ENKRIPSI SMS (SHORT MESSAGE SERVICE) PADA TELEPON SELULAR BERBASIS ANDROID

Becik Gati Anjari
7410040721

Jurusan Teknologi Informasi
Politeknik Elektronika Negeri Surabaya
Institut Teknologi Sepuluh Nopember
Kampus ITS Keputih Sukolilo Surabaya 60111
Telp. 031- 5947280, 031- 5946114, Fax : 031 – 5946114
e-mail : gatianjari@yahoo.com

ABSTRAK

Beberapa tahun terakhir ini, terjadi perkembangan yang pesat pada teknologi telepon selular (ponsel). Salah satunya adalah mulai bermunculan ponsel pintar dengan berbagai fitur dan memiliki sistem operasi kompleks layaknya komputer. Berbagai system operasi untuk ponsel pun bermunculan, diantaranya yang cukup dikenal luas adalah android. Sekalipun ponsel pintar memiliki berbagai fitur, fitur lama seperti Layanan Pesan Singkat atau lebih dikenal dengan SMS masih tetap ramai digunakan. Namun dengan fitur SMS yang ada, timbul pertanyaan mengenai keamanan informasi jika seseorang ingin mengirimkan suatu informasi rahasia melalui fasilitas SMS.

Dengan melakukan enkripsi terhadap teks SMS maka tingkat keamanan informasi dari pesan tersebut dapat ditingkatkan. Dari berbagai macam teknik enkripsi, enkripsi menggunakan metode vigenere yang di modifikasi dengan algoritma fibonancci dipilih sebagai metode dengan beban kerja ringan. Akses terhadap pesan dari aplikasi akan diamankan dengan keharusan memasukkan sandi, sehingga pesan akan aman dari pihak yang tidak berwenang. Jika dirasa keamanan masih kurang bisa ditambah kunci alternatif yang digunakan dalam enkripsi. Sehingga ketika melakukan dekripsi jika tidak mengisikan kunci alternative yang sesuai pesan tidak terdekripsi dengan sesuai sehingga informasi tidak terbaca.

Kata kunci : sms, vigenere , fibonancci, dekripsi, enkripsi.

.

ABSTRACT

The last few years, there have been rapid development in mobile phone technology. One of it is the emerging smart phone that have many features and has a complex operating system like a computer. Various operating system for mobile phones also appear, including a fairly well-known is the android. Although the smart phone has various features, old features such as Short Message Service or better known as the SMS is still favoured to use. But the current SMS features, a question arises about the security of the information contained in the text when someone wants to send confidential information by sending a SMS.

By encrypting the text in the SMS the information security level of the message can be improved. From various kinds of encryption techniques, encryption using a modified vigenere method with fibonancci algorithm chosen as a method with light workload. Access to the messages in the application will be secured by the necessity to enter a password, so the message will be safe from unauthorized parties. If it is felt need to be more secure, we can add extra security by adding a custom key for encryption. So when decrypting the message, if the custom key inserted does'nt correct. The result of the decryption is not the correct information.

Keywords: sms, vigenere, fibonancci, decryption, encryption.

1. PENDAHULUAN

1.1 LATAR BELAKANG

Beberapa tahun terakhir ini terjadi perkembangan yang pesat pada teknologi, salah satunya adalah telepon selular (ponsel). Mulai dari ponsel yang hanya bisa digunakan untuk bicara dan sms hingga "ponsel cerdas" (*smart phone*) yang memiliki berbagai fungsi seperti *multimedia*, *multiplayer games*, transfer data, video *streaming* dan lain-lain. Berbagai perangkat lunak untuk mengembangkan aplikasi ponselpun bermunculan, diantaranya yang cukup dikenal luas adalah android . Salah satu fasilitas yang disediakan ponsel adalah untuk melakukan pengiriman data berupa pesan singkat melalui *Short Message Service* (SMS). Namun dengan fasilitas SMS yang ada, timbul pertanyaan mengenai keamanan informasi jika seseorang ingin mengirimkan suatu informasi rahasia melalui fasilitas SMS. Di luar negeri pemanfaatan SMS untuk mengirim pesan rahasia telah lebih dulu dikembangkan. Misalnya di Inggris sebuah perusahaan operator telepon selular, staellium UK, mengeluarkan layanan bernama "*stealth text*" yang dapat digunakan untuk mengirim pesan dengan aman, yaitu dengan cara menghapus pesan secara otomatis segera setelah 40 detik pesan dibaca atau yang dikenal dengan nama *self-destruct text message*. Ada juga pengamanan sms dengan menggunakan kriptografi sms yang memanfaatkan kunci untuk medekripsikan sms yang telah di enkripsi

Oleh karena itu, penulis akan mencoba membuat sebuah aplikasi pengamanan sms dengan metode vigenere untuk mengenkripsi data yang berjalan pada system operasi android sehingga pemilih handphone yang berbasis android dapat melakukan pertukaran data (sms) dengan lebih aman dan nyaman.

1.2 RUMUSAN MASALAH

- Bagaimana mengimplementasikan teknologi enkripsi dan dekripsi sms pada handphone yang berbasis android dengan menggunakan metode vigenere modifikasi fibonanci

1.3 BATASAN MASALAH

- Perangkat lunak yang di bangun hanya dapat di jalankan pada ponsel yang memiliki system operasi android minimal versi 2.1
- Dua belah pihak pengguna harus sama-sama menggunakan menggunakan aplikasi ini

1.4 TUJUAN PROYEK AKHIR

- Membangkitkan kata kunci menggunakan bilangan fibonacci untuk menghilangkan perulangan kata kunci pada sandi vigenere
- Membuat aplikasi yang lebih aman untuk pertukaran data (sms) agar privasi mengguna lebih terjamin.

2. TINJAUAN PUSTAKA

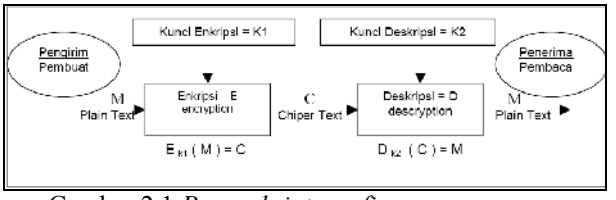
2.1 Cryptography

2.1.1 Sejarah Cryptografi

Cryptography sendiri berasal dari bahasa Yunani, dari kata Crypto, yang berarti rahasia, dan Graphein, yang berarti tulisan, sehingga kriptografi dapat didefinisikan sebagai metode untuk menyamarkan (merahasiakan) isi dari data sehingga data tidak mudah untuk dibaca oleh orang yang tidak berhak untuk membacanya.

2.1.2 Proses Kriptografi

Proses dari kriptografi dapat dijelaskan dalam gambar berikut:



Gambar 2.1 *Proses kriptografi secara umum*

Proses kriptografi diawali dengan mengubah data dalam bentuk plaintext (tulisan atau pesan awal yang dapat dibaca) menjadi chipertext(tulisan atau pesan rahasia yang tidak dapat lagi dibaca dengan mudah) dengan menggunakan algoritma yang mentransposisikan (mengubah posisi) tiiap-tiap karakter / bit pada plaintext dan dengan cara mensubstitusikan (mengganti) tiap-tiap karakter / bit pada plaintext sehingga dihasilkan tulisan atau data yang berbeda sama sekali dengan data awal. Metode pengubahan plaintext menjadi chipertext di tempat pengirim atau pembuat data dinamakan dengan Metode Enkripsi, dengan menggunakan kunci enkripsi. Di tempat penerima atau pembaca data, chipertext yang diterima kemudian diubah kembali menjadi plaintext dengan menggunakan Metode Dekripsi, yang membalikkan kembali posisi ataupun isi dari data yang diterima dalam keadaan tidak dapat dibaca, kembali menjadi data yang mudah untuk dibaca, dengan menggunakan kunci dekripsi.

2.1.3 Metode Vigenère Cipher

Vigenère cipher adalah salah satu algoritma kriptografi klasik yang diperkenalkan pada abad 16

atau kira-kira pada tahun 1986. Algoritma kriptografi ini dipublikasikan oleh seorang diplomat dan juga kriptologis yang berasal dari Prancis, yaitu Blaise de Vigenère, namun sebenarnya algoritma ini telah digambarkan sebelumnya pada buku *La Cifra del Sig. Giovan Batista Belaso*, sebuah buku yang ditulis oleh Giovan Batista Belaso, pada tahun 1553.

Cara kerja dari Vigenère cipher ini mirip dengan Caesar cipher, yaitu mengenkripsi plainteks pada pesan dengan cara menggeser huruf pada pesan tersebut sejauh nilai kunci pada deret alphabet. Vigenère cipher adalah salah satu algoritma kriptografi klasik yang menggunakan metode substitusi abjad-majemuk. Substitusi abjad-majemuk mengenkripsi setiap huruf yang ada menggunakan kunci yang berbeda, tidak seperti Caesar cipher yang menerapkan metode substitusi abjad-tunggal yang semua huruf di suatu pesan dienkripsi menggunakan kunci yang sama.

Vigenère cipher yang menerapkan metode substitusi abjad-majemuk tidak memiliki permasalahan tersebut karena setiap huruf pada pesan yang dienkripsi dengan Vigenère cipher ini akan digeser dengan nilai yang berbeda tergantung dengan kunci yang diberikan. Kunci yang digunakan pada Vigenère cipher berbeda dengan yang digunakan pada Caesar cipher. Jika pada Caesar cipher kuncinya hanya satu nilai saja, maka pada Vigenère cipher kunci yang digunakan berbentuk deretan huruf. Kunci yang berbetuk deretan kata tersebut akan memungkinkan setiap huruf plainteks untuk dienkripsi dengan kunci yang berbeda. Jika panjang kunci yang digunakan lebih pendek dari panjang plainteks maka kunci akan diulang sampai panjang kunci sama dengan panjang plainteks. Algoritma ini akan meminimalkan kemungkinan dipecahkannya cipherteks jika satu huruf plainteks diketahui**Metode Kasiski**

Friedrich Kasiski adalah orang yang pertama kali memecahkan Vigènere cipher pada Tahun 1863. Metode Kasiski membantu menemukan panjang kunci Vigenere cipher. Metode Kasiski memanfaatkan keuntungan bahwa bahasa Inggris tidak hanya mengandung perulangan huruf, tetapi juga perulangan pasangan huruf atau tripel huruf, seperti TH,THE,dsb.

Perulangan kelompok huruf ini ada kemungkinan menghasilkan kriptogram yang berulang.

Contoh1:

Plainteks : CRYPTO IS SHORT FOR CRYPTOGRAPHY

Kunci : abcdab cd abcda bcd abcdabcdabcd

Cipherteks : CSASTP KV SIQUT GQU CSASTPIUAQJB

Pada contoh ini, CRYPTO dienkripsi menjadi kriptogram yang sama, yaitu CSATP. Tetapi kasus seperti ini tidak selalu demikian, misalnya pada contoh berikut ini.

Contoh 2:

Plainteks : CRYPTO IS SHORT FOR CRYPTOGRAPHY

Kunci : abcdef ab cdefa bcd efabcdefabcd

Cipherteks : CSASXT IT UKWST GQU CWYQVRKWAQJB

Pada contoh di atas, CRYPTO tidak dienkripsi menjadi kriptogram yang sama. Mengapa bisa demikian?

Secara intuitif: jika jarak antara dua buah string yang berulang di dalam plainteks merupakan kelipatan dari panjang kunci, maka string yang sama tersebut akan muncul menjadi kriptogram yang sama pula di dalam cipherteks.

Pada Contoh 1,

- kunci = abcd
- panjang kunci = 4
- jarak antara dua CRYPTO yang berulang = 16
- jarak antara dua CRYPTO yang berulang = 16
- 16 = kelipatan 4

CRYPTO dienkripsi menjadi kriptogram yang sama∴

Pada Contoh 2,

- kunci = abcdf
- panjang kunci = 6
- jarak antara dua CRYPTO yang berulang = 16
- 16 bukan kelipatan 6

CRYPTO tidak dienkripsi menjadi kriptogram yang sama∴

Goal metode Kasiski: mencari dua atau lebih kriptogram yang berulang untuk menentukan panjang kunci.

Langkah-langkah metode Kasiski:

Temukan semua kriptogram yang berulang di dalam cipherteks (pesan yang panjang biasanya mengandung kriptogram yang berulang).

Hitung jarak antara kriptogram yang berulang.

Hitung semua faktor (pembagi) dari jarak tersebut (faktor pembagi menyatakan panjang kunci yang mungkin).

Tentukan irisan dari himpunan faktor pembagi tersebut. Nilai yang muncul di dalam irisan menyatakan angka yang muncul pada semua faktor pembagi dari jarak-jarak tersebut. Nilai tersebut mungkin adalah panjang kunci. Hal ini karena string yang berulang dapat muncul bertindihan (coincidence).

Contoh:

DYDUXRMHTVDVNQDQNWDYDUXRMHARTJGWNQD

Kriptogram yang berulang adalah DYUDUXRM dan NQD. Jarak antara dua buah perulangan DYUDUXRM adalah 18. Semua faktor pembagi 18 adalah {18, 9, 6, 3, 2} Jarak antara dua buah

perulangan NQD adalah 20. Semua faktor pembagi 20 adalah {20, 10, 5, 4, 2}. Irisan dari kedua buah himpunan tersebut adalah 2 Panjang kunci kemungkinan besar adalah 2. Setelah panjang kunci diketahui, maka langkah berikutnya menentukan kata kunci. Kata kunci dapat ditentukan dengan menggunakan exhaustive key serach. Jika panjang kunci = p, maka jumlah kunci yang harsu dicoba adalah 26p. Namun lebih mangkus menggunakan teknik analisis frekuensi. Langkah-langkahnya sbb: Misalkan panjang kunci yang sudah berhasil dideduksi adalah n. Setiap huruf kelipatan ke-n pasti dienkripsi dengan huruf kunci yang sama. Kelompokkan setiap huruf ke-n bersama-sama sehingga kriptanalis memiliki n buah "pesan", masing-masing dienkripsi dengan substitusi alfabet-tunggal (dalam hal ini Caesar cipher). Tiap-tiap pesan dari hasil langkah 1 dapat dipecahkan dengan teknik analisis frekuensi. Dari hasil langkah 3 kriptanalis dapat menyusun huruf-huruf kunci. Atau, kriptanalis dapat menerka kata yang membantu untuk memecahkan cipherteks Contoh:

LJVBQ STENZ LQMED LJVMA MPKAU FAVAT LJVDA YYVNF JQLNP LJVHK VTRNF LJVCM LKETA LJVHU YJVSF KRFTT WEFUX VHZNP
Kriptogram yang berulang adalah LJV.
Jarak LJV ke-1 dengan LJV ke-2 = 15
Jarak LJV ke-2 dengan LJV ke-3 = 15
Jarak LJV ke-3 dengan LJV ke-4 = 15
Jarak LJV ke-4 dengan LJV ke-5 = 10
Jarak LJV ke-5 dengan LJV ke-6 = 10
Faktor pembagi 15 = {3, 5, 15}
Faktor pembagi 10 = {2, 5, 10}
Irisan kedua himpunan ini = 5. Jadi, panjang kunci diperkirakan = 5 Kelompokkan "pesan" setiap kelipatan ke-5

2.3 Bilangan Fibonacci

Seiring berjalanya waktu maka kemampuan kriptoanalis pun berkembang,sampai akhirnya vinenere chipper yang memiliki predikat sandi terkut pada masa itu pun dapat di runtuhkan oleh metode kasiski.Dengan metode kasiski ,dapat di ketahui bahwa kelemahan vigenere chipper ini terdapat pada kunciny.karna jika kunci lebih pendek dari pada plaintextnya akan menimbulkan perulangan kata kunci sampai panjang kuncinya sama dengan plantextnya.Pada kali ini penulis akan mengadaptasi bilangan Fibonacci untuk membangkitkan karakter dari mulai panjang kunci di tambah satu sampai sepanjang plantextnya sehingga tidak terjadi perulangan kunci Formulanya sebagai berikut :

U(n)−U(n-1)+U(n-2)
Keterangan :
U − karakter yang dicari
n = urutan karakter yang dicari

Gambar 2.3 *Rumus fibonnanci*

Namun jika hanya di modifikasi seperti itu ,akan rentan dilakukan penebakan terhadap plaintextnya,sehingga pada hal ini ,urutan Fibonacci tersebut dilakukan modifikasi menjadi :

Un = U(n-k)+U(n-k+m)
Keterangan : Un= karakter kunci ke-n ,
k =panjang kunci masukan

m= 1 +(∑ (karakter_tiap_kunci)mod(k-1))

m adalah variable penambahan dalam pembangkitan kunci di mana m bersifat dinamis karena akan menyesuaikan dengan panjang kunci yang dimasukan .Kunci yang di masukan minimal terbentuk dari dua karakter. Dengan menggunakan variable m ini rumus di atas akan lebih dinamis ,sehingga urutan yang di jumlahkan

Contoh : Kunci masukan :INIKUNCI
K=8,m= 1+((8+13+8+10+20+13+2+8)mod7)=6
Sehingga : U9=U1+U7=I(8) + C(2)=K(10 mod 36)

U10=U2+U8=N(13)+I(8)=V(21 mod36)
U11= U3+U9=I(8)+K(10) = S(18 mod 36)
U12= U4+U10 = K(10)+V(21)=F(31 MOD 36)

Dan selanjutnya sampai U (panjang plaintext)
Plaintext : SAYA SUKA KRIPTOGRAFI
Kunci : INIK UNCI KVSFMSOAYVQ
Chippertext : ANGK MHMI UMAUFGURYAY

2.4 Android

2.4.1 Sejarah Android

Android adalah sistem operasi untuk telepon seluler yang berbasis Linux. Android juga menyediakan platform terbuka bagi para pengembang guna menciptakan aplikasi mereka sendiri untuk digunakan oleh bermacam peranti bergerak. Android merupakan sebuah sistem operasi untuk telepon seluler seperti halnya Symbian pada Nokia, Palm dan Windows Mobile yang sebelumnya sudah terlebih dahulu kita kenal selama ini.

Sistem Android dipakai di telepon pertama kali pada tanggal 22 Oktober 2008 untuk HTC Dream. Pada beberapa bulan kemudian di tahun berikutnya Operating System Android sudah banyak sekali dipakai oleh berbagai jenis telepon celullar.

Android disebut sebagai OS yang kuat, cepat dan juga sangat baik.

3.PERANCANGAN SISTEM

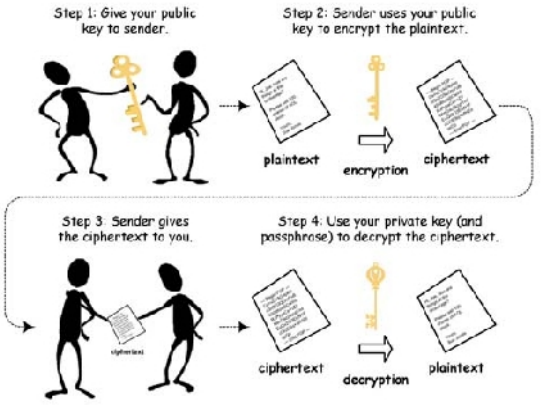
Perancangan sistem ini terdiri atas beberapa tahap yang akan diuraikan pada sub bab di bawah ini.

3.1 Perancangan Data

Dalam bab ini akan dibahas mengenai langkah – langkah dalam perancangan sistem dalam pembuatan aplikasi tugas akhir beserta penjelasan di tiap tahapnya.

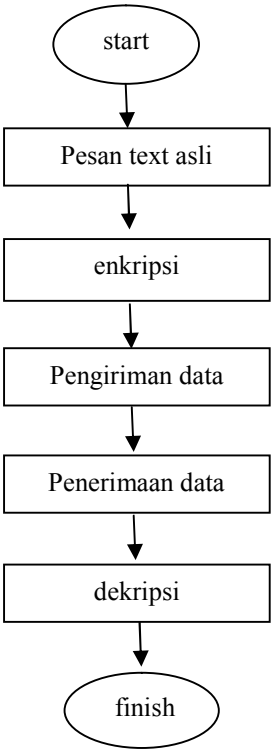
3.1 Perancangan Sistem

Dalam perancangan sistem pembuatan aplikasi tugas akhir ini karena aplikasinya sederhana maka tidak dibutuhkan suatu kondisi yang terlalu rumit. Secara umum gambaran sistem adalah pengirim pesan dapat mengenkrip pesan yang akan dikirim melalui layanan sms.. Karena pesan yang diterima dalam keadaan terenkrip, maka harus ada pendekrip pesan supaya pesan aslinya bisa dibaca oleh penerima pesan. Sehingga pada handphone receiver(penerima) harus dibuat program pendekrip. Untuk lebih jelasnya dapat dilihat pada sketsa pengiriman sms pada gambar di bawah ini :



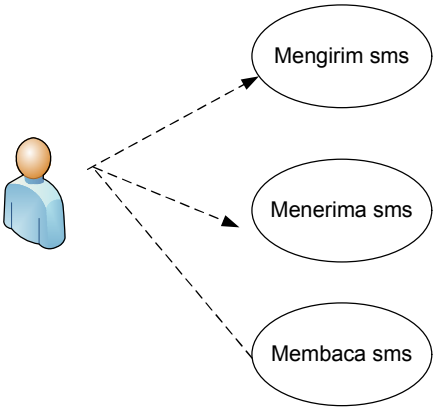
Gambar 3.1 *proses encrypt-decrypt*

Gambar di atas merupakan gambaran kasar cara kerja sistem perangkat lunak pada tugas akhir ini. Cara kerja sistem akan dibagi-bagi lagi ke dalam beberapa tahapan proses supaya dapat dilihat dengan lebih jelas. Tahapan prosesnya dibagai menjadi 8 tahap sebelum tercipta sebuah system yang nantinya bisa mengirim pesan via sms dengan menggunakan enkripsi. Jika digambarkan dalam bentuk diagramnya akan tampak seperti pada gambar berikut :



Sebelum melakukan pengiriman sms, pesan dapat dienkripsiKemudian sms dikirim dan diterima oleh handphone penerima. Agar dapat dibaca oleh penerima, maka harus dilakukan proses kebalikannya yaitu jika dienkripsi maka dilakukan dekrip setelah itu sms baru dapat dibaca sesuai pesan aslinya.

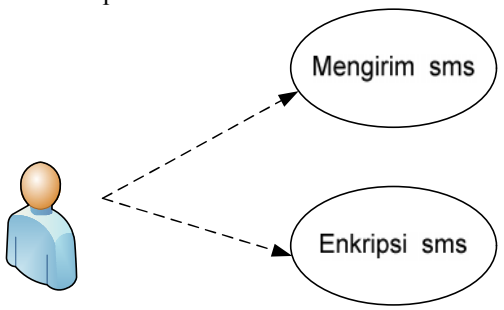
Setelah aplikasi dibuka, untuk menulis pesan maka pilih menu tulis SMS. Setelah semua selesai diketikkan, pengguna dapat memilih menu Kirim untuk langsung mengirim SMS, menu enkrip untuk enkripsi pesan.



Gambar 3.2 *Use Case Utama*

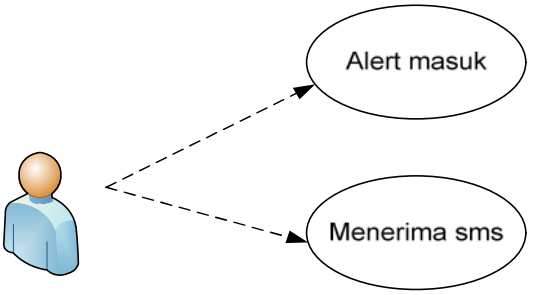
Use Case di atas menggambarkan bahwa pengguna mengetik pesan pada teksbox yang nantinya akan diambil karakter-karakter yang ada di dalamnya. Kemudian pesan akan diterima oleh nomor yang dituju. Penerima dapat membaca pesan secara normal jika memiliki aplikasi yang sama.

Untuk lebih jelasnya akan dilakukan penjelasan pada tahapan proses selanjutnya. Sebelum pengirim mengirimkan pesan maka pada saat selesai mengetik pesan, pengirim bisa melakukan enkripsi baru mengirim pesan tersebut. Penjelasan secara detail dapat dilihat pada *UseCase* di bawah



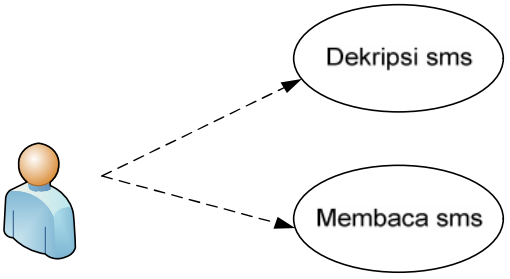
Gambar 3.3 *Use Case Kirim*

Pada proses selanjutnya, setelah pengirim mengirimkan pesannya maka pada aplikasi yang ada pada penerima akan ada pemberitahuan berupa *alert* masuk. Saat terdapat alert masuk, pesan akan secara otomatis tersimpan pada penampung sms android lalu aplikasi akan mengakses pesan ini ketika akan di dekripsi pada *inbox*. Untuk lebih jelasnya dapat dilihat pada gambar *UseCase* di bawah ini :



Gambar 3.4 *Use Case Alert*

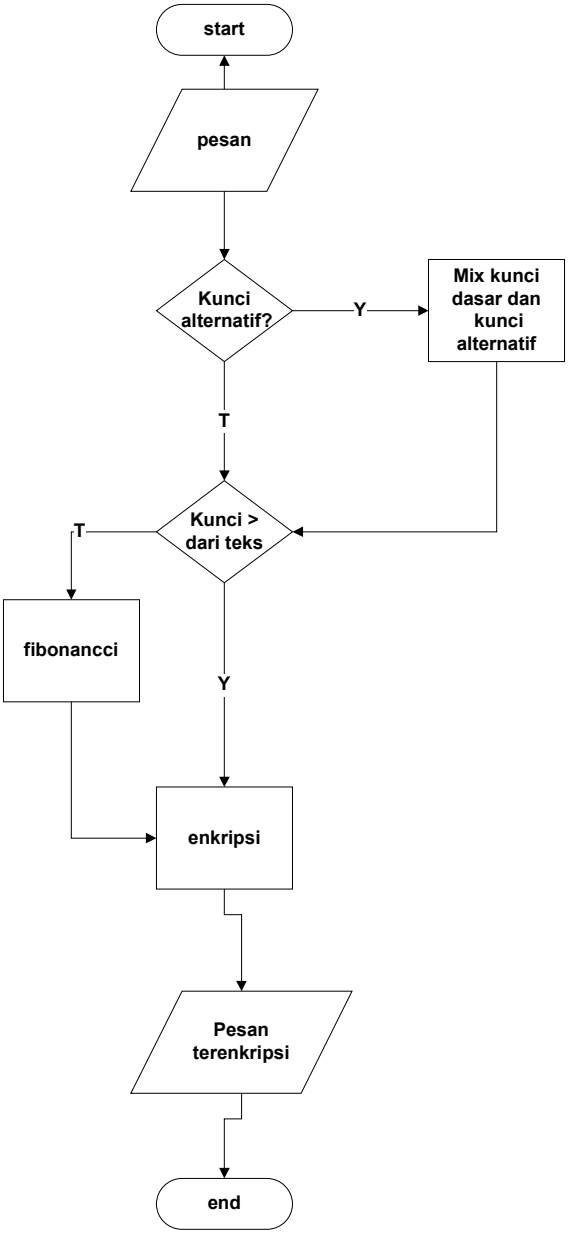
Pesan dapat dibaca melalui menu kotak pesan dan dapat memilih pesan yang spesifik untuk dilakukan dekripsi. Untuk lebih jelasnya dapat dilihat pada gambar *UseCase* di bawah ini :



Gambar 3.5 UseCase Terima

3.1.1 Enkripsi SMS

Proses enkripsi dilakukan dengan metode vigenere di tambah dengan metode bilangan fibonancci. Sedangkan kunci yang digunakan sebagai acuan dalam melakukan enkripsi vingeneri adalah kunci yang di tetapkan di dalam aplikasi dan bisa diubah dengan menambahkan kunci alternatif. Ketika panjang pesan lebih panjang dari pada panjang kunci maka kunci akan di tambah dengan metode fibonancci untuk melakukan enkripsi sehingga tidak ada perulangan kunci untuk menutupi kelemahan algoritma vigenere.



3.1.2 Fibonannci

Fibonancci di gunakan pada saat panjang plaintext(pesan) lebih panjang dari pada kunci yang di tetapkan , Dilakukan dengan cara membangkitkan

karakter kunci dari mulai panjang kunci di tambah satu sampai sepanjang plantextnya sehingga tidak terjadi perulangan kunci Formulanya sebagai berikut:

U(n)=U(n-1)+U(n-2)
Keterangan :
U = karakter yang dicari
n = urutan karakter yang dicari

Gambar.3.6 *Rumus fibonancci asli*

Namun jika hanya di modifikasiseperti itu ,akan rentan dilakukan penebakan terhadap plaintextnya, sehingga dalam hal ini, urutan Fibonacci tersebut dilakukan modifikasi menjadi :

Un = U(n-k)+U(n-k+m)

Keterangan : Un= karakter kunci ke-n , k =panjang kunci masukan

m= 1 +(∑ (karakter_tiap_kunci)mod(k-1))

m adalah variable penambahan dalam pembangkitan kunci di mana m bersifat dinamis karena akan menyesuaikan dengan panjang kunci yang dimasukan. Kunci yang di masukan minimal terbentuk dari dua karakter. Dengan menggunakan variable m ini rumus di atas akan lebih dinamis, sehingga urutan yang di jumlahkan.
Contoh : Kunci masukan :INIKUNCI

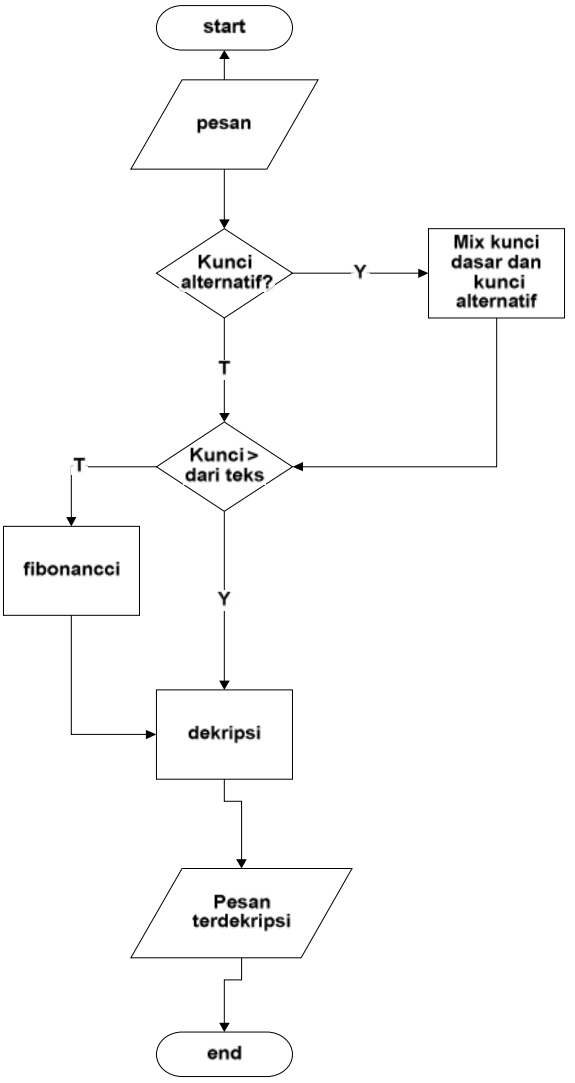
K=8,m= 1+((8+13+8+10+20+13+2+8)mod7)=6

Sehingga :
U9=U1+U7=I(8) + C(2)=K(10 mod 36)
U10=U2+U8=N(13)+I(8)=V(21 mod36)
U11= U3+U9=I(8)+K(10) = S(18 mod 36)
U12= U4+U10 = K(10)+V(21)=F(31 MOD 36)

Dan selanjutnya sampai U (panjang plaintext)
Plaintext : SAYA SUKA KRIPTOGRAFI
Kunci : INIK UNCI KVSFMSOAYVQ
Chippertext : ANGK MHMI UMAUFGURYA

3.1.3 Dekripsi

Dekripsi dilakukan dengan cara melakukan pengecekan apakah ada kunci alternatif yang di berikan. Jika ada maka kunci dasar akan di gabung dengan kunci alternative yang di berikan. Lalu di cek panjang kunci dengan teks yang terenkripsi, jika panjang kunci lebih panjang dari pada panjang teks yang terenkripsi maka di lakukan proses fi bonancci sehingga panjang kunci sama dengan panjang teks yang terenkripsi lalu dilakukan dekripsi dengan menggunakan kunci yang baru terbentuk.
Berikut penjelasan flowchartnya :



4.HASIL DAN ANALISA

Kalimat	*Key Tambahan*	*Jumlah karakter sebelum di enkripsi*	*Jumlah kAarakter sesudah di enkripsi*	*Pembengkakan karakter*
perc0b@@n mengguku r jumlah kar4kter?!	-	*36*	*36*	*0%*
perc0b@@n mengguku r jumlah kar4kter?!	√	*36*	*36*	*0%*
Kriptografi adalah	-	*18*	*18*	*0%*
Kriptografi adalah	√	*18*	*18*	*0%*

***Tabel 4.1** Tabel hasil percobaan*

.

Pada percobaan di hasilkan kesimpulan bahwah jumlah karakter plaintext sebelum dan sesudah di encryption berjumlah sama.

4.2.2 Analisa Perulangan yang terjadi berdasarkan metode pembangkit kunci

Ujicoba ini digunakan untuk mengukur tingkat perulangan kata pada hasil enkripsi yang murni menggunakan vingenere dan yang menggunakan vingenere yang kuncinya telah di modifikasi dengan metode fibonancci .Tujuan dari ujicoba ini adalah untuk mengetahui seberapa efektifkah pengaruh dari Metode fibonancci yang menutupi kekurangan dari vingenere murni yang mampu di tembus oleh metode kasiski dengan menemukan karakter berulang pada hasil enkripsi. Jika Menggunakan vigenere saja ketika ada perulangan kata pada plaint text di mungkinkan hasil encryptnya juga berulang seperti tampilan berikut :

Plaintext :
CRYPTO IS SHORT FOR **CRYPTO**GRAPHY

Kunci :
abcdab cd abcda bcd **abcdab**cdabcd

Cipherteks :
CSASTP KV SIQUT GQU **CSASTP**IUAQJB

Kalimat	*Metode*	*Jumlah karakter yang berulang Pada palintext*	*Jumlah karakter yang berulah Setelah di encrypt*	*Prosentase Karakter berualang*
CRYPTO IS SHORT FOR CRYPTOGRAPHY	***VINGENERE***	***8***	***8***	***8/32= 0,25%***
CRYPTO IS SHORT FOR CRYPTOGRAPHY	***VINGENERE FIBONACCI***	***8***	***0***	***0/32 0%***
CRYPTO IS SHORT FOR CRYPTOGRAPHY	***VIGENERE FIBONANCCI KEY TAMBAHAN***	***8***	***0***	***0/32 0%***

Pada hasil percobaan di atas membuktikan bahwa dengan fibonancci ataupun fibonannci dengan key tambahan menghilangkan kelemahan dari vigenere dimana jika ada kata yang di ulang maka akan menimbulkan hasil enkripsi yang memiliki kata yang berulang juga .

5. KESIMPULAN

Berdasarkan hasil percobaan pada bab sebelumnya, maka dapat disimpulkan bahwa :

1. Jumlah Karakter yang di enkripsi sesudah dan sebelumnya adalah sama banyaknya.
2. Enkripsi menggunakan Vigenere yang telah di modifikasi dengan fibonancci dan key tambahan dapat menghilangkan kelemahan metode vigenere yang dapat di tembus oleh metode kasiski melalui karakter yang berulang
3. Dengan memberikan kunci tambahan keamanan dan privasi pengguna lebih terjamin.

SARAN

Berikut merupakan beberapa saran yang dapat digunakan untuk pengembangan aplikasi kedepannya :

1. Menambahkan notifikasi pada aplikasi ketika menerima sms baru untuk mempercepat dekripsi.
2. Memberikan alternative pembuka aplikasi selain kunci pola
3. Memberikan pilihan untuk mengubah tema aplikasi.

6.DAFTAR PUSTAKA

1. Rick Rogers, John Lombardo, Zigurd Mednicks, Blake Meike. 2009. *Android Application Development.* Sebastopol: O'Reilly Media Inc

2. Nazruddin Safaat H .2011.Pemograman Android Mobile SmartPhone dan Tablet Pc Berbasis Android :Bandung .INFORMATIKA

3. (http://developer.android.com/guide/index html)

4. http://web.si.its-sby.edu/kurikulum/materi/alpro/pengantarjava.html