

PERANCANGAN ENKRIPSI DAN DESKRIPSI DENGAN METODE *ALPHA-QWERTY REVERSE* PADA APLIKASI *SHORT MESSAGE SERVICE* BERBASIS ANDROID

Muhammad Eka Putra^{1*}, Suroso¹, Adewasti¹

¹Program Studi Teknik Telekomunikasi, Jurusan Teknik Elektro, Politeknik Negeri Sriwijaya
Jl. Srijaya Negara, Bukit Besar, Ilir Barat 1, Kota Palembang, Sumatera Selatan

*Email: eka543.ep@gmail.com

Abstrak

Teknologi telepon seluler menyediakan beberapa layanan yang dapat digunakan untuk berkomunikasi. Salah satu dari layanan tersebut adalah SMS (*Short Message Service*). Dari sisi keamanan informasi, keamanan SMS belum terjamin karena memiliki keterbatasan dalam melakukan pertukaran informasi. Biasanya informasi tersebut bersifat rahasia/penting sehingga diperlukan sistem yang bisa memberikan pengamanan terhadap informasi SMS yang ditukarkan antar pengguna pada telepon seluler berbasis android. Untuk penjaminan keamanan pada layanan SMS diperlukan suatu penerapan metode pengamanan. Salah satunya adalah dengan menggunakan algoritma kriptografi. Metode pengamanan SMS yang digunakan adalah metode *alpha-qwerty reverse*. Metode *alpha-qwerty reverse* yaitu metode dengan mengambil dari perpanjangan urutan keyboard *qwerty*. Software yang digunakan dalam perancangan metode pada aplikasi menggunakan software *eclipse*. Hasil akhir dari penelitian ini menghasilkan keamanan pesan pada layanan SMS dengan cara enkripsi dan deskripsi menggunakan metode *alpha-qwerty reverse*.

Kata kunci: *alpha-qwerty reverse*, deskripsi, enkripsi, *Short Message Service* (SMS)

1. PENDAHULUAN

Sarana yang penting bagi manusia untuk saling menyampaikan sebuah informasi yaitu dengan melakukan komunikasi. Keanekaragaman komunikasi telah banyak digunakan oleh manusia dari zaman ke zaman. Perkembangan teknologi informasi yang pesat telah menunjukkan cara berkomunikasi yang beragam bagi manusia (Harini dan Utami, 2012). Salah satu teknologi informasi tersebut yaitu telepon seluler. Telepon seluler memiliki fasilitas yang digunakan untuk mengirim dan menerima informasi dengan menggunakan layanan *Short Message Service* (SMS).

Menurut Amaliasari (2015), SMS merupakan salah satu layanan yang praktis dan banyak dikenal pada telepon bergerak (*mobile devices*). Meskipun praktis, kondisi ini belum menjamin penuh keamanan pengiriman informasi. Sistem tidak bisa menjamin keamanan kandungan informasi manakala terjadi kesalahan dalam pengiriman (Harini dan Utami, 2012). Selain itu, layanan SMS memiliki celah kelemahan pada keamanan yang dapat disalahgunakan oleh *provider* yang dapat menimbulkan ancaman SMS *Interception*. Untuk mencegah hal tersebut, maka layanan SMS perlu dilengkapi dengan fasilitas tambahan keamanan yang menggunakan algoritma kriptografi.

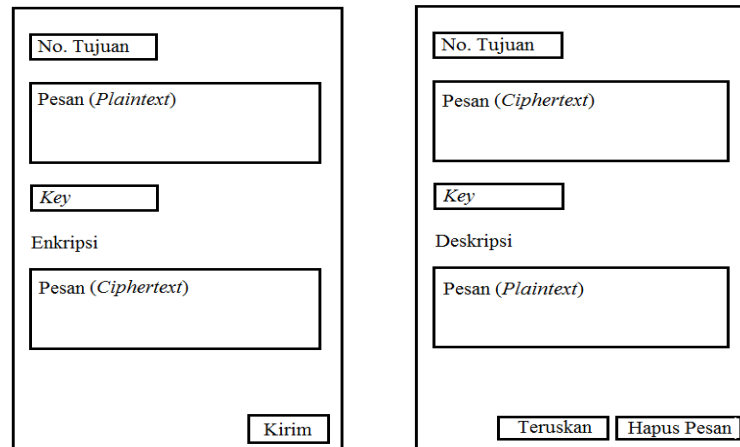
Kriptografi merupakan ilmu yang mempelajari bagaimana supaya informasi baik berupa pesan atau dokumen kita agar tetap aman dan tidak bisa dibaca oleh pihak yang tidak seharusnya. Di dalam algoritmanya memiliki dua macam yaitu algoritma kriptografi klasik yang menggunakan mode karakter dan algoritma kriptografi modern yang menggunakan mode bit. Pada algoritma kriptografi modern jika diimplementasikan dalam enkripsi dan deskripsi SMS mengakibatkan pesan SMS yang sebelumnya mempunyai maksimal 160 karakter, akan melebihi maksimal karakter yang sudah terdapat pada aplikasi SMS. Hal ini dapat terlihat dari ukuran pesan yang tersandi menjadi lebih besar dari pesan aslinya dengan menggunakan mode bit, bahkan bisa dua sampai empat kali ukuran pesan aslinya (Ayu, 2014).

Melihat permasalahan tersebut, maka penulis ingin mencoba melakukan perancangan enkripsi dan deskripsi dengan metode *alpha-qwerty reverse* pada aplikasi *Short Message Service* (SMS) berbasis android.

2. METODOLOGI

2.1. Perancangan Tampilan Desain Aplikasi

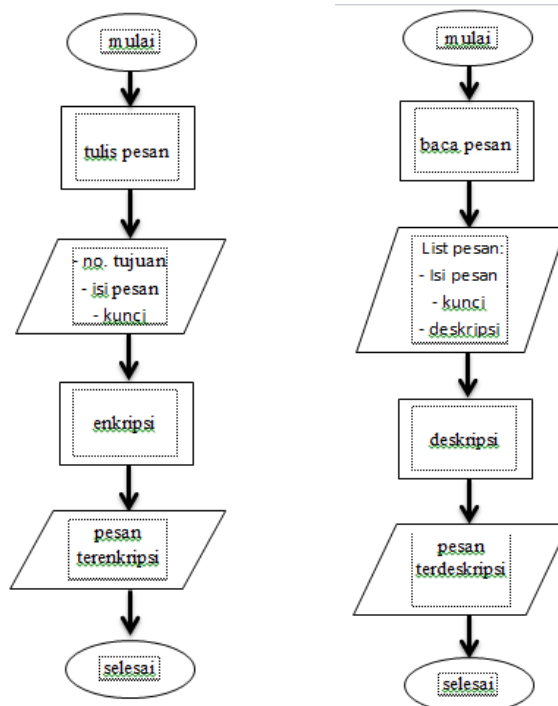
Adapun rancangan desain tampilan enkripsi dan deskripsi pada aplikasi *Short Message Service* yang akan dibuat dapat dilihat pada gambar 1.



Gambar 1. Rancangan desain tampilan enkripsi (kiri) dan deskripsi (kanan)

2.2. Perancangan Perintah *Layout*

Dalam perancangan ini, akan dilakukan proses pengiriman serta penerimaan yang dilakukan antara pengirim pesan dan penerima pesan. Berikut *flowchart* perancangan pengiriman dan penerimaan pesan.



Gambar 2. Flowchart perancangan pengiriman (kiri) dan penerimaan pesan (kanan)

Dalam perancangan perintah menggunakan sistem urutan teks biasa dan urutan teks *keyboard* (Rahmani dkk., 2012). Pada sistem urutan teks biasa dapat dilihat pada tabel berikut:

Tabel 1. Tabel sistem urutan teks biasa

a	b	c	d	e	f	g	h	i	j	K	l	m	n	o
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
p	q	r	s	t	u	v	w	x	y	Z	A	B	C	D

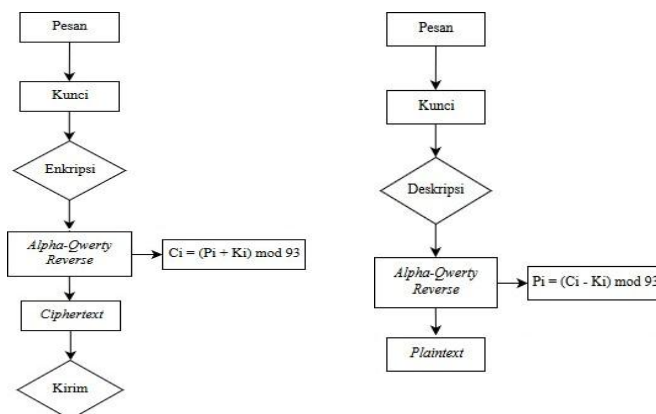
15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7
45	46	47	48	49	50	51	52	53	54	55	56	57	58	59
8	9	'	~	!	@	#	\$	%	^	&	*	()	_
60	61	62	63	64	65	66	67	68	69	70	71	72	73	74
-	=	+	{	}	[]		;	:	“	<	>	,	.
75	76	77	78	79	80	81	82	83	84	85	86	87	88	89
?	/													
90	91	92												

Selain sistem urutan teks biasa, perancangan ini menggunakan sistem urutan teks *keyboard* yang dapat dilihat pada tabel berikut:

Tabel 2. Tabel sistem urutan teks keyboard

q	w	e	r	t	y	u	i	o	p	a	s	d	f	g
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
h	j	k	l	z	x	c	v	b	n	m	Q	W	E	R
15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
T	Y	U	I	O	P	A	S	D	F	G	H	J	K	L
30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
Z	X	C	V	B	N	M	'	~	!	@	#	\$	%	^
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
“	<	>	,	.	?	/	0	1	2	3	4	5	6	7
75	76	77	78	79	80	81	82	83	84	85	86	87	88	89
8	9													
90	91	92												

Saat proses metode *alpha-qwerty reverse*, urutan karakter yang digunakan adalah sistem urutan teks *keyboard* untuk *plaintext* dan kunci serta urutan teks biasa untuk *ciphertext*. Selain itu, perancangan perintah pada aplikasi dibagi menjadi dua yaitu perancangan perintah enkripsi di dalam pengiriman pesan dan perancangan perintah deskripsi di dalam penerimaan pesan. Berikut *flowchart* dalam proses enkripsi dan deskripsi sebagai berikut.



Gambar 3. Flowchart perancangan perintah enkripsi (kiri) dan deskripsi (kanan)

Pada metode *alpha-qwerty reverse* memiliki rumus enkripsi dan deskripsi. Saat perancangan perintah enkripsi, *plaintext* akan dijumlahkan terhadap kunci dengan rumus sebagai berikut:

$$C_i = (P_i + K_i) \text{ mod } 93 \tag{1}$$

Sedangkan pada perancangan perintah deskripsi akan dikurangkan terhadap kunci dengan rumus sebagai berikut:

$$P_i = (C_i - K_i) \text{ mod } 93 \tag{2}$$

Keterangan:

C_i = nilai desimal karakter *ciphertext* ke- i

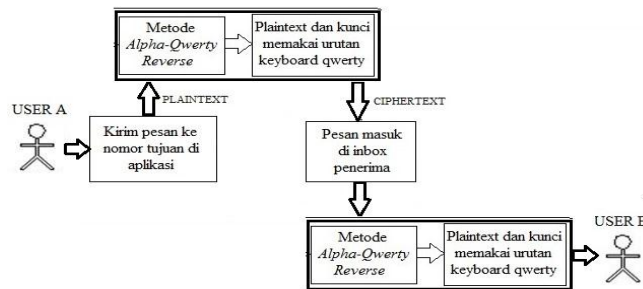
P_i = nilai desimal karakter *plaintext* ke- i

K_i = nilai desimal karakter kunci ke- i

Mod 93 karena berdasarkan ketentuan metode

2.3. Tes Kinerja Sistem

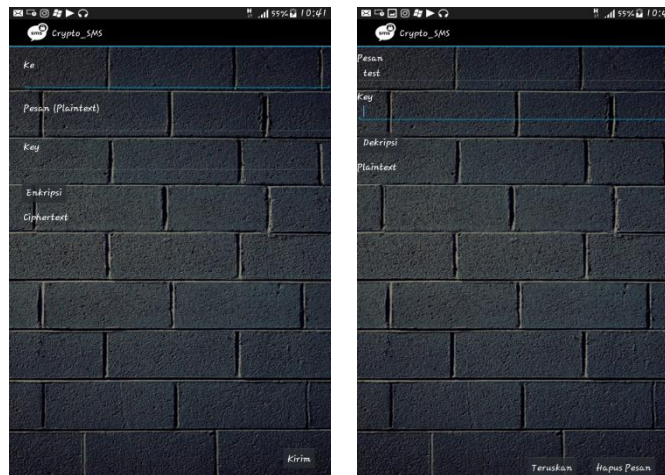
Kinerja sistem secara keseluruhan yang berfungsi untuk mengetahui proses enkripsi dan deskripsi pada aplikasi dengan hasil yang diharapkan. Tes kinerja sistem yang dilakukan yaitu dengan cara pengujian secara langsung pada aplikasi dan pengujian secara teoritis.



Gambar 4. Blok diagram proses enkripsi dan deskripsi yang diharapkan

3. HASIL DAN PEMBAHASAN

3.1. Tampilan Enkripsi dan Deskripsi



Gambar 5. Tampilan enkripsi (kiri) dan deskripsi (kanan) pada aplikasi

3.2. Pengujian Enkripsi pada Aplikasi

Pengujian ini akan dilakukan menggunakan telepon seluler dengan 5 sampel *plaintext* dengan kunci “polsri” dan 5 sampel *plaintext* dengan kunci “kripto123”. Berikut hasil pengujian yang telah dilakukan.

Tabel 3. Hasil pengujian enkripsi

<i>Plaintext</i>	Kunci	Hasil Uji Aplikasi (<i>Ciphertext</i>)	Hasil Uji Teori (<i>Ciphertext</i>)	Status Pengujian
hello	polsri	ykKDI	ykKDI	Sama
telekomunikasi	polsri	nkKnupIoQsurup	nkKnupIoQsurup	Sama
Kriptografi123#	polsri	0lzuhpXlCyk?aa_	0lzuhpXlCyk?aa_	Sama
0613 4035 1620	polsri	/didca/amk<ca?	/didca/amk<ca?	Sama
Password :		SsDwepmur”c	SsDwepmur”c	
321_Hello	polsri	a/0fzBq	a/0fzBq	Sama
hello	kripto123	GfzBm	GfzBm	Sama
telekomunikasi	kripto123	vfzlvqp?qyurul	vfzlvqp?qyurul	Sama
Kriptografi123#	kripto123	8gosiqe>cEk?a.!	8gosiqe>cEk?a.!	Sama
0613 4035 1620	kripto123	g/?bdb(=)q<ca<	g/?bdb(=)q<ca<	Sama
Password :				
321_Hello	kripto123	Onsufq<d:/c a>(f<kJl	Onsufq<d:/c a>(f<kJl	Sama

3.3. Pengujian Deskripsi pada Aplikasi

Pengujian ini akan dilakukan menggunakan telepon seluler dengan 5 sampel *ciphertext* dengan kunci “polsri” dan 5 sampel *ciphertext* dengan kunci “kripto123”. Berikut hasil pengujian yang telah dilakukan.

Tabel 4. Hasil pengujian deskripsi

<i>Ciphertext</i>	Kunci	Hasil Uji Aplikasi (<i>Plaintext</i>)	Hasil Uji Teori (<i>Plaintext</i>)	Status Pengujian
ykKDI	polsri	hello	hello	Sama
nkKnupIoQsurup	polsri	telekomunikasi	telekomunikasi	Sama
0lzuhpXlCyk?aa_	polsri	Kriptografi123#	Kriptografi123#	Sama
/didca/amk<ca?	polsri	0613 4035 1620	0613 4035 1620	Sama
SsDwepmur”c		Password : 321_Hello	Password : 321_Hello	
a/0fzBq	polsri			Sama
GfzBm	kripto123	hello	hello	Sama
vfzlvqp?qyurul	kripto123	telekomunikasi	telekomunikasi	Sama
8gosiqe>cEk?a.!	kripto123	Kriptografi123#	Kriptografi123#	Sama
g/?bdb(=)q<ca<	kripto123	0613 4035 1620	0613 4035 1620	Sama
Onsufq<d:/c				
a>(f<kJl	kripto123	Password : 321_Hello	Password : 321_Hello	Sama

3.4. Analisa

Uji tes pada aplikasi tersebut dilakukan menggunakan telepon seluler serta menggunakan teori. Dapat dilihat pada pengujian enkripsi, *ciphertext* yang dihasilkan saat pengujian aplikasi sama dengan pengujian teori. Begitu juga dengan pengujian deskripsi, *plaintext* yang dihasilkan saat pengujian aplikasi sama dengan pengujian teori. Berdasarkan hasil tersebut, maka perancangan telah dikatakan berhasil pada enkripsi maupun dekripsi pada aplikasi *Short Message Service* berbasis android.

4. KESIMPULAN

1.1 Kesimpulan

Beberapa kesimpulan yang dapat ditarik berdasarkan hasil dan pembahasan penulisan makalah ini adalah sebagai berikut:

- (1) Ketika dienkrpsi, pesan yang dikirim berupa *plaintext* dengan kunci akan menghasilkan *ciphertext* dengan status pengujian sama

- (2) Ketika dideskripsi, pesan yang dikirim berupa *ciphertext* dengan kunci akan menghasilkan *plaintext* dengan status pengujian sama
- (3) Enkripsi dan deskripsi pada aplikasi *Short Message Service* bekerja dengan baik dikarenakan hasil keluaran pada aplikasi sesuai dengan hasil teori.

1.2 Saran

Adapun saran yang dapat disampaikan yaitu dengan berjalannya perancangan algoritma kriptografi metode *alpha-qwerty reverse* pada aplikasi *Short Message Service* berbasis android diharapkan juga mampu mengembangkan serta mencari tahu tingkat keamanan metode tersebut.

DAFTAR PUSTAKA

- Amaliasari, R.D. Implementasi Algoritma Enkripsi AES dan *Vigenere Cipher* pada Aplikasi SMS Berbasis Android. www.eprints.dinus.ac.id. Diakses: 21 Mei 2017, jam 09.00.
- Ayu, T.K., (2014), Aplikasi SMS Berbasis Android dengan Enkripsi *Vigenere Running Key*, Skripsi, Universitas Sanata Dharma, Yogyakarta, Indonesia.
- Harini, R.T. dan Utami, E. Aplikasi Enkripsi SMS dengan Modifikasi *Vigenere Cipher* pada Ponsel Android. www.ojs.amikom.ac.id. Diakses: 21 Mei 2017, jam 08.45.
- Rahmani, Md.K.I., Wadhwa, N., Malhotra, V. *Alpha-Qwerty Cipher: An Extended Vigenere Cipher*. www.airccse.org. Diakses: 21 Mei 2017, jam 09.45.