# PENINGKATAN SISTEM KEAMANAN PESAN PADA PERANGKAT MOBILE ANDROID DENGAN ENKRIPSI DEKRIPSI MENGGUNAKAN ALGORITMA AFFINE CIPHER DAN VIGENERE CIPHER

**Khozinul Asror**[1]

Mahasiswa Program Studi Teknik Informatika-S1, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro Semarang
Jl. Imam Bonjol No. 207, Jl.Nakula No.5-11, Semarang, Kode Pos.50131, Telp.(024) 3517261
Email : khozinul.asror9@gmail.com

---

***Abstrak***

*Perkembangan teknologi komunikasi yang begitu pesat telah memberikan manfaat yang begitu besar.Salah satunya dalam penyampaian informasi melalui pesan singkat (SMS) pada telpon sellular.Dalam penelitian ini dirumuskan masalah tentang bagaimana mengimplementasikan algoritma Affine cipher dan Vigenere cipher untuk keamanan pesan pada perangkat mobile android agar dapat menjadi lebih aman. Sedangkan tujuan dari penelitian ini adalah untuk merancang keamananpesanpada perangkat mobile android menggunakan enkripsi Affine cipher dan Vigenere cipher, serta mengimplementasikannya ke dalam sebuah apliaksi android menggunakan pemprogaman java. Affine cipher dan Vigenere cipher merupakan bagian dari algoritma simetris. Proses enkripsi dan proses dekripsi pada algoritma Affine cipher membutuhkan dua kunci, sedangkan proses enkripsi dan dekripsi menggunakan Vigener cipher membutuhkan satu kunci. Dengan memanfaatkan algoritma ini pesan yang dikirim akan menjadi lebih aman karena menggunakan 3 kunci. karakter yang di gunakan juga tidak sebatas huruf abjad namun angka dan symbol juga termasuk di dalamnya. Hasil dari aplikasi menggunakan algoritma affine ciper dan vigenere ciper dapat mengamankan pesan lebih kuat dari pada hanya menggunakan algoritma affine cipher.*

***Kata Kunci:*** *Android, Kriptografi, Keamanan Pesan, Affine cipher, Vigenere Cipher*

***Abstract***

*The development of communication technologies is so rapid has provided benefits so great. one in the way of delivery information by short messages (SMS) to a cellular phone. In this study, formulated the problem of how to implement algorithms Affine cipher and Vigenere cipher for security messages on a mobile device android to be more secure. While the purpose of this study is to design a security message on a mobile device using the Android Affine encryption cipher and Vigenere cipher, and implement them into an android application using java program. Affine cipher and Vigenere cipher is part of a symmetric algorithm. Encryption and decryption process on Affine cipher algorithm requires two keys, where the encryption and decryption process requires the use Vigener cipher key. By utilizing this algorithm message sent will be more secure because it use 3 keys. This is using not limited character to letters of the alphabet, but also the numbers and symbols are included. Results of the application using affine cipher algorithms and cipher vigenere can secure a stronger message than just using an affine cipher algorithm.*

***Keywords:*** *Android, Criptography, Secure Messages, Affine cipher, Vigenere Cipher*

# 1. PENDAHULUAN

## 1.1 Latar Belakang

Perkembangan teknologi komunikasi yang begitu pesat telah memberikan manfaat yang begitu besar, Salah satunya dalam penyampaian informasi. Penyampaian informasi yang paling dekat dengan masarakat saat ini adalah telpon sellular atau yang sekarang *Booming* dengan nama *Smartphone*. Sistem operasi yang popular di gunakan pada *Smartphone* di dominasi oleh system operasi Android. Penggunaan Android ini dapat diperuntukan untuk melakukan panggilan telepon dan pengiriman pesan menggunakan SMS dll.

SMS (Short Message Service) adalah sebuah layanan komunikasi yang ada pada telepon selluler untuk mengirim dan menerima pesan-pesan pendek. Dalam penyampaian informasi menggunakan SMS ini belum ada suatu keamanan yang dapat menjamin keamanan pesan yang di sampaikan, karena dalam melakukan SMS menggunakan aplikasi bawaan ponsel, SMS yang di kirim masih berupa teks yang terbuka dan belum diproteksi. Selain itu pengiriman sms yang dilakukan tidak sampai ke penerima secara langsung melainkan melawati 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 di buktikan dari beberapa kasus yang di tangani kepolisian, dimana pihak tersebut meminta transkip sms ke operator GSM untuk dijadikan bahan penyelidikan di persidangan **[**1**].** Selain itu ada resiko lain yang dapat mengancam keamanan isi pesan yaitu *SMS Spoofing, SMS Snooping, dan SMS interception* [**2**].

*SMS Spoofing* merupakan pengiriman sms dimana nomor pengirim yang tertera bukanlah nomor pengirim yang sebenarnya, sedangkan untuk *SMS Snooping* ini lebih sering terjadi karena kelalaian pengguna telpon selluar. *SMS Snooping* lebih sering terjadi karena kelalaian pengguna telepon seluler. Contohnya ketika seseorang meminjamkan telepon selulernya pada orang lain untuk menggunakan telepon selulernya. Pada saat itu orang tersebut dapat dengan sengaja atau tidak membuka isi pesan yang ada pada inbox sms. Celah keamanan terbesar pada layanan komunikasi SMS adalah pada saat SMS tersebut sedang dikirim melalui jaringan SMS. SMS bekerja pada jaringan nirkabel yang memungkinkan terjadinya pencurian isi pesan SMS ketika dalam proses transmisi dari pengirim ke penerima, kasus ini disebut *SMS Interception.*

Dengan adanya beberapa ancaman diatas dan timbul suatu usaha untuk mengembangkan sistem keamanan pada layanan SMS yang mampu menjaga keamanan isi pesan untuk menutupi celah keamanan SMS. Agar dapat menjaga kerahasiaan pesan dapat diterapkan konsep kriptografi dengan cara mengenkripsinya. *Enkripsi* adalah Proses mengubah suatu informasi asli yang disebut plaintext menjadi sebuah sandi yang tidak dapat terbaca yang disebut ciphertext, sedangkan proses menguraikan cipherteks menjadi informasi asli disebut Dekripsi. Untuk itu dibutuhkan suatu metode yang dapat mengenkripsi dan dekripsi suatu pesan, salah satunya dengan algorima Affine Cipher dan Vigenere cipher.

## 1.2 Rumusan Masalah

Berdasarkan latar belakang diatas maka rumusan masalah dalam tugas akhir ini yaitu Bagaimana menerapkan algoritma Affine Cipher dan Vigenere Cipher untuk enkripsi pesan (SMS)

pada perangkat mobile android agar pesan (SMS) menjadi lebih aman ?

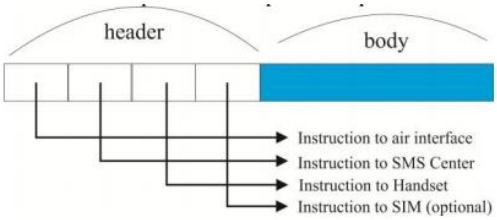
### 1.3 Tujuan

Dari rumusan masalah yang telah disebutkan, maka tujuan penelitian yaitu perancangan keamanan layanan pesan sms menggunakan algoritma Affine Cipher dan Vigenere Cipher yang di implementasikan ke dalam perangkat mobile android yang di tujukan untuk menjaga integritas dan keamanan isi pesan

## 2. Tinjauan Pustaka

### 2.1 Short Messages Service (SMS)

SMS (Short Message Service) merupakan sebuah layanan komunikasi yang ada pada telepon seluler untuk mengirim dan menerima pesan-pesan pendek. SMS pertama kali ikenalkan pada tanggal 3 Desember 1982.Ada beberapa jaringan yang bisa dipakai ntuk mengirim SMS. Beberapa jaringan yang terkenal adalah GSM, TDMA, CDMA, GPRS, DGE, WCDMA, dan UMTS . Dari jaringan-jaringan tersebut, yang paling populer di dunia dalah GSM (Global System for Mobile Communication) [5]. Struktur sebuah pesan SMS dapat dilihat pada Gambar dibawah




**Gambar 1.** Struktur sebuah pesan SMS

Dari gambar daitas terlihat bahwa pesan SMS pada dasarnya terdiri atas message body dan headernya. Header SMS terdiri atas instruksi-instruksi yang ditujukan kepada SMSC, IM, maupun kepada ponsel itu sendiri. Sedangkan message body adalah konten utama dari MS berupa pesan yang ditulis oleh pengirim. Sebuah pesan SMS berukuran maksimal 60 arakter. Di mana setiap karakter memiliki panjang 7 bit. Menurut [5] SMS memiliki empat buah komponen utama . Komponen-komponen tersebut adalah:

1. Cell Tower
   Cell Tower bertanggung jawab untuk mentransmisikan suara dan data SMS) antara ponsel dan MSC (Mobile Switching Center). Semua transmisi dikendalikan oleh cell tower.
2. Mobile Switching Center (MSC)
   MSC adalah sebuah saklar yang dikontrol oleh komputer yang berfungsi ntuk mengatur operasi jaringan yang berjalan secara otomatis. MSC secara otomatis mengontrol panggilan telepon dan dan merutekannya ke ponsel yang tepat pada sebuah service area. MSC dihubungkan ke base station oleh channel gelombang mikro, dan dihubungkan ke PSTN (Public Telephone Network) melalui sambungan telepon.
3. SMSC (SMS Center)
   Ketika mengirim SMS, SMS akan disimpan sementara di SMSC. SMSC ertindak sebagai sebuah tempat penyimpanan, dan pem-forward SMS.ama halnya dengan MSC, SMSC menjamin SMS akan sampai pada pengguna. MS disimpan di jaringan sampai ponsel penerima tersedia di jaringan. Hal ini membuat pengguna dapat menerima atau mentransmisikan SMS kapanpun.
4. Gateway Mobile Switching Center (GMSC)
   SMSC berkomunikasi dengan jaringan TCP/IP melalui GMSC. GMSC erupakan sebuah MSC yang dapat menerima SMS dari SMSC.

### 2.2 Android

Android merupakan sistem operasi yang berbasiskan Linux kernel, dan

dirancang untuk perangkat mobile touchscreenseperti smartphone dan komputer tablet. Android merupakan sistem operasi open source. Ada empat keuntungan dari sistem operasi open source. Keuntungan pertama, sistem operasi ini gratis.Kedua, semua orang bebas memodifikasi sistem yang ada. Ketiga, pengguna tidak harus menggunakan perangkat lunak berbayar yang hanya bisa bersinergi dengan perangkat lunak berbayar yang lain dari perusahaan yang sama. Keempat, banyaknya orang yang ikut mengembangkan sistem membuat sistem operasi open source selalu diperbaharui, dan sistem keamannnya pun lebih baik.

Android merupakan sistem operasi yang paling popular [8].Dari 227 negara yang terrekam datanya oleh StatCounter, ada 135 negara yang pasarnya dikuasai oleh Android. Android menyediakan developing tools tersendiri untuk para pengembang aplikasi. Pengembangan aplikasi Android menggunakan bahasa pemrograman Java. Fitur yang tersedia di Android antara lain:

- Framework aplikasi yang mendukung penggantian komponen dan reusable
- Dalvik virtual machine
- Integrated browser
- Grafik berdasarkan OpenGL
- SQLite untuk penyimpanan data
- Multimedia support linkungan Development yang lengkap dan kaya termasuk perangkat emulator, tools untuk debugging, profil dan kinerja memori, dan plugin untuk IDE Eclipse.

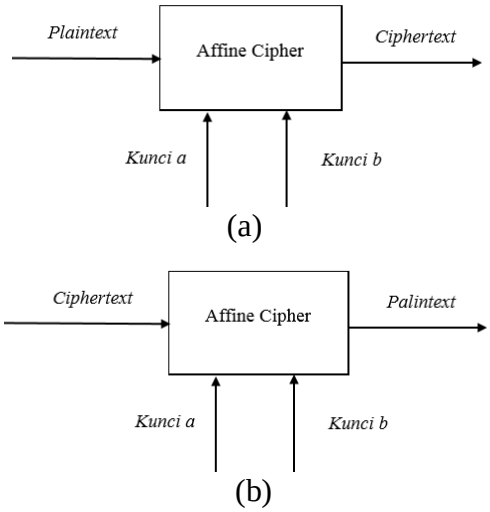
## 2.3 Affine Cipher

Metode Affine cipher merupakan kriptografi dengan kunci simetris, yaitu jika kunci yang digunakan untuk enkripsi sama dengan kunci untuk dekripsi. Plainteks (P*i*) dikonversikan dengan tabel konversi, kemudian untuk memperoleh cipherteks (C*i*), plainteks dienkripsi menggunakan persamaan :

$C_i = (a\ P_i + b) \bmod 90$ ……. *(1)*

dengan *a* adalah kunci pertama yang harus relatif prima dengan 90 dan *b* adalah kunci kedua yang dipilih bebas. Untuk melakukan dekripsi kunci yang dipakai haruslah sama dengan kunci yang digunakan pada proses enkripsi. Agar dapat memperoleh *plaintext* maka invers *a (mod 90)*, dinyatakan dengan $a^{-1}$. Jika $a^{-1}$ ada, maka dekripsi akan dilakukan dengan persamaan

$P_i = a^{-1}(C_i - b) \bmod 26$ ……. *(2)*




**Gambar 2.** *Proses Enkripsi (a) dan dekripsi (b) Affine Cipher*

Gambar diatas menjelaskan tahapan proses enkripsi dan dekripsi dimana proses enkripsi menggunakan 2 buah kunci dan untuk proses dekripsi haruslah maneggunakan kunci yang sama.

## 2.4 Vigenere Cipher

Vigenere Cipher adalah salah satu jenis kriptografi kalsik yang pada dasarnya melakukan subtitusi cipher abjad majemuk (polyalphabetic substitution). Metode ini pertama kali dipublikasikan oleh seorang diplomat (sekaligus seorang kriptologis) Prancis, Blaise de Vigenere pada abad ke-16,

tepatnya pada tahun 1586. Vigenere cipher merupakan bagian dari algoritma kriptografi klasik yang sangat dikenal karena menggunakan rumus matematika, selain itu Vigenere cipher juga dapat menggunakan tabel Vigenere untuk melakukan enkripsi *plaintext* ataupun dekripsi *ciphertext.* Tabel Vigenere ini digunakann untuk memperoleh *ciphertext* berdasarkan kunci yang sudah ditentukan. Jika panjang kunci lebih pendek dari *plainext* maka maka kunci akan diulang penggunaannya secara periodic.

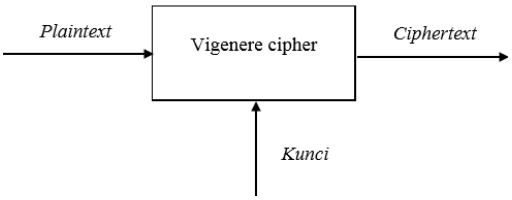
Enkripsi dengan metode Vigenere cipher, menggunakan persegi Vigenere dengan cara tarik garis vertikal dari huruf *plaintext* ke bawah, lalu tarik garis horizontal dari huruf kunci kekanan. Perpotongan kedua garis tersebut menyatakan huruf *ciphertext nya*. Dekripsi pada Vigenere cipher dilakukan dengan cara yang berkebalikan, yaitu menarik garis horizontal dari huruf kunci sampai ke huruf cipherteks yang dituju, lalu dari huruf cipherteks tarik garis vertikal sampai ke huruf plainteks. Secara matematis, misalkan kunci sepanjang m adalah rangkaian ***k1,k2,…km*** plainteks adalah rangkaian ***p1,p2,…pm*** dan cipherteks adalah rangkaian ***c1,c2, … cm*** sehingga enkripsi pada Vigenere cipher dapat dinyatakan dengan :

$$C_i = (P_i + K_r) \bmod 26 \ldots\ldots\ldots (3)$$

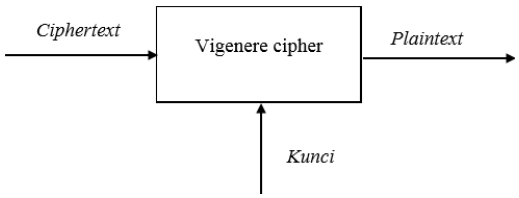
Sedangkan untuk proses dekripsi di gunakan rumus :

$$P_i = ((C_i - K_r) + 26) \bmod 26$$

$$\ldots\ldots\ldots (4)$$




*(a)*




*(b)*

**Gambar 3.** *Proses Enkripsi (a) dan dekripsi (b)Vigenere Cipher*

Gambar diatas menjelaskan tahapan proses enkripsi dan dekripsi dimana proses enkripsi menggunakan 1 buah kunci dan untuk proses dekripsi haruslah maneggunakan kunci yang sama.

## 2.5 Modifikasi Affine cipher dan vigenere cipher

Metode modifikasi Affine cipher dengan Vigenere cipher merupakan penyandian cipher baru, dengan cara menggabungkan dua buah metode yaitu Affine cipher dengan Vigenere cipher. Mengetahui Affine cipher memiliki kelemahan yaitu huruf atau karakter pada plainteks setelah dienkripsi akan sama pada cipherteks, sehingga untuk mengecohkan kriptanalisis maka ditambahkan angka 1,2,3,4,5,6,7.8.9.0 dan beberapa karakter !@#$%^&*()-_=+[]{}\|;:,.<>/? serta mengkombinasikan dengan Vigenere cipher yang memiliki karakteristik cipher alfabet majemuk yaitu huruf atau karakter yang sama pada plainteks, kemungkinan kecil akan sama di cipherteksnya. Bertambahnya ukuran konversi dan penggabungan metode Affine cipher dengan Vigenere cipher, sehingga semakin menambah tingkat kesulitan. Jika dalam hal ini kriptanalisis hanya mengetahui metode Affine cipher dan metode Vigenere cipher, mengetahui alur enkripsi maupun dekripsi serta bisa menemukan ukuran konversi maka kriptanalisis akan melakukan empat percobaan. Empat percobaan yang akan dilakukan oleh kriptanalisis yaitu

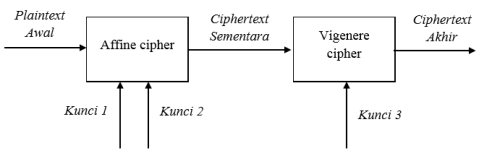
penggunaan kunci pertama (a) yang syaratnya relatif prima dengan 90 adalah sebanyak 24 kali percobaan (1,3,5,**7**,11,13,17,19,23,29,31,37,41,43, 47,53,59,61,67,71,73,79,83,89) penggunaan kunci kedua (b) sebanyak 90 kali percobaan (0,1,2,3 … 89) Jadi, pada Affine cipher kriptanalisis akan melakukan percobaan sebanyak a x b = 24 x 89 = 2136 kali percobaan. Sedangkan, pada Vigenere cipher yaitu penggunaan kunci ketiga sebanyak kr = $\sum_{k=1}^{k} 90^n$ dengan $k \leq Pi$ dan $n$ adalah panjang kunci ketiga. Misalkan panjang kunci ketiga adalah 5 sehingga percobaan menjadi $90^5$ = 590490000 kali percobaan dan penggunaan aturan konversi sebanyak

$$\mathrm{P}(n,r)^n = \frac{n!}{(n-r)!} = P(90{,}90)\frac{90!}{(90-90)!} = 90!\ \text{percobaan}$$

Karena pada modifikasi Affine cipher dan dengan Vigenere cipher merupakan penggabungan dua buah metode sehingga kriptanalisis harus melakukan percobaan sebanyak *a x b x* $k_r$ *x m! = (2136 x* $\sum_{n=1}^{k} 90^n$ x 90!*)* kali percobaan.

a. Proses enkripsi modivikasi affine dan vigenere cipher

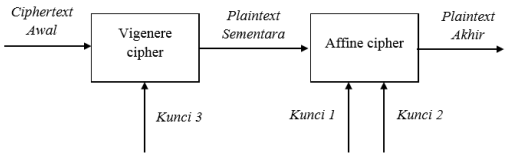
Proses enkripsi pesan pada gabungan kedua algoriitma ini tahapannya adalah yang pertama dilakukan dengan menggunakan algortima affine chipper, setelah didapat cipertex sementara baru kemudian di enkripsi lagi dengan vigenere chipper, barulah didapat cipertex ahir yang nantinya akan di gunakan untuk proses dekripsi untuk menghasilkan plainteks awal. berikut ini adalah gambar alur proses enkripsi pesan.




*Gambar 4. Proses Enkripsi Menggunakan Affine dan Vigenere Cipher*

b. Proses dekripsi modivikasi affine dan vigenere cipher

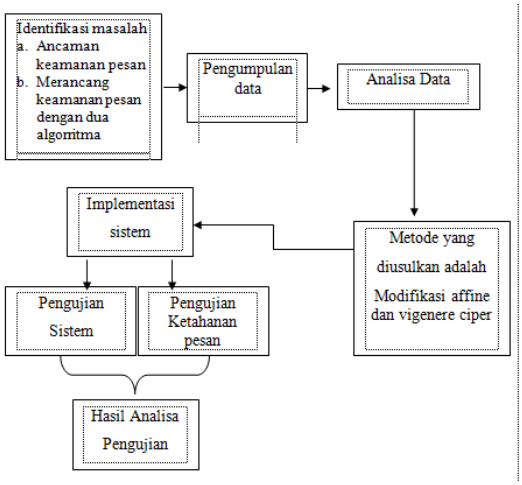
Proses dekripsi ini adalah kebalikan dari proses enkripsi, preoses dekripsi ini dilakukan mulai dengan algoritma vigenere telbeih dahulu kemudian menggunakan algoritma affine chipper. Dibawah ini adalah alur proses dekripsi pesan.




**Gambar 5.** *Proses Dekripsi Menggunakan Vigenere dan Affine Cipher*

Proses enkripsi dan dekripsi pada Affine cipher mengunakan 2 kunci, sedangkan pada Vigenere cipher menggunakan 1 kunci. Gabungan dari algoritma Affine cipher dan Vigenere cipher menghasilkan satu metode baru yang engkripsi dan dekripsinya dilakukan dengan menggunakan 3 kunci. Penggunaan dari gabungan kedua algoritma ini, yaitu affine cipher dan vigenere chiper menjadi lebih kuat di bandingkan hanya menggunakan algoritma Affine cipher saja atau Vigenere cipher saja [4].

## 3. METODE PENELITIAN




**Gambar 6.** Bagan penelitian

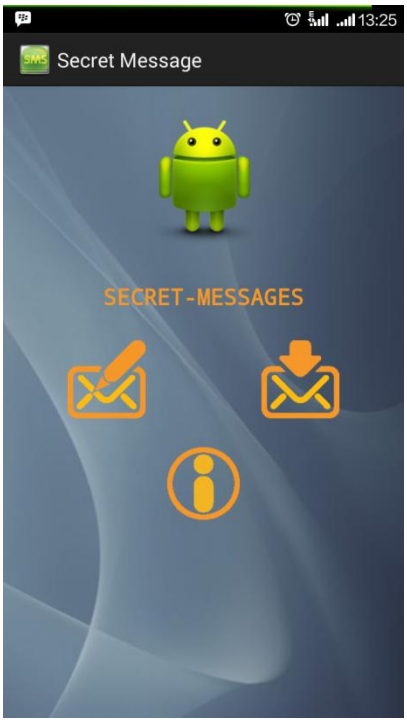
a. Identifikasi masalah
   Identifikasi Masalah adalah tahap awal dari penelitian ini. Masalah yang di identifikasikan adalah keamanan pesan dalam perangkat mobile android.
b. Pengumpulan data
   Pengumpulan data diperoleh dari kajian jurnal dan landasan teori. dalam hal ini tentang keamanan pesan pada mobile android
c. Analisa data
   Analisa data pada penelitian ini dilakukan dalam dua tahap yaitu pada saat proses enkripsi dan dekripsi pesan.
d. Metode yang diusulkan
   Dalam penelitian ini menggunakan metode Waterfall untuk merancang aplikasinya dan menggunakan modifikasi algoritma affine cipher dan vigenere cipher untuk keamanan pesannya.
e. Implementasi dan pengujian
   Implementasi pada penelitian ini di wujudkan dalam bentuk aplikasi system keamanan pesan menggunakan bahasa pemprogaman java dan di uji dengan blackbox testing.
f. Hasil analaisa pengujian
   Hasil analisa pengujian merupakan kesimpulan dari pengujian terhadap aplikasi yang sudah di buat sudah sesuai atau tidak.

## 4. ANALISIS HASIL PENELITIAN DAN PEMBAHASAN

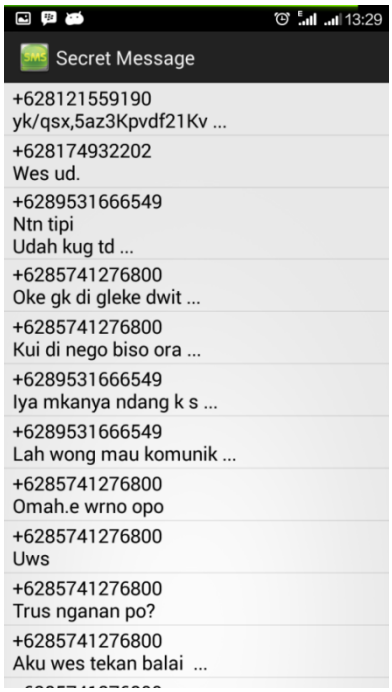
### 4.1 Analisis sistem

System yang akan di bangun dalam penelitian ini adalah sebuah aplikasi pesan yang mampu mengenkripsi dan dekripsi pesan untuk keamanan sebuah pesan. Aplikasi ini di implementasikan menggunakan algoritma affine cipher dan vigenere cipher.Affine chipper di gunakan untuk mengenkripsi pesan pertama dan kemudian di enkripsi lagi dengan vigenere cipher. gabungan dari kedua algoritma ini di gunakan untuk meningkatkan keamanan pesan

### 4.2 Implementasi




**Gambar 7.** Merupakan tampilan halaman utama menu dari apliaksi




**Gambar 8.** Merupakan tampilan halaman kotak masuk dari apliaksi

## 4.3 Pengujian

Pengujian yang akan dilakukan haruslah mengikuti langkah-langkah pengujian yang sudah direncanakan pada bab 3 sebelumnya. Untuk melakukan pengujian di butuhkan 2 buah smartphone , 1 untuk pengirim pesan dan 1 untuk penerima pesan. Pengujian yang pertama adalah dengan blaxbox testing. Sedangkan untuk pengujian ketahanan pesannya di gunakan Brute force attack .

- Pengujian dengan blackbok testing

  Pengujian black box (black book testing) adalah salah satu metode pengujian perangkat lunak yang berfokus pada sisi fungsionalitas, khususnya pada input output aplikasi (apakah sudah sesuai dengan yang diharapkan apa belum).berikut adalah hasil pengujian pada black box testing:

*Tabel 4.2.Pengujian fungsionalitas aplikasi Pesan*

| No | Skenario Pengujian | Test –Case | Hasil yang diharapkan | Hasil Pengujian | Kesimpulan |
|---|---|---|---|---|---|
| 1 | Hanya mengisi nomor tujuan dan mengosongkan formisi pesan, lalu langsung mengklik tombol 'kirim'. | No tujuan: Form Pesan: - | Aplikasi akan langsungmengirim pesan kosong" | Sesuai / Tidak sesuai | Valid |
| 2 | Mengisi No tujuan dan form pesan, tanpa klik tombol enkripi lalu langsung mengklik tombol 'kirim'. | No tujuan: - form pesan: - Tombol enkripsi : - | Aplikasi akan langsung mengirim pesan tanpa di enkripsi" | Sesuai / Tidak sesuai | Valid |
| 3 | Mengisi No tujuan dan form pesan, kmudian klik tombol enkripsi lalu langsung mengklik tombol 'kirim'. | No tujuan: - form pesan: - Tombol enkripsi : -. | Aplikasi akan langsung mengirim pesan dan pesan telah terenkripsi" | Sesuai / Tidak sesuai | Valid |

Kemudian pengujian akan dilanjutkan dengan menguji pesan yang akan dikirim dari pengirim ke penerima apakah input dan outputnya sudah sesuai apa belum, skenarionya adalah sebagai berikut :

*Tabel 4.3.Pengujian pengiriman dan penerimaan pesan*

| No | Pesan sms | Key | Enkripsi | dari | Ke | Dekripsi | Ket. |
|---|---|---|---|---|---|---|---|
| 1 | hay apa kabar? | qwerty | J5Eq2_yvSz 97)T | Alfa | Beta | hai apa kaber ? | Valid |
| 2 | saya lagi sibuk. | qwerty | ,5azstYIEq Y6QSc | Alfa | Beta | saya lagi sibuk. | Valid |
| 3 | Besok saya mau bimbingan bisa tidak pak? | qwerty | 6>=8hx,5azs 1yQd7T16W nD28p@E.2 xDW8zhx$5 S0 | Alfa | Beta | Besok saya 1au bi1bingan bisa tidak pak? | Tidak Valid |
| 4 | Revisi lagi bro… hahaha | qwerty | }>FR YPrmDTx6? ucejJ5.z | Alfa | Beta | Revisi lagi bro… hahaha | Valid |
| 5 | Besok saya daftar siding. | qwerty | 6>=8hx,5azs }yB;z:x,W8 z3Kb | Alfa | Beta | Besok saya daftar siding. | Valid |
| 6 | Pendaftaran sidang terahir tanggal 10 oktober bro, lo daftar kapan ? | nokia | !{t@i:Bs)iwn [I4vx,h]+]sB A[n.qj AsdzxXJx@ 4Sjdqmcs6iw n$q*Aw_h. | Alfa | Beta | Pendaftaran sidang terahir tanggal 10 oktober bro, lo daftar kapan ? | Valid |
| 7 | Break your jail to be success | nokia | 3]-qOmk1C@m VsIVmB1hp +n/Cw0[]{Z K | alfa | Beta | Break your jail to be success | Valid |
| 8 | you have 2 choise, now or letter ! | miracle | iyLZ?tF=h9Z yEuN{}Ebuu Uh8@bg%, 2}.@S | alfa | Beta | you have 2 choise, now or letter ! | Valid |

Dari 10 hasil pengujian pengiriman sms diatas terbukti aplikasi ini belum

sempurna karena ada 1 sms yang hasil dekripsinya masih belum sesuai. 1 sms tersebut yang belum sesuai ini karena terdapat karakter “m” yang jika di ekripsinya menjadi “1”.

## 5. KESIMPULAN DAN SARAN

### 5.1 Kesimpulan

Berdasarkan pembahasan dan hasil evaluasi dari bab-bab sebelumnya, maka dapat diambil kesimpulan bahwa :

1. Aplikasi keamanan pesan dapat di bangun dengan menggunakan algoritma affine dan vigenere cipher dengan bahasa pemprogaman java.
2. Modifikasi Affine cipher dan Vigenere cipher menghasilkan cipherteks yang memiliki karakter yang berbeda dengan plainteks, karena karakter yang digunakan berjumlah 90. akibatnya cipherteks tidak mudah didekripsi oleh kriptanalisis, karena melalui dua kali proses penyandian yang cipherteksnya mempunyai karakteristik dari cipher alfabet majemuk.
3. Untuk dapat mengetahui sebuah password modifikasi Affine cipher dan Vigenere cipher harus mengetahui 3 buah kunci atau dengan melakukan percobaan sebanyak a x b x kr x m! = (2136 x $\sum_{n=1}^{k} 90^n$ x 90!) kali percobaan.
4. Aplikasi keamanan pesan dengan algoritma affine dan vigenere ciper telah dilakukan percobaan sebanyak 10 kali, dengan hasil pengujian hanya satu kali pengujian saja yang tidak berhasil di dekripsi kembali. Sehingga aplikasi menggunakan algoritma affine ciper dan vigenere ciper dapat dikatakan bisa mengamankan pesan dengan tingkat keamanan 90%.

### 5.2 Saran

Dalam penerapan enkripsi menggunakan algoritma Affine cipher dan Vigenere cipher pada aplikasi secret message terdapat beberapa hal yang perlu diperhatikan supaya menjadi lebih baik kedepannya, diantaranya sebagai berikut :

1) Penerapan algoritma Affine cipher dan Vigeere cipher pada aplikasi secret messages ini belum sempurna, ada beberapa karakter yang tidak bisa di dekripsi kembali yaitu karakter “m”, untuk itu aplikasi perlu di kembangkan lagi.
2) Untuk pengembangan aplikasi selanjutnya dapat di tambahkan fungsi balas pesan dan cara memberian kunci kepada orang yang akan menerima pesan tersebut agar penerima dapat membaca isi pesan yang dikirim.
3) Untuk implementasi lebih lanjut, bisa dilakukan dengan algoritma hybrid affine dan vigenere cipher.

## 6. DAFTAR PUSTAKA


[1] Safaat Nazruddin, *Pemprogaman Aplikasi Mobile Smartphone dan Tablet PC Berbasis Android*, 2nd ed. Bandung: Informatika Bandung, 2012.

[2] Andi Kurniawan Dwi P, "Penerapan Algoritma Vigenere Cipher pada Aplikasi SMS Android," 2012.

[3] Raditia Akbar, "IMPLEMENTASI ENKRIPSI DEKRIPSI ALGORITMA AFFINE CHIPER BERBASIS ANDROID," *SKRIPSI*, MARET 2013.

[4] Juliadi and dkk, "Kriptografi Klasik Dengan Metode Modifikasi Affine Cipher Yang Diperkuat Dengan Vigenere Cipher," *Buletin Ilmiah Matematika Statistik*, vol. 2, no. 2, pp. 87 - 92, 2013.

[5] Yudistira, "Pembangunan Aplikasi Client SMS dengan Enkripsi Menggunakan

Algoritma Twofish pada Telepon Sellular Android," *Prosiding Teknik Elektro & Informatika*, vol. 1, no. 1, Mei 2012.

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

[7] Hartini and Sri Primaini, "KRIPTOGRAFI PASSWORDMENGGUNAKAN MODIFIKASI METODE AFFINE CIPHERS," vol. 2, no. 1, oktober 2013.

[8] Amir hasan. (2015, agustus) TEKNIK PENYALAHGUNAAN DAN KECURANGAN (FRAUD) KOMPUTER. [Online]. http://amirhasanseak.blogspot.co.id/2013/05/teknik-penyalahgunaan-dan-kecurangan.html