ENKRIPSI SMS PADA TELEPON SELULAR MENGGUNAKAN METODE SKIPJACK BERBASIS ANDROID

SKRIPSI

Disusun Oleh :
I Made Yoga Yasa Prathama
09.18.150

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
INSTITUT TEKNOLOGI NASIONAL MALANG
2015

LEMBAR PERSETUJUAN DAN PENGESAHAN

ENKRIPSI SMS PADA TELEPON SELULAR MENGGUNAKAN METODE SKIPJACK BERBASIS ANDROID

SKRIPSI

Disusun dan Diajukan untuk melengkapi dan memenuhi persyaratan guna mencapai Gelar Sarjana Teknik Informatika Strata Satu (S-1)

Disusun Oleh :
I Made Yoga Yasa Prathama
09.18.150

Diperiksa dan Disetujui,

Dosen Pembimbing I	Dosen Pembimbing II
Joseph Dedy Irawan, ST, MT	**Sonny Prasetio ST., MT.**
NIP. 197404162005011002	**NIP.P.1031000433**

Ketua Program Studi Teknik Informatika S-1

Joseph Dedy Irawan, ST, MT
NIP. 197404162005011002

PROGRAM STUDI TEKNIK INFORMATIKA S-1
FAKULTAS TEKNOLOGI INDUSTRI
INSTITUT TEKNOLOGI NASIONAL MALANG

ENKRIPSI SMS PADA TELEPON SELULAR MENGGUNAKAN METODE SKIPJACK BERBASIS ANDROID

I Made Yoga Yasa Prathama

Program studi Teknik Informatika S-1
Fakultas Teknologi Industri
Institut Teknologi Nasional Malang (ITN Malang)
E-mail: pr4th4m4@gmail.com

Abstrak

Keamanan sangat penting dalam segala aspek untuk melindungi data. Pesan teks pada hand phone yaitu sms (*short message service*) merupakan salah satu data penting yang memerlukan sistem keamanan data. Keamanan data digunakan untuk menjaga kerahasiaan data penting kita pada perangkat *hand phone*. Proses enkripsi digunakan agar pesan tidak dapat dibaca oleh pihak lain yang tidak diinginkan. Sedangkan proses dekripsi digunakan agar pesan dapat dibaca kembali oleh pihak yang dituju.

Metode Skipjack merupakan salah satu metode pengamanan data yang dikembangkan oleh *National Security Agency* (NSA) di Amerika Serikat yang digunakan untuk menjamin keamanan (*security*) dan privasi komunikasi via telepon. Metode skipjack merupakan suatu metode yang sederhana dimana implementasinya tidak memerlukan perhitungan – perhitungan yang rumit dan hanya melibatkan 2 buah operasi matematik kriptografi yaitu XOR dan permutasi.

Analisis hasil pengujian dilakukan setelah dilakukannya pengujian terhadap aplikasi yang dibuat. Hasil pengujian didapat bahwa setiap proses yang ada pada aplikasi dapat berjalan sesuai dengan ke inginan, aplikasi dapat digunakan pada handphone dengan spesifikasi tertentu yaitu dapat menginstal aplikasi berbasis android minimum 4.3. Setiap hand phone harus memiliki aplikasi yang sama untuk melakukan proses pengiriman pesan enkripsi dan dekripsi.

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Tuhan yang Maha Esa, penyusunan skripsi yang berjudul " Enkripsi Pada Telepon Seluler Menggunakan Metode Skipjack Berbasis Android " dapat diselesaikan dengan baik.

Penulis menyadari bahwa dalam proses penulisan skripsi ini banyak mengalami kendala, namun berkat bantuan, bimbingan, kerjasama dari berbagai pihak dan berkah dari Tuhan yang Maha Esa sehingga kendala – kendala yang dihadapi tersebut dapat diatasi. Untuk itu penulis menyampaikan ucapan terima kasih dan penghargaan kepada Bapak Joseph Dedy Irawan, ST., MT., selaku pembimbing I dan Bapak Sonny Prasetio ST., MT., selaku pembimbing II yang telah dengan sabar, tekun, tulus dan ikhlas meluangkan waktu, tenaga dan pikiran memberikan bimbingan, motivasi, arahan, dan saran-saran yang sangat berharga kepada penulis selama menyusun skripsi.

Selanjutnya ucapan terima kasih penulis sampaikan pula kepada:

1. Tuhan Yang Maha Esa
2. Ibu dan Ayah yang sangat banyak memberikan bantuan moril, materil, arahan, dan selalu mendoakan keberhasilan dan keselamatan selama menempuh pendidikan.
3. Dr. Ir. Lalu Mulyadi, MT, selaku Rektor Institut Teknologi Nasional Malang.
4. Ir. Anang Subardi, MT, selaku Dekan Fakultas Teknologi Industri, Institut Teknologi Nasional Malang.
5. Joseph Dedy Irawan, ST, MT, selaku Ketua Program Studi Teknik Informatika, Institut Teknologi Nasional Malang.
6. Sonny Prasetio, ST, MT, selaku Sekertaris Program Studi Teknik Informatika, Institut Teknologi Nasional Malang.
7. Semua dosen Program Studi Teknik Informatika yang telah membantu dalam penulisan dan masukan.
8. Semua teman seperjuangan yang telah membantu dalam terselesaikannya skripsi ini.

Dengan segala kerendahan hati penulis menyadari masih banyak terdapat kekurangan-kekurangan, sehingga penulis mengharapkan adanya saran dan kritik yang bersifat membangun demi kesempurnaan skripsi ini.

Malang, November 2015

I Made Yoga Yasa P.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Beberapa tahun terakhir ini terjadi perkembangan yang pesat pada teknologi, salah satunya adalah telepon selular (ponsel). Mulai dari ponsel yang hanya bisa digunakan untuk bicara dan sms hingga ponsela cerdas (*smart phone*) yang memiliki berbagai fungsi seperti multimedia, multiplayer games, transfer data, video streaming dan lain-lain. Berbagai perangkat lunak untuk mengembangkan aplikasi ponselpun bermunculan, diantaranya yang cukup dikenal luas adalah android .

Salah satu fasilitas yang disediakan ponsel adalah untuk melakukan pengiriman data berupa pesan singkat melalui *Short Message Service* (SMS). Namun dengan fasilitas SMS yang ada, timbul pertanyaan mengenai keamanan informasi jika seseorang ingin mengirimkan suatu informasi rahasia melalui fasilitas SMS.

Di luar negeri pemanfaatan SMS untuk mengirim pesan rahasia telah lebih dulu dikembangkan. Misalnya di Inggris sebuah perusahaan operator telepon selular, staellium UK, mengeluarkan layanan bernama stealth text yang dapat digunakan untuk mengirim pesan dengan aman, yaitu dengan cara menghapus pesan secara otomatis segera setelah 40 detik pesan dibaca atau yang dikenal dengan nama *self - destruct text message*. Ada juga pengamanan sms dengan menggunakan kriptografi sms yang memanfaatkan kunci untuk medekripsikan sms yang telah di enkripsi.

Oleh karena itu, penulis akan mencoba membuat sebuah aplikasi pengamanan sms dengan metode skipjack untuk mengenkripsi data yang berjalan pada system operasi android sehingga pemilik handphone yang berbasis android dapat melakukan pertukaran data (sms) dengan lebih aman dan nyaman.

1.2 Rumusan Masalah

Bagaimana mengimplementasikan teknologi enkripsi dan dekripsi sms pada handphone yang berbasis android dengan menggunakan metode skipjack.

1.3 Batasan Masalah

Agar pembahasan penelitian tidak meluas, maka penulis perlu memberikan beberapa batasan masalah antara lain :

1. Perangkat lunak yang di bangun hanya dapat di jalankan pada ponsel yang memiliki system operasi android.
2. Minimum reqruitment perangkat lunak handphone yang digunakan adalah android 4.3 Sampai android 5.0.
3. Dua belah pihak pengguna harus sama-sama menggunakan aplikasi pesan rahasia agar pesan dapat di enkripsi dan dekripsi.
4. Aplikasi yang di buat hanya untuk enkripsi dan dekripsi pesan berbentuk teks.
5. Pengiriman pesan menggunakan pulsa.

1.4 Tujuan

Skripsi ini bertujuan membuat aplikasi yang lebih aman untuk pertukaran data (sms) agar privasi pengguna lebih terjamin.

1.5 Metodologi

Metode yang digunakan dalam pembahasan skrpsi ini adalah :

1. Metode literatur

   Mencari referensi – referensi yang berhubungan dengan perencanaan dan pembuatan aplikasi yang akan dibuat.
2. Perancangan Aplikasi

   Sebelum melaksanakan pembuatan aplikasi, dilakukan perancangan terhadap aplikasi yang meliputi, merancang layout aplikasi, serta penalaran metode yang digunakan.
3. Pembuatan Aplikasi

BAB II

LANDASAN TEORI

2.1 Sejarah Kriptografi

Pada zaman Romawi kuno dikisahkan pada suatu saat, ketika Julius Caesar ingin mengirimkan suatu pesan rahasia kepada seorang Jenderal di medan perang. Pesan tersebut mengandung rahasia, Julius Cesar tidak ingin pesan tersebut terbuka ditengah jalan. Disini Julius Caesar menemukan suatu cara agar pesan tidak dapat dipahami oleh siapapun kecuali Jenderalnya saja, yaitu dengan mengacak pesan yang akan dikirim. Kriptografi berasal dari bahasa Yunani, menurut bahasa dibagi menjadi dua, yaitu kripto dan graphia, *kripto* berarti *secret* (rahasia) dan *graphia* berarti *writing* (tulisan).

Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ketempat lain. Orang yang melakukan ini disebut *Cryptographer*. Sebuah pesan atau data yang masi asli disebut *plaintext* atau *cleartext*, maka pesan atau data yang telah diubah atau dienkripsi disebut *chipertext*. Kriptografi ini bertujuan untuk menjaga kerahasiaan informasi yang terkandung dalam data sehingga informasi tersebut. [1]

2.1.1 Komponen Kriptografi

Pada dasarnya, *cryptography* terdiri dari beberapa komponen seperti:

a. Enkripsi : enkripsi merupakan hal yang sangat penting dalam *cryptography* sebagai pengamanan atas data yang dikirimkan agar rahasia terjaga. Pesan aslinya disebut *plaintext* yang diubah menjadi kode-kode yang tidak dimengerti.

b. Dekripsi : dekripsi merupakan kebalikan dari enkripsi, pesan yang telah dienkripsi dikembalikan kebentuk asalnya (*plaintext*), yang disebut dekripsi pesan. Algoritma yang digunakan untuk dekripsi tentu berbeda dengan yang digunakan untuk enkripsi.

c. Kunci : kunci yang dimaksud disini adalah kunci yang dipakai untuk melakukan enkripsi dan dekripsi. Kunci terbagi dalam dua bagian yakni kunci pribadi (*private key*) dan kunci umum (*publik key*).

d. *Chipertext* : merupakan suatu pesan yang sudah melalui pesan proses enkripsi. Pesan yang ada pada *chipertext* tidak bisa dibaca karena berisi karakter-karakter yang tidak memiliki makna (arti).

e. *Plaintext* : sering juga disebut *cleartext* merupakan pesan bermakna yang ditulis atau diketik dan plaintext ini yang akan diproses menggunakan algoritma *cryptography* agar menjadi *chipertext*.

f. *Cryptanalysis* : bisa diartikan sebagai analisis sandi suatu ilmu untuk mendapatkan *plaintext* tanpa harus mengetahui kunci secara wajar. Jika suatu *chipertext* berhasil menjadi *plaintext* tanpa menggunakan kunci yang sah. [1]

2.1.2 Kode ASCII (*American Standard Code For Information Interchange*)

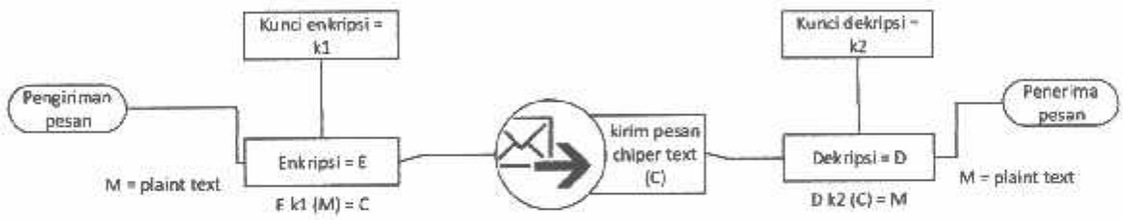
ASCII merupakan suatu standard internasional dalam kode huruf dan simbol seperti Hex dan Unicode tetapi ASCII lebih bersifat universal, kode ASCII digunakkan oleh komputer untuk menunjukan teks. Kode ASCII memiliki komposisi 7 bit bilangan biner, namun ASCII disimpan sebagai sandi 8 bit dengan menambahkan satu angka 0 sebagai bit significant paling tinggi. Tabel ASCII dapat dilihat pada Tabel 2.1 :

Tabel 2.1 : Tabel ASCII [2]

Hex	Dec	Char		Hex	Dec	Char	Hex	Dec	Char	Hex	Dec	Char
0x00	0	NULL	null	0x20	32	Space	0x40	64	@	0x60	96	`
0x01	1	SOH	Start of heading	0x21	33	!	0x41	65	A	0x61	97	a
0x02	2	STX	Start of text	0x22	34	"	0x42	66	B	0x62	98	b
0x03	3	ETX	End of text	0x23	35	#	0x43	67	C	0x63	99	c
0x04	4	EOT	End of transmission	0x24	36	$	0x44	68	D	0x64	100	d
0x05	5	ENQ	Enquiry	0x25	37	%	0x45	69	E	0x65	101	e
0x06	6	ACK	Acknowledge	0x26	38	&	0x46	70	F	0x66	102	f
0x07	7	BELL	Bell	0x27	39	'	0x47	71	G	0x67	103	g
0x08	8	BS	Backspace	0x28	40	(	0x48	72	H	0x68	104	h
0x09	9	TAB	Horizontal tab	0x29	41	)	0x49	73	I	0x69	105	i
0x0A	10	LF	New line	0x2A	42	*	0x4A	74	J	0x6A	106	j
0x0B	11	VT	Vertical tab	0x2B	43	+	0x4B	75	K	0x6B	107	k
0x0C	12	FF	Form feed	0x2C	44	,	0x4C	76	L	0x6C	108	l
0x0D	13	CR	Carriage return	0x2D	45	-	0x4D	77	M	0x6D	109	m
0x0E	14	SO	Shift out	0x2E	46	.	0x4E	78	N	0x6E	110	n
0x0F	15	SI	Shift in	0x2F	47	/	0x4F	79	O	0x6F	111	o
0x10	16	DLE	Data link escape	0x30	48	0	0x50	80	P	0x70	112	p
0x11	17	DC1	Device control 1	0x31	49	1	0x51	81	Q	0x71	113	q
0x12	18	DC2	Device control 2	0x32	50	2	0x52	82	R	0x72	114	r
0x13	19	DC3	Device control 3	0x33	51	3	0x53	83	S	0x73	115	s
0x14	20	DC4	Device control 4	0x34	52	4	0x54	84	T	0x74	116	t
0x15	21	NAK	Negative ack	0x35	53	5	0x55	85	U	0x75	117	u
0x16	22	SYN	Synchronous idle	0x36	54	6	0x56	86	V	0x76	118	v
0x17	23	ETB	End transmission block	0x37	55	7	0x57	87	W	0x77	119	w
0x18	24	CAN	Cancel	0x38	56	8	0x58	88	X	0x78	120	x
0x19	25	EM	End of medium	0x39	57	9	0x59	89	Y	0x79	121	y
0x1A	26	SUB	Substitute	0x3A	58	:	0x5A	90	Z	0x7A	122	z
0x1B	27	ESC	Escape	0x3B	59	;	0x5B	91	[	0x7B	123	{
0x1C	28	FS	File separator	0x3C	60	<	0x5C	92	\	0x7C	124	|
0x1D	29	GS	Group separator	0x3D	61	=	0x5D	93	]	0x7D	125	}
0x1E	30	RS	Record separator	0x3E	62	>	0x5E	94	^	0x7E	126	~
0x1F	31	US	Unit separator	0x3F	63	?	0x5F	95	_	0x7F	127	DEL

2.1.3 Proses Kriptografi

Proses kriptografi diawali dengan mengubah data dalam bentuk *plaintext* (tulisan atau pesan awal yang dapat dibaca) menjadi *chipertext* (tulisan atau pesan rahasia yang tidak dapat lagi dibaca dengan mudah) dengan menggunakan algoritma yang mentransposisikan (mengubah posisi) tiap - tiap karakter / bit pada *plaintext* dan dengan cara mensubstitusikan (mengganti) tiap-tiap karakter / bit pada *plaintext* sehingga dihasilkan tulisan atau data yang berbeda sama sekali dengan data awal. Metode pengubahan *plaintext* menjadi chipertext di tempat pengirim atau pembuat data dinamakan dengan Metode enkripsi, dengan menggunakan kunci enkripsi. Di tempat penerima atau pembaca data, *chipertext* yang diterima kemudian diubah kembali menjadi plaintext dengan menggunakan Metode dekripsi, yang membalikkan kembali posisi ataupun isi dari data yang diterima dalam keadaan tidak dapat dibaca, kembali menjadi data yang mudah untuk dibaca, dengan menggunakan kunci dekripsi. Proses dari kriptografi dapat dilihat pada blok diagram pada Gambar 2.1 :



Gambar 2.1 : Blok diagram proses kriptografi [2]

2.2 Algoritma Skipjack

Algoritma Skipjack mengenkripsi plaintext 64 bit menjadi ciphertext 64 bit dengan jumlah putaran sebanyak 32 putaran yang menggunakan kunci rahasia yang berukuran 80 bit. Modus enkripsi dan dekripsi dari metode Skipjack mirip dengan metode DES yakni : Electronic Code Book Mode, Cipher Block Chaining Mode, Cipher Feed back Mode, dan Output FeedbackMode. Proses enkripsi dalam metode Skipjack terhadap suatu blok data dilakukan dengan menggunakan dua buah rule secara bergantian yakni rule A dan rule B. Sedangkan pada proses dekripsi, rule yang digunakan merupakan kebalikan (*inverse*) dari rule A dan rule B yakni rule A^{-1} dan rule B^{-1}. Operasi matematik kriptografi yang digunakan di dalam rule A, rule B, rule A^{-1}, dan rule B^{-1} tersebut adalah XOR dan permutasi. Operasi permutasi dilakukan dengan menggunakan sebuah tabel substitusi yang disebut dengan F-Table dan kunci rahasia.

bit 56, cv7 : bit 57 sampai bit 64, cv8 : bit 65 sampai bit 72, cv9 : bit 73 sampai bit 80

Catatan : Bit 1 dimulai dari posisi bit paling tinggi (MSB, Most Significant Bit).

2.2.2 Algoritma Permutasi

Fungsi permutasi pada metode Skipjack disebut dengan permutasi G yang merupakan 4 round dari struktur Feistel. Fungsi round tersebut merupakan tabel substitusi byte yang fixed, yang dinamakan F-Table. Masing-masing round dari permutasi G juga memasukkan sebuah cryptovariable. Permutasi G dilakukan pada proses enkripsi di awal setiap rule yakni rule A dan rule B. Sedangkan pada proses dekripsi, permutasi yang dilakukan merupakan kebalikan (inverse) dari permutasi G yang disebut dengan permutasi G^{-1} yang dilakukan di awal setiap rule A^{-1} dan rule B^{-1}. Sebagai masukan (input) untuk melakukan proses permutasi adalah seperempat bagian dari blok plaintext ataupun blok ciphertext dalam bentuk heksadesimal yang berukuran 16 bit.

Berikut ini adalah langkah – langkah dari permutasi G dan permutasi G^{-1} :

1. Untuk permutasi G, G(Word = g1 || g2) = g_5 || g_6 di mana g_1 adalah byte pertama dari Word (high byte) dan g_2 adalah byte kedua dari Word (low byte) dan sebagai hasilnya (output) adalah gabungan antara g_5 dengan g_6. Untuk g_3, g_4, g_5, dan g_6 . Rumus permutasi G ditunjukan pada Persamaan 2.1 :

$$g_i = F(g_{i-1} \oplus cv_{4k+i-3}) \oplus g_{i-2}$$

Persamaan 2.1 : Rumus permutasi G

di mana $3 \leq i \leq 6$ (i awal = 3), k pada proses enkripsi putaran pertama adalah 0, F merupakan tabel substitusi atau F-Table, dan CV_{4k+i-3} adalah cryptovariable dengan indeks (4k+i-3) dalam cryptovariable schedule. Sesuai dengan rumus : gi = F(gi-1⊕cv_{4k+i-3}) ⊕g_{i-2}, maka akan didapat Persamaan 2.2:

$$g_3 = F(g_2 \oplus CV_{4k}) \oplus g1 \quad ; \quad g_4 = F(g_3 \oplus CV_{4k}+1) \oplus g_2$$
$$g_5 = F(g_4 \oplus CV_{4k+2}) \oplus g3 \quad ; \quad g_6 = F(g_5 \oplus CV_{4k+3}) \oplus g_4$$

Persamaan 2.2 : Rumus permutasi G saat proses enkripsi

2.2.3 Algoritma Enkripsi Metode Skipjack

Pada metode Skipjack, sebuah blok plaintext yang hendak dienkripsi terlebih dahulu akan dikonversikan ke dalam bentuk heksadesimal. Nilai heksadesimal tersebut merupakan nilai ASCII (American Standard Code for Information Interchange) dari masing - masing karakter yang ada dalam blok plaintext tersebut. Setelah proses konversi dilakukan, blok plaintext yang sudah dalam bentuk heksadesimal tersebut akan dibagi menjadi 4 bagian yang disebut dengan Word yang dinyatakan dengan W_1^0, W_2^0, W_3^0, W_4^0 dengan masing-masing Word berukuran 16 bit. 4 -Word blok data tersebut akan dienkripsi secara bergantian menggunakan dua buah rule yaitu ruleA dan ruleB sebanyak 32 putaran yakni : 8 putaran pertama dilakukan dengan rule A, kemudian 8 putaran kedua dilakukan dengan rule B, lalu 8 putaran ketiga dilakukan dengan rule A dan 8 putaran terakhir dengan rule B. Ciphertext adalah W_1^{32}, W_2^{32}, W_{33}^2, W_4^{32}. Terdapat dua variabel penting dalam proses enkripsi yaitu counter dan k dimana pada awal putaran pertama, counter = 1 dan k = 0.

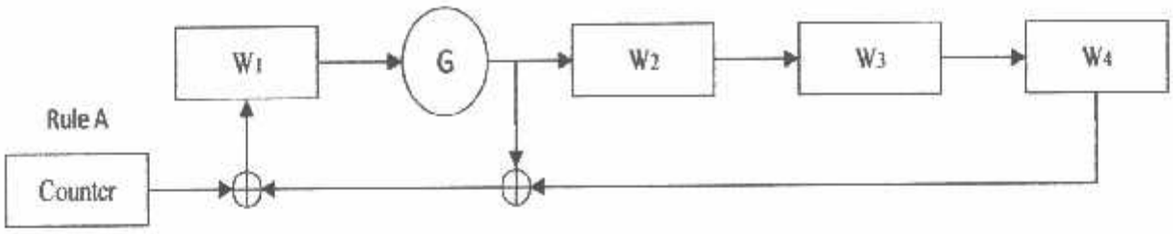
Langkah – langkah dari rule A adalah sebagai berikut :

1. Lakukan permutasi G dengan inputW1k.
2. W_1^{k+1} merupakan hasil dari operasi XOR antara output permutasi G, W_4^k, dan counter.
3. W_2^{k+1} merupakan output dari permutasi G.
4. $W_3^{k+1} = W_2^k$.
5. $W_4^{k+1} = W_3^k$.
6. counter dan k ditambah satu.

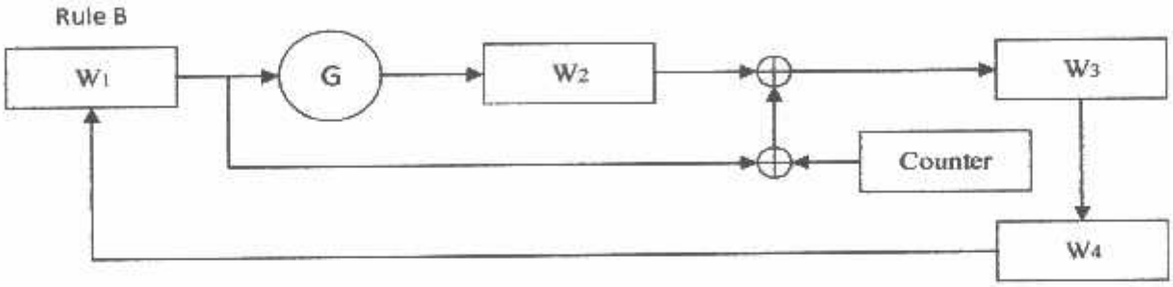
Langkah – langkah dari rule B adalah sebagai berikut :

1. Lakukan permutasi G dengan inputW1k.
2. $W_1^{k+1} = W_4^k$.
3. W_2^{k+1} merupakan output dari permutasi G.
4. W_3^{k+1} merupakan hasil dari operasi XOR antara W_1^k, W_2^k, dan counter.
5. $W_4^{k+1} = W_3^k$.
6. counter dan k ditambah satu. [4]

Diagram rule A dan rule B ditunjukan pada Gambar 2.3 dan gambar 2.4 :



Gambar 2.3 : Blok diagram rule A [2]



Gambar 2.4 : Blok diagram rule B [2]

2.2.4 Algoritma Dekripsi Metode Skipjack

Sama halnya dengan proses enkripsi, sebuah blok ciphertext yang hendak didekripsi terlebih dahulu akan dikonversikan ke dalam bentuk heksadesimal sesuai dengan nilai ASCII dari masing - masing karakter yang ada dalam blok ciphertext tersebut. Setelah proses konversi dilakukan, blok ciphertext tersebut akan dibagi menjadi 4 bagian yang disebut dengan Word yang dinyatakan dengan W_1^{32}, W_2^{32}, W_3^{32}, W_4^{32} dengan masing-masing Word berukuran 16 bit. 4-Word blok data tersebut akan didekripsi secara bergantian menggunakan dua buah rule yaitu ruleA^{-1} dan ruleB^{-1} sebanyak 32 putaran yakni :

8 putaran pertama dilakukan dengan rule B^{-1}, kemudian 8 putaran kedua dilakukan dengan rule A^{-1}, lalu 8 putaran ketiga dilakukan dengan rule B^{-1} dan 8 putaran terakhir dengan rule A^{-1}. Plaintext adalah W_1^0, W_2^0,W_3^0, W_4^0. Terdapat dua variabel penting dalam proses dekripsi yaitu counter dan k dimana pada awal putaran pertama, counter = 32 dan k = 32.

Langkah – langkah dari ruleA^{-1} adalah sebagai berikut :

1. Lakukan permutasi G^{-1} dengan inputW_2^k.
2. W_1^{k-1} merupakan output dari permutasi G^{-1}.
3. $W_2^{k-1} = W_3^k$.

4. $W_3^{k-1} = W_4^k$.

5. W^{4k-1}= merupakan hasil dari operasi XOR antara W_1^k, W_2^k dan counter.

6. counter dan k dikurangi satu.

Langkah – langkah dari rule B^{-1} adalah sebagai berikut :

1. Lakukan permutasi G^{-1} dengan inputW_2^k.

2. W_1^{k-1} merupakan output dari permutasi G^{-1}.

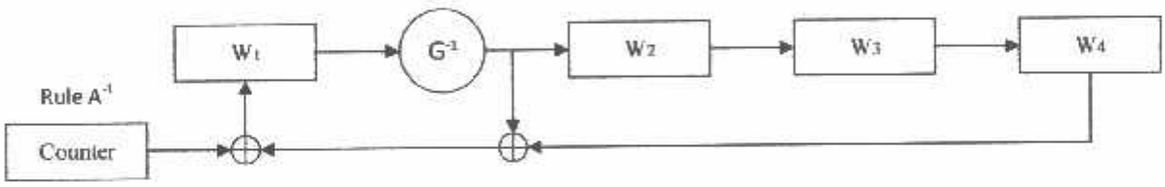
3. W_2^{k-1} merupakan hasil dari operasi XOR antara output permutasi G^{-1}, W_3^k, dan counter.

4. $W_3^{k-1} = W_4^k$.

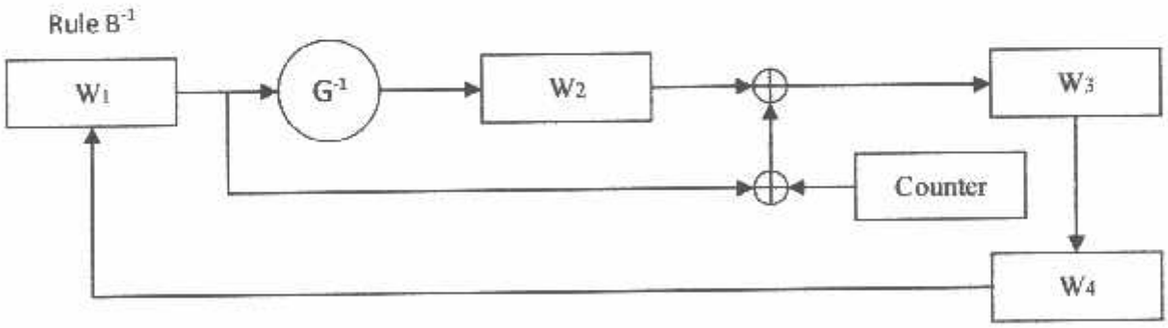
5. $W_4^{k-1} = W_1^k$.

6. counter dan k dikurangi satu. [4]

Berikut ini adalah Gambar 2.5 diagram rule A^{-1} dan Gambar 2.6 rule B^{-1} :



Gambar 2.5 : Blok diagram rule A^{-1} [2]



Gambar 2.6 : Blok diagram rule B^{-1} [2]

2.3.1 Fitur Pada Android

Fitur – fitur yang terdapat pada perangkat smartphone berbasis Android antara lain :

1. Dalvik Virtual Machine, merupakan Java Runtime Environment yang telah dioptimasi untuk device atau perangkat dengan ukuran memori yang kecil. Fitur machine ini menjadikan aplikasi dapat dijalankan dengan baik pada perangkat berbasis Android.
2. Touch-screen atau layar sentuh. Fitur ini cukup fenomenal karena belum terdapat pada perangkat ponsel yang lama. Dengan menggunakan fitur ini maka proses navigasi menu menjadi lebih mudah karena pengguna hanya memilih dan menekan menu yang akan dijalankan tanpa perlu harus melakukan scroll ke atas-bawah atau samping kiri-kanan.
3. Multipage : User dapat menambahkan halaman baru pada layar sehingga tampilan ikon aplikasi pada layar semakin banyak. Hal ini berguna untuk semakin mempercepat akses ke berbagai aplikasi.
4. Bersifat terbuka (open source) sehingga user dapat mempelajari, membuat serta memodifikasi sesuai keinginan tanpa harus membayar.
5. Kualitas suara dan grafik yang bagus karena dalam sistem Android telah tersedia dengan standar suara dan video seperti MP3, AAC.
6. Tersedianya berbagai macam library/services yang dapat langsung digunakan, seperti browser, GPS, kamera, Bluetooth, dan Wifi.
7. Miracast, sebuah bentuk protokol yang memperbolehkan perangkat baru semacam Nexus 4 untuk melakukan streaming audio dan video pada televisi yang mempunyai fitur Miracast. Fitur ini memiliki kemiripan dengan Airplay yang dimilki oleh sejumlah perangkat keluaran Apple.
8. Gesture Typing Keyboard. Sebenarnya fitur mirip dengan swipe keyboard yang sudah lama diperkenalkan, tetapi Google menyempurnakannya dalam Android 4.2 dengan memberikan akurasi yang lebih baik dan respon yang lebih cepat.

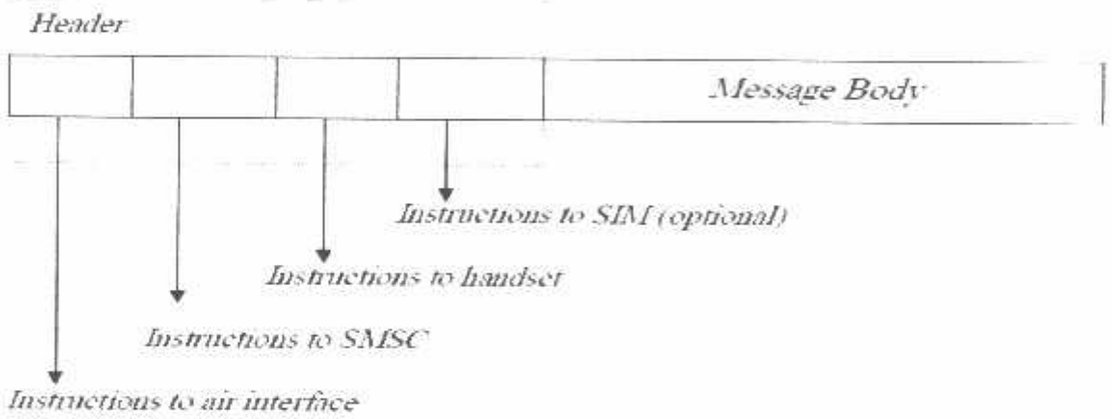
2.3.2 Eclipse

Eclipse adalah sebuah IDE (Integrated Development Environment) untuk mengembangkan perangkat lunak dan dapat dijalankan di semua platform (platform independent).

Berikut ini adalah sifat dari Eclipse:

2.4 Struktur Pesan SMS

Struktur Pesan SMS pada gambar 2.13 dapat terlihat bahwa pada sebuah paket pesan SMS terdiri dari header dan body. Header pesan terdiri dari instruksi-instruksi kepada komponen-komponen yang bekerja dalam jaringan SMS. Pada instruksi-instruksi tersebut, terdapat informasi yang diperlukan selama pengiriman pesan seperti informasi validitas pesan, dan informasi - informasi lainnya. Pada bagian message body, terdapat isi dari pengirim pesan yang akan dikirimkan. Panjang isi pesan pada sebuah paket SMS berukuran maksimal 160 karakter, dimana setiap karakter memiliki panjang 7 bit. Beberapa aplikasi standar telepon selular dapat mendukung panjang pesan dengan karakter sepanjang 8 bit (panjang pesan maksimum 140 karakter) dan karakter yang lebih panjang lainnya seperti 16 bit, namun karakter sepanjang 8 bit dan 16 bit ini tidak didukung oleh semua aplikasi standar telepon selular. Pada umumnya karakter sepanjang 8 bit dan 7 bit digunakan untuk menampilkan data seperti gambar dan simbol. Struktur pesan pada sebuah paket SMS dapat dilihat pada Gambar 2.9 :



Gambar 2.9 : Struktur pesan SMS [9]

BAB III

ANALISA DAN PERANCANGAN SISTEM

3.1 Analisa Sistem

Analisa sistem adalah penguraian dari suatu sistem yang utuh ke dalam bagian-bagian komponennya dengan maksud untuk mengidentifikasi dan mengevaluasi permasalahan. Bagian analisis ini terdiri atas analisa fungsional, analisa performansi, gambaran sistem dari sudut pandang user yang dinyatakan dalam use case diagram, dan gambaran alur sistem.

3.1.1 Kebutuhan Fungsional

Adalah jenis kebutuhan yang berisikan proses-proses apa saja yang diberikan oleh perangkat lunak yang akan dibangun.

Kebutuhan fungsional Aplikasi Enkripsi ini meliputi :

a. Tulis Pesan
b. Enkripsi pesan
c. Dekripsi pesan
d. Kirim pesan
e. Buka pesan
f. Balas pesan

3.1.2 Kebutuhan Non Fungsional

Adalah kebutuhan yang tidak secara langsung terkait pada aplikasi yang akan dibuat atau dikembangkan.

Kebutuhan non fungsional meliputi :

Untuk input data menggunakan keyboard dan mouse.

a. Perangkat lunak pembuatan aplikasi menggunakan software Eclipse sebagai editor.
b. ADT (android Development tools) sebagai plugin untuk mengembangkan aplikasi android.
c. SDK (Stkamurt Development Kit) sebagai library dan emulator.
d. Komputer untuk pembuatan aplikasi memiliki spesifikasi :
    1. Cpu amd phenom X4
    2. Ram 8 gb ddr 3

3. Memori penyimpanan 120 gb ssd
4. Motherboard asrock extrem III
5. Monitor LED 22,5 inch
6. Vga xfx 1 gb DDR 5 256-bit
7. Operating system windows 7 64-bit

e. Untuk pengujian aplikasi menggunakan perangkat :

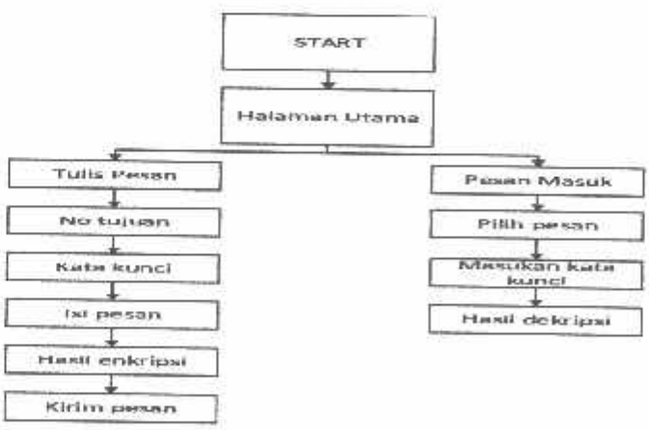
1. Lenovo dengan spesifikas :
   a) Cpu octa core 1.5 GHZ
   b) Ram 2 gb
   c) Sistem operasi android Lollipop 5.0
2. Asus zenfone dengan spesifikasi :
   a) Cpu dual core 1,3 GHZ
   b) Ram 2 gb
   c) Sistem operasi android 4.3
3. Samsung core duos

3.2 Perancangan

Dalam pembuatan Aplikasi enkrpsi sms ini terdapat sebuah perancangan yang meliputi struktur menu, SOP (Standart Operating Prosedure), dan flowchart aplikasi.

3.2.1 Struktur Menu

Pada perancangan struktur menu akan menampilkan perancangan susunun menu yang ada pada aplikasi pesan rahasia. Tampilan rancangan struktur menu dapat dilihat pada Gambar 3.1 :



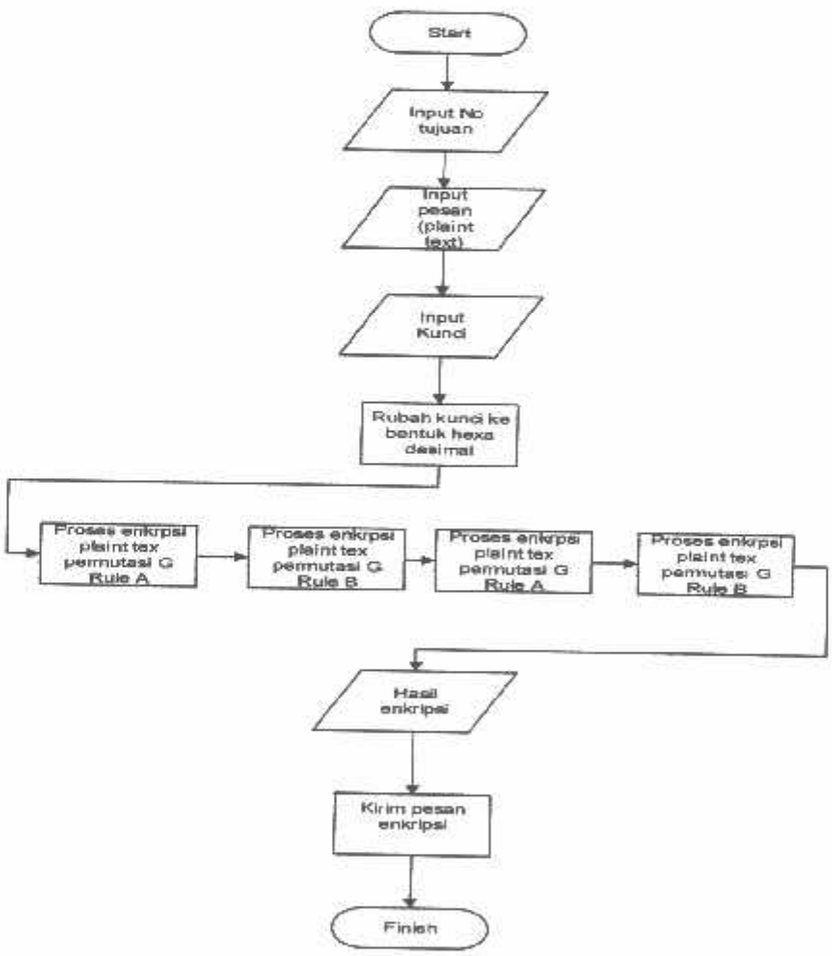
Gambar 3.1 : Tampilan struktur menu aplikasi

3.2.2 Flowchart

Flowchart adalah diagram yang menggunakan notasi-notasi untuk menggambarkan arus proses dari sistem secara keseluruhan. Flowchart scring digunakan untuk menggambarkan arus proses dari sistem yang telah ada atau sistem yang baru yang akan dikembangkan secara logika tanpa mempertimbangkan lingkungan fisik dimana data tersebut mengalir.

A. Flowchart Enkripsi Pesan

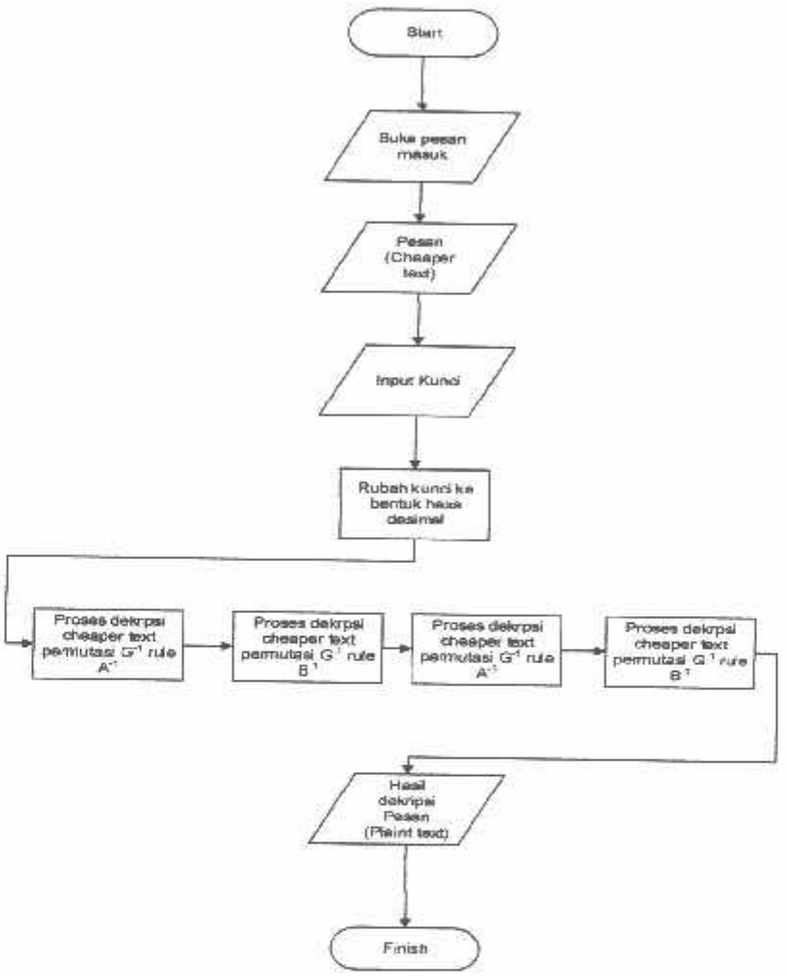
Flowchart enkripsi menunjukan bagamana proses enkripsi pesan / plaint text menjadi cheaper text. Yang dimulai dengan memsaukan pesan (plaint text) dan kata kunci, kemudian dilanjutkan dengan prosaes enkripsi menggunakan rule A dan B yang diawali permutasi G. Proses enkripsi dapat dilakukan beberapa kali hingga data yang kita kirim lebih aman. Flow chart enkripsi ditunjjukan pada Gambar 3.2 :



Gambar 3.2 : Flow chart enkripsi

B. Flowchart dekripsi Pesan

Flowchart dekripsi menunjukan bagaimana proses dekripsi pesan (cheaper text) menjadi plaint text. Diawali dengan membuka pesan yang diterim, kemudian memasukan kata kunci yang digunakan sebelumnya pada saat proses enkripsi. Dengan menggunakan rule A^{-1} dan B^{-1} yang diawali proses permutasi G^{-1}, sehingga pesan dapat di baca oleh penerima. flowchart dekripsi ditunjukan pada Gambar 3.3 :



Gambar 3.3 : Flow chart dekripsi

3.2.3 Perancangan Layout Aplikasi

Ada beberapa komponen yang terdapat pada perancangan layout aplikasi enkripsi pesan ini, diantaranya link penghubung antar Halaman. Dibuat dengan halaman utama menampilkan menu pesan yang masuk, kemudian ada halaman pesan baru, dan halaman baca pesan.

A. Halaman Utama

Halaman ini pertama kali muncul saat aplikasi dibuka. Tampilan layout halaman utama dapat dilhat pada Gambar 3.4 :

Gambar 3.4 : Tampilan halaman utama

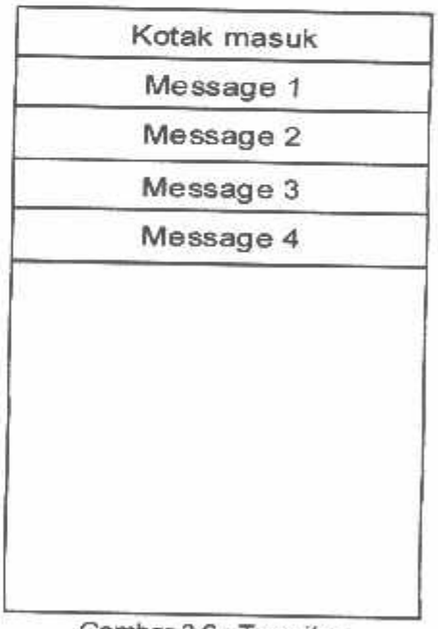
B. Halaman Pesan Baru

Halaman ini akan menampilkan teks box untuk mengisi no tujuan pesan, pesan yang akan dikirm, kata kunci yang akan digunakan untuk enkripsi pesan, tombol enkripsi, dan tombol kirim. layout tampilan menu halaman pesan baru dapat dlihat pada gambar 3.5 :

Gambar 3.5 : tampilan menu pesan baru

C. Halaman Kotak Masuk

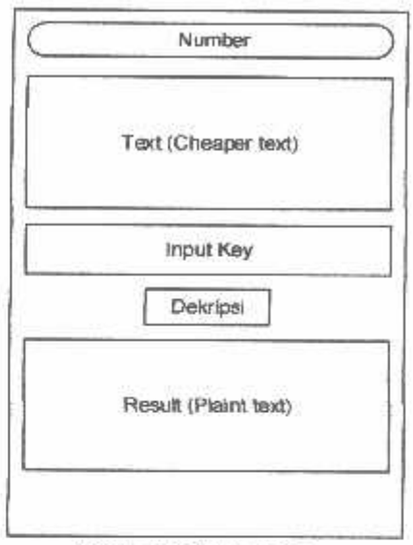
Halaman ini akan menampilkan no pengirim pesan, obrolan yang sedang berlangsung antara pengirim dan penerima pesan, teks box untuk mengisi kata kunci yang akan digunakan untuk enkripsi / dekripsi pesan, teks box untuk membalas pesan dan tombol kirim. layout tampilan menu halaman pesan masuk dapat dlihat pada Gambar 3.6 :



Gambar 3.6 : Tampilan halaman kotak masuk

D. Halaman Baca Pesan

Menampilkan halaman untuk melakukan pembacaan pesan dan proses dekripsi pesan yang ada pada kotak masuk. Layout halaman baca pesan dapat dilihat pada Gambar 3.7 :



Gambar 3.7 :Tampilan halaman Baca Pesan

BAB IV

IMPLEMENTASI DAN PENGUJIAN

4.1 Implementasi Program

Dalam proses pengimplementasian program penulis menggunakan perangkat komputer yang memiliki spesifikasi hardware dan software yang digunakan antara lain :

a. Proccesor AMD Phanoem X4
b. Ram 8Gb
c. VGA Card XFX HD 6790 1Gb 256-bit
d. Memory penyimmpanan menggunakan SSD 128GB
e. Operating system menggunakan Win 7 64-bit.
f. Untuk pembuatan aplikasi penulis menggunakan Eclipse Luna

Untuk pembuatan tampilan layout aplikasi penulis menggunakan rancangan tampilan layout yang ada pada BAB III.

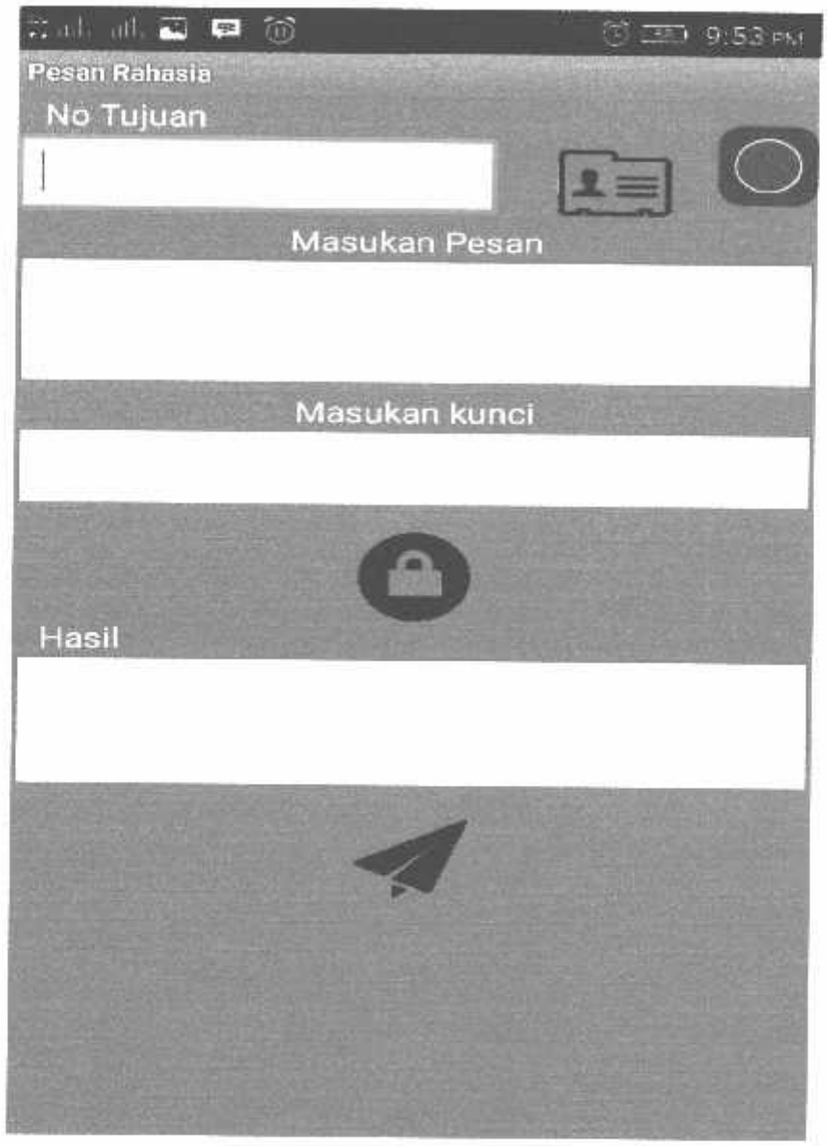
4.1.1 Halaman Menu Utama

Saat membuka aplikasi akan menampilkan halaman utama yang berisi beberapa submenu antara lain tulis pesan, baca pesan dan bantuan. Tampilan halaman utama dapat dilihat pada Gambar 4.1 :

Gambar 4.1 : Tampilan halaman utama

4.1.3 Halaman Tulis Pesan Baru

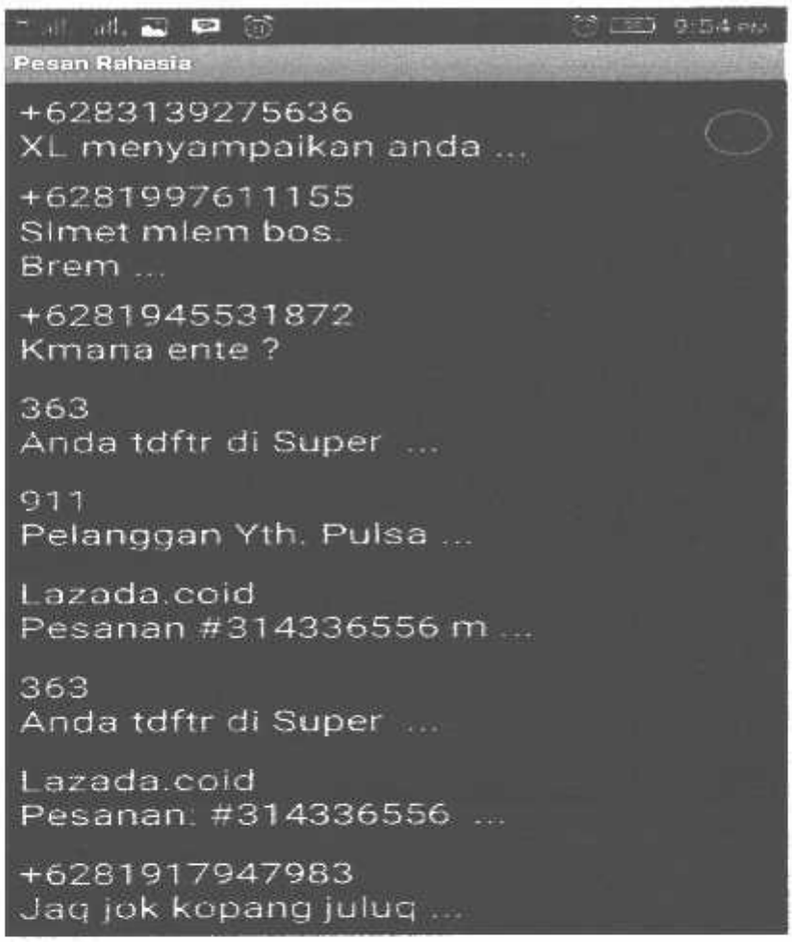
Menu tulis pesan akan menampilkan halaman untuk menulis pesan baru. Pada halaman ini berisikan text field untuk input no tujuan, text field untuk mengetik pesan, text field untuk menuliskan kata kunci, tombol kontak untuk melihat kontak yang ada pada handphone, tombol lock untuk mengenkripsi pesan, dan tombol send untuk mengirim pesan. Tampilan halaman tulis pesan baru dapat dilihat pada Gambar 4.2:



Gambar 4.2 : Tampilan tulis pesan baru

4.1.4Halaman Pesan Masuk

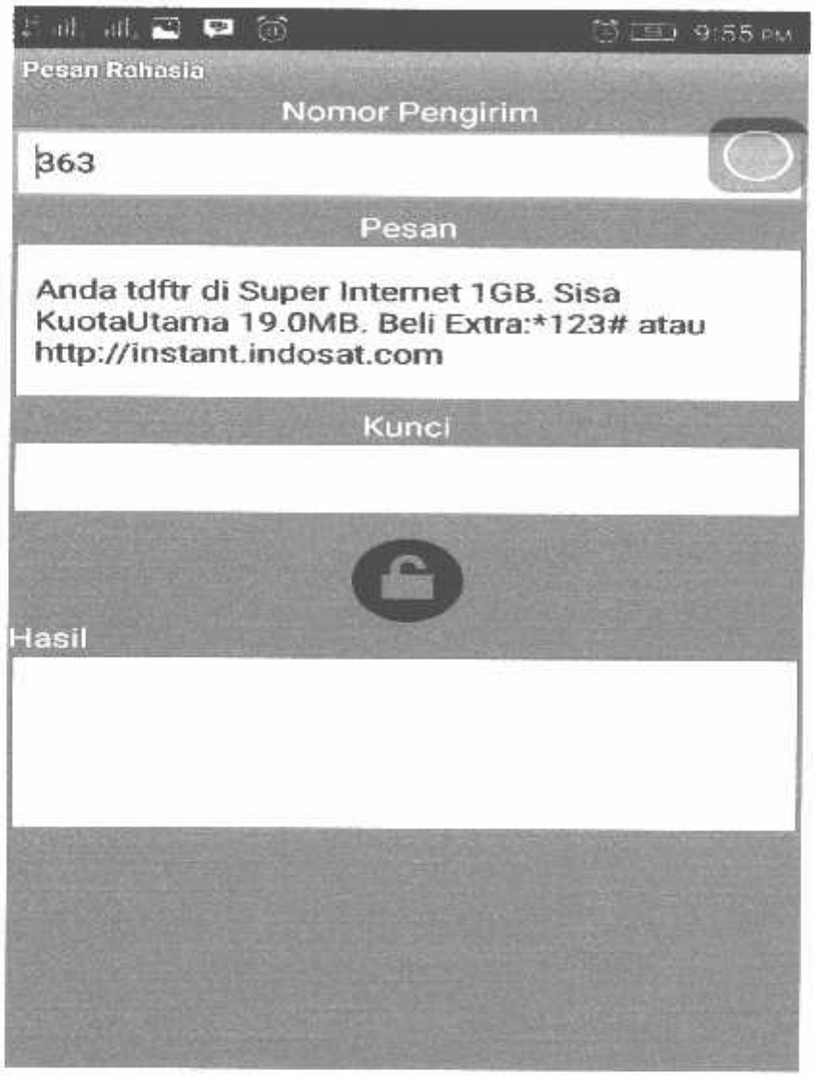
Pada halaman ini akan Menampilkan list dari pesan sms yang masuk. Tampilan layout halaman pesan masuk dapat dilihat pada Gambar 4.3 :



Gambar 4.3 : Tampilan halaman pesan masuk

4.1.5 Halaman Baca Pesan

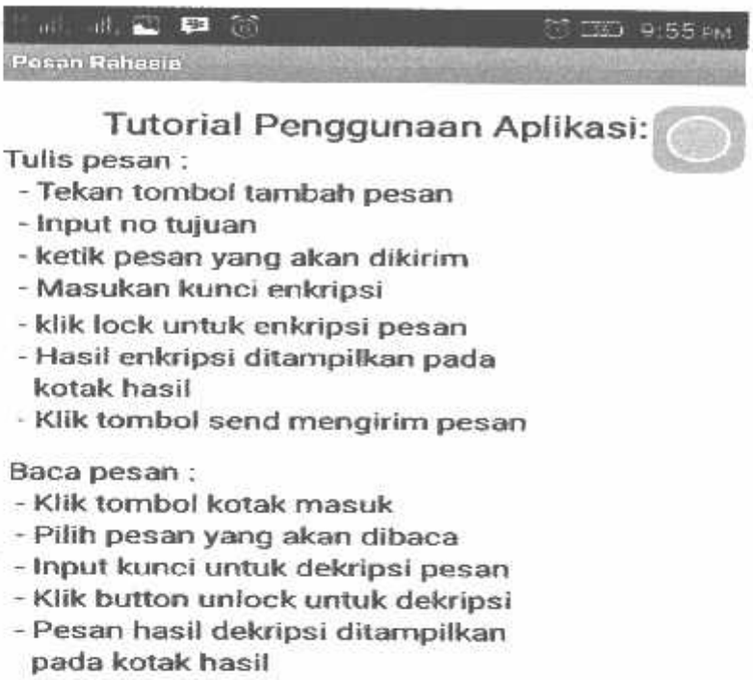
Pada halaman baca pesan akan menampilkan kolom no pengirim pesan, kolom pesan yang diterima, kolom kunci untuk memasukan password, tombol unlock untuk mendekripsi pesan, dan kolom hasil untul menampilkan pesan setelah dilakukan proses dekripsi. Tampilan layot baca pesan dapat dilihat pada Gambar 4.4:



Gambar 4.4 : Tampilan halaman baca pesan

4.1.6 Halaman Tutorial

Bila pengguna menekan tombol question pada tampilan home, maka aplikasi akan menampilkan halaman tutorial. Pada halaman ini akan diberi tahu bagaimana cara penggunaan aplikasi pesan rahasia ini. Tampilan halaman tutorial dapat dilihat pada Gambar 4.5 :



Gambar 4.5 : Tampilan halaman tutorial

4.2 Pengujian Program

Dalam proses pengujian penulis melakukan pembahasan tentang proses perhitungan pengolahan kata kunci dan proses enkripsi secara manual. Dan hasil pengujian program disertakan pada tabel.

4.2.1 Pengolahan KataKunci

Pengolahan kata kunci adalah proses yang pertama dilakukan sebelum melakukan proses enkripsi dan dekripsi pada metode skipjack. Berikut contoh pengolahan kunci yang bertujuan untuk mendapatkan 10 sub kunci.

Kunci = madeyogayp

Rubah kunci kebentuk hexadesimal = 6D616465796F67617970

Kemudian bagi kunci menjadi 10 sub kunci masing – masing 8 bit :

cv[0] = 6D ; cv[1] = 61 ; cv[2] = 64 ; cv[3] = 65 ; cv[4] = 79 ; cv[5] = 6F ; cv[6] = 67 ; cv [7] = 61 ; cv[8] = 79 ; cv[9] = 70 .

4.2.2 Proses Permutasi

Proses permutasi dilakukan saat pertama kali melakukan proses enkripsi, yaitu pada saat awal rule A dan rule B. Pelaksanaan permutasi G dengan input string dengan panjang 16 bit dalam bentuk heksadesimal sebagai berikut :

Input : 6D6F, k = 0

g1 = 6D , g2 = 6F

g3 = F (g2 $\oplus$ cv [(4 x K) mod 10] $\oplus$ g1

cv [(4 x K) mod 10] = cv [0] = 6D

g2 = 6F = 01101111

cv[0] = 6D = 01101011 $\oplus$

00000100

F (00000100) = F (02) = 67

F (67) = 01101110

g1 (6D) = 01101011 $\oplus$

g3 = 00000101 = 0A

g4 = F (g3 $\oplus$ cv [((4 x K)+1) mod 10] $\oplus$ g2

cv [((4 x K)+1) mod 10] = cv [1] = 61

g3 = 0A = 00000101

cv[1] = 61 = 01101000 $\oplus$

01101101

F (01101101) = F (6B) = 56

F (56) = 10100110

g2 (6F) = 01101111 ⊕

g4 = 11001001 = 39

g5 – F (g4 ⊕ cv [((4 x K)+2) mod 10] ⊕ g3

cv [((4 x K)+2) mod 10] = cv [2] = 64

g4 = 39 = 11001001

cv[2] = 64 = 01100010 ⊕

10101011

F (10101011) = F (5D) – 0b

F (0b) – 00001101

g3 (0A) = 00000101 ⊕

g5 = 00001000 = 01

g6 = F (g5 ⊕ cv [((4 x K)+3) mod 10] ⊕ g4

cv [((4 x K)+3) mod 10] = cv [3] = 65

g5 = 01 = 00001000

cv[3] = 65 = 01101010 ⊕

01100010

F (01100010) = F (64) = a7

F (a7) = 01011110

g4 (39) = 11001001 ⊕

g6 = 10010111 = 9E

G = g5 + g6 = 019E

Permutas G^{-1} merupakan inverse atau kebalikan dari permutasi G, yang dilakukan saat proses dekripsi pada awal setiap pelaksanaan rule A^{-1} dan rule B^{-1}.

4.2.3 Proses Enkripsi

Proses enkripsi pada metode skipjack memiliki 32 putaran dengan menggunakan 10 buah sub kunci yang merupakan hasil pembagian dari sebuah kunci enkripsi. Berikut proses enkripsi metode skipjack :

Plaint text = halo

Kunci = madeyogayp

Ubah kunci ke bentuk heksadesimal kemudian bagi menjadi 10 subkunci =

cv[0] = 6D ; cv[1] = 61 ; cv[2] = 64 ; cv[3] = 65 ; cv[4] = 79 ; cv[5] = 6F ; cv[6] = 67 ; cv [7] = 61 ; cv[8] = 79 ; cv[9] = 70

Proses enkripsi :

Ubah plaintext dalam bentuk heksadesimal : 68616C6F

Bagi plaintext menjadi 2 bagian sebagai berikt : w1(0) = 6861, w2(0) = 6C6F.

Putaran ke-1 (Rule A, K = 0 , Counter = 1)

G (w1(0)) = G (68) = g5 + g6 – 019E

g1 = 6D , g2 = 6F

g3 = F (g2 $\oplus$ cv [(4 x K) mod 10] $\oplus$ g1

cv [(4 x K) mod 10] = cv [0] = 6D

g2 = 6F = 01101111

cv[0] = 6D = 01101011 $\oplus$

00000100

F (00000100) = F (02) = 67

F (67) = 01101110

g1 (6D) = 01101011 ⊕

g3 = 00000101 = 0A

g4 = F (g3 ⊕ cv [((4 x K)+1) mod 10] ⊕ g2

cv [((4 x K)+1) mod 10] = cv [1] = 61

g3 = 0A = 00000101

cv[1] = 61 = 01101000 ⊕

01101101

F (01101101) = F (6B) = 56

F (56) = 10100110

g2 (6F) = 01101111 ⊕

g4 = 11001001 = 39

g5 = F (g4 ⊕ cv [((4 x K)+2) mod 10] ⊕ g3

cv [((4 x K)+2) mod 10] = cv [2] = 64

g4 = 39 = 11001001

cv[2] = 64 = 01100010 ⊕

10101011

F (10101011) = F (5D) = 0b

F (0b) = 00001101

g3 (0A) = 00000101 ⊕

g5 = 00001000 = 01

g6 = F (g5 ⊕ cv [((4 x K)+3) mod 10] ⊕ g4

cv [((4 x K)+3) mod 10] = cv [3] = 65

g5 = 01 = 00001000

cv[3] = 65 = 01101010 ⊕

01100010

F (01100010) = F (64) – a7

F (a7) = 01011110

g4 (39) = 11001001 ⊕

g6 = 10010111 = 9E

G = g5 + g6 = 019E

W1(1) = G(W1(0)) ⊕w2(0) ⊕Counter

G(w1(0)) = 019E = 0000100010010111

W2 (0) = 6C6F = 0110001101101111⊕

= 0110101111111000

Counter = 1 = 1000000000000000⊕

= 1110 1011 1111 1000 = 7DF1

W2(1) = G(w1(0)) = G (6861) = 019E

Hasil chipertext dari rule A putaran ke – 1 = w1(1) + w2(1) = 7DF1 019E

4.2.4 Hasil Pengujian Aplikasi

Dalam proses melakukan pengujian aplikasi penulis menggunakan beberapa perangkat yang berbeda agar penulis dapat mengetahui apakah aplikasi dapat berjalan sesuai dengan keinginan pada device yang berbeda. Penulis juga melakukan pengujian yang di bantu oleh beberapa pengguna agar dapat mengetahui kekurangan dari aplikasi ini, sehingga dapat digunakan sebagai bahan pengembangan aplikasi ini di kemudian harinnya. Hasil dari pengujian dapat dilihat pada Tabel 4.1 dan Tabel 4.2 :

Tabel 4.1 : Hasil pengujian dari beberapa perangkat yang berbeda

Proses Yang Dilakukan	Perangkat Yang Digunakan			Persentase
	Lenovo A7000	Samsung Core Duos	Asus Zenfone 5	
Membuka aplikasi	Berhasil	Berhasil	Berhasil	100%
elakukan proses menulis pesan	Berhasil	Berhasil	Berhasil	100%
Melakukan proses enkripsi	Berhasil	Berhasil	Berhasil	100%
Melakukan pengiriman pesan	Berhasil	Berhasil	Berhasil	100%
Membuka pesan masuk	Berhasil	Berhasil	Berhasil	100%
elakukan proses dekripsi pesan	Berhasil	Berhasil	Berhasil	100%
Memasukan no pengirim dari kontak telpon	Berhasil	Berhasil	Berhasil	100%
lakukan proses pindah halaman	Berhasil	Berhasil	Berhasil	100%

Tabel 4.2 : Hasil pengujian yang dilakukan oleh pengguna

Pengujian yang dilakukan	Tanggapan	Jumlah user	Persentase	Total jumlah user
Tampilan antar muka	Menarik	8	80%	10
	Cukup menarik	1	10%	
	Kurang menarik	1	10%	
Performa aplikasi dalam proses enkripsi dan dekripsi	Cepat	7	70%	
	Cukup cepat	3	30%	
	Lambat	-	0%	
Kemudahan dalam pengoperasian	Mudah	8	80%	
	Cukup mudah	2	30%	
	Susah	-	0%	

BAB V

PENUTUP

5.1 Kesimpulan

Setelah melakukan pengujian terhadap aplikasi diperoleh beberapa kesimpulan sebagai berikut :

1. Semua fitur aplikasi dapat bekerja 100% pada 3 tipe ponsel yang berbeda, yaitu : Lenovo A7000, Samsung Core Duos, Asus Zenfone 5.
2. Tampilan aplikasi dapat disimpulkan cukup menarik sebab dari 10 pengguna hanya 1 orang yang memberikan tanggapan kurang menarik.
3. Pengujian performa aplikasi dapat disimpulkan aplikasi dapat bekerja dengan cepat dalam proses enkripsi dan dekripsi. Karena dari 10 orang pengguna 70% menyatakan cepat dan 30% menyatakan cukup cepat.
4. Untuk kemudahan dalam penggunaan disimpulkan aplikasi dapat digunakan dengan mudah oleh pengguna. Sebab dari 10 orang pengguna 80% pengguna mengatakan mudah dan 20% mengatakan cukup mudah.

5.2 Saran

Adapun saran yang penulis berikan untuk pengembangan aplikasi ini kedepanya antara lain :

1. Perlu penambahan fitur save password, agar pengguna tidak selalu memasukan kata kunci apa bila membaca sms dari no yang sama.
2. Design layout pada halaman baca pesan perlu di tambahkan list fragment, agar pesan dari no handphone yang sama berada pada satu thread pesan.
3. Penambahan pop up notifikasi bila ada pesan yang masuk.

DAFTAR PUSTAKA

[1]. Fajar, Dimas Mei, Agustus 2014, Aplikasi Data Keamanan SMS Menggunakan Metode Enkripsi Berbasis Android.

[2]. Suprianto, Desember 2007, Sistem Pengkodean Data Pada File Teks Pada Keamanan Informasi Dengan Menggunakan Metode Skipjack, Jurnal Computech & Bisnis, Vol.1, No.2.

[3]. Knudsen, Lars, Wagner, David, 2001, On the structure of Skipjack, Department of Informatics, University of Bergen, https://www.cs.berkeley.edu/~daw/papers/skipjack-dam01.pdf.

[4]. Kim, Jongsung, Raphael C. W. Phan, Advanced Differential – Style Cryptanalysis of the NSA's Skipjack Block Cipher, 2009, Center for Information Security Technologies (CIST),KoreaUniversity,https://dspace.lboro.ac.uk/dspacejspui/bitstream/2134/8159/1/kim.pdf.

[5]. Suorianto, Desember 2007, Sistem Pengkodean Data Pada File Teks Pada Keamanan Informasi Dengan Menggunakan Metode Skipjack, STMIK Mardira Indonesia, Bandung, JurnalComputech& Bisnis, Vol. 1, No. 2, http://research.lppm-stmik.ibbi.ac.id/document/.

[6]. Huda, arif akbarul. 24 jam pintar pemrograman android, ebook version 2.1.

[7]. Nazruddin Safaat H. 2011. Pemograman Android Mobile Smartphone dan Tablet Pc Berbasis Android, informatika, Bandung.

[8]. Maulida, Arta. 2007, Boomingnya Android. http://ilmukomouter.com/, 20 November 15.

[9]. Tri Hikmawan, Agung, 2009, Pengembangan Sistem SMS Gateway Berbasis WEB, Fakultas Teknologi Informasi, Institut Teknologi Sepuluh November Surabaya.

LAMPIRAN

PROGRAM STUDI TEKNIK INFORMATIKA S-1FAKULTAS TEKNOLOGI INDUSTRIINSTITUT TEKNOLOGI NASIONAL MALANG

BERITA ACARA UJIAN SKRIPSI
FAKULTAS TEKNOLOGI INDUSTRI

Nama : I Made Yoga Yasa Prathama
NIM : 09.18.150
Jurusan : Teknik Informatika S-1
Judul : Enkripsi SMS Pada Telepon Seluler Menggunakan Metode Skipjack Berbasis Android

Dipertahankan dihadapan Majelis Penguji Skripsi Jenjang Strata Satu (S-1) pada :
Hari : Rabu
Tanggal : 29Agustus 2015

Panitia Ujian Skripsi
Ketua Majelis Penguji

Joseph Dedy Irawan, ST., MT
NIP. 197404162005011002

AnggotaPenguji :

Penguji Pertama	Penguji Kedua
Yosep Agus Pranoto, ST. MT	**Suryo Adi Wibowo, ST. MT**
NIP.P. 1031000432	**NIP.P. 1031000438**

PROGRAM STUDI TEKNIK INFORMATIKA S-1

FAKULTAS TEKNOLOGI INDUSTRI

INSTITUT TEKNOLOGI NASIONAL

MALANG

FORMULIR PERBAIKAN UJIAN SKRIPSI

Nama : I Made Yoga Yasa Prathama
NIM : 09.18.150
Jurusan : Teknik Informatika S-1
Judul :. Enkripsi SMS Pada Telepon Seluler Menggunakan Metode Skipjack Berbasis Android

Dosen Penguji	Revisi	Paraf
Dosen Penguji 1	1. Penambahan sumber referensi pada gambar. 2. Nama persamaan pada bab II. 3. Perbaiki bab IV. 4. Pemberian nama tabel di atas. 5. Kesimpulan berdasarkan hasil pengujian. 6. Hilangkan bullet	25/11 2015

Dosen Penguji Pertama

Yosep Agus Pranoto, ST. MT
NIP.P. 1031000432

PROGRAM STUDI TEKNIK INFORMATIKA S-1

FAKULTAS TEKNOLOGI INDUSTRI

INSTITUT TEKNOLOGI NASIONAL

MALANG

FORMULIR PERBAIKAN UJIAN SKRIPSI

Nama : I Made Yoga Yasa Prathama
NIM : 09.18.150
Jurusan : Teknik Informatika S-1
Judul : Enkripsi SMS Pada Telepon Seluler Menggunakan Metode Skipjack Berbasis Android

Dosen Penguji	Revisi	Paraf
Dosen Penguji 2	1. Penambahan menu tutorial pada program	
	2. Penambahan citasi+ daftar pustaka	
	3. Hasil Pengujian pada tabel dimasukan di kesimpulan & saran	
	4. Batasan masalah minimum reqruitment	
	5. Istilah asing.	

Penguji Kedua

Survo Adi Widowo, ST. MT
NIP.P. 1031000438

INSTITUT TEKNOLOGI NASIONAL
Jl. Bendungan Sigura-Gura No. 2
MALANG

Malang, 28 Mei 2013

Lampiran : 1(Satu) berkas
Perihal : Kesediaan sebagai Pembimbing Skripsi

Kepada : Yth. Bpk/Ibu **Sonny Prasetio, ST.,MT.**
Dosen Pembina Prodi Teknik Informatika S-1
Institut Teknologi Nasional
MALANG

Yang bertanda tangan dibawah ini:

Nama : I MADE YOGA YASA PRATHAMA
Nim : 0918150
Prodi : Teknik Informatika S-1

Dengan ini mengajukan permohonan, kiranya Bapak/Ibu bersedia menjadi Dosen Pembimbing ~~Utama~~ / Pendamping *), untuk penyusunan Skripsi dengan judul (Proposal Terlampir) :

Enkripsi SMS Pada Telepon Selular Menggunakan Metode Skipjack Berbasisi Android

Adapun tugas tersebut sebagai salah satu syarat untuk menempuh Ujian Akhir Sarjana Teknik.
Demikian permohonan kami dan atas kesediaan Bapak/Ibu kami sampaikan terima kasih.

Prodi T. Informatika S-1
K e t u a,

Joseph Dedy Irawan,ST., MT.
NIP : 197404162005021002

Hormat Kami,

I MADE YOGA YASA PRATHAMA

Form S-3a

INSTITUT TEKNOLOGI NASIONAL
Jln. Bendungan Sigura-gura No. 2
Jln. Raya Karanglo Km2
M A L A N G

PERNYATAAN KESEDIAAN DALAM PEMBIMBINGAN SKRIPSI

Sesuai permohonan dari mahasiswa/i :

Nama : I MADE YOGA YASA PRATHAMA

Nim : 0918150

Program Studi : Teknik Informatika

Dengan ini menyatakan bersedia / ~~tidak bersedia~~.*) membimbing skripsi dari mahasiswa tersebut dengan judul :

*Enkripsi SMS Pada Telepon Selular Menggu*nakan Metode Skipjack Berbasisi Android

Demikian Surat Pernyataan ini kami buat agar dipergunakan seperlunya.

Malang, 4- Juni - 2015

Hormat Kami,

Sonny Prasetio, ST.,MT.
NIP.P.1031000433

Catatan :
Setelah disetujui agar formulir ini diserahkan mahasiswa/i yg bersangkutan kepada Jurusan untuk diproses lebih lanjut
*) coret yang tidak perlu

Form S-3b

A. File java tulis pesan baru :

```
package com.pesanenkripsi;
import java.util.ArrayList;
import android.app.Activity;
import android.content.BroadcastReceiver;
import android.content.ContentResolver;
import android.content.Context;
import android.content.Intent;
import android.content.IntentFilter;
import android.database.Cursor;
import android.net.Uri;
import android.os.Bundle;
//import android.provider.Contacts;
//import android.provider.Contacts.People;
//import android.provider.ContactsContract.CommonDataKinds.Phone;
import android.provider.ContactsContract;
import android.telephony.SmsManager;
import android.view.View;
import android.widget.Button;
import android.widget.EditText;
import android.widget.Toast;
public class Tulis_pesan extends Activity {
        private EditText kunci,pesan,hasil,NoTujuan;
        private Button enkripsi,kirim,contact;
        private String Skunci,Spesan,hexenkrip,no,pesanEnkrip;
        private byte[] enkrip;
        final static int RQS_PICK_CONTACT = 1;
                @Override
          public void onCreate(Bundle savedInstanceState) {
            super.onCreate(savedInstanceState);
            setContentView(R.layout.main);
            kunci=(EditText) findViewById(R.id.kunci);
            pesan=(EditText) findViewById(R.id.pesan);
            hasil=(EditText) findViewById(R.id.hasil);
            NoTujuan=(EditText)findViewById(R.id.NoTujuan);
            enkripsi=(Button)findViewById(R.id.enkrip);
            kirim=(Button)findViewById(R.id.kirim);
            contact=(Button) findViewById(R.id.contact);
            hasil.setFocusable(false);
            //ambil kontak telp
            contact.setOnClickListener(new View.OnClickListener(){
              @Override
              public void onClick(View v) {
                    kontak();
              }
```

```
});

enkripsi.setOnClickListener(new Button.OnClickListener() {
  @Override
                public void onClick(View v) {
                        enkrip();
  }

});

kirim.setOnClickListener(new Button.OnClickListener() {
  @Override
                public void onClick(View v) {
          send();
  }
});

  }

//konvert dari byte array ke hexa string
private String byteArrayToHexString(byte[] b) {
          StringBuffer sb = new StringBuffer(b.length * 2);
          for (int i = 0; i < b.length; i++) {
                int v = b[i] & 0xff;
                if (v < 16) {
                        sb.append('0');
                }
                sb.append(Integer.toHexString(v));
          }
          return sb.toString().toUpperCase();
  }

//operasi load kontak
private void kontak() {
          Intent intent = new Intent(Intent.ACTION_PICK,
  ContactsContract.Contacts.CONTENT_URI);
  startActivityForResult(intent, RQS_PICK_CONTACT);
  }
    //operasi enkrip
  private void enkrip() {
          //memanggil class RC6.java
  Skipjack skipjack=new Skipjack();
  Skunci=kunci.getText().toString();
  Spesan=pesan.getText().toString();
```

```
            //pengecekan panjang kunci
            if (Skunci.length()==0){
               Toast.makeText(getBaseContext(),"Kunci belum terisi",
Toast.LENGTH_SHORT).show();
            }
             else if (Skunci.length()>0 && Spesan.length()>0) {
               //mengenkripsi pesan
               enkrip=skipjack.encrypt(Spesan.getBytes(), Skunci.getBytes());
               //mengubah hasil enkripsi ke bentuk heksadesimal
               hexenkrip=byteArrayToHexString(enkrip);
               //hexenkrip = new String(enkrip);
               //cetak hasil enkrip dalam bentuk heksadesimal
               hasil.setText(hexenkrip);
            }
            else {
                     Toast.makeText(getBaseContext(),"Pesan Tidak Boleh Kosong!!",
Toast.LENGTH_SHORT).show();
            }
               }

               //operasi kirim pesan
               private void send() {
                     no=NoTujuan.getText().toString();
               pesanEnkrip=hasil.getText().toString();
               if(no.length()>0 && pesanEnkrip.length()>0) {
                     sendSMS(no,pesanEnkrip);
                           pindah();
               }
               else if (no.length()>0 && hasil.length()==0) {
                     Toast.makeText(getBaseContext(),"Pesan Kosong / Belum
Terenkripsi", Toast.LENGTH_SHORT).show();
               }
               else {
                     Toast.makeText(getBaseContext(),"Nomor Tujuan Belum Terisi",
Toast.LENGTH_SHORT).show();
               }
               }

               //kembali ke menu utama
               public void pindah() {
                     Intent i=new Intent(this,Halaman_utama.class);
                     startActivity(i);
               }

               //ambil nomor dari kontak hp
            @Override
```

```
        protected void onActivityResult(int requestCode, int resultCode, Intent data) {
            super.onActivityResult(requestCode, resultCode, data);
            if (requestCode == RQS_PICK_CONTACT &&
resultCode==Activity.RESULT_OK) {
                Uri contactData = data.getData();
                ContentResolver cr = getContentResolver();
                Cursor cur = managedQuery(contactData, null, null, null, null);
                if (cur.getCount() > 0) {
                    while (cur.moveToNext()) {
                        //ambil id contact
                        String id = cur.getString(cur
                        .getColumnIndex(ContactsContract.Contacts._ID));
                        //cek jumlah nomor pada contact yg dipilih
                        if (Integer
                                .parseInt(cur.getString(cur

        .getColumnIndex(ContactsContract.Contacts.HAS_PHONE_NUMBER))) > 0) {
                                Cursor pCur = cr
                                //query ke SQLite Contact

        .query(ContactsContract.CommonDataKinds.Phone.CONTENT_URI,
                                null,

        ContactsContract.CommonDataKinds.Phone.CONTACT_ID
                                + " = ?", new String[] { id },
                                null);

                                while (pCur.moveToNext()) {
                                    //ambil nomor berdasarkan id
yang dipilih
                                    String nomorHp = pCur
                                    .getString(pCur

        .getColumnIndex(ContactsContract.CommonDataKinds.Phone.DATA));
                                    NoTujuan.setText(nomorHp);
                                }
                                pCur.close();
                        }
                    }
                }
            }
        }

            //metod pengiriman SMS dan Laporan pengiriman
        private void sendSMS(String phoneNumber,String message) {
            String SENT="SMS_SENT";
```

```
            //PendingIntent sentPI=PendingIntent.getBroadcast(this,0,new
Intent(SENT),0);
            registerReceiver(new BroadcastReceiver() {

                        @Override
                        public void onReceive(Context arg0,Intent arg1) {
                        switch(getResultCode()) {
                                    case Activity.RESULT_OK:
                                                Toast.makeText(getBaseContext(),"SMS
Sent", Toast.LENGTH_SHORT).show();
                                                break;
                                    case Activity.RESULT_CANCELED:
                                                Toast.makeText(getBaseContext(),"SMS
not delivered", Toast.LENGTH_SHORT).show();
                                    break;
                                    case
SmsManager.RESULT_ERROR_GENERIC_FAILURE:

        Toast.makeText(getBaseContext(),"Generic failure",
Toast.LENGTH_SHORT).show();
                                                break;
                                    case
SmsManager.RESULT_ERROR_NO_SERVICE:
                                                Toast.makeText(getBaseContext(),"No
Service", Toast.LENGTH_SHORT).show();
                                                break;
                                    case
SmsManager.RESULT_ERROR_NULL_PDU:
                                                Toast.makeText(getBaseContext(),"Null
PDU", Toast.LENGTH_SHORT).show();
                                                break;
                                    case
SmsManager.RESULT_ERROR_RADIO_OFF:

        Toast.makeText(getBaseContext(),"Radio Off", Toast.LENGTH_SHORT).show();
                                                break;
                                    }
                        }
            }, new IntentFilter(SENT));

            SmsManager sms=SmsManager.getDefault();
            //sms.sendTextMessage(phoneNumber,null, message, sentPI, sentPI);
            ArrayList<String> parts = sms.divideMessage(message);
            sms.sendMultipartTextMessage(phoneNumber, null, parts, null, null);
        }
}
```

B. File java untuk enkripsi pesan :

```
package com.pesanenkripsi;

public class Skipjack {

        //public skipjack(){}
    private int w=32, r=20;
        private int Pw=0xb7e15163, Qw=0x9e3779b9;

        private int[] S;


        //konversi
        private int[] convBytesWords(byte[] key, int u, int c) {
                int[] tmp = new int[c];
                for (int i = 0; i < tmp.length; i++)
                        tmp[i] = 0;

                for (int i = 0, off = 0; i < c; i++)
                        tmp[i] = ((key[off++] & 0xFF)) | ((key[off++] & 0xFF) << 8)
                                        | ((key[off++] & 0xFF) << 16) | ((key[off++] & 0xFF)
<< 24);

                return tmp;
        }


        //penjadwalan kunci
        private int[] generateSubkeys(byte[] key) {

                int u = w / 8;
                int c = key.length / u;
                int t = 2 * r + 4;

                int[] L = convBytesWords(key, u, c);

                int[] S = new int[t];
                S[0] = Pw;
                for (int i = 1; i < t; i++)
                        S[i] = S[i - 1] + Qw;

                int A = 0;
                int B = 0;
                int k = 0, j = 0;

                int v = 3 * Math.max(c, t);
```

```
        for (int i = 0; i < v; i++) {
                A = S[k] = rotl((S[k] + A + B), 3);
                B = L[j] = rotl(L[j] + A + B, A + B);
                k = (k + 1) % t;
                j = (j + 1) % c;
        }

        return S;
}

//penggeseran bit kekiri
private int rotl(int val, int pas) {
        return (val << pas) | (val >>> (32 - pas));
}

//penggeseran bit ke kanan
private int rotr(int val, int pas) {
        return (val >>> pas) | (val << (32-pas));
}


//memecah blok cipertext kedalam 4 register
private byte[] decryptBloc(byte[] input) {
        byte[] tmp = new byte[input.length];
        int t,u;
        int aux;
        int[] data = new int[input.length/4];

        for(int i =0;i<data.length;i++)
                data[i] = 0;
        int off = 0;

        for(int i=0;i<data.length;i++){
                data[i] =       ((input[off++]&0xff))|
                                        ((input[off++]&0xff) << 8) |
                                        ((input[off++]&0xff) << 16) |
                                        ((input[off++]&0xff) << 24);
        }

        int A = data[0],B = data[1],C = data[2],D = data[3];

        C = C - S[2*r+3];
        A = A - S[2*r+2];
        for(int i = r;i>=1;i--) {
                aux = D;
                D = C;
                C = B;
                B = A;
                A = aux;
```

```
                u = rotl(D*(2*D+1),5);
                t = rotl(B*(2*B + 1),5);
                C = rotr(C-S[2*i + 1],t) ^ u;
                A = rotr(A-S[2*i],u) ^ t;
        }

        D = D - S[1];
        B = B - S[0];

        data[0] = A;data[1] = B;data[2] = C;data[3] = D;

        for(int i = 0;i<tmp.length;i++) {
                tmp[i] = (byte)((data[i/4] >>> (i%4)*8) & 0xff);
        }

        return tmp;
}


//memecah blok plaintext kedalam 4 register
private byte[] encryptBloc(byte[] input) {

        byte[] tmp = new byte[input.length];
        int t,u;
        int aux;
        int[] data = new int[input.length/4];
        for(int i =0;i<data.length;i++)
                data[i] = 0;
        int off = 0;
        for(int i=0;i<data.length;i++) {
                data[i] =       ((input[off++]&0xff))|
                                        ((input[off++]&0xff) << 8) |
                                        ((input[off++]&0xff) << 16) |
                                        ((input[off++]&0xff) << 24);
        }

        int A = data[0],B = data[1],C = data[2],D = data[3];

        B = B + S[0];
        D = D + S[1];
        for(int i = 1;i<=r;i++) {
                t = rotl(B*(2*B+1),5);
                u = rotl(D*(2*D+1),5);
                A = rotl(A^t,u)+S[2*i];
                C = rotl(C^u,t)+S[2*i+1];

                aux = A;
                A = B;
                B = C;
                C = D;
```

```
                D = aux;
            }
            A = A + S[2*r+2];
            C = C + S[2*r+3];

            data[0] = A;data[1] = B;data[2] = C;data[3] = D;

            for(int i = 0;i<tmp.length;i++) {
                tmp[i] = (byte)((data[i/4] >>> (i%4)*8) & 0xff);
            }

            return tmp;
    }

    //proses awal kunci
    private static byte[] paddingKey(byte[] key){
int l=0;
if(key.length==1){
    l=3;
}
else
    l=key.length%4;
    byte[]key2=new byte[key.length+l];

for(int i=0;i<key2.length;i++){
    if(i<key.length){
            key2[i]=key[i];
        }
    else{
       key2[i]=0;
        }
            }
return key2;
    }

    /*private byte[] paddingKey(byte[] key) {
            //      int l = key.length%4;
            int l=0;
    if(key.length%2==0)
            l = key.length%2;
    else if(key.length%3==0)
       l=key.length%3;
    else if(key.length%5==0)
       l=key.length%5;
    else if(key.length%7==0)
       l=key.length%7;

            for(int i=0;i<l;i++)
                key[key.length+i] = 0;
            return key;
```

```
}
*/

//fungsi untuk melakukan enkripsi skipjack
public byte[] encrypt(byte[] data, byte[] key) {

        byte[] bloc = new byte[16];
        key = paddingKey(key);
        S = generateSubkeys(key);

        int lenght = 16 - data.length % 16;
        byte[] padding = new byte[lenght];
        padding[0] = (byte) 0x80;

        for (int i = 1; i < lenght; i++)
                padding[i] = 0;
        int count = 0;
        byte[] tmp = new byte[data.length+lenght];

        int i;
        for(i=0;i<data.length+lenght;i++) {
                if(i>0 && i%16 == 0) {
                        bloc = encryptBloc(bloc);
                        System.arraycopy(bloc, 0, tmp, i-16, bloc.length);
                }

                if (i < data.length)
                        bloc[i % 16] = data[i];
                else {

                        bloc[i % 16] = padding[count];
                        count++;
                        if(count>lenght-1) count = 1;
                }
        }
        bloc = encryptBloc(bloc);
        System.arraycopy(bloc, 0, tmp, i - 16, bloc.length);
        return tmp;
}

//fungsi untuk melakukan dekripsi skipjack
public byte[] decrypt(byte[] data, byte[] key) {
        byte[] tmp = new byte[data.length];
        byte[] bloc = new byte[16];
        key = paddingKey(key);
        S = generateSubkeys(key);

        int i;
        for(i=0;i<data.length;i++) {
                if(i>0 && i%16 == 0) {
```

```
                        bloc = decryptBloc(bloc);
                        System.arraycopy(bloc, 0, tmp, i-16, bloc.length);
                }

                if (i < data.length)
                        bloc[i % 16] = data[i];
        }

        bloc = decryptBloc(bloc);
        System.arraycopy(bloc, 0, tmp, i - 16, bloc.length);

        tmp = deletePadding(tmp);
        return tmp;
    }


    //proses penghilangan padding pada key
    private byte[] deletePadding(byte[] input) {
        int count = 0;

        int i = input.length - 1;
        while (input[i] == 0) {
                count++;
                i--;
        }

        byte[] tmp = new byte[input.length - count - 1];
        System.arraycopy(input, 0, tmp, 0, tmp.length);
        return tmp;
    }
}
```

C. File java untuk baca pesan :

```
package com.pesanenkripsi;
import android.app.Activity;
import android.os.Bundle;
import android.view.View;
import android.widget.Button;
import android.widget.EditText;
import android.widget.Toast;

public class Baca_pesan extends Activity {
        private EditText kunci,pesan,hasil2,noPengirim;
        private Button dekripsi;
        private byte[] dekrip,bpesan;
        private String Skunci,Spesan,hasildekrip;
        //String arrayisi[]=new String[2];

        @Override
        public void onCreate(Bundle savedInstanceState) {
                super.onCreate(savedInstanceState);
           setContentView(R.layout.baca_sms);

           Bundle extras=getIntent().getExtras();
           String no=extras.getString(Pesan_masuk.nosms);
           String isi=extras.getString(Pesan_masuk.isisms);

           kunci=(EditText) findViewById(R.id.kunci2);
           pesan=(EditText) findViewById(R.id.pesan2);
           hasil2=(EditText) findViewById(R.id.hasil2);
           noPengirim=(EditText)findViewById(R.id.noPengirim);
           dekripsi=(Button)findViewById(R.id.dekrip);
           pesan.setFocusable(false);
           hasil2.setFocusable(false);

           noPengirim.setText(no);
           pesan.setText(isi);

           /*
           //membuat 2 buah array untuk no HP dan Isi SMS
           int count=0;
           arrayisi[0]="";
           for(int i=0;i<isi.length();i++) {
                if(isi.charAt(i)!=':'){
                        arrayisi[count]+=isi.charAt(i);
                }
```

```
            else if( isi.charAt(i)==':') {
                arrayisi[count+1]="";
                count++;
                }
            }

            //mengambil pesan ke dalam textbox
            noPengirim.setText(arrayisi[0]);
            pesan.setText(arrayisi[1]);
            */

            dekripsi.setOnClickListener(new Button.OnClickListener() {
                @Override
                public void onClick(View v) {
                        dekrip();
                }
            });
        }

        private void dekrip() {
                try{
                //memanggil class Skipjack.java
                Skipjack=new Skipjack();
                Skunci=kunci.getText().toString();
                Spesan=pesan.getText().toString();

                        if(Skunci.length()>0) {
                        //mengubah pesan enkripsi heksa ke byte
                                bpesan=hex2Byte(Spesan);
                                //bpesan= Spesan.getBytes();
                        //dekripsi pesan
                        dekrip=Skipjack.decrypt(bpesan, Skunci.getBytes());
                        //hasil deksripsi pesan dalam bentuk byte di ubah ke bentuk string
                        hasildekrip=new String(dekrip);
                        //hasil dekripsi di cetak
                        hasil2.setText(hasildekrip);

                }
                else {
                  Toast.makeText(getBaseContext(),"kunci tidak boleh kosong",
Toast.LENGTH_SHORT).show();
                }
                  }
                        catch(Exception e){
                                Toast.makeText(getBaseContext(), "Bukan SMS
Terenkripsi",Toast.LENGTH_LONG).show();
```

```
                }
        }

        //konversi hexa ke byte
    private byte[] hex2Byte(String str) {
      byte[] bytes = new byte[str.length() / 2];
      for (int i = 0; i < bytes.length; i++)
      {
        bytes[i] = (byte) Integer
            .parseInt(str.substring(2 * i, 2 * i + 2), 16);
      }
      return bytes;
    }
}
```

D. Java file untuk halaman utama :

```
package com.pesanenkripsi;
import android.app.Activity;
import android.content.Intent;
import android.os.Bundle;
import android.view.View;
import android.widget.Button;

//method menampilkan menu utama dan actifity ketika tombol di klik
public class Halaman_utama extends Activity {
        Button tulispesan,bacasms;

        @Override
        public void onCreate(Bundle savedInstanceState) {
          super.onCreate(savedInstanceState);

          setContentView(R.layout.awal);
          tulispesan=(Button)findViewById(R.id.TulisPesan);
          bacasms=(Button)findViewById(R.id.bacasms);


          tulispesan.setOnClickListener(new Button.OnClickListener() {
              @Override
                  public void onClick(View v) {
                      tulispesan();
              }
```

```
        });

            bacasms.setOnClickListener(new Button.OnClickListener() {
          @Override
                public void onClick(View v) {
                    inbox();
          }
        });

                }

    //memanggil form pesan
    public void tulispesan() {
            Intent i=new Intent(this,Tulis_pesan.class);
            startActivity(i);
    }

    //memanggil form inbox
    public void inbox() {
            Intent i=new Intent(this,Pesan_masuk.class);
            startActivity(i);
    }


}
```

E. XML File Untuk Tampilan Home :

```
<?xml version="1.0" encoding="utf-8"?>
<LinearLayout xmlns:android="http://schemas.android.com/apk/res/android"
   android:layout_width="fill_parent"
   android:layout_height="fill_parent"
   android:background="#DCDCDC"
   android:orientation="vertical" >

   <TextView
      android:id="@+id/textView2"
      android:layout_width="wrap_content"
      android:layout_height="wrap_content"
      android:layout_gravity="center"
      android:text="SECURE MESSAGE"
      android:textColor="#000000"
      android:textSize="30sp"
      android:textStyle="bold"
      android:typeface="monospace" />

   <LinearLayout
```

```
        android:layout_height="94dp" >

        <RelativeLayout
            android:id="@+id/relativeLayout7"
            android:layout_width="match_parent"
            android:layout_height="wrap_content"
            android:layout_alignParentBottom="true"
            android:layout_alignParentLeft="true" >

            <Button
                android:id="@+id/bacasms"
                android:layout_width="70dp"
                android:layout_height="70dp"
                android:layout_alignParentBottom="true"
                android:layout_alignParentRight="true"
                android:layout_marginRight="24dp"
                android:background="@drawable/gmaillogin96" />

            <Button
                android:id="@+id/TulisPesan"
                android:layout_width="70dp"
                android:layout_height="70dp"
                android:layout_alignParentBottom="true"
                android:layout_alignParentLeft="true"
                android:layout_marginLeft="20dp"
                android:background="@drawable/newmessage96" />

        </RelativeLayout>

    </RelativeLayout>
</LinearLayout>

<Button
    android:id="@+id/about"
    android:layout_width="40dp"
    android:layout_height="40dp"
    android:layout_alignParentBottom="true"
    android:layout_alignRight="@+id/linearLayout1"
    android:layout_marginBottom="30dp"
    android:background="@drawable/question57" />

<TextView
    android:id="@+id/textView1"
    android:layout_width="wrap_content"
    android:layout_height="wrap_content"
    android:layout_alignLeft="@+id/linearLayout1"
    android:layout_below="@+id/linearLayout1"
    android:layout_marginLeft="18dp"
    android:text="Tulis pesan"
    android:textColor="#000000"
```

```
    android:id="@+id/linearLayout4"
    android:layout_width="280dp"
    android:layout_height="20dp"
    android:orientation="vertical" >

</LinearLayout>

<RelativeLayout
    android:id="@+id/relativeLayout4"
    android:layout_width="match_parent"
    android:layout_height="wrap_content" >

    <LinearLayout
        android:id="@+id/linearLayout5"
        android:layout_width="280dp"
        android:layout_height="140dp"
        android:layout_alignParentTop="true"
        android:layout_centerHorizontal="true"
        android:orientation="vertical" >

        <ImageView
            android:id="@+id/imageView1"
            android:layout_width="match_parent"
            android:layout_height="wrap_content"
            android:src="@drawable/chatting1" />

    </LinearLayout>
</RelativeLayout>

<RelativeLayout
    android:id="@+id/relativeLayout5"
    android:layout_width="match_parent"
    android:layout_height="wrap_content" >
</RelativeLayout>

<RelativeLayout
    android:id="@+id/relativeLayout3"
    android:layout_width="match_parent"
    android:layout_height="match_parent" >

    <LinearLayout
        android:id="@+id/linearLayout1"
        android:layout_width="280dip"
        android:layout_height="wrap_content"
        android:layout_centerHorizontal="true"
        android:orientation="vertical" >

        <RelativeLayout
            android:id="@+id/relativeLayout2"
            android:layout_width="match_parent"
```

```
        android:layout_width="50dp"
        android:layout_height="50dp"
        android:layout_alignParentTop="true"
        android:layout_centerHorizontal="true"
        android:layout_marginTop="10dp"
        android:background="@drawable/lock7" />

</RelativeLayout>

<TextView
   android:id="@+id/textView4"
   android:layout_width="fill_parent"
   android:layout_height="wrap_content"
   android:text="  Hasil"
   android:textAppearance="?android:attr/textAppearanceMedium" />


<ScrollView
   android:id="@+id/scrollView2"
   android:layout_width="match_parent"
   android:layout_height="wrap_content" >

   <LinearLayout
      android:id="@+id/linearLayout2"
      android:layout_width="match_parent"
      android:layout_height="match_parent"
      android:orientation="vertical" >

            <EditText
               android:id="@+id/hasil"
               android:layout_width="match_parent"
               android:layout_height="78dp"
               android:inputType="textMultiLine"
               android:scrollbarStyle="insideOverlay"
               android:scrollbars="vertical" />

            </LinearLayout>
      </ScrollView>

<RelativeLayout
   android:id="@+id/relativeLayout3"
   android:layout_width="match_parent"
   android:layout_height="match_parent" >

      <Button
         android:id="@+id/kirim"
         android:layout_width="50dp"
         android:layout_height="50dp"
         android:layout_alignParentTop="true"
         android:layout_centerHorizontal="true"
```

```
        android:textColorHint="#000000" />

    <TextView
        android:id="@+id/textView3"
        android:layout_width="wrap_content"
        android:layout_height="wrap_content"
        android:layout_alignBaseline="@ id/textView1"
        android:layout_alignBottom="@+id/textView1"
        android:layout_alignRight="@+id/linearLayout1"
        android:layout_marginRight="15dp"
        android:text="Kotak Masuk"
        android:textColor="#000000" />

  </RelativeLayout>

</LinearLayout>
```

F. XML File Tampilan Tulis Pesan :

```
<?xml version="1.0" encoding="utf-8"?>
<LinearLayout xmlns:android="http://schemas.android.com/apk/res/android"
    android:layout_width="match_parent"
    android:layout_height="match_parent"
    android:background="#708090"
    android:orientation="horizontal" >

    <ScrollView
        android:id="@+id/scrollView1"
        android:layout_width="match_parent"
        android:layout_height="wrap_content" >

        <LinearLayout
            android:id="@+id/linearLayout1"
            android:layout_width="match_parent"
            android:layout_height="wrap_content"
            android:orientation="vertical"
            >

            <TableLayout
                android:id="@+id/tableLayout1"
                android:layout_width="match_parent"
                android:layout_height="wrap_content" >

                <TextView
                    android:id="@+id/textView2"
                    android:layout_width="wrap_content"
                    android:layout_height="wrap_content"
                    android:text="  No Tujuan"
                    android:textAppearance="?android:attr/textAppearanceMedium" />
```

```
        <RelativeLayout
            android:id="@+id/relativeLayout1"
            android:layout_width="wrap_content"
            android:layout_height="wrap_content" >

            <EditText
                android:id="@+id/NoTujuan"
                android:layout_width="216dp"
                android:layout_height="wrap_content"
                android:inputType="phone" >

                <requestFocus />
            </EditText>

            <Button
                android:id="@+id/contact"
                android:layout_width="50dp"
                android:layout_height="45dp"
                android:layout_alignBottom="@+id/NoTujuan"
                android:layout_alignParentTop="true"
                android:layout_marginLeft="27dp"
                android:layout_toRightOf="@+id/NoTujuan"
                android:background="@drawable/contact00" />

        </RelativeLayout>


    </TableLayout>

<TextView
    android:id="@+id/textView1"
    android:layout_width="wrap_content"
    android:layout_height="wrap_content"
    android:layout_gravity="center"
    android:text="Masukan Pesan"
    android:textAppearance="?android:attr/textAppearanceMedium" />


<ScrollView
    android:id="@+id/scrollView2"
    android:layout_width="match_parent"
    android:layout_height="wrap_content" >

    <LinearLayout
        android:id="@+id/linearLayout2"
        android:layout_width="match_parent"
        android:layout_height="wrap_content"
        android:orientation="vertical" >
```

```
        <EditText
            android:id="@+id/pesan"
            android:layout_width="match_parent"
            android:layout_height="76dp"
            android:ems="10"
            android:inputType="textMultiLine"
            android:scrollbars="vertical" />

    </LinearLayout>
</ScrollView>

<TextView
    android:id="@+id/textView3"
    android:layout_width="wrap_content"
    android:layout_height="wrap_content"
    android:layout_gravity="center"
    android:text="Masukan kunci"
    android:textAppearance="?android:attr/textAppearanceMedium" />


<ScrollView
    android:id="@+id/scrollView2"
    android:layout_width="match_parent"
    android:layout_height="wrap_content" >

    <LinearLayout
        android:id="@+id/linearLayout2"
        android:layout_width="match_parent"
        android:layout_height="match_parent"
        android:orientation="vertical" >

        <EditText
            android:id="@+id/kunci"
            android:layout_width="match_parent"
            android:layout_height="wrap_content"
            android:ems="10"
            android:scrollbarAlwaysDrawVerticalTrack="true"
            android:scrollbarStyle="insideOverlay"
            android:scrollbars="vertical" />

</LinearLayout>
</ScrollView>

<RelativeLayout
    android:id="@+id/relativeLayout2"
    android:layout_width="match_parent"
    android:layout_height="match_parent" >

        <Button
            android:id="@+id/enkrip"
```

```
        android:layout_marginTop="10dp"
        android:background="@drawable/news37" />

  </RelativeLayout>

    </LinearLayout>
  </ScrollView>


</LinearLayout>
```

G. XML File Tampilan Pesan Masuk :

```
<?xml version="1.0" encoding="utf-8"?>
<LinearLayout xmlns:android="http://schemas.android.com/apk/res/android"
   android:layout_width="fill_parent"
   android:layout_height="fill_parent"
   android:background="#708090"
   android:orientation="vertical" >


   <ListView
      android:id="@+id/list"
      android:layout_width="match_parent"
      android:layout_height="wrap_content"
      android:background="#708090" >

   </ListView>
</LinearLayout>
```

H. XML File Tampilan Baca Pesan :

```
<?xml version="1.0" encoding="utf-8"?>
<LinearLayout xmlns:android="http://schemas.android.com/apk/res/android"
   android:layout_width="match_parent"
   android:layout_height="match_parent"
   android:background="#708090"
   android:orientation="vertical" >


   <ScrollView
      android:id="@+id/scrollView1"
      android:layout_width="match_parent"
      android:layout_height="wrap_content" >

      <LinearLayout
         android:id="@+id/linearLayout1"
         android:layout_width="match_parent"
```

```
android:layout_height="989dp"
android:orientation="vertical" >

<TextView
   android:id="@+id/textView1"
   android:layout_width="wrap_content"
   android:layout_height="wrap_content"
   android:layout_gravity="center"
   android:text="Nomor Pengirim"
   android:textAppearance="?android:attr/textAppearanceMedium" />

<EditText
   android:id="@+id/noPengirim"
   android:layout_width="match_parent"
   android:layout_height="wrap_content"
   android:inputType="phone" >

   <requestFocus />
</EditText>

<TextView
   android:id="@+id/textView2"
   android:layout_width="wrap_content"
   android:layout_height="wrap_content"
   android:layout_gravity="center"
   android:text="Pesan"
   android:textAppearance="?android:attr/textAppearanceMedium" />

<ScrollView
   android:id="@+id/scrollView2"
   android:layout_width="match_parent"
   android:layout_height="wrap_content" >

   <LinearLayout
      android:id="@+id/linearLayout2"
      android:layout_width="match_parent"
      android:layout_height="wrap_content"
      android:orientation="vertical" >

      <EditText
         android:id="@+id/pesan2"
         android:layout_width="match_parent"
         android:layout_height="99dp"
         android:editable="false"
         android:enabled="true"
         android:inputType="textMultiLine" />
   </LinearLayout>
</ScrollView>

<TextView
```

```
    android:id="@+id/textView3"
    android:layout_width="wrap_content"
    android:layout_height="wrap_content"
    android:layout_gravity="center"
    android:text="Kunci"
    android:textAppearance="?android:attr/textAppearanceMedium" />

  <ScrollView
    android:id="@+id/scrollView3"
    android:layout_width="match_parent"
    android:layout_height="wrap_content">

    <LinearLayout
      android:id="@+id/linearLayout3"
      android:layout_width="match_parent"
      android:layout_height="wrap_content"
      android:orientation="vertical">

      <EditText
        android:id="@+id/kunci2"
        android:layout_width="match_parent"
        android:layout_height="wrap_content" />
    </LinearLayout>
  </ScrollView>

  <RelativeLayout
    android:id="@+id/relativeLayout2"
    android:layout_width="match_parent"
    android:layout_height="match_parent">

    <Button
      android:id="@+id/dekrip"
      android:layout_width="50dp"
      android:layout_height="50dp"
      android:layout_alignParentTop="true"
      android:layout_centerHorizontal="true"
      android:layout_marginTop="10dp"
      android:background="@drawable/unlocked2" />
  </RelativeLayout>

  <TextView
    android:id="@+id/textView4"
    android:layout_width="wrap_content"
    android:layout_height="wrap_content"
    android:text="Hasil"
    android:textAppearance="?android:attr/textAppearanceMedium" />

  <ScrollView
    android:id="@+id/scrollView4"
    android:layout_width="match_parent"
```

```
        android:layout_height="wrap_content">

        <LinearLayout
          android:id="@+id/linearLayout4"
          android:layout_width="match_parent"
          android:layout_height="wrap_content"
          android:orientation="vertical" >
        </LinearLayout>
      </ScrollView>
    </LinearLayout>
  </ScrollView>

  <EditText
    android:id="@+id/hasil2"
    android:layout_width="match_parent"
    android:layout_height="109dp"
    android:editable="false"
    android:ems="10"
    android:inputType="textMultiLine" />

</LinearLayout>
```

I. XML File Tampilan Tutorial :

```
<?xml version="1.0" encoding="utf-8"?>
<LinearLayout xmlns:android="http://schemas.android.com/apk/res/android"
  android:layout_width="match_parent"
  android:layout_height="match_parent"
  android:orientation="vertical"
  android:background="#ffffff"
  >

      <RelativeLayout
        android:id="@+id/relativeLayout3"
        android:layout_width="match_parent"
        android:layout_height="14dp"
        android:orientation="vertical" >

   </RelativeLayout>

  <RelativeLayout
    android:id="@+id/relativeLayout1"
    android:layout_width="match_parent"
    android:layout_height="wrap_content"
    >

  </RelativeLayout>

  <LinearLayout
```

```
    android:id="@+id/linearLayout1"
    android:layout_width="match_parent"
    android:layout_height="wrap_content"
    android:orientation="vertical"
    >

    <RelativeLayout
      android:id="@+id/relativeLayout2"
      android:layout_width="match_parent"
      android:layout_height="wrap_content">

      <TextView
        android:id="@+id/textView1"
        android:layout_width="fill_parent"
        android:layout_height="wrap_content"
        android:layout_alignParentTop="true"
        android:gravity="center"
        android:text="Tutorial Penggunaan Aplikasi:"
        android:textAppearance="?android:attr/textAppearanceLarge"
        android:textColor="#000000" />

    </RelativeLayout>
</LinearLayout>

<LinearLayout
    android:id="@+id/linearLayout2"
    android:layout_width="match_parent"
    android:layout_height="wrap_content"
    android:orientation="vertical"
    >

    <RelativeLayout
      android:id="@+id/relativeLayout3"
      android:layout_width="match_parent"
      android:layout_height="wrap_content"
      >

      <TextView
        android:id="@+id/textView2"
        android:layout_width="fill_parent"
        android:layout_height="wrap_content"
        android:layout_alignParentLeft="true"
        android:layout_alignParentTop="true"
        android:text="Tulis pesan :"
        android:textAppearance="?android:attr/textAppearanceMedium"
        android:textColor="#000000" />

    </RelativeLayout>
</LinearLayout>
```

```
        <RelativeLayout
    android:id="@+id/relativeLayout4"
    android:layout_width="match_parent"
    android:layout_height="wrap_content"
    >

    <TextView
        android:id="@+id/TextView07"
        android:layout_width="fill_parent"
        android:layout_height="wrap_content"
        android:layout_alignParentLeft="true"
        android:layout_alignParentTop="true"
        android:text=" - Tekan tombol tambah pesan"
        android:textAppearance="?android:attr/textAppearanceMedium"
        android:textColor="#000000" />

</RelativeLayout>

<RelativeLayout
    android:id="@+id/relativeLayout5"
    android:layout_width="match_parent"
    android:layout_height="wrap_content"
    >

    <TextView
        android:id="@+id/textView7"
        android:layout_width="fill_parent"
        android:layout_height="wrap_content"
        android:layout_alignParentTop="true"
        android:layout_centerHorizontal="true"
        android:text=" - Input no tujuan"
        android:textAppearance="?android:attr/textAppearanceMedium"
        android:textColor="#000000" />

</RelativeLayout>

        <RelativeLayout
    android:id="@+id/relativeLayout5"
    android:layout_width="match_parent"
    android:layout_height="wrap_content"
    >

</RelativeLayout>

<RelativeLayout
    android:id="@+id/relativeLayout6"
    android:layout_width="match_parent"
    android:layout_height="wrap_content"
    >
```

```
    <TextView
        android:id="@+id/textView9"
        android:layout_width="fill_parent"
        android:layout_height="wrap_content"
        android:layout_alignParentTop="true"
        android:layout_centerHorizontal="true"
        android:text=" - ketik pesan yang akan dikirim"
        android:textAppearance="?android:attr/textAppearanceMedium"
        android:textColor="#000000" />

</RelativeLayout>

<RelativeLayout
    android:id="@+id/relativeLayout7"
    android:layout_width="match_parent"
    android:layout_height="wrap_content"
    >

</RelativeLayout>

<RelativeLayout
    android:id="@+id/RelativeLayout01"
    android:layout_width="match_parent"
    android:layout_height="25dp"
    android:orientation="vertical">

    <TextView
        android:id="@+id/TextView02"
        android:layout_width="fill_parent"
        android:layout_height="wrap_content"
        android:layout_alignParentLeft="true"
        android:layout_alignParentTop="true"
        android:text=" - Masukan kunci enkripsi"
        android:textAppearance="?android:attr/textAppearanceMedium"
        android:textColor="#000000" />

</RelativeLayout>

<TextView
    android:id="@+id/TextView03"
    android:layout_width="fill_parent"
    android:layout_height="wrap_content"
    android:text=" - klik lock untuk enkripsi pesan"
    android:textAppearance="?android:attr/textAppearanceMedium"
    android:textColor="#000000" />

<TextView
    android:id="@+id/TextView01"
    android:layout_width="fill_parent"
    android:layout_height="wrap_content"
```

```
    android:text=" - Hasil enkripsi ditampilkan pada "
    android:textAppearance="?android:attr/textAppearanceMedium"
    android:textColor="#000000" />

  <TextView
    android:id="@+id/TextView04"
    android:layout_width="fill_parent"
    android:layout_height="wrap_content"
    android:text="  kotak hasil"
    android:textAppearance="?android:attr/textAppearanceMedium"
    android:textColor="#000000" />

  <TextView
    android:id="@+id/TextView05"
    android:layout_width="fill_parent"
    android:layout_height="wrap_content"
    android:text=" - Klik tombol send mengirim pesan"
    android:textAppearance="?android:attr/textAppearanceMedium"
    android:textColor="#000000" />

  <RelativeLayout
    android:id="@+id/RelativeLayout02"
    android:layout_width="match_parent"
    android:layout_height="14dp"
    android:orientation="vertical" >

    <RelativeLayout
      android:id="@+id/RelativeLayout03"
      android:layout_width="match_parent"
      android:layout_height="14dp"
      android:layout_alignParentLeft="true"
      android:layout_alignParentTop="true"
      android:orientation="vertical" >
    </RelativeLayout>
  </RelativeLayout>

  <TextView
    android:id="@+id/TextView06"
    android:layout_width="fill_parent"
    android:layout_height="wrap_content"
    android:text=" Baca pesan :"
    android:textAppearance="?android:attr/textAppearanceMedium"
    android:textColor="#000000" />

  <TextView
    android:id="@+id/textView6"
    android:layout_width="fill_parent"
    android:layout_height="wrap_content"
    android:text=" - Klik tombol kotak masuk"
    android:textAppearance="?android:attr/textAppearanceMedium"
```

```
        android:textColor="#000000" />

    <TextView
        android:id="@+id/TextView08"
        android:layout_width="fill_parent"
        android:layout_height="wrap_content"
        android:text=" - Pilih pesan yang akan dibaca"
        android:textAppearance="?android:attr/textAppearanceMedium"
        android:textColor="#000000" />

    <TextView
        android:id="@+id/TextView09"
        android:layout_width="fill_parent"
        android:layout_height="wrap_content"
        android:text=" - Input kunci untuk dekripsi pesan"
        android:textAppearance="?android:attr/textAppearanceMedium"
        android:textColor="#000000" />

    <TextView
        android:id="@+id/TextView10"
        android:layout_width="fill_parent"
        android:layout_height="wrap_content"
        android:text=" - Klik button unlock untuk dekripsi"
        android:textAppearance="?android:attr/textAppearanceMedium"
        android:textColor="#000000" />

    <TextView
        android:id="@+id/TextView11"
        android:layout_width="fill_parent"
        android:layout_height="wrap_content"
        android:text=" - Pesan hasil dekripsi ditampilkan "
        android:textAppearance="?android:attr/textAppearanceMedium"
        android:textColor="#000000" />

    <TextView
        android:id="@+id/TextView12"
        android:layout_width="fill_parent"
        android:layout_height="wrap_content"
        android:text="   pada kotak hasil"
        android:textAppearance="?android:attr/textAppearanceMedium"
        android:textColor="#000000" />

</LinearLayout>
```