APLIKASI *SECURE MESSAGE* BERBASIS ANDROID PADA PT. DENASTI ARRASHVIA INDONESIA

Pipin Farida Ariyani[1)], Ikhwanul Muslimin[2)]
[1,2]Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan, 12260
pipin.faridaariyani@budiluhur.ac.id[1)], ikhwanulmuslimin9@gmail.com[2)]

Abstract

Message security is indispensable in PT. Denasti Arrashvia Indonesia engaged in the field of food and beverage consultants, because PT. Denasti Arrashvia Indonesia are often still use SMS to communicate with the client in the process of running a business. The problem has been PT. Denasti Arrashvia Indonesia always interacting with the client about the project by exchange messages about important matters relating to cooperation such as the cost of the project, formulation of food or drink, as well as everything that should only be known between internal and client only. It would be very risky if known by their business rivals. Cryptographic methods may be one solution to the problem by designed and built secure messaging applications. Applications built on mobile devices based on Android. The method used for cryptography is to combine algorithms Rivest Code 6 (RC6) and Vigenere Cipher in the encryption and decryption process. The final result of this application is to implement the algorithm Rivest Code 6 (RC6) and Vigenere Cipher into encryption and decryption functions with SMS applications in mobile devices. The conclusion of this research is PT. Denasti Arrashvia Indonesia has a mobile-based applications to exchange messages securely with clients or colleagues by implementing algorithms Rivest Code 6 (RC6) and Vigenere Cipher.

Keywords: *SMS, Kriptografi, Rivest Code 6, Vigenere Cipher*

Abstrak

Pengamanan pesan merupakan hal yang sangat diperlukan pada PT. Denasti Arrashvia Indonesia yang bergerak pada bidang konsultan makanan dan minuman, karena dalam proses menjalankan bisnis seringkali PT. Denasti Arrashvia Indonesia masih menggunakan sms untuk berkomunikasi dengan client. Permasalahannya selama ini PT. Denasti Arrashvia Indonesia selalu berinteraksi dengan para client mengenai projek yang sedang dikerjakan seringkali bertukar pesan tentang hal-hal penting yang berkaitan dengan kerjasama seperti biaya projek, formulasi makanan atau minuman, serta segala sesuatu yang hanya boleh diketahui antara internal perusahaan dan client saja , akan sangat merugikan jika hal-hal tersebut diketahui oleh rival bisnis mereka. Dengan permasalahan di atas dirancang dan dibangun aplikasi pesan yang aman dengan kriptografi. Aplikasi dibangun pada perangkat mobile berbasis android. Metode yang digunakan untuk kriptografi adalah dengan mengkombinasikan algoritma Rivest Code 6 (RC6) dan Vigenere Cipher dalam satu proses enkripsi dan dekripsi. Hasil akhir yang didapat dari aplikasi ini adalah mengimplementasikan algoritma Rivest Code 6 (RC6) dan Vigenere Cipher pada fungsi enkripsi dan dekripsi dengan aplikasi SMS dalam perangkat mobile. Kesimpulan dari penelitian ini adalah PT. Denasti Arrashvia Indonesia memiliki suatu aplikasi berbasis mobile untuk bertukar pesan dengan aman dengan para client atau kolega dengan pengimplentasian algoritma Rivest Code 6 (RC6) dan Vigenere Cipher.

Kata kunci *: SMS, Kriptografi, Rivest Code 6, Vigenere Cipher*

1. PENDAHULUAN

Penerapan tata kelola Tenologi Informasi dan Komunikasi saat ini sudah menjadi kebutuhan dan tuntutan pada PT. Denasti Arrashvia Indonesia yang bergerak pada bidang Konsultan Makanan dan Minuman. Penggunaan SMS dalam berkomunikasi mengenai bahan makanan dan minuman masih dilakukan oleh PT. Denasti Arrashvia Indonesia. Dalam peningkatan kualitas layanan, faktor keamanan informasi merupakan aspek yang sangat penting diperhatikan. Berkaitan dengan pengamanan, salah satu teknik pengamanan data yang akan digunakan adalah kriptografi. Kriptografi menggunakan berbagai macam teknik dalam upaya untuk mengamankan data. Data tersebut harus tetap rahasia selama pengiriman dan harus tetap utuh pada saat penerimaan di tujuan. Untuk memenuhi hal tersebut, dilakukan proses penyandian (enkripsi dan dekripsi) terhadap data yang akan dirimkan. Data yang akan menjadi objek kriptografi adalah teks dari pesan SMS, karena SMS bawaan ponsel masih berupa teks terbuka yang belum terproteksi selain itu

pengiriman SMS harus melewati SMSC. Dengan dibutuhkan suatu metode dan aplikasi yang dapat mempertimbangkan solusi *encrypted end to end* dengan melakukan enkripsi terhadap SMS. Algoritma *Rivest Code 6* dan *Vigenere Cipher* dipilih untuk memperkuat enkripsi data yang akan diterapkan.

Berdasarkan latar belakang masalah, maka dapat dirumuskan masalah sebagai berikut:

a. Bagaimana merancang dan membangun aplikasi enkripsi SMS pada perangkat *mobile* berbasis Android ?
b. Bagaimana mengkombinasikan antara algoritma *Rivest Code 6* dan *Vigenere Cipher* ?
c. Bagaimana mengintegrasikan metode kriptografi dengan aplikasi SMS pada perangkat Android ?
d. Bagaimana mengimplementasikan proses enkripsi dan dekripsi pesan SMS pada perangkat *mobile* dengan menggunakan algoritma *Rivest Code 6* dan *Vigenere Cipher* agar dapat menjaga keamanan pesan SMS ?

Dari identifikasi masalah yang ada, penelitian ini memiliki tujuan, untuk menerapkan algoritma kriptografi *Rivest Code 6* dan *Vigenere Cipher* yang akan diimplementasikan menjadi sebuah aplikasi yang dapat mengenkripsi dan mendekripsi, adapun tujuan dari aplikasi ini yaitu:

a. Dapat merancang dan membangun aplikasi SMS terenkripsi pada perangkat *mobile* berbasis android.
b. Bisa mengkombinasikan pesan SMS dengan cara mengenkripsi pesan dan kunci dienkripsi oleh algoritma *Rivest Code 6* dan kemudian setelah itu dienkripsi menggunakan algoritma *Vigenere Cipher.*
c. Dapat mengintegrasikan metode kriptografi dengan aplikasi SMS dalam perangkat *mobile.*
d. Berjalannya fungsi enkripsi dan dekripsi pada aplikasi SMS yang dibuat pada perangkat *mobile* dengan mengimplementasikan algoritma *Rivest Code 6* dan *Vigenere Cipher.*

Penelitian ini memiliki keterbatasan dari sisi waktu dan sumber daya lainnya, maka permasalahan dibatasi pada beberapa hal, yaitu:

a. Pada aplikasi ini yang akan dienkripsi hanya berupa teks.
b. Aplikasi yang dibangun berbasis android.
c. Pembuatan hanya dengan algoritma *Rivest Code 6* dan *Vigenere Cipher.*
d. Tidak membahas kelemahan dan kelebihan algoritma *Rivest Code 6* dan *Vigenere Cipher.*
e. Jenis perangkat *mobile* android minimal versi 2.2 (Gingerbread) API 17.

2. LANDASAN TEORI

2.1. Kriptografi

Kriptografi berasal dari bahasa Yunani, *crypto* dan *graphia*. *Crypto* berarti *secret* (rahasia) dan *graphia* berarti *writing* (tulisan). Definisi terminology kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya kedalam bentuk yang tidak dapat dimengerti lagi maknanya [1].

Pada dasarnya komponen kriptografi terdiri dari beberapa komponen, seperti [2]:

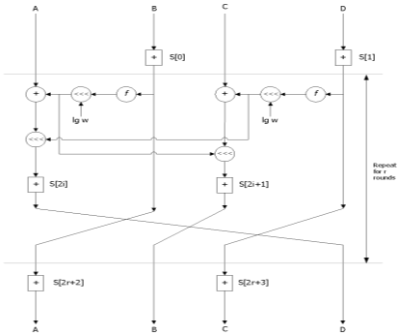
a. Enkripsi
   Merupakan hal yang sangat penting dalam kriptografi, merupakan cara pengamanan data yang dikirimkan sehingga terjaga kerahasiannya. Pada prosesnya pesan asli diubah menjadi kode yang tidak dimengerti.
b. Dekripsi
   Merupakan kebalikan dari enkripsi. Proses mengubah Pesan yang telah dienkripsi dikembalikan ke bentuk asalnya.
c. Kunci
   Kunci disini untuk membuka atau yang akan dipakai untuk enkripsi dan dekripsi.
d. *Plaintext*
   Sering disebut dengan *clear text* / pesan asli. Dapat berupa teks, gambar, suara, video yang menjadi suatu informasi yang menjadi objek dari enkripsi dan dekripsi. *Plaintext* (dalam penerapan berupa SMS) merupakan pesan yang mempunyai makna. *Plaintext* inilah yang diproses menggunakan algoritma kriptografi menjadi pesan kode yang tidak dimengerti.
e. *Ciphertext*
   Merupakan suatu pesan yang telah melalui proses enkripsi. Pesan yang ada pada teks-kode ini tidak bisa dibaca karena berupa karakter-karakter yang tidak mempunyai makna (arti).
f. *Cryptanalis*
   Praktisi yang akan mencoba / membobol suatu algoritma yang dipakai pada proses enkripsi dan dekripsi.

2.2. Algoritma Rivest Code 6

Algoritma Rivest Code 6 (RC6) adalah algoritma yang menggunakan kunci simetris (kunci enkripsi sama dengan kunci dekripsi). Dirancang oleh Ronald Linn Rivest, Matt J.B Robshaw, Ray Sydney dan Yuqin Lisa Yin dari laboratorium RSA.

Letak perbedaan yang mendasari dari RC6 terhadap varian-varian sebelumnya adalah langkah transformasi dan perbedaan banyak register. Register diperlukan untuk penempatan blok data yang diolah pada algoritma sehingga algoritma mengolah data pada tiap register yang ada. Pada algoritma RC5 membagi *plaintext* ke dalam 2 register. RC6 yang membagi *plaintext* ke dalam 4 register. RC6 mempunyai 3 parameter, sehingga dituliskan sebagai RC-*w/r/b*. Ketiga parameter tersebut berarti besar suku kata dalam bit register *w* (32, 64 atau 128 bit), banyak iterasi *r* yang tidak boleh bernilai negatif, dan panjang kata kunci dalam *bytes b*. Saat algoritma RC6 masuk kandidat AES, ditetapkan nilai *w* =32 bit, *r* = 20 dan *b* bervariasi antara 16, 24 dan 32 *byte.* Pemilihan *w* = 32 bit mengindikasikan bahwa operasi-operasi yang ada pada algoritma RC6 seperti penjumlahan, pengurangan, perkalian, XOR, dan *shift* dilakukan pada operand berupa tepat 32 bit bilangan biner.[3]

Karena RC6 memecah blok 128 bit menjadi 4 buah blok 32 bit, maka algoritma RC6 bekerja dengan 4 buah register 32 bit A, B, C, D. *Byte* yang pertama dari *plaintext* atau *ciphertext* ditempatkan pada *byte* A, sedangkan *byte* yang terakhirnya ditempatkan pada *byte* D. Dalam prosesnya, akan didapatkan (A, B, C, D) = (B, C, D, A) yang diartikan bahwa nilai yang terletak pada sisi kanan berasal dari register di sisi kiri. Diagram blok berikut akan menjelaskan proses enkripsi yang terjadi pada algoritma RC6 [3].



Gambar 1:Diagram Blok Enkripsi RC6

2.3. Algoritma Vigenere Cipher

Vigenere Cipher adalah suatu algoritma kriptografi klasik yang ditemukan oleh Giovan Battista Bellaso. Beliau menuliskan metodenya tersebut pada bukunya yang berjudul La Cifra del Sig. Giovan Battista Bellaso pada tahun 1553. Nama Vigenere sendiri diambil dari seorang yang bernama Biaise de Vigenere. Nama Vigenere diambil sebagai nama algoritma ini karena beliau menemukan kunci yang lebih kuat lagi untuk algoritma ini dengan metode *autokey cipher* meskipun algoritma dasarnya terlah ditemukan lebih dahulu oleh Giovan Battista Bellaso.

Algoritma ini menjadi terkenal karena cukup sulit dipecahkan. Matematikawan Charles Lutwidge Dodgson menyatakan bahwa algoritma ini tidak terpecahkan. Pada tahun 1917, ilmuwan Amerika menyebutkan bahwa Vigenere Cipher adalah sesuatu yang tidak mungkin untuk ditranslasikan. Namun hal ini terbantahkan sejak Kasiski berhasil memecahkan algoritma pada abad ke-19.

Vigenere Cipher menggunakan bujur sangkar untuk melakukan enkripsi. Pada bujur sangkar tersebut, kolom paling kiri menyatakan huruf-huruf kunci, dan baris paling atas menyatakan *plaintext*, sedangkan karakter-karakter lainnya menunjukkan karakter *ciphertext*. Karakter *ciphertext* ditentukan dengan menggunakan prinsip *Caesar Cipher*. Kunci : $K_1,K_2,\ldots K_n$ K_i untuk $1 \leq i \leq m$ menyatakan jumlah pergeseran pada huruf ke-*i*.karakter*ciphertext c* $(p) = (p + k_i)$ mod 26 [4].

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Gambar 2: Bujur Sangkar Vigenere Cipher

Bujur sangkar *VigenereCipher* digunakan untuk mendapatkan *ciphertext* dengan menggunakan kunci yang telah ditentukan. Jika panjang kunci lebih pendek daripada panjang *plaintext*, maka kunci diulang penggunaannya (sistem periodik). Jika panjang kunci adalah m, maka periodenya adalah m.

Penggunaan bujur sangkar *Vigenere Cipher* pada enkripsi serupa dengan penjumlahan (dalam desimal) *plaintext* dengan kunci, lalu modul 26, sehingga dapat dirumuskan sebagai berikut [5]:

Enkripsi : ci = E (pi) = (pi + ki) mod 26
Dekripsi : pi = D (ci) = (ci - ki) mod 26

Dekripsi *Vigenere Cipher* dengan menggunakan bujur sangkar *Vigenere Cipher* dilakukan dengan cara kebalikan dari enkripsi, yaitu dengan menarik garis mendatar dari huruf kunci sampai ke huruf *ciphertext* yang ditunjukkan, kemudian dari huruf *ciphertext*

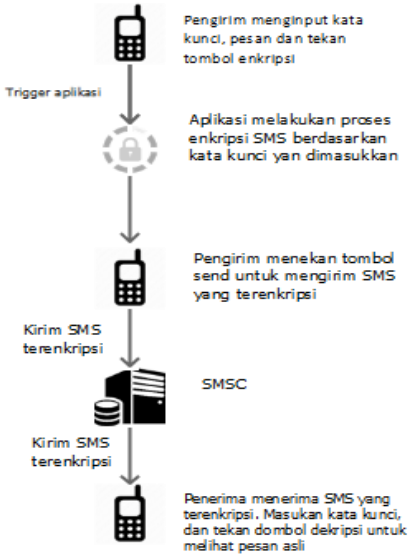
tersebut tarik garis vertikal ke atas sampai ke huruf *plaintext*.

Untuk memecahkan *Vigenere Cipher*, perlu mengetahui kuncinya. Jika periode atau panjang kunci (m) diketahui, maka kunci dapat ditebak dengan *exhaust search*. Namun diperlukan hingga 26^m kali percobaan untuk mendapatkan kunci yang menghasilkan *plaintext* sesuai.

3. RANCANGAN SISTEM DAN APLIKASI

3.1. Perancangan Progam

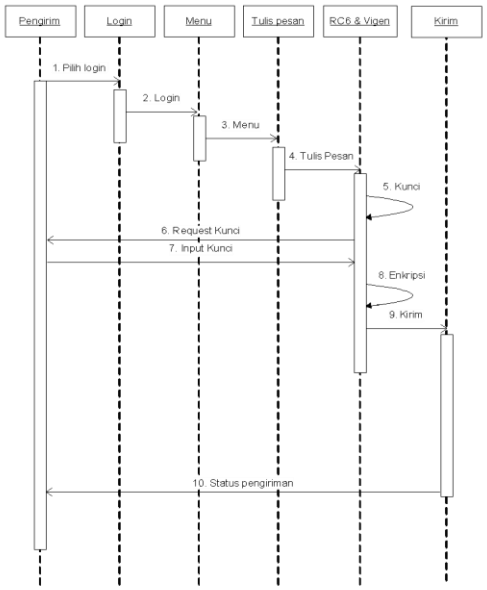
Aplikasi *secure message* ini memiliki beberapa modul atau fungsi yang menunjang satu sama lain. Pengirim pesan menulis pesan singkat lalu memasukkan kata kunci yang ditentukan dan menekan tombol kirim untuk mengirim pesan SMS dan otomatis pesan terenkripsi terkirim. Pesan yang terkirim ke SMSC sudah terenkripsi dan aman dari kebocoran informasi oleh pihak-pihak yang tidak bertanggung jawab, lalu dari sisi penerima, melakukan pembacaan pesan melalui aplikasi *secure message* dengan memasukkan kata kunci yang sama dengan kata kunci pengirim pesan, dan menekan tombol dekripsi untuk melihat pesan asli yang tersembunyi.



Gambar 3: Rancangan Pola Kerja Sistem

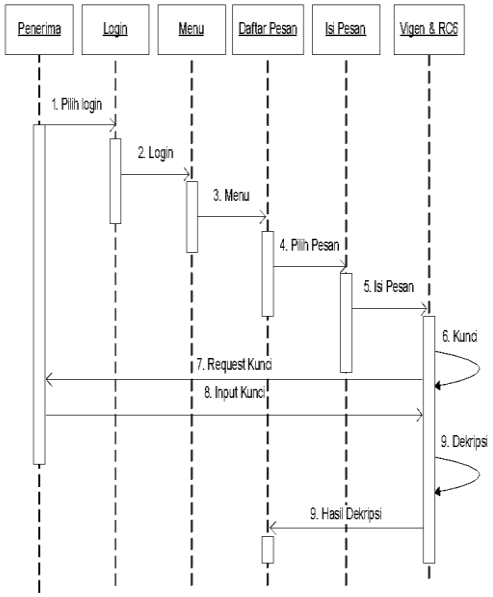
3.2. *Sequence Diagram*

Di bawah ini terlihat aktifitas *user* untuk melakukan login. Setelah login dipilih sistem kemudian memanggil sistem menu, proses selanjutnya memilih menu tulis pesan. Setelah menulis pesan dipilih sistem kemudian memanggil fungsi tulis pesan. Setelah pesan ditulis, proses selanjutnya adalah *user* diminta untuk memasuki kunci enkripsi pada fungsi Riverst Code 6 dan Vigenere Cipher setelah itu proses mengenkripsi pesan yang telah ditulis. Setelah pesan selesai dienkripsi maka hasil enkripsi akan tampil pada fungsi tulis pesan dan kemudian pesan dapat dikirim dan pengirim mendapat pesan status pengiriman.



Gambar 4: Sequence Diagram Tulis Pesan

Kebalikan dari proses enkripsi di atas, berikut ini adalah diagram baca pesan yang akan diterapkan pada aplikasi *secure message* berikut ini.

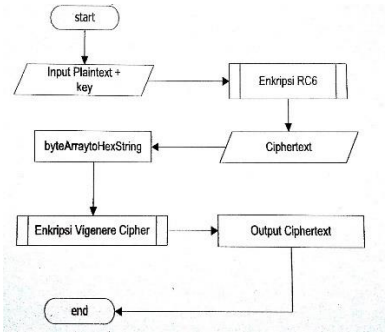


Gambar 5: Sequence Diagram Baca Pesan

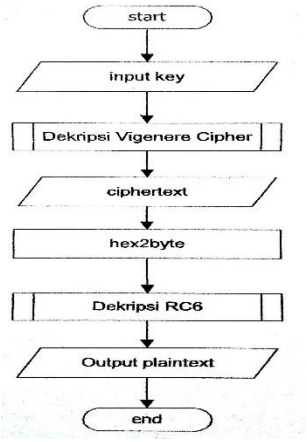
3.3. *Flowchart*

Di bawah ini menjelaskan tentang flowchart proses enkripsi dan dekripsi dimana user menginput plaintext dan kunci lalu dienkripsi menggunakan algoritma Rivest Code 6, setelah dienkripsi ciphertext yang berbentuk kumpulan byte diubah menjadi bilangan hexa yang selanjutnya dienkripsi menggunakan algoritma

Vigenere Cipher yang akan menjadi hasil keluaran / output. Untuk dekripsi kebalikan dari proses enkripsi.



Gambar 6: Flowchart Proses Enkripsi



Gambar 7: Flowchart Proses Dekripsi

4. HASIL DAN PEMBAHASAN

Agar aplikasi *secure message* berjalan dengan baik, spesifikasi perangkat yang digunakan untuk implementasi aplikasi ini juga harus mendukung. Spesifikasi yang digunakan pada saat pembuatan aplikasi ini, diantaranya adalah:

a. Perangkat Keras

Dalam pembuatan aplikasi *secure message*, *requirement* perangkat keras (*hardware*) yang digunakan untuk implementasi aplikasi ini adalah sebagai berikut:

1) Laptop Acer Aspire 4732Z
   a) Processor, Intel Dual Core CPU
   b) RAM (*Random Acces Memory*) 2GB
2) Smartphone Xiaomi Redmi 2
   a) CPU, Quad-Core 1,2GHz
   b) RAM, 1GB

b. Perangkat Lunak

Dalam pembuatan aplikasi *secure message*, *requirement* perangkat lunak (*software*) yang digunakan untuk implementasi aplikasi ini adalah sebagai berikut:

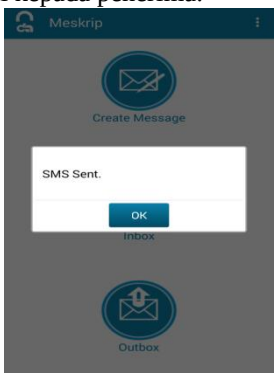
1) Sistem Operasi Windows 7 Ultimate 32-bit
2) Android Studio

4.1. Tampilan Uji Coba Proses Enkripsi

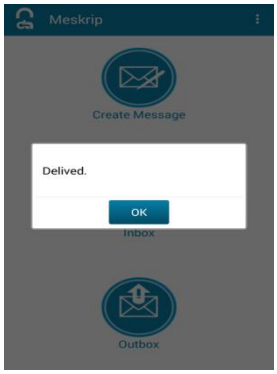
Untuk melakukan proses enkripsi *user* dapat memilih menu *Create Message*, setelah itu menginput nomor tujuan sebagai contoh nomor tujuan adalah 081282527376, kunci "Kunci123" dan isi pesan "Pesan". Pada gambar 8 memperlihatkan tampilan awal nomor tujuan, kunci dan isi pesan yang akan di dekripsi.

Gambar 8: Data yang akan Dienkripsi

Jika pesan berhasil maka akan muncul notifikasi bahwa pesan terkirim, dan ketika muncul notifikasi "delived" yang berarti pesan telah sampai kepada penerima.



Gambar 9: Notifikasi Pesan Berhasil Terkirim



Gambar 10: Notifikasi Pesan Telah Berhasil Sampai Ke Penerima

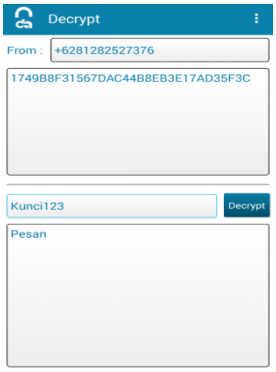
4.2. Tampilan Uji Coba Proses Dekripsi

Untuk melakukan proses dekripsi *user* dapat memilih menu *Inbox*. Pilih daftar pesan, lalu muncul tampilan halaman *decrypt*. Pada gambar 11 memperlihatkan tampilan awal dari proses dekripsi dengan data nomor tujuan

"081282527376", kunci "Kunci123" dan isi pesan "Pesan".

Gambar 11: Tampilan Layar Inbox

Pada gambar 12 terlihat pesan berhasil di dekripsi dari nomor tujuan "081282527376" dengan kunci "Kunci123".



Gambar 12: Tampilan Layar Berhasil Mendekripsi

4.3. Pengujian Validasi

Pengujian validasi dilakukan untuk mengetahui bahwa aplikasi dapat memenuhi kebutuhan fungsional untuk melakukan enkripsi *plaintext* menjadi *ciphertext* dan mendekripsikan *ciphertext* menjadi *plaintext* kembali. Pesan yang diujikan adalah data pesan yang dikumpulkan peneliti. Sedangkan, kunci yang digunakan bervariasi. Pada proses pengiriman SMS dilakukan dengan bantuan provider agar sampai ke tempat nomor tujuan. Daftar pesan yang dienkripsi ditunjukan tabel sebagai berikut :

Tabel 1: Pengujian Validasi

No	Pesan SMS	Key	Enkripsi	Dekripsi
1	21 Karakter dan angka	123	54136B96F87C5C9CCB8C48D61E71C1F4BEAAAF5EF92520E42FD7FF9B9B35495F	21 Karakter dan angka
2	Spesial karakter !@#$	(*)	E1C4BCB551E2D4BB950B97CF6EDAF5ACEF7D8B5CC09AD395DD1B5129257C108C	Spesial karakter !@#$
3	21 Karakter dan angka	(*)	D0521A36D0FC2ECA569CA22EF9AB4D066ECFD9056D0EBCB04564F498DFC43030	21 Karakter dan angka
4	Spesial karakter !@#$	123	0E505EB441762D9282F5791E58C16414A135EE8A6A42D7287AB3C39C56266870	Spesial karakter !@#$

Pada tabel 2 akan dilakukan proses pengujian panjang maksimal karakter SMS yang bisa dikirimkan dengan enkripsi maupun dengan yang tidak terenkripsi.

Tabel 2: Pengujian Panjang Karakter Pesan Dan Kunci

No	Panjang karakter	Panjang Kunci	Status
1	10 karakter	2 karakter	Berhasil terkirim
		30 karakter	Berhasil terkirim
		32 karakter	Berhasil terkirim
2	79 karakter	2 karakter	Berhasil terkirim
		30 karakter	Berhasil terkirim
		32 karakter	Berhasil terkirim
3	80 karakter	2 karakter	Gagal terkirim

		30 karakter	Gagal terkirim
		32 karakter	Gagal terkirim
4	80 karakter	No key	Berhasil terkirim
5	150 karakter	No key	Berhasil terkir
6	160 karakter	No key	Berhasil terkirim
7	161 karakter	No key	Gagal terkirim

4.4. Pengujian Kecepatan Proses

Pengujian kecepatan proses dilakukan untuk mengetahui proses enkripsi dan dekripsi sebagai acuan analisis terhadap kecepatan proses. Pengujian dengan menggunakan 3 smartphone android yaitu Xiaomi Redmi 2 dengan RAM 1GB, Lenovo A859 dengan RAM 1GB, dan ASUS Zenfone 5 dengan RAM 1GB.

Tabel 3: Pengujian Kecepatan Proses Enkripsi

Panjang Pesan	Panjang Kunci	Enkripsi (Detik)	Dekripsi (Detik)	Hardware
20	5	0.716	0.007	Xiaomi Redmi 2
30	5	0.796	0.009	
40	5	0.921	0.009	
20	10	0.808	0.007	
30	10	0.999	0.006	
40	10	0.762	0.008	
20	5	0.103	0.008	Lenovo A859
30	5	0.035	0.018	
40	5	0.033	0.01	
20	10	0.03	0.012	
30	10	0.032	0.023	
40	10	0.038	0.018	
20	5	0.789	0.006	Asus Zenfone 5
30	5	0.267	0.019	
40	5	0.023	0.009	
20	10	0.104	0.006	
30	10	0.890	0.005	
40	10	0.056	0.007	

4.5. Evaluasi Program

Evaluasi program merupakan tahap akhir yang perlu dilakukan dalam pengembangan suatu aplikasi perangkat lunak. Evaluasi program bertujuan untuk mengetahui hasil yang telah dicapai oleh aplikasi yang dibuat dan menentukan kekurangan dan kelebihan aplikasi. Berdasarkan hasil uji coba program, data kuesioner dan eksekusi yang dilakukan, maka didapat beberapa kelebihan dan kekurangan pada aplikasi *secure message* berbasis android adalah sebagai berikut:

A. Kelebihan Aplikasi

1) Dapat mengirim pesan terenkripsi maupun pesan yang tidak terenkripsi.
2) Proses enkripsi yang cepat dan aman karena menggunakan 2 algoritma, Rivest Code 6 dan Vigenere Cipher.
3) Fitur ganti password, memudahkan *user* untuk mengganti password.
4) Dengan adanya fitur login, autentikasi data lebih terjaga.
5) Adanya notifikasi pesan tidak terkirim, apabila *device* dalam status *airplane mode* dan apabila tidak ada jaringan.
6) *User* tidak dapat memasukan nama yang sama ketika melakukan proses registrasi baru pada 1 perangkat.
7) *Design user interface* yang *simple*, memudahkan *user* menggunakan aplikasi *secure message* ini.
8) Input kunci dapat kurang dari 8 karakter.

B. Kekurangan Aplikasi

1) Duplikasi nama *user* yang sama ketika aplikasi di install pada 2 perangkat device yang berbeda.
2) Waktu proses enkrip dan dekrip yang fluktuatif, meskipun panjang kunci dan pesan sama, tetapi waktu proses sering kali berbeda.
3) Panjang pesan tidak terenkripsi hanya mencapai 160 karakter. Jika lebih dari 160 karakter pesan yang tidak terenkripsi tidak bisa dikirim.
4) Panjang pesan terenkripsi hanya mencapai 79 karakter dengan panjang kunci 1 karakter. Lebih dari 79 karakter pesan tidak bisa di kirim.
5) Notifikasi *alert* pesan terkirim yang serta merta tidak langsung hilang, harus dengan 2 sampai 4 kali klik baru *alert* akan hilang.

5. KESIMPULAN

Berdasarkan perancangan, pembuatan, analisa program dan uji coba dari aplikasi pengamanan data ini, maka dapat diambil suatu kesimpulan sebagai berikut:

a. Aplikasi sms terenkripsi dapat dibuat pada perangkat mobile berbasis android, menggunakan algoritma RC6 dan Vigenere cipher.
b. Proses pengiriman pesan SMS menjadi lebih aman karena adanya fitur enkripsi.
c. Dapat menggabungkan algoritma RC6 dan Vigenere cipher dalam satu proses enkripsi dekripsi.
d. Waktu proses enkripsi dan dekripsi yang cepat.

e. Dengan adanya aplikasi pengamanan data ini, dapat memperkecil terjadinya pencurian, manipulasi data, dan penyalahgunaan data.
f. Pengamanan data menjadi lebih mudah dan cepat dengan tingkat keamanan yang tinggi.

Aplikasi kriptografi ini belum sempurna, dan masih memerlukan banyak perbaikan untuk meningkatkan efektifitas pekerjaan. Beberapa saran dapat diberikan untuk mengembangkan aplikasi ini lebih lanjut, yaitu :

a. Aplikasi ini diharapkan dapat ditingkatkan kinerjanya sehingga tidak hanya dapat mengenkripsi pesan jenis *teks*, namun bisa mengirim MMS (*Multimedia Message*) terenkripsi. Seperti Gambar dokumen spreadsheet, mp3, dan lainnya.
b. Untuk memudahkan pencarian pesan perlu adanya fitur *search* pada *inbox* atau *outbox*.
c. Menklasifikasikan tampilan pesan-pesan yang berada di *inbox* menjadi satu berdasarkan kategori pengirim pesan sms.
d. Menklasifikasikan tampilan pesan-pesan yang berada di *outbox* menjadi satu berdasarkan kategori pesan sms yang telah dikirim.
e. Mengklasifikasikan pesan berdasarkan tanggal dan waktu pengiriman atau menerima sms.
f. Perlu adanya fitur pin dan unpin terhadap pesan yang sudah dibaca dan yang belum dibaca
g. Adanya pengembangan untuk fitur *forward* untuk meneruskan pesan SMS ke orang lain.
h. Adanya fitur *draft* untuk menyimpan sms yang hendak dikirim kemudian.
i. Adanya fitur *template* untuk mengirim sms sesuai dengan *template* sms yang sudah diatur.

DAFTAR PUSTAKA

[1] Arius, D., 2008. *Pengatar Ilmu Kriptografi Teori Analisis dan Implementasi*

[2] Aryana P. H, et al. 2012, *Implementasi Enkripsi Data Dengan Algoritma Vigenere Cipher*, Seminar NasionalTeknologi Informasi dan Komunikasi (SENTIKA 2012), Maret 2012, Program StudiTeknikInformatika, STMIK Dharma Putra Tangerang.

[3] Defni, R. Indri, 2014, *Enkripsi SMS (Short Message Service) Pada Telepon Selular Berbasis Android Dengan Metode RC6*, Jurnal Momentum, Volume 16, No 1, Februari 2014, Politeknik Negeri Padang.

[4] Munir, Rinaldi, 2006. "*Kriptografi*", Penerbit Informatika, Bandung

[5] Abd H., I. Uzzin Nadhori, Setiawardhana, 2010, *Pembuatan Perangkat Lunak Media Pembelajaran Kriptografi Klasik*, Makalah Seminar Proyek Akhir PENS-ITS, Institut Teknologi Sepuluh November.