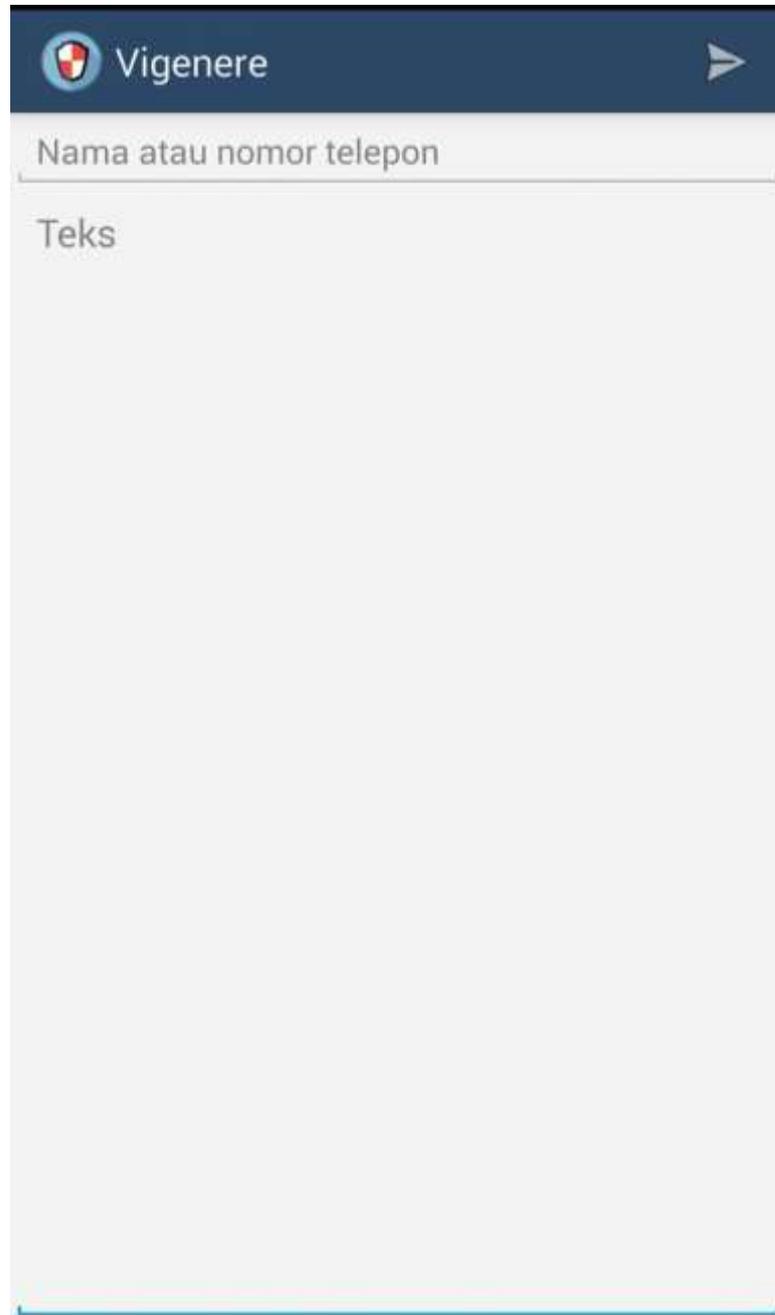
Gambar.IV.1. Tampilan Tampilan Awal Aplikasi Vigenere

2. Tampilan Menu Pesan Baru

Halaman menu pesan baru merupakan halaman yang akan menampilkan menu pesan baru. Pada halaman pesan baru ini terdapat beberapa komponen yang mendukung proses enkripsi pesan, yaitu :

- a. Nama atau nomor telepon, yaitu field yang menampung nomor telepon yang ingin dikirim pesan sms.
- b. Teks, yaitu field yang menampung teks yang akan dienkripsi.
- c. Enkripsi, tombol untuk membuka dan menampilkan halaman enkripsi pesan.

Adapun tampilan menu untuk membuat pesan baru terlihat seperti pada gambar IV.2 berikut :



Gambar.IV.2. Tampilan Menu Pesan Baru

3. Tampilan Menu Enkripsi Pesan

Halaman menu enkripsi pesan merupakan halaman yang akan menampilkan menu enkripsi pesan. Pada halaman enkripsi ini terdapat beberapa komponen yang mendukung proses enkripsi pesan, yaitu :

- a. Kata sandi, merupakan field yang menampung kunci.
- b. Enkripsi pesan, merupakan tombol untuk melakukan proses enkripsi pesan.
- c. Pesan chipper, merupakan field yang menampung hasil enkripsi yang telah diproses oleh sistem.
- d. Kirim, yaitu tombol untuk melakukan pengiriman pesan.
- e. Batal, yaitu tombol untuk membatalkan proses pengiriman pesan.

Tampilan menu untuk mengenkripsi pesan terlihat seperti pada gambar IV.3 berikut :



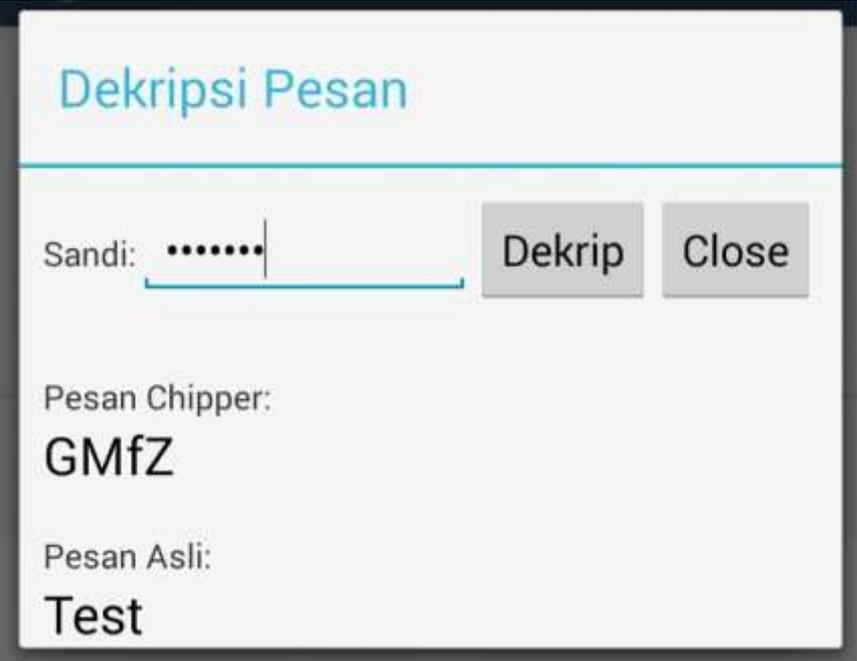
Gambar.IV.3. Tampilan Menu Enkripsi Pesan

4. Tampilan Menu Dekripsi Pesan

Halaman menu dekripsi pesan merupakan halaman yang akan menampilkan menu dekripsi pesan. Pada halaman dekripsi pesan ini terdapat beberapa komponen yang mendukung proses dekripsi pesan, yaitu :

- a. Kata sandi, merupakan field yang menampung kunci.
- b. Dekripsi pesan, merupakan tombol untuk melakukan proses dekripsi pesan.
- c. Close, merupakan tombol untuk keluar dari halaman dekripsi pesan.
- d. Pesan chipper, merupakan field yang menampung pesan enkripsi.
- f. Pesan asli, merupakan field yang menampung hasil dekripsi pesan yang telah diproses oleh sistem.

Adapun tampilan menu untuk deskripsi pesan terlihat seperti pada gambar IV.4 berikut :



The image shows a software interface for decrypting a message. It features a title bar 'Dekripsi Pesan'. Below the title, there is a label 'Sandi:' followed by a text input field containing seven dots, indicating a password. To the right of the input field are two buttons: 'Dekrip' and 'Close'. Below the password field, there is a label 'Pesan Chipper:' followed by the text 'GMfZ'. At the bottom, there is a label 'Pesan Asli:' followed by the text 'Test'.

Gambar.IV.4. Tampilan Menu Dekripsi Pesan

IV.2. Pembahasan

Salah satu fungsi dan tujuan perancangan dan pengembangan sistem yang diusulkan sebagai pengamanan data sms. Pengamanan data sms yang dilakukan sistem adalah dengan memanipulasi data sms masukan dan menghasilkan data sms yang tepat kepada *user*, maka perlu mengetahui tingkat keakuratan sistem dalam melakukan enkripsi dan dekripsi data sms. Pada pembahasan sebelumnya, penulis sudah menjabarkan metode yang digunakan dalam penelitian ini, yaitu metode *Vigenere Cipher*.

Metode ini akan melakukan manipulasi data sms pada setiap huruf pesan aslinya digeser sebanyak satu huruf pada kunci. Karena dalam metode *Vigenere*, proses enkripsi dan dekripsi berdasarkan kumpulan karakter yang akan dihitung dan diberi nilai secara berurutan, maka karakter yang digunakan pada aplikasi ini dapat dilihat pada Tabel IV.1.

Tabel IV.1. Kumpulan Karakter dan Nilainya

[spasi]	0	1	2	3	4	5	6	7	8	9
0	1	2	3	4	5	6	7	8	9	10
A	B	C	D	E	F	G	H	I	J	K
11	12	13	14	15	16	17	18	19	20	21
L	M	N	O	P	Q	R	S	T	U	V
22	23	24	25	26	27	28	29	30	31	32
W	X	Y	Z	a	B	C	d	e	f	g
33	34	35	36	37	38	39	40	41	42	43
h	i	j	k	l	M	N	o	p	q	r
44	45	46	47	48	49	50	51	52	53	54
s	t	u	v	w	X	Y	z			
55	56	57	58	59	60	61	62			

IV.2.1. Pembahasan Enkripsi Pesan

Hasil yang diperoleh dari proses enkripsi berupa teks untuk membuktikan keakuratan atau kebenaran hasil enkripsi pada sistem, maka .untuk membuktikan secara manual, maka pertama kali dilakukan adalah memasukkan teks atau plainteks dan kunci yang akan dibandingkan dengan sistem, yaitu :

Pesan : PIN ATM saya 188223

Kunci: R1T4ArDaNA

Langkah selanjutnya yang akan dilakukan adalah dengan mengubah karakter PIN ATM saya 188223 kedalam bentuk angka, begitu juga dengan kunci berdasarkan kumpulan karakter yang telah ditentukan sebelumnya. Adapun hasil pengubahan ini adalah sebagai berikut :

Pesan : 26,19,24,0,11,30,23,0,55,37,61,37,0,2,9,9,3,3,4

Kunci: 28,2,30,5,11,54,14,37,24,11,28,2,30,5,11,54,14,37,24

Untuk mendapatkan *ciphertext*, maka hitung nilai $(P+K) \text{ Mod } 63$, sehingga diperoleh hasil perhitungan sebagai berikut :

Tabel IV.2. Hasil Perhitungan Enkripsi

P	26	19	24	0	11	30	23	0	55	37	61	37	0	2	9	9	3	3	4
K	28	2	30	5	11	54	14	37	24	11	28	2	30	5	11	54	14	37	24
C	r	K	R	4	L	K	a	a	F	l	P	C	T	6	J	spasi	G	d	R

Dimana,

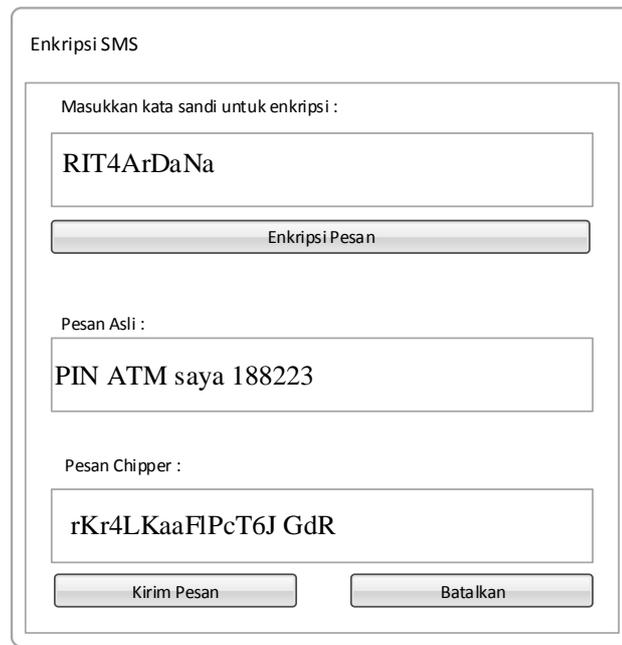
P = Pesan

K= Kunci

C= Cipherteks

Berdasarkan hasil perhitungan seperti yang ditunjukkan pada Tabel IV.2 di atas maka :

$C = rKr4LKaaFIPcT6J GdR$



The image shows a web-based interface for SMS encryption. The title is "Enkripsi SMS". It contains three input fields and two buttons. The first field is labeled "Masukkan kata sandi untuk enkripsi :" and contains the text "RIT4ArDaNa". Below it is a button labeled "Enkripsi Pesan". The second field is labeled "Pesan Asli :" and contains the text "PIN ATM saya 188223". Below it is a field labeled "Pesan Chipper :" containing the text "rKr4LKaaFIPcT6J GdR". At the bottom are two buttons: "Kirim Pesan" and "Batalan".

Gambar IV.5 Hasil Enkripsi Pada Sistem

Dari hasil perhitungan secara manual dengan hasil perhitungan pada sistem dapat dikatakan bahwa proses enkripsi yang dilakukan sistem sangat akurat hal tersebut dibuktikan dengan hasil yang diperoleh dari perhitungan secara manual dengan hasil perhitungan sistem adalah sama.

IV.2.2. Pembahasan Dekripsi Pesan

Hasil yang diperoleh dari proses enkripsi berupa teks untuk membuktikan keakuratan atau kebenaran hasil dekripsi pesan pada sistem, maka .untuk membuktikan secara manual, maka pertama kali dilakukan adalah memasukkan teks atau *ciphertext* dan kunci yang akan dibandingkan dengan sistem, yaitu :

Chipper: rKr4LKaaFlPcT6J GdR

Kunci: R1T4ArDaNA

Langkah selanjutnya yang akan dilakukan adalah dengan mengubah karakter Potensi Utama kedalam bentuk angka, begitu juga dengan kunci berdasarkan kumpulan karakter yang telah ditentukan sebelumnya. Adapun hasil pengubahan ini adalah sebagai berikut :

Chipper: : 54,21,54,5,22,21,37,37,16,48,26,39,30,7,20,0,17,40,28

Kunci: 28,2,30,5,11,54,14,37,24,11,28,2,30,5,11,54,14,37,24

Untuk mendapatkan *plaintext*, maka hitung nilai $(C-K) \text{ Mod } 63$, sehingga diperoleh hasil perhitungan sebagai berikut :

Tabel IV.3. Hasil Perhitungan Enkripsi

C	54	21	54	5	22	21	37	37	16	48	26	39	30	7	20	0	17	40	28
K	28	2	30	5	11	54	14	37	24	11	28	2	30	5	11	54	14	37	24
P	P	I	N	spasi	A	T	M		s	a	y	a	spasi	1	8	8	2	2	3

Dimana,

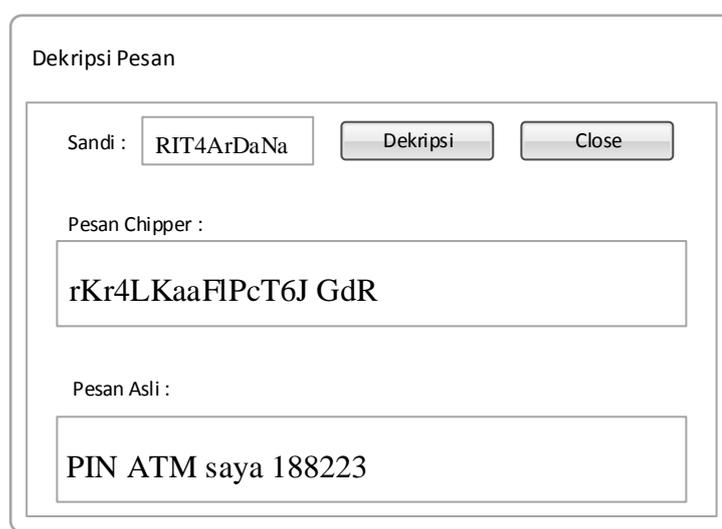
P = Pesan

K= Kunci

C= Cipherteks

Berdasarkan hasil perhitungan seperti yang ditunjukkan pada Tabel IV.2 di atas maka :

P = PIN ATM saya 188223



Dekripsi Pesan

Sandi : RIT4ArDaNa Dekripsi Close

Pesan Chipper :

rKr4LKaaFIPcT6J GdR

Pesan Asli :

PIN ATM saya 188223

Gambar IV.6 Hasil Dekripsi Pada Sistem

Dari hasil perhitungan secara manual dengan hasil perhitungan pada sistem dapat dikatakan bahwa proses dekripsi yang dilakukan sistem sangat akurat hal tersebut dibuktikan dengan hasil yang diperoleh dari perhitungan secara manual dengan hasil perhitungan sistem adalah sama.

IV.2.3. Uji Coba

Pada uji coba ini menjelaskan mengenai hasil evaluasi sistem yang dilakukan pada aplikasi Rancang Bangun Aplikasi Keamanan Data SMS Dengan Menggunakan Kriptografi Vigenere Cipher Berbasis Android. *Black box testing* adalah metode pengujian dimana penilaian terhadap aplikasi bukan terletak pada spesifikasi logika/fungsi aplikasi tersebut, tetapi input dan output. Dengan berbagai input yang diberikan akan dievaluasi apakah suatu sistem/aplikasi dapat

memberikan output yang sesuai dengan harapan penguji. Adapun hasil pengujian atau pun uji coba sistem pada beberapa komponen sebagai berikut :

Tabel IV.4 Hasil Pengujian Aplikasi Sms

Komponen	Proses	Hasil	Y/T
Halaman pesan baru	Nomor telepon	Menampilkan informasi untuk memasukkan nomor telepon	Y
	Pesan teks kosong	Menampilkan informasi untuk memasukkan pesan teks	Y
	Pesan teks sudah benar dan dikirim	Menampilkan informasi bahwa pesan sudah dikirim	T
	Pesan sudah dikirim	Menampilkan pesan yang terkirim pada halaman utama	Y
	Mengklik tombol enkripsi	Menampilkan halaman enkripsi	Y
Halaman Enkripsi Pesan	Kunci kosong	Menampilkan informasi untuk memasukkan kunci	Y
	Mengklik tombol enkripsi	Menampilkan informasi pesan telah dienkripsi	Y
	Mengklik tombol kirim	Mengirim pesan	Y
	Mengklik tombol batal	Menghapus semua teks yang terdapat pada field	T
Halaman Deskripsi Pesan	Pesan Chipper	Menampilkan informasi pesan enkripsi.	Y
	Kunci kosong	Menampilkan informasi untuk memasukkan kunci	Y
	Mengklik tombol Deskripsi pesan	Menampilkan informasi pesan telah dienkripsi	Y
	Mengklik tombol close	Menampilkan informasi menutup proses deskripsi	Y
	Pesan Asli	Menampilkan informasi pesan yang telah di deskripsi	Y

IV.2.4. Spesifikasi kebutuhan Aplikasi

Aplikasi yang dihasilkan hanya dapat dilajan pada perangkat seluler dengan sistem operasi android dengan spesifikasi kebutuhan sebagai berikut :

1. Satu unit laptop dengan spesifikasi sebagai berikut :
 - a. Processor Intel Core I3

- b. Memory 4 Gb
 - c. Hardisk 500 Gb
2. Perangkat Lunak dengan spesifikasi sebagai berikut :
- a. *Android*
 - b. *Intellij idea*
 - c. *Java sdk*
 - d. *Android sdk*
 - e. *Genymotion*
3. Pengujian Sistem
- a. Tampilan sistem
 - b. Proses enkripsi data sms
 - c. Proses deskripsi data sms
 - d. Perhitungan Algoritma Kriptografi Vigenere Chipper

IV.3. Kelebihan dan Kekurangan Sistem

Setiap sistem memiliki kelebihan dan kekurangan, berikut ini adalah kelebihan dan kekurangan sistem yang telah dibuat.

IV.3.1. Kelebihan Sistem

Kelebihan sistem ini diantaranya yaitu:

1. Tampilan program lebih menarik.
2. Meningkatnya jaminan keamanan dan privasi dalam proses transmisi data dalam sms akan memberi kenyamanan pengguna dalam melakukan komunikasi.

3. Kecilnya kemungkinan terjadi penyadapan komunikasi oleh *Man In The Middle* akan mengurangi tingkat kejahatan *cyber*.
4. Diketuainya tingkat keamanan enkripsi data menggunakan algoritma vigenere chipper akan meningkatkan kesadaran *programmer* lain dalam upaya menjaga data pribadi pengguna aplikasi yang dibuatnya.

IV.3.2. Kekurangan Sistem

Adapun kekurangan sistem yang telah dibuat diantaranya yaitu:

1. Aplikasi yang dibangun tidak dapat melakukan enkripsi dan dekripsi terhadap dokumen ataupun file.
2. Aplikasi yang dibangun akan tertutup otomatis jika ada jenis simbol yang dimasukkan pada proses enkripsi pesan.
3. Tampilan data sms dalam aplikasi vigenere tidak dapat dirubah sesuai dengan keinginan *user*.