Penerapan Kriptografi Pada Teks Pesan dengan Menggunakan Metode *Vigenere Cipher* Berbasis Android

Angga Aditya Permana[1]

[1]Teknik Informatika, FakultasTeknik, Universitas Muhammadiyah Tangerang
Jl. Perintis Kemerdekaan I No.33, Babakan, Kec. Tangerang, Kota Tangerang, Banten 15118

Penulis untuk Korespondensio/E-mail: anggaumt@gmail.com

Abstrak - **Perkembangan teknologi khususnya dalam bidang komunikasi antar manusia sudah sangat mudah dilakukan dengan telepon genggam dan fiturnya sangat bervariasi. Pertukaran informasi jarak jauh ini menuntut keamanan terhadap kerahasiaan informasi yang dipertukarkan. Oleh karena itu, metode kriptografi dilakukan untuk mengamankan informasi tersebut. Salah satu metode kriptografi untuk penyandian teks adalah metode *Vigenere Cipher*. Penelitian ini bertujuan untuk membangun aplikasi kriptografi teks pesan pada *smartphone* berbasis android dengan metode *Vigenere Cipher*. Metode ini mengenkripsi teks pesan menjadi pesan rahasia yang kemudian hasilnya diteruskan sebagai teks pesan ke aplikasi pengiriman pesan seperti aplikasi SMS (*Short Message Service)*, Whatsapp, Line, dan sejenisnya untuk selanjutnya didekripsi. Penelitian ini menghasilkan aplikasi berbasis android yang dapat mengirimkan teks pesan terenkripsi menggunakan metode *Vigenere Cipher* untuk memberikan keamanan lebih pada proses pertukaran informasi.**

Kata Kunci – *Cryptography, Vigenere Cipher, Android.*

Abstract – **Mobile phones and its various features allow humans to communicate in this technology development era. The information secrecy especially during long range information exchange is very noteworthy. So that, those information can be protected by cryptography method. *Vigenere Cipher* is one of cryptography method for text encoding. The aim of this study is to construct application of text message cryptography on android Smartphone using *Vigenere Cipher* method. This method encrypted text message into secret message then forwarded this information to other applications like SMS (Short Message Service), Whatsapp, Line and so on then being decrypted. Android based application was resulted which allow to send encrypted text message using *Vigenere Cipher* to provide more security in the process of information exchange.**

Keywords *- Cryptography, Vigenere Cipher, Android.*

PENDAHULUAN

Berkomunikasi adalah salah satu kegiatan dasar dalam kehidupan manusia, yang memungkinkan manusia dapat bertukar informasi dengan manusia lainnya. Informasi-informasi tersebut dapat di olah menjadi informasi baru yang berguna bagi manusia itu sendiri dan orang lain. Pada masa sekarang ini manusia sudah menemukan banyak alat yang dapat digunakan untuk berkomunikasi satu sama lain tanpa mengkhawatirkan jarak yang memisahkan, seperti surat, SMS (*Short Message Service*), telepon, dan sejenisnya. Kehidupan manusia sekarang ini sudah sangat dimudahkan oleh alat-alat tersebut, namun bukan berarti hal tersebut tidak memiliki kekurangan. Informasi pada alat-alat komunikasi tersebut dapat dengan mudah dilihat oleh orang lain, baik penyedia layanan atau orang-orang yang berniat mendapatkan informasi untuk keperluan mereka sendiri atau biasa disebut *hacker*.

Hal tersebut dapat dihindari dengan merahasiakan pesan atau informasi yang hanya dapat dimengerti oleh orang-orang tertentu. Ilmu tersebut dikenal dengan nama Kriptografi (*Cryptography*). Pada zaman *Romawi* era raja Julius Caesar, kriptografi digunakan untuk

keperluan berperang. Kriptografi sudah banyak digunakan oleh banyak bidang khususnya dalam bidang informatika, seperti membuat penyandian pada teks *password* yang digunakan pengguna untuk *login* ke dalam sistem berbasis digital agar tidak dapat dimengerti oleh orang yang tidak berkepentingan.

Kriptografi memiliki dua konsep yang penting, yaitu enkripsi dan dekripsi. Enkripsi mengubah informasi atau data menjadi bentuk yang hampir tidak dikenali seperti informasi awal menggunakan algoritma tertentu, sedangkan dekripsi mengubah bentuk tersamar tersebut menjadi informasi awal. Salah satu metode yang dapat dilakukan adalah metode *Vigenere Cipher*. Metode *Vigenere Cipher* menyembunyikan pesan berupa teks melalui teknik substitusi dengan mengubah setiap huruf menjadi huruf lain berdasarkan kunci yang digunakan. Metode ini dapat mengubah pesan menggunakan kombinasi 26 huruf alfabet dan memerlukan waktu cukup lama untuk memecahkan algoritma tersebut, sehingga keamanan pesan dapat terjaga.

TINJAUAN PUSTAKA

Kriptografi

Kriptografi adalah bidang ilmu yang mempelajari tentang cara untuk menjaga keamanan pesan dalam proses pengiriman dengan menggunakan metode penyandian tertentu, dengan tujuan agar informasi dalam pesan tersebut tidak disalahgunakan oleh orang yang bukan penerima aslinya. Kriptografi memiliki beragam metode untuk menyandikan pesan atau informasi yang ingin kita sembunyikan, seperti *Caesar Cipher*, *Affine*, *Monoalphabetic*, *Polyalphabetic*, *Vigenere*, Transposisi, dan banyak lagi metode-metode dalam kriptografi ini (Nurnawati, 2008) [1].

Vigenere Cipher

Vigenere Cipher adalah salah satu metode penyandian dalam kriptografi. Metode *Vigenere* melakukan penyandian dengan menggunakan tabel diagram dengan huruf alfabet yang terurut secara diagonal (Gambar 1). Setelah itu kita akan menaruh satu-satu huruf dari *plain text* di bagian atas dan *key* pada bagian kiri. Lalu mencari titik temu antara huruf tersebut dan mendapatkan *chiper text* yang di inginkan, begitu seterusnya sampai *plain text* terakhir. Jika jumlah *key* tidak mencukupi maka mulai dari huruf pertama lagi (Subimawanto, 2014) [2].

Android

Android adalah sistem operasi (*Operating System*) yang umumnya digunakan pada perangkat dengan navigasi *full touch screen* yang biasa dimiliki oleh *smartphone* dan komputer tablet. Android sudah diambil alih oleh perusahaan *Google Inc* yang telah membelinya pada tahun 2005 dari *Android Inc*. Google menyediakan *software/tools* yang dikembangkan khusus untuk dijadikan alat pengembang aplikasi android yang diberi nama "*Android Studio*". *Android Studio* dikembangkan dengan menggunakan bahasa *Java* dengan menambahkan *library-library* khusus yang diperuntukan untuk membuat aplikasi android. *Android studio* menggunakan metode *native code* yang memisahkan antara *view* dan *controller* (Permana, 2016) [3].

	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
W	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 1. Tabel *Vigenere*

METODE PENELITIAN

Gambaran Umum Sistem

Aplikasi kriptografiyang dibangun akan diterapkan pada *smartphone* berbasis android. Teks pesan dapat dienkripsi menggunakan metode *Vigenere Cipher* menjadi pesan rahasia yang sulit untuk dipahami oleh manusia menggunakan *IDE Android Studio* yang dapat mengenkripsi sebuah pesan dan meneruskan hasilnya sebagai teks pesan ke aplikasi pengiriman pesan seperti aplikasi SMS, Whatsapp, Line, dan sejenisnya.

Rumus yang Digunakan

Vigenere Cipher adalah metode yang menggukan tabel *vigenere* untuk mengenkripsi sebuah teks. Akan tetapi di dalam sebuah sistem berbasis digital tidak memungkinkan menjadikan sebuah tabel sebagai referensi untuk memproses program. Proses enkripsi dilakukan menggunakan rumus aritmatika sebagai berikut:

$$C_i = (P_i + K_i) - 26 \quad (1)$$

Atau bisa juga dengan:

$$P_i = (C_i - K_i) mod(26) \quad (2)$$

P adalah variabel yang mendefinisikan *plain text. K* digunakan untuk mendefinisikan kunci *(Key). C* adalah variabel dari *chiper text*. Huruf *i* adalah variabel indeks yang mendefinisikan alamat lokasi dari setiap huruf dalam satu kalimat pesan.

Rumus dibawah ini digunakan untuk dekripsi:

$$P_i = (C_i - K_i) Mod(26) \quad (3)$$

Atau bisa juga dengan:

$$P_i = (C_i - K_i), +26 \; jika \; hasil \; minus \quad (4)$$

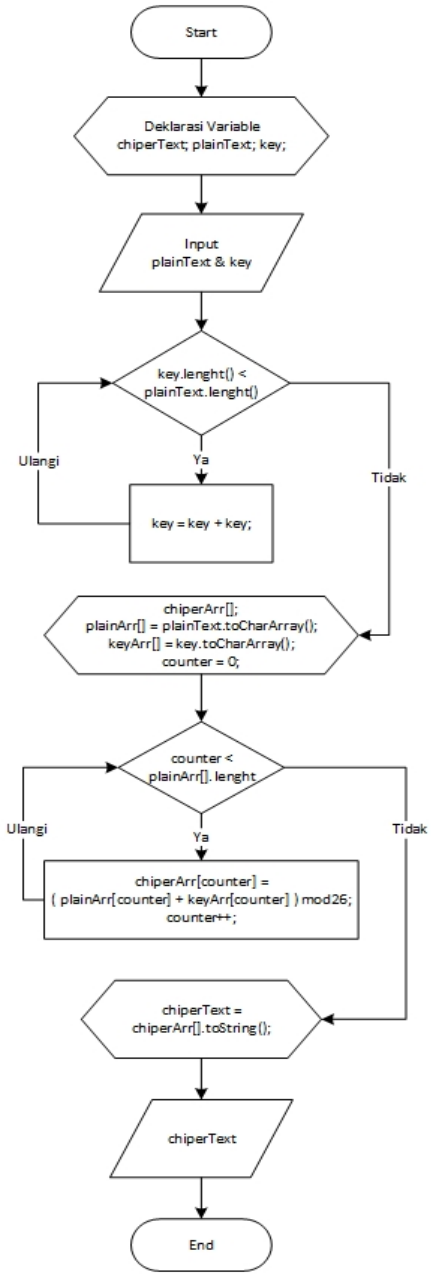
Penjelasan rumus dekripsi tidak jauh beda dengan rumus enkripsi. Mereka hanya memiliki perbedaan yang tidak terlalu banyak. Hasil dari "*C - K*" ditambahkan 26 jika hasilnya minus.

Alur Program

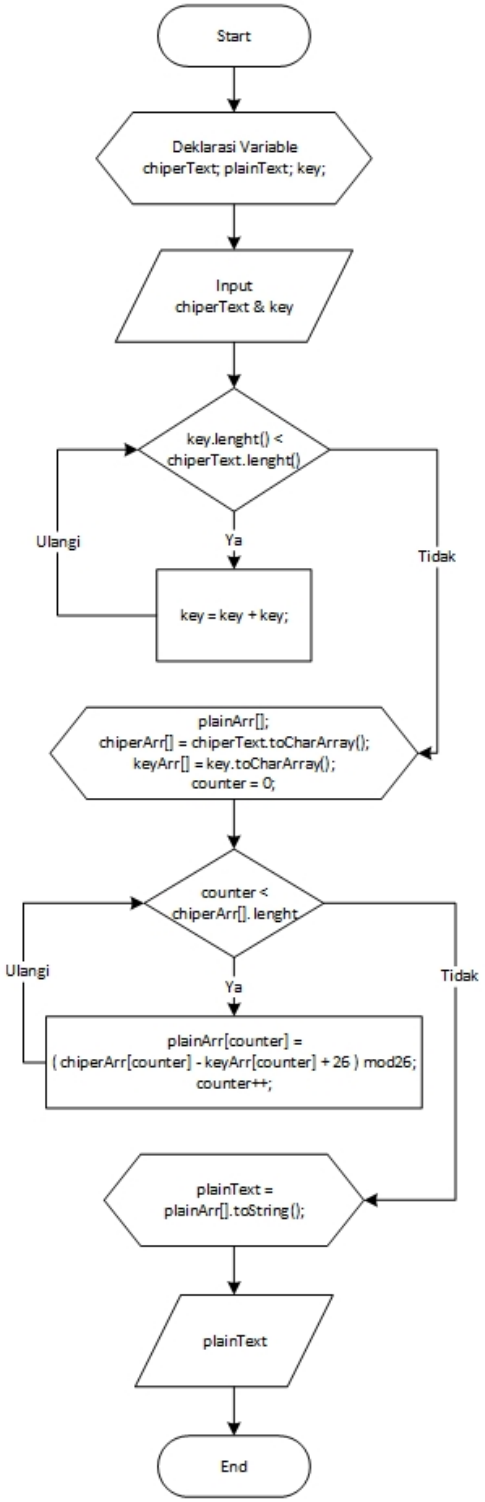
Gambar 2 menggambarkan algoritma dari kriptografi *Vigenere Cipher* pada proses enkripsi. Enkripsi dimulai dari mendeklarasi variabel, memasukan *plain text* dan *key* sampai akhirnya *plain text* tersebut terenkripsi dengan algoritma *Vigenere Cipher* dan menjadi *chiper text* yang diterapkan pada aplikasi android dengan bahasa Java. Gambar 3 adalah diagram yang menggambarkan proses dekripsi pada aplikasi kriptografi yang dibuat, dimulai dari mendeklarasi variabel, memasukan *chiper text* dan *key* sampai akhirnya *chiper text* tersebut menjadi *plain text* kembali dan selesai.

Pengujian Sistem

Pengujian dilakukan menggunakan *black box* yang merupakan pengujian dengan mengamati hasil eksekusi melalui data uji dan memeriksa fungsional dari perangkat lunak. *Black box* dapat menunjukkan fungsi perangkat lunak tentang cara pengoperasian serta pemantauan proses pemasukan dan pengeluaran data telah berjalan sebagaimana mestinya. *Black Box* memiliki kelebihan dapat memilih *subset test* secara efektif dan efesien, dapat menemukan cacat dan dapat membantu memaksimalkan testing *investment.* Selain itu *black box* juga memiliki kekurangan yaitu masih terdapat kemungkinan beberapa jalur eksekusi yang belum pernah diuji oleh *tester.*



Gambar 2. *Flowchart* Enkripsi

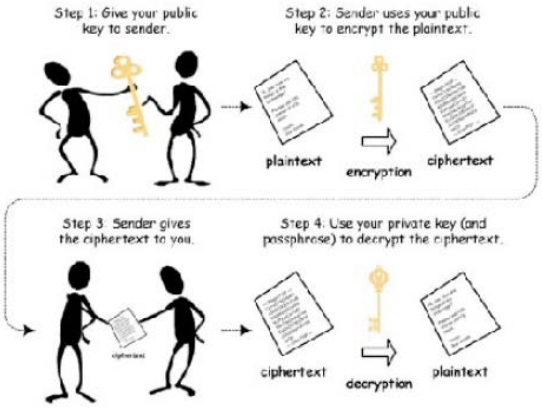


Gambar 3. *Flowchart* Dekripsi

HASIL DAN PEMBAHASAN

Perancangan Sistem Aplikasi Kriptografi

Sistem ini dirancang sedemikian rupa, sehingga pengirim pesan dapat mengenkripsi pesan (*plain text*) yang akan dikirim melalui aplikasi. Pesan yang akan dikirim akan diterima oleh penerima pesan dalam keadaan terenkripsi (*chiper text*), sehingga penerima pesan harus melakukan deksripsi pada pesan tersebut dengan bertukar kunci (*key*) untuk mengubah *chiper text* menjadi *plain text* awal. Sistem berhasil dirancang dengan skema di bawah ini (Gambar 4) [4]. Sistem kriptografi teks pesan pada penelitian ini merupakan salah satu teknik yang dilakukan untuk menjaga keamanan pesan. Proses enkripsi dan dekripsi metode *Vigenere Cipher* ini dilakukan dengan mengubah isi pesan yang akan dikirim [5].



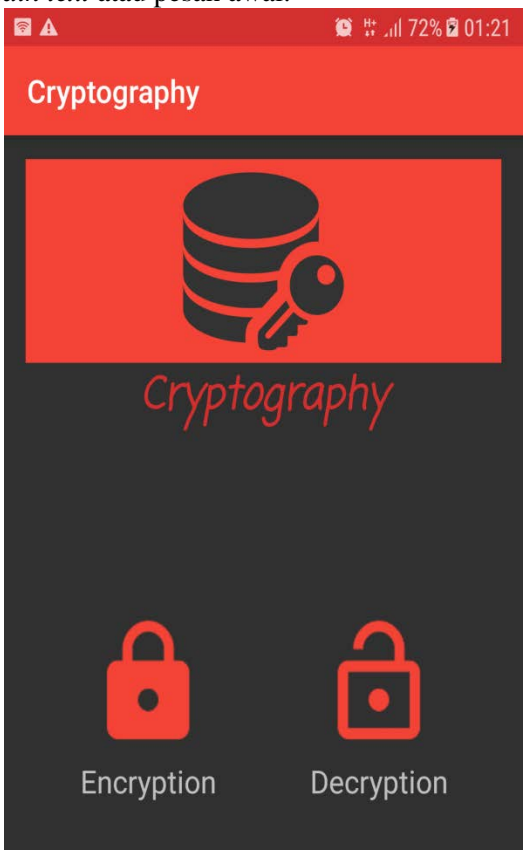
Sumber: Anjari, 2012

Gambar 4. Perancangan Sistem

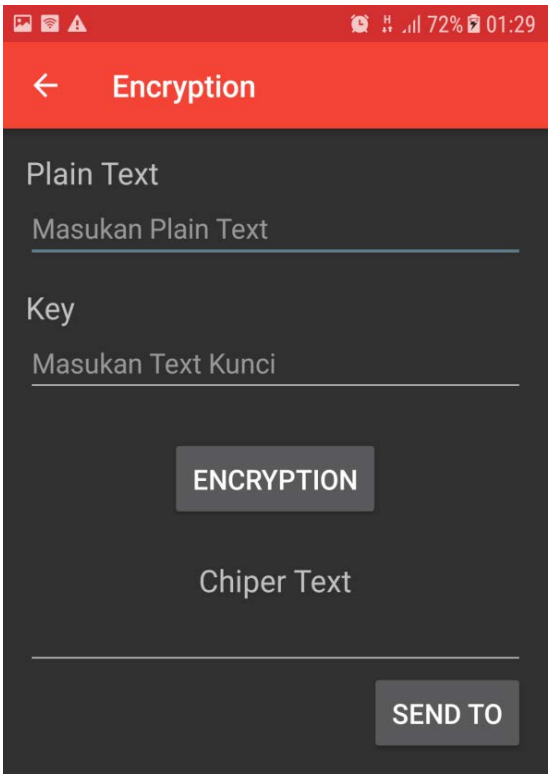
Implementasi Sistem Aplikasi Kriptografi

Implementasi sistem aplikasi kriptografi dapat dilihat dari tampilan *user interface* yang terdiri dari halaman depan (*main menu*) serta 2 fitur utama yaitu enkripsi dan dekripsi. Gambar 5 merupakan halaman pembuka awal dari aplikasi kriptografi yang akan tampil saat pertama kali membuka aplikasi ini. Halaman depan ini berisi nama aplikasi yang dibuat, logo aplikasi dan menu yang ada pada aplikasi, yaitu enkripsi atau dekripsi. Gambar 6 merupakan halaman enkripsi pesan yang akan tampil setelah memilih menu *Encryption* yang terdiri dari *plain text* yang harus diisi dengan teks yang akan dienkripsi oleh pengirim pesan, *key* atau kunci rahasia dan tombol *encryption* untuk mengubah *plain text* menjadi *chiper text* atau pesan rahasia. Gambar 7 merupakan halaman dekripsi pesan yang akan tampil setelah memilih menu *Decryption* yang terdiri dari *chiper text* yang harus diisi dengan teks terenkripsi yang sudah diterima oleh penerima pesan, *key* atau kunci rahasia dan tombol

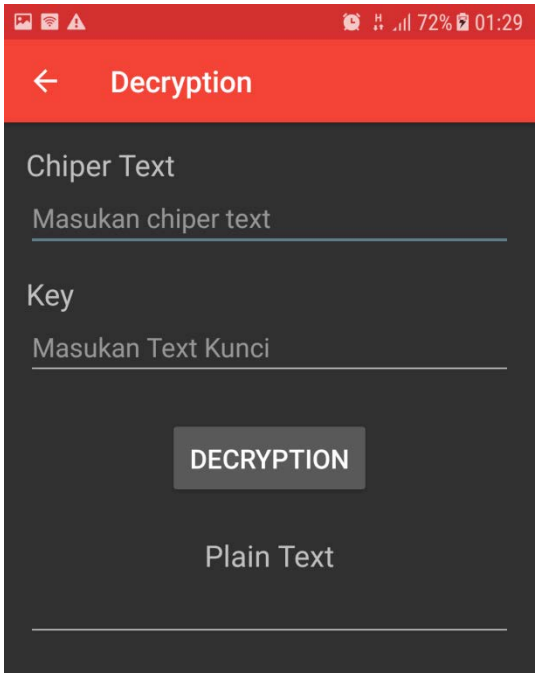
decryption untuk mengubah *chiper text* menjadi *plain text* atau pesan awal.



Gambar 5. *User Interface* Menu Utama.



Gambar 6. *User Interface* Enkripsi.



Gambar 7. *User Interface* Dekripsi.

Pengujian Sistem Aplikasi Kriptografi

Hasil pengujian sistem aplikasi kriptografi yang dilakukan dengan pengujian *blackbox* dapat dilihat pada Tabel 1. Skenario yang diujikan adalah dengan mengosongkan kolom kunci dan memasukkan kunci yang berbeda pada saat enkripsi dan dekripsi. Hasil yang diharapkan apabila kolom kunci dikosongkan adalah sistem akan menolak dan muncul "Isi juga *key* nya!", sedangkan apabila kunci yang dimasukkan berbeda, hasilnya *plain text* tidak sesuai dengan *plain text* asli dan kedua hasilnya valid.

Tabel 1. Hasil Pengujian *Black Box*.

No	Skenario Pengujian	Test Case	Hasil yang diharapkan	Hasil Pengujian	Kesimpulan
1	Mengosongkan Kolom Kunci		Sistem akan menolak dan muncul "Isi Juga key nya !"		Valid
2	Mencoba memasukan key yang berbeda pada saat enkripsi dan dekripsi		Plain text tidak sesuai dengan plain text asli		Valid

KESIMPULAN

Proses enkripsi dan dekripsi teks pesan pada aplikasi kriptografi berhasil dilakukan, sehingga dapat diasumsikan metode *Vigenere Cipher* dapat diterapkan pada aplikasi ini dengan *smartphone* berbasis android.

DAFTAR PUSTAKA

[1] E.K. Nurnawati. Analisis Kriptografi menggunakan algoritm avigenere cipher dengan mode operasi *cipher block chaining* (CBC). Prosiding Seminar Nasional Aplikasi Sains dan Teknologi. 1. 266, 2008.

[2] D. Subimawanto, F. Ihsani, J. Hindharta, M.C. Kamu, M. Rendianto, V.A. Pratama. Implementasi algoritma kriptografi kode caesar, vigenere, dan transposisi untuk sistem proteksi penggunaan pesan singkat (SMS) pada *smartphone* android.Prosiding Seminar Ilmiah Nasional Komputer dan Sistem Intelijen. 8. 146, 2014.

[3] A.A. Permana. Model layanan informasi lokasi masjid di wilayah kota Tangerang menggunakan perangkat bergerak (*mobile device*). 5. 2016.

[4] B.G. Anjari. Enkripsi SMS (*short message service*) pada telepon selular berbasis android. http://repo.pens.ac.id/1547/1/PAPER_ENKRIPSI_v1.pdf. 2012(Diakses pada 14 Maret 2018)

[5] H.R. Hatta, M. Ardi, S. Maharani. Aplikasi kriptografi pesan *short message service* pada *smartphone* berbasis android dengan metode *playfair cipher*. 4. 24, 2017.