E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 07, Nomor 03, September 2022 : 680–691

IMPLEMENTASI VIGENERE CIPHER PADA APLIKASI *MYPRICHAT* END-TO-END ENCRYPTED SMS BERBASIS ANDROID

Allin Junikhah
Program Studi Teknik Informatika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang
Jl. Gajayana 50, Malang 65144, Indonesia
e-mail: allin@uin-malang.ac.id

ABSTRAK

Teknologi Short Message Service (SMS) merupakan teknologi yang tidak asing lagi dalam masyarakat. Teknologi layanan pengiriman pesan singkat ini memiliki kelebihan tersendiri jika dibandingkan teknologi messanger instan yang banyak dikenal dewasa ini. Teknologi SMS tidak memerlukan jaringan internet bagi sisi penerima, sehingga dapat dipastikan pesan akan selalu tersampaikan. Teknologi ini juga dapat digunakan pada seluruh tipe telepon selular manapun. SMS masih banyak digunakan dalam aktifitas perpesanan teks singkat terlebih yang berhubungan dengan otentikasi akun pribadi, yang memastikan agar pesan diterima baik oleh penerima. Semakin berkembangnya teknologi dan mudahnya mendapatkan informasi pada era sekarang ini, semakin masyarakat memahami pentingnya pengamanan dalam data informasi pribadi termasuk pada komunikasi pesan teks, terlebih untuk pesan rahasia yang sangat sensitif yang tidak berhak dikonsumsi oleh pihak lain yang tidak berkepentingan. Karena pada dasarnya data yang terdapat pada SMS merupakan teks terang atau plainteks. End-to-end encryption (E2EE) merupakan mekanisme dimana komunikasi pesan hanya dapat diakses oleh pengirim dan penerima data. Memanfaatkan sisi kelebihan SMS sebagai media komunikasi serta menggunakan mekanisme end-to-and encryption, aplikasi MyPriChat (My Private Chat) dibangun. Aplikasi ini merupakan aplikasi mobile yang memanfaatkan teknologi SMS dengan tambahan fitur pengamanan enkripsi yang mengimplementasikan algoritma Vigenere Cipher. Aplikasi ini dibangun pada sistem operasi berbasis Android. Untuk dapat memanfaatkan aplikasi enkripsi SMS MyPriChat yaitu dengan melakukan instalasi baik pada telepon seluler user pengirim maupun user penerima. Pada tahap pengujian, aplikasi enkripsi SMS MyPriChat telah dapat berjalan pada emulator maupun telepon seluler dengan baik. Aplikasi ini diharapkan dapat memberikan suatu pilihan dalam berkomunikasi, selain sebagai suatu aplikasi yang memberikan layanan komunikasi pesan teks, sekaligus dapat mengamankan pesan teks yang dikirimkan.

***Kata Kunci**: Android, Enkripsi, SMS, Vigenere Cipher.*

ABSTRACT

Short Message Service (SMS) technology is a technology that is not foreign to the community. This short message service technology has its own advantages when compared to the instant messanger technology that is widely known today. SMS technology does not require internet networking for the recipient side, so you can be sure the message will always be delivered. This technology can also be used on any type of cellular phone. SMS is still widely used in short text messaging activities, especially those related to personal account authentication, which ensures that messages are received well by the recipient. The development of technology and the ease of obtaining information in this era, people more understand the importance of securing personal information data, including text message communication, especially for very sensitive secret messages that do not have the right to be consumed by unauthorized parties. Because basically the data contained in SMS is plain text. End-to-end encryption (E2EE) is a mechanism whereby message communication can only be accessed by the sender and recipient of the data. Taking advantage of the advantages of SMS as a communication medium and using an end-to-and encryption mechanism, the MyPriChat (My Private Chat) application was built. This application is a mobile application that utilizes SMS technology with additional encryption security features that implement the Vigenere Cipher algorithm. This application is built on an Android-based operating system. To use the MyPriChat SMS encryption application, that is by installing it on both the sending and receiving users' mobile phones. At the testing stage, MyPriChat SMS encryption application has been able to run on emulators and mobile phones well. This application is expected to provide an option in communicating, being an application that provides text message communication services, and also being able to secure sent text messages.

***Keywords**: Android, Encryption, SMS, Vigenere Cipher.*

I. PENDAHULUAN

TEKNOLOGI *Short Message Service* (SMS) merupakan teknologi yang tidak asing lagi dalam masyarakat. SMS merupakan suatu teknologi layanan pengiriman pesan singkat melalui telepon genggam yang bekerja pada jaringan nirkabel. Teknologi layanan pengiriman pesan singkat ini memiliki kelebihan tersendiri jika dibandingkan teknologi *messanger* instan yang banyak dikenal dewasa ini. Menurut majalah Forbes dalam salah satu artikelnya, "*The original and still most universal global messaging platform is SMS"* [1]. Teknologi SMS

E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 07, Nomor 03, September 2022 : 680–691

tidak memerlukan jaringan internet bagi sisi penerima, sehingga dapat dipastikan pesan akan selalu tersampaikan. Teknologi ini juga dapat digunakan pada seluruh tipe telepon selular manapun. SMS masih banyak digunakan dalam aktifitas perpesanan teks singkat terlebih yang berhubungan dengan otentikasi akun pribadi, yang memastikan agar pesan diterima baik oleh penerima.

Semakin berkembangnya teknologi dan mudahnya mendapatkan informasi pada era sekarang ini, semakin masyarakat memahami pentingnya pengamanan dalam data informasi pribadi termasuk pada komunikasi pesan teks. Salah satu bentuk pengamanan informasi adalah dengan melakukan enkripsi menggunakan metode atau teknik kriptografi [2]. Ketika suatu pesan dikirim dari suatu tempat ke tempat lain, isi pesan tersebut mungkin dapat disadap oleh pihak lain yang tidak berhak untuk mengetahui isi pesan tersebut. Untuk menjaga pesan, maka pesan tersebut dapat diubah menjadi suatu kode yang tidak dapat dimengerti oleh pihak lain [3].

Seperti kutipan salah seorang peneliti keamanan terkemuka dari Gartner Research, Nick Jones: "*Don't Use SMS for Confidential Communication*" [4] (Jangan gunakan SMS untuk komunikasi rahasia). Secara jelas dapat diartikan begitu rentannya keamanan pada SMS. Dapat dimungkinkan terjadi resiko keamanan pada SMS seperti SMS *Spoofing*, SMS *Snooping*, atau SMS *Interception*. SMS *Interception* merupakan celah keamanan terbesar pada komunikasi SMS, hal ini dikarenakan SMS bekerja pada jaringan nirkabel yag memungkinkan pencurian data pesan SMS ketika masih dalam transmisi dari pengirim ke penerima.

Dengan pertimbangan tersebut maka sangat diperlukan sekali suatu aplikasi yang mempertimbangkan solusi *end-to-end encrypted* pada perangkat dengan fitur keamanan sebagai fitur tambahan dengan tetap memanfaatkan kelebihan teknologi SMS yang ada.

Proses enkripsi yang dilakukan dalam pengembangan sistem aplikasi *mobile* ini yaitu menggunakan algoritma Vigenere Cipher. Vigenere Cipher merupakan salah satu algoritma klasik. Algoritma ini memiliki kelebihan tersendiri dibandingkan algoritma klasik yang lain, seperti halnya algoritma Caesar Cipher dan Hill Cipher. Seperti dalam salah satu penelitian "*Perbandingan Hasil Performa Optimasi Transposisi Hill Cipher dan Vigenere Cipher pada Citra Digital*" [5], menggunakan Vigenere Cipher citra hasil enkripsi masih menunjukkan karakteristik citra aslinya, hanya komposisi warnanya saja yang berubah. Optimasi transposisi yang dilakukan memberikan kinerja yang cukup baik karena secara visual citra hasil enkripsi Vigenere Cipher menjadi terlihat jauh lebih acak [5]. Vigenere Cipher mungkin adalah contoh terbaik dari cipher alphabet majemuk manual [6]. Jika pada Caesar Cipher kuncinya hanya satu nilai saja, maka pada Vigenere Cipher kunci yang digunakan berbentuk deretan huruf. Kunci yang berbetuk deretan kata tersebut akan memungkinkan setiap huruf plainteks untuk dienkripsi dengan kunci yang berbeda [7]. Kelebihan sandi ini dibanding sandi Caesar dan sandi monoalfabetik lainnya adalah sandi ini tidak begitu rentan terhadap metode pemecahan sandi yang disebut analisis frekuensi [8]. Vigenere cipher dikenal luas karena cara kerjanya yang mudah dimengerti dan dijalankan serta bagi para pemula akan sulit untuk dipecahkan. Pada saat kejayaannya, Vigenere Cipher dijuluki sebagai *le chiffre indenchiffrable* (bahasa perancis: "sandi yang tak terpecahkan") [9].

Aplikasi *MyPriChat* (*My Private Chat*) merupakan aplikasi enkripsi SMS berbasis Android dengan memanfaatkan algoritma Vigenere Cipher yang dibangun dengan harapan dapat memberikan suatu pilihan yang tepat, selain sebagai suatu aplikasi yang memberikan layanan komunikasi pesan teks, tetapi juga dapat mengamankan pesan teks yang dikirimkan.

Dalam penelitian ini selain memanfaatkan algoritma Vigenere Cipher dalam proses enkripsi pesan SMS juga sekaligus menguji bagaimana algoritma Vigenere Cipher dapat melakukan proses dekripsi untuk dapat menghasilkan pesan teks semula (plainteks) dengan baik. Proses pengujian kunci juga dilakukan dalam penelitian ini, untuk mengetahui seberapa besar pengaruh kunci pada algoritma Vigenere Cipher bekerja, baik dari sisi keberhasilan proses dekripsi maupun sisi performa algoritma.

Sistem operasi Android digunakan dengan pertimbangan yaitu pada saat ini, sudah banyak vendor smartphone yang memproduksi berbasis android, hal ini terjadi karena android adalah sistem operasi yang *open source* sehingga bebas didistribusikan dan dipakai oleh vendor manapun. Android itu sendiri sangat lengkap baik dari segi sistem operasi, aplikasi dan tool pengembangan, market aplikasi serta dukungan yang sangat tinggi dari komunitas *open source* didunia [10].

II. METODE PENELITIAN

A. *Short Message Service (SMS)*

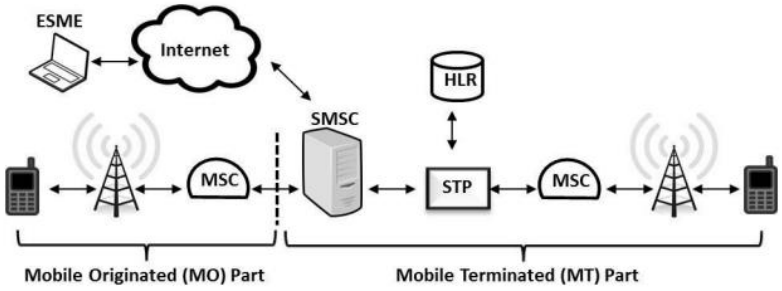
Short Message Service (SMS) adalah suatu fasilitas untuk mengirim dan menerima suatu pesan singkat berupa

E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 07, Nomor 03, September 2022 : 680–691

teks melalui perangkat nirkabel, dalam hal ini adalah telepon selular [11]. SMS memiliki kelebihan pada pengiriman data pesan, selain pada harganya yang murah, SMS akan mengantarkan data pesan pada tujuan yang dimungkinkan tidak aktif atau diluar service area, dalam kondisi ini penerima tetap dapat menerima pesan SMS jika telepon selular sudah aktif kembali.

Berikut ini skema cara kerja SMS:



Gambar. 1. Alur Kerja SMS [12]

Pesan SMS tidak secara langsung dikirimkan kepada telepon seluler yang dituju tetapi melewati serangkaian prosedur seperti yang terlihat pada Gambar 1. Pesan SMS akan dikirimkan kepada *Mobile Switching Center* (MSC) yang kemudian akan diteruskan pada SMSC yang berada pada kantor operator telepon. *Short Message Service Centre* (SMSC) akan memberikan indikasi respon positive (ACK) atau negative (NACK) yang menandakan pesan belum atau sudah disimpan. SMSC sendiri bertindak sebagai sistem yang berfungsi menyimpan dan mengirimkan kembali pesan-pesan jika kondisi penerima sedang tidak dalam kondisi aktif atau tidak dapat dijangkau. Dengan kata lain jaringan akan menjamin pengiriman SMS.

B. Keamanan SMS

Pada alur kerja SMS, dengan tersimpannya pesan pada SMSC (*Short Message Service Centre*) maka penyerang bisa mendapatkan pesan dengan melakukan penyusupan pada SMSC tersebut. Hal ini membuktikan bahwa jalur komunikasi SMS memerlukan sebuah teknologi enkripsi yang mampu menghalangi semua ancaman keamanan tersebut [13]. SMS bukan merupakan pilihan terbaik untuk komunikasi yang aman. Kebanyakan user tidak menyadari betapa mudahnya mencuri isi sebuah pesan. Spesifikasi dan teknologi mendasar dari SMS masih banyak terdapat celah keamanan yang menyebabkan SMS bukan merupakan jalur aman untuk pertukaran informasi. Dibutuhkan *channel* komunikasi yang aman yang mempertimbangkan solusi *encrypted end to end* pada perangkat dengan fitur keamanan sebagai fitur tambahan [14].

Berikut ini beberapa macam permasalahan yang terjadi pada SMS:

1) *SMS Spoofing*, merupakan sebuah pengiriman sms dimana nomor pengirim yang tertera bukanlah nomer pengirim yang sebenarnya.
2) *SMS Snooping*, hal ini lebih sering terjadi karena kesalahan pengguna telepon seluler. Contohnya ketika pemilik telepon seluler meminjamkan telepon tersebut kepada orang lain untuk menggunakan telepon miliknya dan baik disengaja atau tidak orang lain tersebut membuka data SMS yang masih tersimpan di dalam perangkat telepon seluler tersebut.
3) *SMS Interception*, merupakan suatu keadaan pencurian data pesan SMS ketika masih dalam transmisi dari pengirim ke penerima.

C. Kriptografi

Kriptografi merupakan ilmu dan seni untuk menjaga kerahasian pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Kriptografi bertujuan untuk memberi layanan keamanan (yang juga dinamakan sebagai aspek-aspek keamanan) sebagai berikut [15]:

1) *Kerahasiaan (confidentiality)*
   Adalah layanan yang ditujukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak-pihak yang tidak berhak.
2) *Integritas data (data integrity)*
   Adalah layanan yang menjamin bahwa pesan masih asli, utuh atau belum pernah dimanipulasi selama pengiriman.

E-ISSN : 2540 - 8984

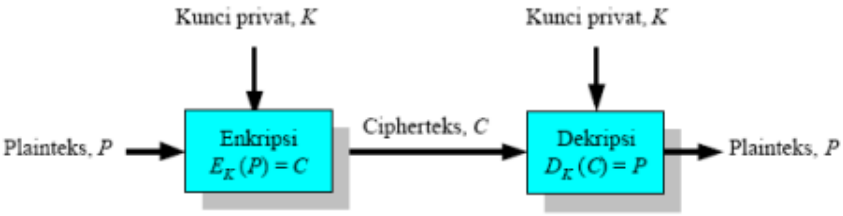
JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 07, Nomor 03, September 2022 : 680–691

3) *Otentikasi (authentication)*
Adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (user authentication atau entity authentication) maupun mengidentifikasi kebenaran sumber pesan (*data origin authentication*).

4) *Nirpenyangkalan (non-repudiation)*
Adalah layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan.

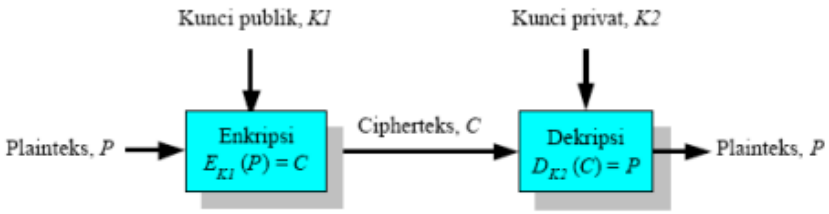
Kriptografi berdasarkan kunci yang digunakan untuk enkripsi dan dekripsi dibagi menjadi dua macam kriptografi, antara lain kriptografi kunci simetri dan kunci asimetri.

1) *Kriptografi Kunci Simetri*
Merupakan kriptografi dimana kunci yang digunakan untuk enkripsi maupun dekripsi merupakan kunci yang sama.



Gambar. 2. Skema Kriptografi Kunci Simetri [15]

2) *Kriptografi Kunci Asimetri*
Merupakan kriptografi dimana kunci yang digunakan untuk enkripsi berbeda dengan kunci yang digunakan untuk dekripsi.



Gambar. 3. Skema Kriptografi Kunci Asimetri [15]

D. *Algoritma Vigenere Cipher*

Sandi Vigenere merupakan bentuk sederhana dari sandi substitusi polialfabetik. Kelebihan sandi ini dibanding sandi Caesar dan sandi monoalfabetik lainnya adalah sandi ini tidak begitu rentan terhadap metode pemecahan sandi yang disebut analisis frekuensi. Setiap huruf teks terang digantikan dengan huruf lain yang memiliki perbedaan tertentu pada urutan alfabet [8].

Algoritma Vigenere Cipher menggunakan prinsip yang hampir sama dengan Caesar Cipher dengan menggunakan pergeseran karakter, yaitu suatu karakter plainteks menjadi karakter lain pada cipherteks, hanya saja algoritma ini lebih kuat dan aman dibandingkan Caesar Cipher, karena suatu karakter tidak dienkripsi menjadi huruf yang selalu sama.

Berikut contoh penggunaan algoritma Vigenere Cipher:
Pesan: HALO APA KABAR
Kunci: UINMALIKI

Untuk melakukan enkripsi dengan algoritma Vigenere Cipher, pada kunci dilakukan perulangan kaarakter jika karakter pada kunci kurang dari plainteks. Perulangan akan dilakukan hingga mencapai jumlah karakter plainteks.

Berikut contoh perulangan pada kunci:
Pesan: HALO APA KABAR
Kunci: UINM ALI KIUIN

E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 07, Nomor 03, September 2022 : 680–691

Enkripsi dilakukan dengan menggunakan sebuah tabel yang berbentuk matriks alfabet yang dinamakan bujur sangkar Vigenere atau tabel Vigenere. Perubahan atau pergeseran karakter untuk enkripsi sangat ditentukan oleh kunci yang digunakan.

Berikut ini hasil enkripsi dengan Vigenere Cipher:
Pesan: HALO APA KABAR
Kunci: UINMALIKI
Cipher: BIYA AAI UIVIE

Dapat dilihat pada hasil enkripsi 4 huruf A yang terdapat pada plainteks “HALO APA KABAR” dienkripsi menjadi 2 huruf yang berbeda pada cipherteks “BIYA AAI UIVIE “ menjadi huruf I dan A. Hal inilah yang menjadi kelebihan algoritma Vigenere Cipher dibandingkan algoritma terdahulunya Caesar Cipher. Dengan merujuk pada tabel vigenere dapat dilakukan perhitungan manual untuk proses enkripsi dekripsi dengan mengasumsikan karakter A-Z dengan 0-25.

	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. 4. Tabel Vigenere [8]

Berikut ini rumus enkripsi dekripsi algoritma Vigenere Cipher.
Enkripsi:

$$Ci = \text{Ek}(\text{Pi}) = (\text{Pi} + \text{Ki}) \bmod 26 \quad (1)$$

Dekripsi :

$$Pi = \text{Dk}(\text{Pi}) = (\text{Ci} - \text{Ki}) \bmod 26 \quad (2)$$

Keterangan :
Ci = karakter cipherteks
Pi = karakter plainteks
Ki = karakter kunci

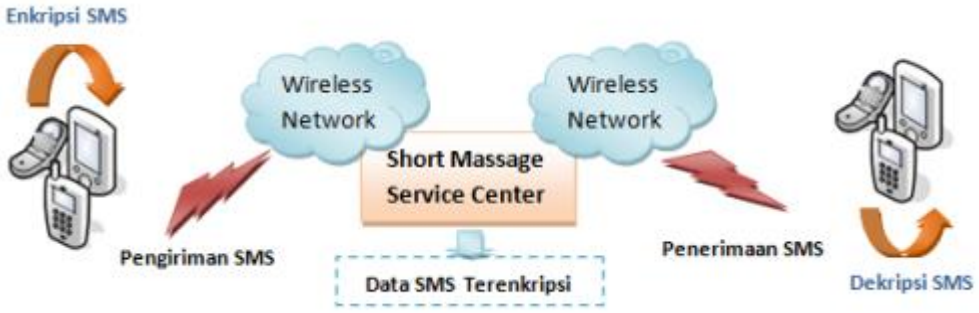
Mekanisme pada aplikasi *MyPriChat*, aplikasi enkripsi SMS berbasis Android, yaitu user pengirim dapat memanfaatkan aplikasi *MyPriChat* yang telah terinstal pada *mobile device* yang dimiliki untuk selanjutnya dilakukan pengenkripsian pada pesan teks sebelum dikirim. User pengirim pada proses enkripsi menggunakan kunci pengenkripsian yang sama dengan kunci pada user penerima. Kunci inilah yang menjadikan pesan teks tersebut *private* tidak dapat terbaca dengan baik selain user yang memiliki kunci, sekalipun orang lain dapat

E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 07, Nomor 03, September 2022 : 680–691

membaca tetapi hanya berupa cipherteks. Data teks terkirim oleh aplikasi memiliki besar yang sama dengan pesan teks asli, karena pada algoritma Vigenere Cipher hanya dilakukan penyandian perkarakter.

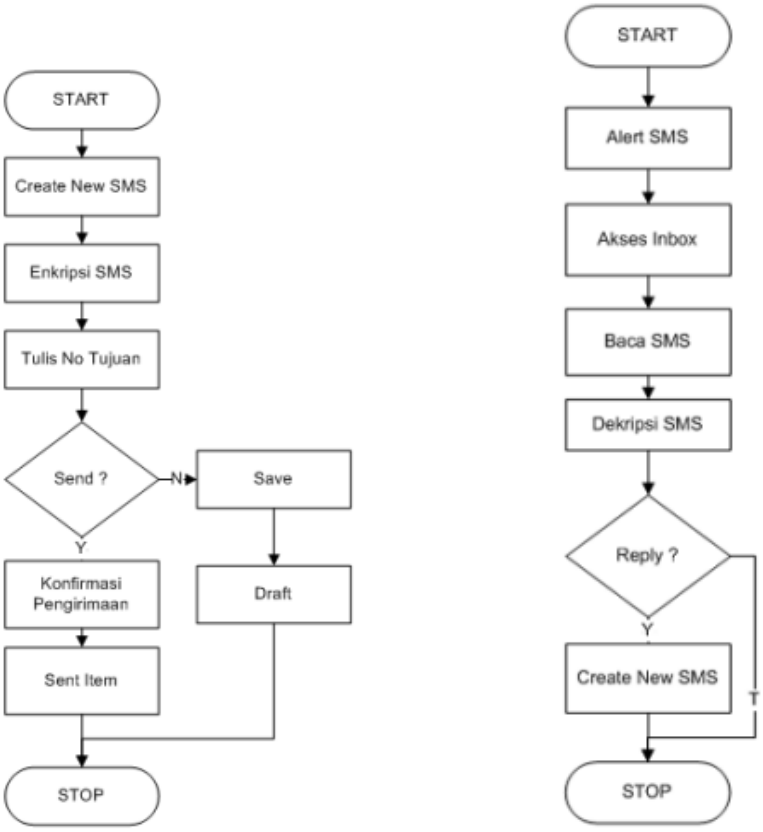
Pesan yang dikirim pada SMS Center akan diteruskan pada no tujuan dari penerima SMS. Berlaku hal yang sama, seorang user penerima juga harus telah menginstall aplikasi untuk dapat mendekripsi pesan yang dikirim oleh user pengirim.



Gambar. 5. Arsitektur *MyPriChat* Aplikasi Enkripsi SMS

E. Flowchart Sistem

Proses perancangan sistem aplikasi enkripsi SMS *MyPriChat* dikembangan dalam bentuk *flowchart* seperti pada Gambar 6 berikut ini. Sistem secara garis besar dibagi menjadi 2 bagian utama, yaitu proses pengiriman SMS dan proses penerimaan SMS.



(a) Flowchart Pengiriman SMS (a) Flowchart Penerimaan SMS

Gambar. 6. Fowchart Sistem Aplikasi Enkripsi SMS *MyPriChat*

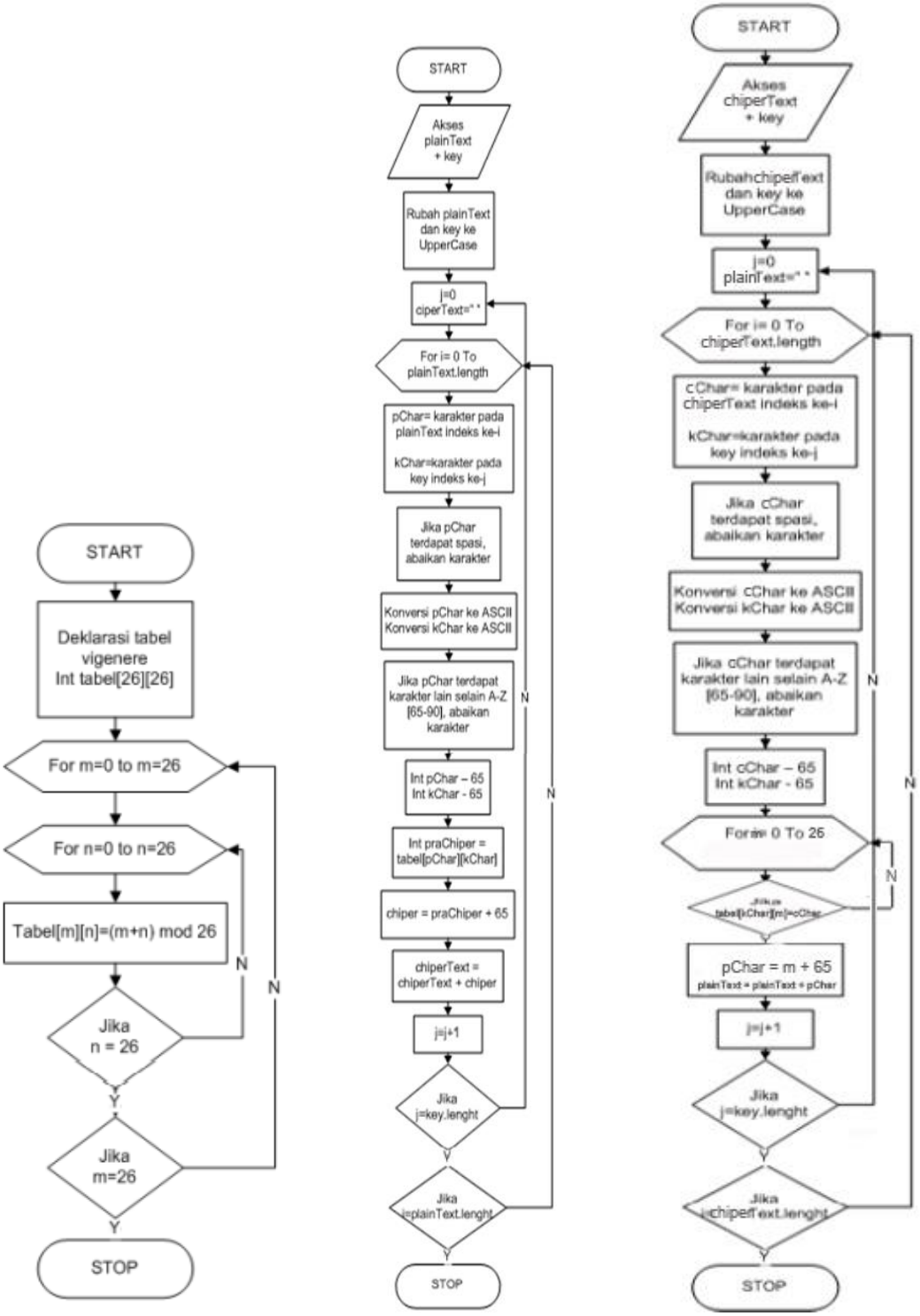
Pada proses penerimaan dan penerimaan SMS dapat diketahui bagaimana alur user mengimplementasikan penggunaan sistem enkripsi SMS *MyPriChat*, yaitu dari proses pembuatan SMS baru, enkripsi, hingga dekripsi pesan yang masuk. Untuk proses enkripsi pada pengiriman pesan dan dekripsi pada penerimaan pesan dilakukan dengan mengimplementasikan algoritma Vigenere Cipher.

E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 07, Nomor 03, September 2022 : 680–691

F. Flowchart Algoritma Vigenere Cipher

Dalam proses enkripsi dan dekripsi pesan, aplikasi *MyPriChat* menggunakan algoritma Vigenere Cipher. Algoritma Vigenere Cipher bekerja merujuk pada tabel Vigenere yang juga akan diimplementasikan pada sistem seperti pada Gambar 7(a). Tabel ini akan digunakan pada proses enkipsi Gambar 7(b) dan juga proses dekripsi Gambar 7(c). Berikut ini gambaran bagimana alur proses Algoritma Vigenere Cipher bekerja.



(a) Flowchart Penempatan Tabel Vigenere Cipher (b) Flowchart Proses Enkripsi (c) Flowchart Proses Dekripsi

Gambar. 7. Flowchart Algoritma Vigenere Cipher

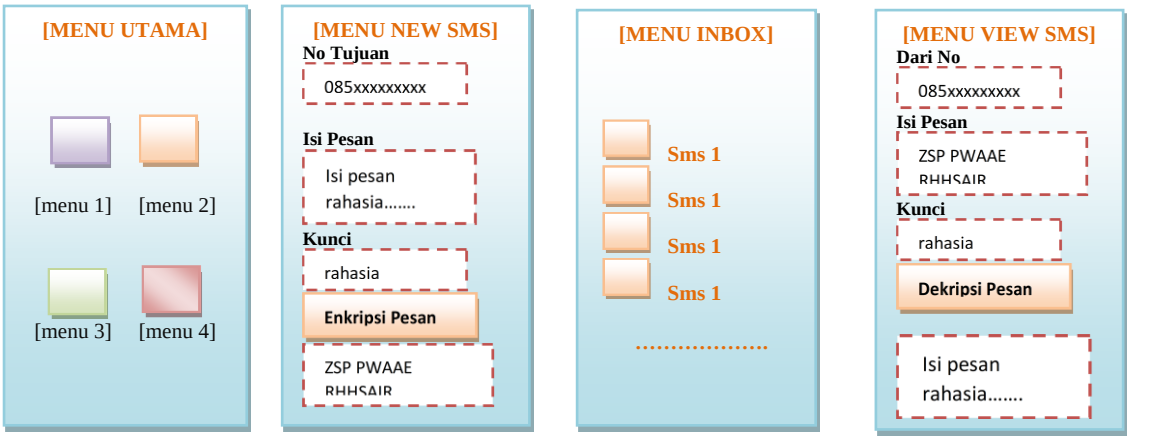
E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 07, Nomor 03, September 2022 : 680–691

G. Desain Interface

Pada tahap perancangan berikutnya adalah mendesain antarmuka untuk aplikasi enkripsi SMS *MyPriChat*. Perancangan antarmuka dilakukan untuk memberikan gambaran bagaimana tampilan sistem aplikasi *mobile* akan dibangun.

Berikut ini desain antarmuka dari apalikasi enkripsi SMS *MyPriChat*:



(a) Menu Utama (b) Menu SMS Baru dan Enkripsi (c) Menu Inbox (d) Menu View SMS dan Dekripsi

Gambar. 8. Desain Antar Muka Aplikasi Enkripsi SMS *MyPriChat*

III. HASIL DAN PEMBAHASAN

A. Implementasi Sistem

Pada tahap implementasi selanjutnya yaitu pengimplementasian beberapa fungsi penting seperti fungsi pengiriman dan penerimaan SMS.

```
<uses-permission android:name="android.permission.SEND_SMS" />
<uses-permission android:name="android.permission.READ_SMS" />
<uses-permission android:name="android.permission.WRITE_SMS" />
<uses-permission android:name="android.permission.RECEIVE_SMS" />
<uses-permission android:name="android.permission.READ_CONTACTS" />
```

Gambar. 9. Potongan Kode Pemrograman Java Perizinan Pengaksesan SMS Built in Pada Android

```
//initialisasi sms manager
SmsManager smsMan = SmsManager.getDefault();
//kirim pesan
smsMan.sendTextMessage(noHP, scAddress: null, isiChiper, sentIntent: null, deliveryIntent: null);
```

Gambar. 10. Potongan Kode Proses Pengiriman SMS Pada Pemrograman Java

B. Implementasi Algoritma Vigenere Cipher

Dalam implementasi algoritma Vigenere Cipher pada sistem digunakan *method* khusus yang menampung fungsi enkripsi maupun dekripsi. Aplikasi enkripsi SMS *MyPriChat* dibangun dengan batasan proses enkripsi dan dekripsi dilakukan sesuai dengan tabel vigenere yang ada. Pesan teks terlebih dahulu dikonversi kedalam bentuk ASCII dimana hanya mengenkripsi pesan teks yang terdiri dari huruf abjad A-Z (ASCII 65-90) dan mengabaikan enkripsi untuk karakter lain. Untuk mempermudah proses enkripsi dan dekripsi, pesan teks terlebih dahulu diubah ke dalam huruf kapital.

E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 07, Nomor 03, September 2022 : 680–691

```
private void enzryptPesan() {
    String noHPl = phoneNumber.getText().toString();
    String isiSmsl = smsBody.getText().toString();
    String isiKuncil = smsKunci.getText().toString();
    String isiChipertext= smsChiper.getText().toString();

    if (!noHPl.isEmpty() && !isiSmsl.isEmpty() && !isiKuncil.isEmpty()) {
        int tabel[][] = new int[26][26];
        for (int m = 0; m < 26; m++) {
            for (int n = 0; n < 26; n++) {
                tabel[m][n] = (m + n) % 26;
            }
        }
        isiSmsl = isiSmsl.toUpperCase();
        isiKuncil = isiKuncil.toUpperCase();
        int j = 0;
        for (int i = 0; i < isiSmsl.length(); i++) {
            char pChar = isiSmsl.charAt(i);
            char kChar = isiKuncil.charAt(j);
            if (pChar == ' ') {
                isiChipertext += pChar;
                continue;
            }
            int asciiP = (int) pChar;
            int asciiK = (int) kChar;
            if (asciiP < 65 || asciiP > 90) {
                isiChipertext += pChar;
                continue;
            }
            int piChar = asciiP - 65;
            int kiChar = asciiK - 65;
            int praChiper = tabel[piChar][kiChar];
            char chiper = (char) (praChiper + 65);
            isiChipertext += chiper;
            j++;
            if (j == isiKuncil.length()) {
                j = 0;
            }
        }
        smsChiper.setText(isiChipertext);
    }
}
```

(a) Potongan Kode Proses Enkripsi

```
private void decryptPesan() {
    String isiSms2 = msg.getText().toString();
    String isiKunci2 = kunciDekrip.getText().toString();
    String plainText= isiplainteks.getText().toString();

    int tabel[][] = new int[26][26];
    for (int m = 0; m < 26; m++) {
        for (int n = 0; n < 26; n++) {
            tabel[m][n] = (m + n) % 26;
        }
    }
    isiSms2 = isiSms2.toUpperCase();
    isiKunci2 = isiKunci2.toUpperCase();
    int j = 0;
    for (int i = 0; i < isiSms2.length(); i++) {
        char cChar = isiSms2.charAt(i);
        char kChar = isiKunci2.charAt(j);
        if (cChar == ' ') {
            plainText += cChar;
            continue;
        }
        int asciiC = (int) cChar;
        int asciiK = (int) kChar;
        if (asciiC < 65 || asciiC > 90) {
            plainText += cChar;
            continue;
        }
        int ciChar = asciiC - 65;
        int kiChar = asciiK - 65;
        for (int m = 0; m < 26; m++) {
            if (tabel[kiChar][m] == ciChar) {
                char pChar = (char) (m + 65);
                plainText += pChar;
            }
        }
        j++;
        if (j == isiKunci2.length()) {
            j = 0;
        }
    }
    isiplainteks.setText(plainText);
}
```

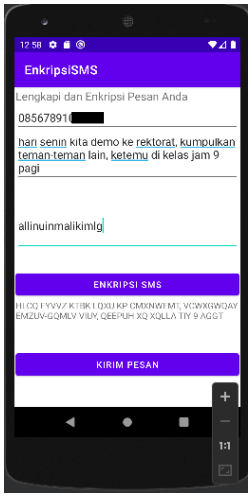
(b) Potongan Kode Proses Dekripsi

Gambar. 11. Potongan Kode Proses Implementasi Vigenere Cipher Pada Pemrograman Java

C. *Implementasi User Interface*

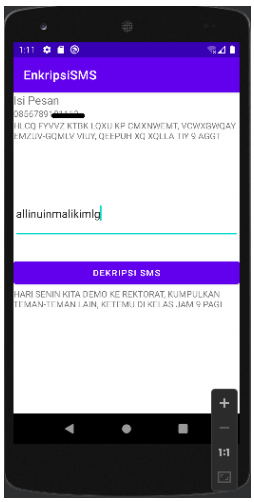
Berikut implementasi user interface dari aplikasi enkripsi SMS *MyPriChat.*

(a) Menu Utama



(b) Menu SMS Baru dan Enkripsi

(c) Menu Inbox



(d) Menu View SMS dan Dekripsi

Gambar 12. Implementasi *User Interface* Pada Sistem

D. *Pengujian dan Analisa Fungsionalitas Sistem*

Pengujian terhadap fungsionalitas sistem dilakukan dengan menguji beberapa fitur aplikasi terhadap kesesuaian input output agar sesuai dengan fungsi yang diharapkan. Pada pengujian proses enkripsi dan dekripsi dilakukan dengan menguji kesesuaian antara data asli, kunci, hasil enkripsi dan dekripsi dengan konsep algoritma Vigenere Cipher yang digunakan. Sedangkan pada pengujian performa akan dilakukan pengujian terhadap ketangguhan aplikasi terhadap algoritma yang diimplementasikan.

E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 07, Nomor 03, September 2022 : 680–691

Berikut ini spesifikasi perangkat mobile yang digunakan dalam pengujian aplikasi enkripsi SMS:

Tabel I.
Spesifikasi Perangkat Pengujian

No.	Kateori	Keterangan
1.	Jenis	Realme 3
2.	Perangkat Lunak	Android 9.0 Pie
3.	CPU	Octa-core (4x2.0 GHz Cortex-A73 & 4x2.0 GHz Cortex-A53)
4.	*Storage*	32GB
5.	RAM	3GB

Tabel II.
Pengujian Fungsionalitas Sistem

No.	Kateori Pengujian	Hasil yang Diharapkan	Kesimpulan Hasil
1.	Instalasi dan pengaksesan aplikasi	Aplikasi terinstal pada ponsel dan dapat di-jalankan dengan baik	Berhasil
2.	Akses menu utama	Menampilkan daftar menu aplikasi	Berhasil
3.	Akses menu Inbox	Menampilkan daftar pesan yang masuk	Berhasil
4.	Akses menu Sent	Menampilkan daftar pesan yang diterima	Berhasil
5.	Pengiriman pesan	Pesan terkirim pada penerima dengan baik	Berhasil
6.	Enkripsi pesan	Menghasilkan pesan cipherteks hasil enkripsi	Berhasil
7.	Penerimaan pesan	Dapat menerima pesan dari user penerima lain	Berhasil
8.	Dekripsi Pesan	Menghasilkan pesan plainteks seperti semula, sebelum dilakukan proses enkripsi	Berhasil

Dari hasil pengujian pada Tabel II dapat dianalisa dan disimpulkan bahwa aplikasi telah berjalan dengan baik. Masing-masing fitur telah memberikan respon atau keluaran yang sesuai dengan yang diharapkan. Baik dari segi aplikasi sebagai pemberi layanan komunikasi pengiriman dan penerimaan SMS, maupun dari segi pengamanan SMS itu sendiri, semua dapat dijalankan dengan baik.

E. Pengujian dan Analisa Kesesuaian Aplikasi Enkripsi SMS MyPriChat dengan Konsep Algoritma Vigenere Cipher

Tabel III.
Perbandingan Enkripsi Dekripsi Tabel Vigenere dengan Aplikasi Enkripsi SMS *MyPriChat*

No	Pesan	Kunci	Enkripsi		Keterangan
			Tabel Vigenere	Aplikasi Enkripsi SMS ***MyPriCat***	
1.	apa kabar	uinmalang	UXN WAMAE	UXN WAMAE	Sesuai
2.	teman-teman	uinmalang	NMZMN-EEZGH	NMZMN-EEZGH	Sesuai
3.	sangat rahasia	uinmalang	MIASAE RNNUAVM	MIASAE RNNUAVM	Sesuai
4.	eksperimen pesan	rahasia	VKZPWZIDEU PWAAE	VKZPWZIDEU PWAAE	Sesuai
5.	pesan penting	rahasia	GEZAF XEETPNY	GEZAF XEETPNY	Sesuai

Dengan melakukan pengujian enkripsi beberapa pesan pendek, seperti yang dapat dilihat pada Tabel III, dapat dianalisa bahwa aplikasi telah memberikan keluaran cipherteks yang sama dengan enkripsi yang dilakukan secara manual yang mengaju pada tabel vigenere. Maka dapat disimpulkan aplikasi enkripsi SMS dengan implementasi algoritma Vigenere Cipher yang telah dibangun dapat berjalan dengan baik.

F. Pengujian dan Analisa Proses Enkripsi dan Dekripsi Pesan

Dari hasil pengujian terhadap proses enkripsi dan dekripsi yang terdapat pada sistem, dapat dianalisa dan disimpulkan bahwa:

1. Ukuran penggunaan kunci tidak berpengaruh terhadap keberhasilan atau kegagalan generate cipherteks maupun plainteks. Baik kunci dengan ukuran karakter yang sama dengan plainteks (plainteks 17, kunci 17), kunci dengan ukuran lebih pendek dari plainteks (plainteks 70, kunci 17), maupun kunci dengan ukuran lebih panjang dari plainteks (plainteks 17, kunci 70). Ketiga kondisi tersebut memberikan keberhasilan dalam proses enkripsi maupun dekripsi. Hal ini sesuai dengan konsep perancangan

E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 07, Nomor 03, September 2022 : 680–691

pengimplementasian algoritma dimana digunakan perulangan karakter jika jumlah karakter kunci yang digunakan kurang dari plainteks.

2. Banyaknya jumlah karakter yang terdapat pada cipherteks akan selalu sama dengan jumlah karakter yang terdapat pada plainteks. Hal ini sesuai dengan konsep algoritma Vigenere Cipher dimana setiap karakter akan dienkripsi menjadi satu karakter lain sesuai tabel vigenere.
3. Hasil dekripsi memberikan pesan yang sama seperti terdapat pada pesan plainteks.

Tabel VI.
Pengujian Enkripsi dan Dekripsi Pesan

No	Plainteks		Kunci		Cipherteks		Hasil Dekripsi	Keterangan
	Teks	∑ Char	Teks	∑ Char	Teks	∑ Char		
1.	Tim B kumpul di markas	17	allinuinmalikimlg	17	TTX J XOUCGL OQ WIDVGS	17	TIM B KUMPUL DI MARKAS	Berhasil
2.	Tim B kumpul di markas	17	inikuncisangat rahasiajangansampai adapihaklainyangtahu sikatjikaadamusuh	70	BVU L EHOXML QO MTIKHS	17	TIM B KUMPUL DI MARKAS	Berhasil
3.	Hari senin kita demo ke rektorat, kumpulkan te-man-teman lain, ketemu di kelas jam 9 pagi	70	inikuncisangat rahasiajangansampai adapihaklainyangtahu sikatjikaadamusuh	70	PNZS MRPQF KVZA WVMV KW ZETTBXAG, CUYEUTKDN IMTAX-EEUNL LNOG, KLNWUE DB TMVAS MAY 9 JSAP	70	HARI SENIN KITA DEMO KE REKTORAT, KUMPULKAN TEMAN-TEMAN LAIN, KETEMU DI KELAS JAM 9 PAGI	Berhasil
4.	Hari senin kita demo ke rektorat, kumpulkan te-man-teman lain, ketemu di kelas jam 9 pagi	70	allinuinmalikimlg	17	HLCQ FYVVZ KTBK LQXU KP CMXNWEMT, VCWXGWQAY EMZUV-GQMLV VIUY, QEEPUH XQ XQLLA TIY 9 AGGT		HARI SENIN KITA DEMO KE REKTORAT, KUMPULKAN TEMAN-TEMAN LAIN, KETEMU DI KELAS JAM 9 PAGI	Berhasil

G. Pengujian Performa Aplikasi Terhadap Implementasi Vigenere Cipher

Tabel V.
Pengujian Performa Aplikasi

No	Jumlah Karakter Plainteks	Jumlah Karakter Kunci	Waktu Enkripsi	Waktu Dekripsi	Keterangan
1.	50	20	1,14 detik	1,21 detik	Berhasil
2.	50	50	1,28 detik	1,33 detik	Berhasil
3.	50	100	1,34 detik	1,28 detik	Berhasil
4.	100	20	2,02 detik	2,13 detik	Berhasil
5.	100	50	2,06 detik	2,00 detik	Berhasil
6.	100	100	2,09 detik	2,07 detik	Berhasil
7.	150	20	2,17 detik	2,23 detik	Berhasil
8.	150	50	2,18 detik	2,16 detik	Berhasil
9.	150	100	2,16 detik	2,24 detik	Berhasil

Dari hasil pengujian pada Tabel V dapat dianalisa dan disimpulkan bahwa:

1. Jumlah karakter pesan (plainteks) akan sangat mempengaruhi waktu dari proses enkripsi maupun dekripsi. Pada tabel pengujian, variasi jumlah karakter pesan (50, 100, dan 150) memiliki waktu eksekusi enkripsi dan dekripsi yang cenderung berbeda. Semakin banyak karakter pesan yang harus di-*generate*, memori yang dibutuhkan semakin besar untuk proses perhitungan atau eksekusi.
2. Jumlah karakter kunci tidak mempengaruhi waktu dari proses enkripsi maupun dekripsi. Pada penggunaan kunci dengan jumlah tertentu tidak mempengaruhi waktu eksekusi enkripsi maupun dekripsi. Seperti telah disinggung sebelumnya, hal ini disebabkan karena konsep perulangan karakter pada kunci. Dapat dikatakan aplikasi secara otomatis mengatur karakter kunci agar sama dengan jumlah karakter plainteks.
3. Dengan pesan berjumlah 150 karakter, aplikasi masih dapat melakukan proses enkripsi dan dekripsi dengan baik.

E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 07, Nomor 03, September 2022 : 680–691

IV. KESIMPULAN

Berdasarkan pada pengujian aplikasi enkripsi SMS *MyPriChat* dengan mengimplementasikan algoritma Vigenere Cipher dapat berjalan pada emulator maupun telepon seluler dengan baik. Aplikasi enkripsi SMS dapat dimanfaatkan dengan melakukan penginstalan aplikasi baik pada telepon seluler user pengirim maupun user penerima.

Aplikasi enkripsi SMS selain memberikan layanan komunikasi SMS, juga dapat mengamankan informasi pesan yang dikirimkan. Algoritma Vigenere Cipher yang diimplementasikan pada sistem berjalan dengan baik sesuai acuan dari tabel vigenere.Aplikasi enkripsi SMS secara otomatis akan mengenkripsi dan mendekripsi pesan sesuai dengan kunci yang dimasukkan oleh user. Aplikasi juga secara otomatis melakukan pengulangan karakter kunci jika jumlah karakter kunci kurang dari jumlah karakter pesan.

Dapat disimpulkan jumlah kunci yang diinputkan user tidak mempengaruhi kegagalan atau keberhasilan proses enkripsi. Hanya saja dimungkinkan dalam sisi keamanan cipherteks akan lebih rentan dilakukan kriptanalisis.

Proses enkripsi dengan algoritma Vigenere Cipher menghasilkan jumlah karakter yang sama dengan jumlah karakter awal. Jumlah karakter pesan sangat mempengaruhi waktu eksekusi enkripsi maupun dekripsi. Semakin banyak pesan yang dienkripsi atau didekripsi maka waktu yang dibutuhkan juga akan lebih lama. Hal ini akan sangat dipengaruhi memori dari telepon seluler yang digunakan.

Dengan otomatisasi pengulangan kunci pada aplikasi, maka jumlah karakter kunci akan disamakan dengan karakter plainteks. Sehingga dapat disimpulkan bahwa banyaknya jumlah karakter kunci tidak berpengaruh pada waktu eksekusi enkripsi maupun dekripsi.

DAFTAR PUSTAKA

[1] Doffman Zak, “https://www.forbes.com/sites/zakdoffman/2020/08/30/google-android-messages-apple-iphone-ipad-imessage-security-update-sms-rcs-whatsapp-encryption/?sh=560da4293ff4,” Aug. 30, 2020.

[2] R. Rihartanto, R. K. Ningsih, A. F. O. Gaffar, and D. S. B. Utomo, “Implementation of vigenere cipher 128 and square rotation in securing text messages,” *Jurnal Teknologi dan Sistem Komputer*, vol. 8, no. 3, pp. 201–209, Jul. 2020, doi: 10.14710/jtsiskom.2020.13476.

[3] Hasugian Buyung S, “PERANAN KRIPTOGRAFI SEBAGAI KEAMANAN SISTEM INFORMASI PADA USAHA KECIL DAN MENENGAH,” *Jurnal Warta*, vol. 53, Jul. 2017.

[4] Jones Nick, “Why Use Secure Sms,” *Gartner Research*, 2002.

[5] B. Firmanto, D. Putri, K. Ningrum, A. Bramanto, and W. Putra, “Perbandingan Hasil Performa Optimasi Transposisi Hill Cipher dan Vigenere Cipher pada Citra Digital,” *SMARTICS Journal*, vol. 7, no. 2, pp. 65–71, 2021, doi: 10.21067/smartics.v7i2.5931.

[6] Pratama Guruh M and Tamatjita E.Nurmiyati, “MODIFIKASI ALGORITMA VIGENERE CIPHER MENGGUNAKAN METODE CATALAN NUMBER DAN DOUBLE COLUMNAR TRANSPOSITION,” *Jurnal On Line Institut Teknologi Dirgantara Adisutjipto*, vol. 4, no. 1, May 2015.

[7] A. Amrulloh and E. Ujianto, “Kriptografi Simetris Menggunakan Algoritma Vigenere Cipher,” *Jurnal CoreIT*, vol. 5, no. 2, 2019, [Online]. Available: https://program.arfianhidayat.com/kriptografi/vig

[8] N. Laila and A. S. Rms, “IMPLEMENTASI STEGANOGRAFI LSB DENGAN ENKRIPSI VIGENERE CIPHER PADA CITRA Implementation of LSB Steganography with Vigenere Cipher Encryption in Image,” *Computer Science Informatics Journal*, vol. 1, no. 2, 2018.

[9] D. Abdullah, “School of Informatics Management and Computing , STMIK Jayakarta PENGAMANAN EMAIL MENGGUNAKAN METODE VIGENERE CIPHER,” *JISAMAR (Journal of Information System, Applied, Management, Accounting and Research*, pp. 2598–8700, 2017, [Online]. Available: http://journal.stmikjayakarta.ac.id/index.php/jisamar

[10] M. Syaifullah, “COMPUTER REMOTE APPLICATIONS BASED ON ANDROID USING WIFI WITH MULTI-TOUCH,” Surabaya, Jul. 2015.

[11] T. S. S. N. Setiawan A, “16481-Article Text-16479-1-10-20080815,” *Jurnal Informatika*, vol. 7, no. 1, 2006, doi: 10.9744/informatika.7.1.pp. 17-23.

[12] O. Osho, O. Y. Ogunleke, and A. A. Falaye, “Frameworks for mitigating identity theft and spamming through bulk messaging,” in *IEEE International Conference on Adaptive Science and Technology, ICAST*, Mar. 2015, vol. 2015-January. doi: 10.1109/ICASTECH.2014.7068119.

[13] Lestari Mei, “Sistem keamanan SMS dengan Metode Vigenere Cipher Berbasis J2ME,” *Jurnal TELEMATIKA MKOM*, vol. 6, no. 2, Sep. 2014.

[14] Prihatini Ekawati, “ASPEK KEAMANAN PADA JALUR KOMUNIKASI SHORT MESSAGE SERVICE Case : SMS SPOOFING,” 2006.

[15] Munir Rinaldi, *Kriptografi*. Bandung: Informatika, 2007.