Kumpulan jurnaL Ilmu Komputer (KLIK)
Volume 04, No.01 Februari 2017
ISSN: 2406-7857

APLIKASI KRIPTOGRAFI PESAN *SHORT MESSAGE SERVICE* PADA *SMARTPHONE* BERBASIS ANDROID DENGAN METODE *PLAYFAIR CIPHER*

Heliza Rahmania Hatta[1)], **Mohamad Ardi**[2)], **Septya Maharani**[3)]
[1,2,3)]Program Studi Ilmu Komputer, FKTI, Universitas Mulawarman
Jalan Barong Tongkok No. 6 Kampus Gunung Kelua Samarinda, Kalimantan Timur
[1]Email : heliza_rahmania@yahoo.com

Abstract

The current technological developments, allows humans to communicate and exchange information remotely. Along with the demands for security against the confidentiality of the information exchanged is increasing. Therefore, it is developing branch of science that studies on ways of securing data or better known as cryptography. Playfair cipher method is one method for text encoding cryptography. This study aims to develop an application of cryptography SMS (Short messsage Service) on the android based smartphone with Playfair cipher method, which can send SMS messages cryptography and receive text messages encrypted and then decrypted. These applications do cryptography in text form letters. The key used in the form of letters. The results of this study are in the form of android-based application that can make sending SMS messages that have been encrypted using the Playfair cipher method, so that the confidentiality of the message can be gated.

Keywords*: Cryptography, SMS, Smartphone, Android, Playfair Cipher.*

Abstrak

Perkembangan teknologi sekarang ini, memungkinkan manusia dapat berkomunikasi dan dapat bertukar informasi secara jarak jauh. Seiring dengan itu tuntutan akan keamanan terhadap kerahasiaan informasi yang saling dipertukarkan tersebut semakin meningkat. Oleh karena itu, dikembangkanlah cabang ilmu yang mempelajari tentang cara-cara pengamanan data atau lebih dikenal dengan Kriptografi. Metode playfair cipher merupakan salah satu metode kriptografi untuk penyandian teks. Penelitian ini bertujuan untuk membangun suatu aplikasi kriptografi pesan SMS (Short Messsage Service) pada smartphone berbasis android dengan metode playfair cipher, yang dapat mengirim kriptografi pesan SMS dan menerima pesan teks terenkripsi yang kemudian didekripsi. Aplikasi ini melakukan kriptografi pada teks berupa huruf. Kunci yang digunakan berupa huruf. Hasil dari penelitian ini adalah berupa aplikasi berbasis android yang dapat melakukan pengiriman pesan SMS yang telah terenkripsi menggunakan metode playfair cipher, sehingga kerahasiaan dari pesan tersebut dapat terjaga keamanannya.

Kata kunci*: Kriptografi, SMS, Smartphone, Android, Playfair Cipher.*

1. PENDAHULUAN

Perkembangan di bidang teknologi dalam beberapa tahun belakangan ini berkembangan begitu pesat, khususnya *smartphone* yang dapat digunakan untuk berbagai macam fungsi [1]. Dari sekian banyak fitur yang dimiliki oleh *smartphone*, salah satunya yang masih banyak digunakan yaitu SMS. Layanan SMS bukan merupakan jalur yang aman dalam pertukaran informasi. Pesan yang dikirim masih berupa teks terbuka yang belum terproteksi selain itu pengiriman SMS yang dilakukan tidak sampai ke penerima secara langsung, akan tetapi pengirirman SMS harus melewati *Short Message Service Center* (SMSC) yang berfungsi mencatat komunikasi yang terjadi antara pengirim dan penerima. Dengan tersimpannya SMS pada SMSC, maka seorang operator dapat memperoleh informasi atau membaca SMS di dalam SMSC tersebut, hal ini dapat dibuktikan dari beberapa kasus yang ditangani pihak kepolisian, kejaksaan atau KPK, di mana pihak-pihak tersebut meminta transkip SMS ke Operator GSM untuk dijadikan bahan penyelidikan di persidangan [2]. Oleh sebab itu, diperlukan kriptografi sebagai ilmu yang mempelajari bagaimana membuat suatu pesan yang dikirim dapat disampaikan kepada penerima dengan aman [3]. Metode *Playfair Cipher* merupakan salah satu metode kriptografi untuk penyandian teks. *Playfair Cipher* termasuk ke dalam *polygram cipher* yang melakukan substitusi secara *bigram* (kelompok yang terdiri dari dua huruf) [4].

Mengacu pada beberapa penelitian sebelumnya yakni Penyandian Citra Menggunakan Metode *Playfair Cipher* yang diimplementasikan untuk menyandikan citra dengan format bmp 24 bit ukuran 256 × 256 pixel [5]. *A Novel Approach for Encryption of Text Messages Using PLAY-FAIR Cipher 6 by 6 Matrix with Four Iteration Steps*, bertujuan untuk membuat algoritma yang kuat dengan memperpanjang matrik *Playfair Cipher* menjadi matriks dimensi 6 × 6 dan menggunakan empat langkah iterasi [6]. Aplikasi *Chatting* Rahasia Menggunakan Algoritma *Vigenere Cipher*, yang bertujuan untuk membangun suatu aplikasi kriptografi yang dapat menyandikan teks dan mengirimkan teks yang terenkripsi melalui jaringan berdasarkan algoritma *Vigenere Cipher* [7].

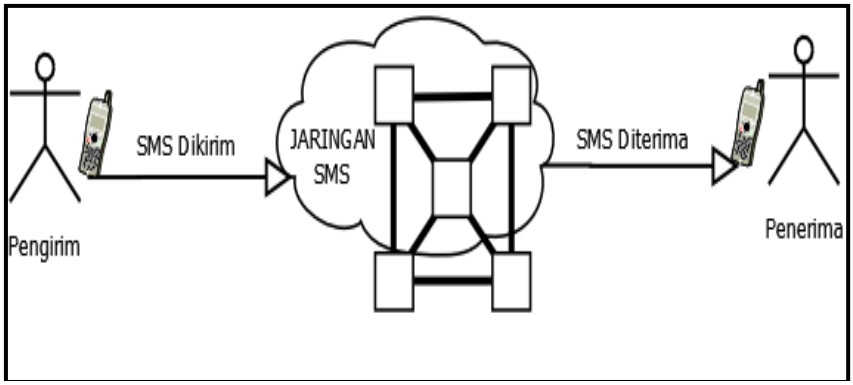
Berdasarkan penelitian-penelitian tersebut dibangun suatu Aplikasi Kriptografi Pesan *Short Message Service* Pada *Smartphone* Berbasis Android Dengan Metode *Playfair Cipher*. Aplikasi ini mengenkripsi pesan SMS dengan metode *Playfair Cipher*, sehingga orang yang tidak berkepentingan dan tidak memiliki hak akses akan mengalami kesulitan untuk melakukan hal-hal yang tidak diinginkan.

2. METODOLOGI PENELITIAN

2.1. Gambaran Umum Sistem

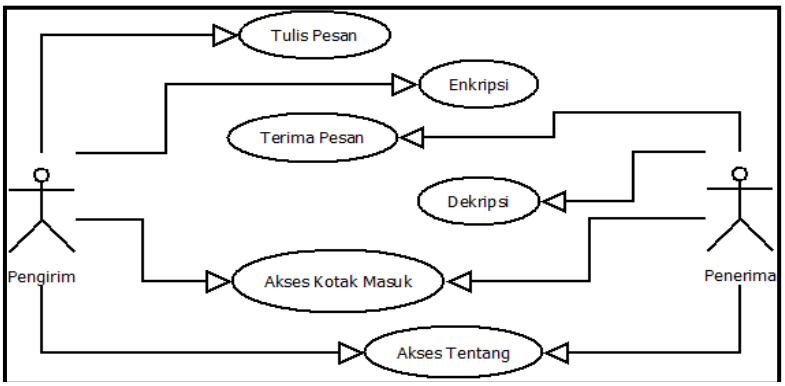
Aplikasi yang dibangun diterapkan pada *smartphone* yang berbasis operasi Android, dan memiliki fungsi untuk melakukan enkripsi dan dekripsi pesan SMS. Aplikasi ini dapat melakukan pengiriman dan menerima pesan SMS. Secara umum arsitektur global perangkat lunak aplikasi adalah pengguna sebagai pihak pengirim mengirimkan pesan SMS kepada pengguna lain yang bertindak sebagai penerima pesan SMS. Pengguna akan berinteraksi dengan aplikasi melalui antarmuka

pengguna yang disediakan oleh aplikasi, pesan yang telah dibuat dikirimkan ke *smartphone* tujuan melalui jaringan SMS. Selanjutnya penerima pesan SMS menerima pesan yang telah dikirim oleh pengirim pesan SMS. Gambar 1 memperlihatkan arsitektur global SMS.



Gambar 1. Arsitektur Global SMS

Hal-hal yang dapat dilakukan oleh pengguna terhadap sistem dapat dilihat pada *use case diagram* pada gambar 2, dimana pengirim dapat melakukan tulis pesan, enkripsi pesan, akses kotak masuk, dan akses tentang. Sedangkan penerima dapat melakukan terima pesan, dekripsi pesan, akses kotak masuk, dan akses tentang.

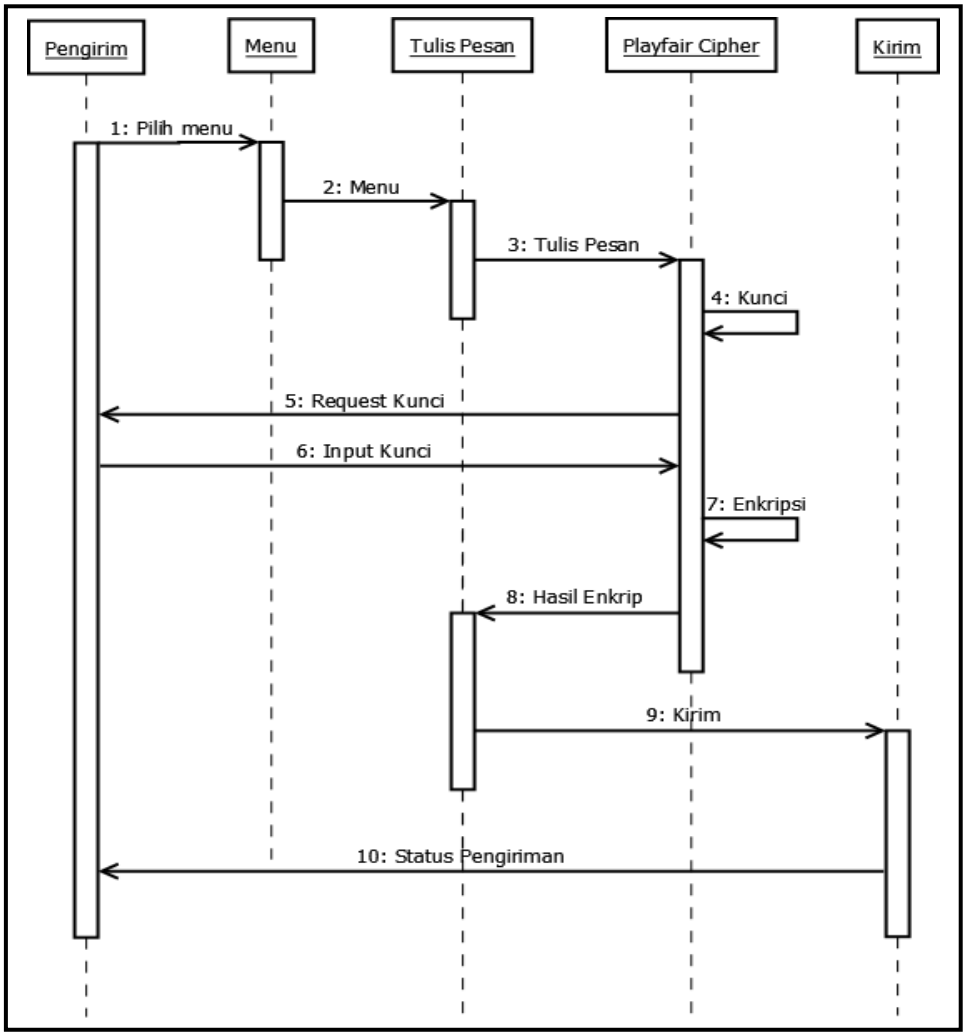


Gambar 2. *Use Case Diagram* Aplikasi Kriptografi SMS

Secara umum aplikasi kriptografi SMS pada *smartphone* berbasis Android dengan metode *Playfair Cipher* ini terdiri dari dua bagian yang penting yaitu tulis pesan dan baca pesan. *Sequence diagram* tulis pesan yang diterapkan dalam aplikasi kriptografi SMS pada *smartphone* berbasis Android dengan metode *Playfair Cipher* dapat dilihat pada gambar 3 dibawah.

Dari gambar 3 tersebut terlihat pengirim memilih menu tulis pesan. Setelah menu tulis pesan di pilih sistem kemudian memanggil fungsi tulis pesan. Setelah pesan selesai ditulis, proses selanjutnya adalah pengguna diminta untuk memasukkan kunci enkripsi pada fungsi *Playfair Cipher* dan mengenkripsi pesan yang ditulis. Setelah pesan selesai di enkripsi maka hasil enkripsi akan tampil pada

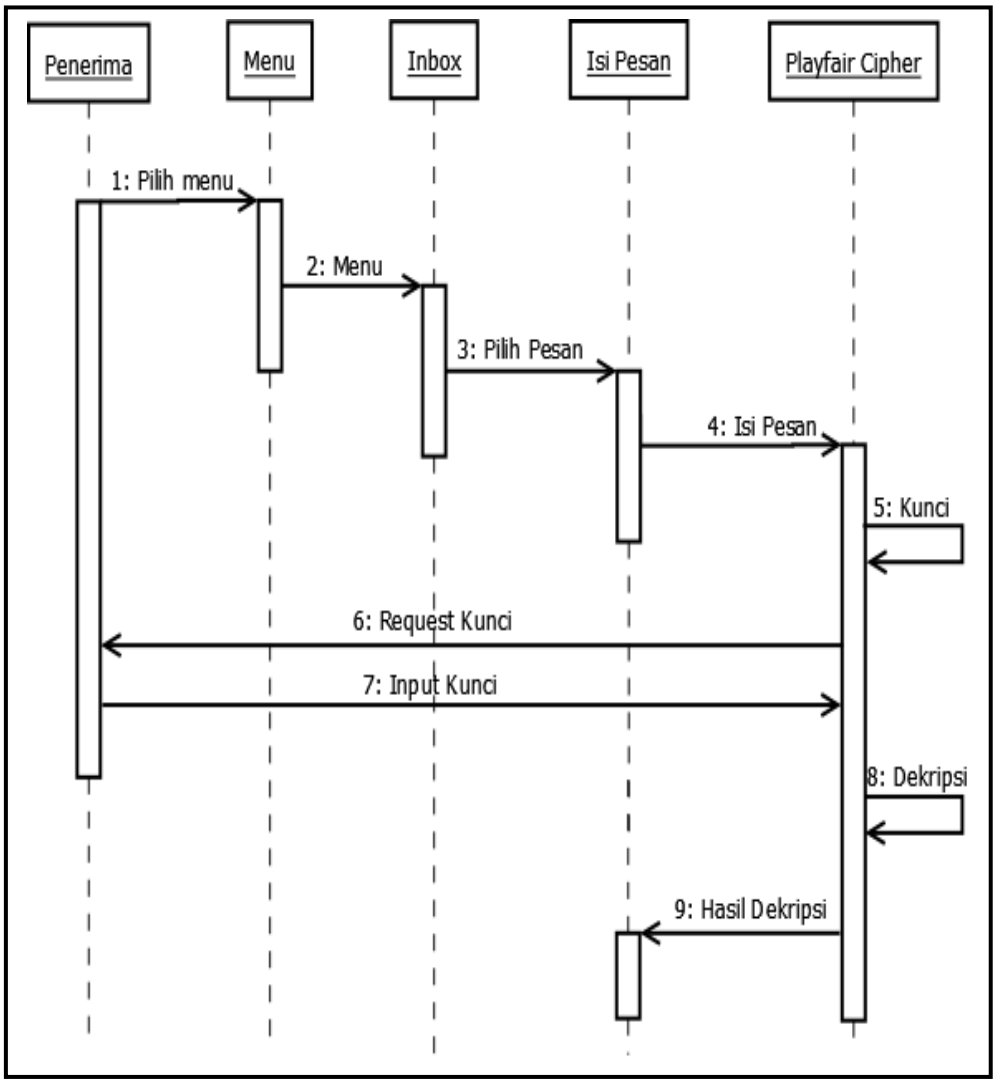
fungsi tulis pesan dan kemudian pesan dapat dikirim dan pengirim mendapat pesan status pengiriman.



Gambar 3. *Sequence Diagram* Tulis Pesan

Kebalikan dari proses di atas, berikut adalah *sequence diagram* baca pesan yang diterapkan dalam aplikasi kriptografi SMS pada *smartphone* berbasis android dengan metode *Playfair Cipher* dapat dilihat pada gambar 4 dibawah.

Dari *Sequence Diagram* Baca SMS di bawah penerima memilih menu *inbox* yang berisi pesan, kemudian dari *inbox* yang berisi pesan dibuka maka sistem meminta untuk pengguna memasukkan kunci yang sama dengan kunci enkripsi pada fungsi *Playfair Cipher*, setelah pengguna memasukkan kunci maka sistem melakukan proses dekripsi yang kemudian hasil pesan akan tampil pada fungsi isi pesan yang dapat dibaca oleh penerima.



Gambar 4. *Sequence Diagram* Baca Pesan

2.2. Tahap Pengembangan Sistem

Pengembangan sistem yang digunakan adalah *waterfall*. Tahapan yang dilakukan dalam pengembangan sistem di antaranya :

a. Tahap Inisiasi dan Perencanaan

Perencanaan dilakukan melalui studi literatur yang digunakan sebagai acuan yakni jurnal yaitu Penyandian Citra Menggunakan Metode *Playfair Cipher*, *A Novel Approach for Encryption of Text Messages Using PLAY-FAIR Cipher 6 by 6 Matrix with Four Iteration Steps*, Pengukuran Kinerja Goodreads *Application Programming Interface* (API) Pada Aplikasi *Mobile* Android (Studi Kasus Untuk Pencarian Data Buku), Aplikasi *Chatting* Rahasia Menggunakan Algoritma *Vigenere Cipher*. Literatur lainnya dari skripsi yaitu Aplikasi Enkripsi dan Dekripsi SMS dengan Metode *Playfair Cipher* pada *Smartphone* berbasis Android. Serta dari buku yaitu Kriptografi, Berbagai Implementasi dan

Pengembangan Aplikasi Mobile Berbasis Android, Membuat Sendiri SMS Gateway Berbasis Protokol SMPP, Pemrograman Aplikasi Mobile Smartphone dan Tablet PC Berbasis Android.

b. Tahap Analisis

Analisis diperlukan untuk menganalisis seluruh kebutuhan yang diperlukan untuk mendukung kerja dari aplikasi kriptografi SMS pada *smartphone* berbasis Android dengan metode *Playfair Cipher* yang dibangun. Kebutuhan sistem pada penelitian ini mencakup kebutuhan perangkat keras (*hardware*) dan kebutuhan perangkat lunak (*software*).

1) Kebutuhan Perangkat Keras (*Hardware*)

Perangkat keras yang dibutuhkan untuk membangun aplikasi kriptografi SMS adalah sebagai berikut :

a) Processor Intel® Core™ i3 CPU M 330 @ 2,13GHz.
b) RAM 4.00 GB DDR3.
c) *Harddisk* 500 GB.

2) Kebutuhan Perangkat Lunak (*Software*)

Perangkat keras yang dibutuhkan untuk membangun aplikasi kriptografi SMS adalah sebagai berikut :

a) JDK 8 *Update* 73.
b) Android Studio 2.2.
c) Sistem Operasi Windows 10 Education N 32-bit.

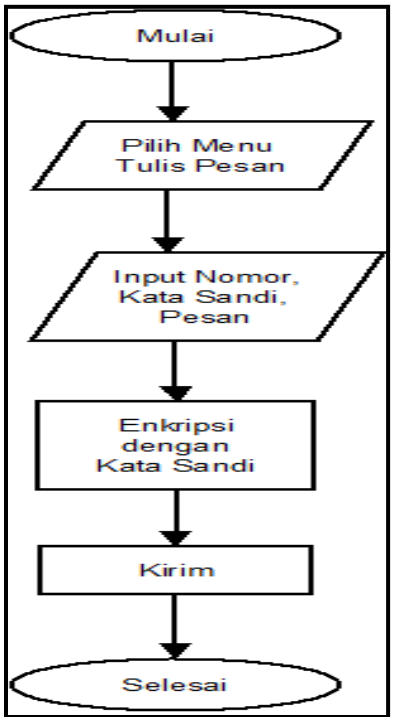
c. Tahap Perancangan

Perancangan sistem adalah proses menyusun rencana-rencana implementasi, user inteface, susunan pilihan menu dan masukan yang dibutuhkan dalam membangun aplikasi kriptografi SMS pada *smartphone* berbasis android dengan metode *Playfair Cipher*. Perancangan sistem memiliki satu menu aplikasi, sehingga pihak pengirim dan penerima dapat melakukan proses yang sama yaitu mengirim dan menerima pesan.

1) Perancangan Proses Enkripsi Pesan

Aplikasi ini mengenkripsikan pesan secara manual, yaitu pengirim dan penerima dapat menentukan kata sandi untuk enkripsi dan dekripsi pesan sesuai kesepakatan bersama. Sehingga ketika pesan dikirim oleh pengirim, terlebih dahulu memasukkan kata sandi yang telah disepakati untuk mengenkripsikan pesan. Gambar 5 dibawah ini memperlihatkan *flowchart* proses enkripsi pesan.

Flowchart perancangan proses enkripsi pesan pada gambar tersebut dimulai dengan memilih menu tulis pesan yang ada pada halaman menu awal aplikasi kriptografi pesan SMS. Selanjutnya memberikan *input* nomor *handphone* tujuan. Kemudian masukkan kata sandi atau kunci, kata sandi enkripsi berupa huruf (angka dan simbol tidak termasuk). Setelah itu, *input* pesan SMS yang akan dikirim. Proses enkripsi dengan kata sandi terjadi ketika menekan tombol kirim yang ada di halaman tulis pesan pada aplikasi kriptografi pesan SMS. Selanjutnya pesan SMS dikirim ke nomor *handphone* tujuan.

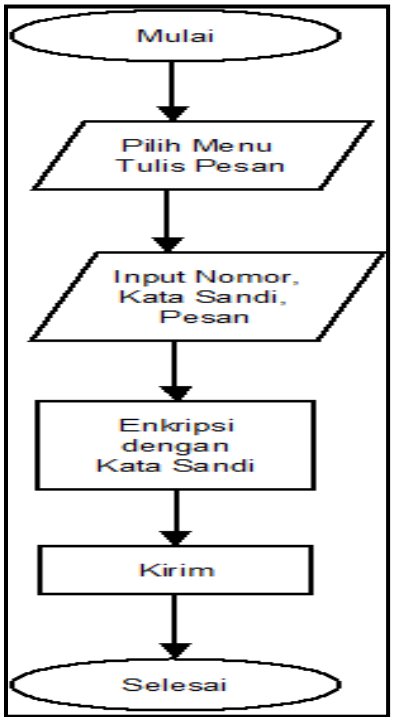


Gambar 5. *Flowchart* Proses Enkripsi Pesan

2) Perancangan Proses Dekripsi Pesan

Aplikasi ini mendekripsikan pesan secara manual yaitu pengirim dan penerima dapat menentukan kata sandi untuk enkripsi dan dekripsi pesan sesuai kesepakatan bersama. Sehingga ketika pesan diterima oleh penerima terlebih dahulu memasukkan kata sandi yang telah disepakati untuk mendekripsikan pesan yang terenkripsi. Gambar 6 dibawah ini memperlihatkan *flowchart* proses dekripsi pesan.

Flowchart perancangan proses dekripsi pesan pada gambar tersebut dimulai dengan memilih menu kotak masuk yang ada pada halaman menu awal aplikasi kriptografi pesan SMS. Selanjutnya memberikan *input* kata sandi atau kunci, kata sandi harus sama pada saat pengirim memasukkan kata sandi. kata sandi dekripsi berupa huruf (angka dan simbol tidak termasuk). Setelah itu, proses dekripsi dengan kata sandi terjadi ketika menekan tombol dekripsi yang ada di halaman dekripsi SMS pada aplikasi kriptografi pesan SMS. Selanjutnya pesan SMS dalam bentuk asli ditampilkan.



Gambar 6. *Flowchart* Proses Dekripsi Pesan

d. Tahap Implementasi

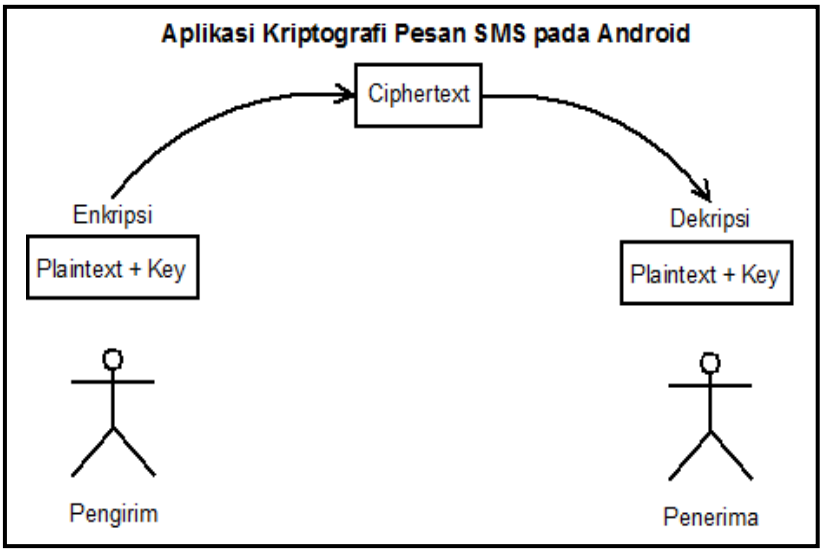
Pada tahap ini dilakukan proses implementasi pengkodean program dalam aplikasi komputer. Proses implementasi menggunakan Android Studio dengan bahasa pemrograman yaitu Java.

e. Tahap Pengujian

Pengujian terhadap sistem aplikasi kriptografi SMS pada *smartphone* berbasis android dengan metode *Playfair Cipher* yakni menggunakan *black box testing*, yakni pengujian yang berfokus pada spesifikasi fungsional dari perangkat lunak. Penguji (*tester*) dapat mendefinisikan kumpulan kondisi *input* dan melakukan pengetesan pada spesifikasi fungsional program, tanpa mengetahui apa sesungguhnya yang terjadi dalam proses sistem (hanya mengetahui *input* dan *output*).

3. HASIL DAN PEMBAHASAN

Sistem kriptografi SMS pada *smartphone* menggunakan metode *Playfair Cipher* merupakan salah satu teknik untuk menjaga keamanan pesan. Proses enkripsi dan dekripsi menggunakan metode *Playfair Cipher* dengan mengubah isi pesan yang akan dikirim. Perancangan sistem untuk aplikasi kriptografi SMS pada *smartphone* dalam penelitian ini diperlihatkan pada gambar 7 sebagai berikut:



Gambar 7. Sistem Kriptografi Pesan SMS

3.1. Implementasi Sistem

Implementasi sistem aplikasi kriptografi SMS pada *smartphone* berbasis android dengan metode *Playfair Cipher* adalah proses pengkodean program dalam aplikasi komputer. Proses implementasi sistem menggunakan Android Studio dengan bahasa pemrograman yaitu Java.

a. Halaman Pemuka Awal

Gambar 8. Halaman Pembuka Awal

Gambar 8 merupakan halaman pembuka awal dari aplikasi kriptografi pesan SMS pada *smartphone* berbasis android dengan metode *Playfair Cipher*. Halaman pembuka awal tampil pertama kali pada saat aplikasi ini dibuka. Pada halaman pembuka awal ini berisi judul aplikasi yang dibuat serta logo

aplikasi.

b. Halaman Menu Awal

Gambar 9. Halaman Menu Awal

Gambar 9 merupakan halaman menu awal pesan yang tampil setelah halaman pembuka awal. Terdapat 5 menu yang ada pada aplikasi, yaitu menu tulis pesan yang berfungsi untuk menulis pesan baru yang akan dikirim, menu kotak masuk yang berfungsi untuk melihat daftar pesan masuk.

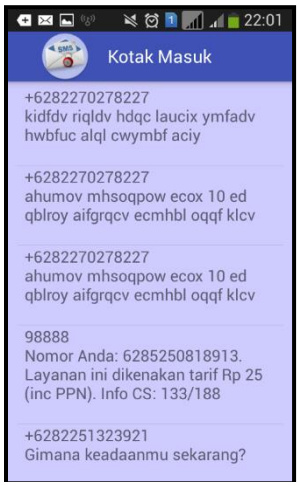
c. Halaman Tulis Pesan

Gambar 10. Halaman Tulis Pesan

Gambar 10 merupakan halaman tulis pesan yang tampil setelah memilih menu tulis pesan. Dihalaman ini terdapat *form* tulis pesan yang terdiri dari nomor *handphone* yang harus diisi dengan nomor tujuan, dapat pula menggunakan tombol kontak jika nomor tujuan tersimpan di kontak *smartphone*. Setelah memilih nomor tujuan, selanjutnya terdapat *form* kata sandi yang harus diisi dengan kata sandi atau kunci yang digunakan untuk

mengenkripsi dan mendekripsi pesan. Kata sandi atau kunci yang digunakan harus berupa huruf (tidak boleh ada angka atau karakter lain), hal ini disebabkan karena penggunaan kata sandi atau kunci dalam proses *Playfair Cipher* memang hanya menggunakan huruf, sehingga angka atau karakter lain selain huruf tidak dikenali oleh *Playfair Cipher*.

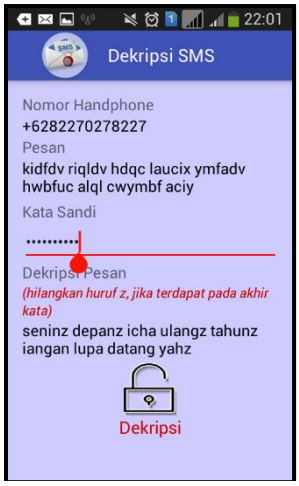
d. Halaman Kotak Masuk



Gambar 11. Halaman Kotak Masuk

Gambar 11 merupakan halaman kotak masuk yang tampil setelah memilih menu kotak masuk. Di dalam halaman ini terdapat daftar pesan masuk yang terbagi berdasarkan nomor pengirim pesan, dan urutan daftar pesan ini tersortir berdasarkan waktu pesan diterima. Untuk membuka pesan dan mengenkripsi pesan pengguna harus memilih salah satu dari daftar pesan yang ada.

e. Halaman Dekripsi SMS

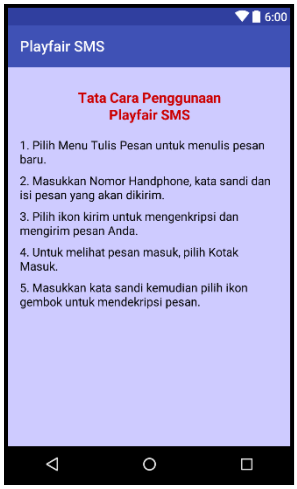


Gambar 12. Halaman Dekripsi SMS

Gambar 12 menampilkan halaman dekripsi pesan setelah memilih salah satu pesan yang akan di dekripsi dari menu kotak masuk. Pada halaman ini terdapat *form* dekripsi pesan yang terdiri dari *form* nomor *handphone* dari pengirim yang otomatis terisi setelah memilih salah satu pesan yang ada di menu kotak masuk, *form* isi pesan enkripsi yang otomatis terisi, *form* kata sandi, dan *form* isi pesan dekripsi, serta sebuah tombol dekripsi.

Pada *form* kata sandi harus diisikan kata sandi atau kunci yang sama dengan kata sandi atau kunci pada menu tulis pesan. Setelah itu pengguna menekan tombol dekripsi, maka pada *form* dekripsi pesan akan menampilkan pesan asli.

f. Halaman Bantuan



Gambar 13. Halaman Bantuan

Gambar 13 merupakan halaman bantuan yang tampil setelah memilih menu bantuan yang terdapat pada halaman menu awal. Pada halaman ini berisi tentang penjelasan tata cara penggunaan aplikasi. Bantuan yang diberikan adalah cara untuk menulis pesan baru, cara untuk melihat pesan masuk, dan cara untuk mengenkripsi dan mendekripsi pesan, dimana untuk mengenkripsi pilih ikon kirim pesan sedangkan untuk mendekripsi pilih ikon gembok.

g. Halaman Tentang

Gambar 14 merupakan halaman tentang yang tampil setelah memilih menu tentang yang terdapat pada halaman menu awal. Pada halaman ini berisi penjelasan fungsi dari aplikasi, logo dari aplikasi, dan email dari pembuat aplikasi yang dapat dihubungi. Penjelasan ini dibuat agar pengguna aplikasi dapat memahami tujuan dibangunnya aplikasi Kriptografi SMS.

Tujuan tersebut yakni untuk mengenkripsi dan dekripsi pesan SMS yang bersifat privasi sehingga dapat mengamankan dan menjaga kerahasiaan isi pesan SMS yang dikirim maupun diterima.

Gambar 14. Halaman Tentang

4. SIMPULAN

Kesimpulan yang dapat diambil berdasarkan penelitian mengenai aplikasi kriptografi pesan SMS pada *smartphone* berbasis android dengan metode *playfair cipher* adalah aplikasi kriptografi pesan SMS dan dapat berjalan di beberapa versi android yakni *Ice Cream Sandwich*, *Jelly Bean*, *Kit Kat*, dan *Lollipop*. Hasil penelitian menunjukkan bahwa enkripsi dan dekripsi pesan berhasil dilakukan sehingga dapat diasumsikan metode *Playfair Cipher* dapat diterapkan pada sistem kriptografi pesan SMS pada aplikasi ini. Hasil penelitian menunjukkan bahwa semakin banyak jumlah karaker yang dikirim maka kecepatan pengiriman pesan SMS semakin lama. Hasil penelitian menunjukkan bahwa perhitungan sistem dengan perhitungan manual mempunyai hasil yang sama.

DAFTAR PUSTAKA

[1] Kusuma, Lutvianus Satria. 2015. "**Aplikasi Enkripsi dan Dekripsi SMS dengan Metode *Playfair Cipher* pada *Smartphone* berbasis Android**". Skripsi Teknik Informatika, Universitas Sanata Dharma.

[2] Safaat, Nazruddin. 2015. ***Berbagai Implementasi dan Pengembangan Aplikasi Mobile Berbasis Android***. Bandung: Informatika.

[3] Pakereng, Magdalena Ariance Ineke. 2008. "**Kriptosistem Menggunakan Algoritma Genetika Pada Data Citra**". *Jurnal Informatika Vol. 9 Nomor 2*. Hal. 137-149.

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

[5] Setyaningsih, Emy. 2009. "**Penyandian Citra Menggunakan Metode *Playfair Cipher***". *Jurnal Teknologi Vol. 2 Nomor 2*. Hal. 213-217.

[6] Chand, Nisarga. dan Bhattacharyya, Subhajit. 2014. *"**A Novel Approach for Encryption of Text Messages Using PLAY-FAIR Cipher 6 by 6 Matrix with Four Iteration Steps**". International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 3 Issue 1*.

[7] Yulianingsih, Pricilia. Hamdani. dan Maharani, Septya. 2014. "**Aplikasi *Chatting* Rahasia Menggunakan Algoritma *Vigenere Cipher***". *Jurnal Informatika Mulawarman Vol. 9 Nomor 1*.