Implementasi Algoritma One Time Pad (OTP) untuk Pengamanan Pesan Short Message Service (SMS)

Muhammad Iqbal Batubara
STMIK Budi Darma Medan, Jl. Sisingamangaraja No. 338 Sp. Limun, Sumatera Utara, Indonesia
E-Mail : iqbalbatubara.budidarma@gmail.com

ABSTRACT

The operating system for mobile devices is growing. Android is a mobile operating system that is now very popular and widely used by people. Android is also a software-based operating system that can be developed in open source so that many developers are now participating in developing applications for Android. For the purposes of security aspects, Android also has provided specifically for cryptographic functions, such as encryption, description, and so on. Message message service (SMS) is a very popular communication technology. By using SMS someone can exchange information. In this case the SMS sent will be encrypted in the development of an Android-based cell phone program for sending SMS messages. The test results show that the use of the One Time Pad (OTP) algorithm can encrypt short messages with text to the destination number. The application can help users to send short messages in a safe, fast, and easy place.

Keywords: Android, encryption, description, cryptography, One Time Pad (OTP) algorithm

PENDAHULUAN

Perkembangan teknologi dibidang komunikasi semangkin tahun semangkin maju. Salah satunya adalah telepon seluler *(ponsel)* dengan banyak fitur dan juga memiliki sistem yang sama dengan komputer. Banyak jenis software untuk mengembangkan sebuah aplikasi ponsel pun tercipta, diantaranya yang cukup dikenal luas adalah *android.* Pada umumnya fasilitas yang disediakan ponsel adalah kebutuhan pengiriman pesan melalui *Short Message Service* (SMS). Umumnya manusia lebih sering menggunakan layanan SMS dibanding layanan telepon kerena biaya yang dipakai realtif mudah dan mudah digunakan [1].

Dengan semakin mudahnya bertukar informasi tanpa batasan jarak dan waktu, dalam menjaga kerahasiahan pesan dibutuhkan teknik dalam mengamankan informasi yang khususnya yang sifatnya penting atau rahasia dengan melakukan enkripsi pesan SMS sebelum dikirim ke tujuan, maka tingkat keamanan informasi dari pesan tersebut dapat dijamin.

Dalam mengatasi permasalahan pengiriman pesan, penulis mencoba membuat pengamankan pesan dengan algoritma *one time pad* untuk mengenkripsi pesan yang berjalan pada sistem operasi *android* sehingga pemilik telepon seluler (ponsel) yang berbasis *android* dapat melakukan pertukaran pesan dengan lebih aman dan nyaman. *One-time pad* terdiri dari deretan karakter-karakter kunci yang akan dibangkitkan secara acak. Sebuah algoritma disebut aman, apabila tidak ditemukan cara untuk menemukan *plaintext*-nya. *Algoritma One Time Pad (OTP)* dinyatakan sulit untuk dipecahkan meskipun diberikan sumber daya yang tinggi. *Algoritma One Time Pad* merupakan jenis algorima simetri yang konvensional dan dalam kriptografi disebut metode Algoritma Vernam yang merupakan jenis teknik kriptografi yang tergolong dalam algoritma klasik dan sederhana, namun cukup handal dan bahkan oleh beberapa orang menganggap sulit untuk dipecahkan dalam kondisi tertentu[2] .

Berdasarkan uraian masalah pada latar belakang di atas, maka yang menjadi rumusan masalah penelitian ini adalah :

1. Bagaimana proses *enkripsi* dan *dekripsi* pengamanan pesan?
2. Bagaimana mengimplementasikan algoritma *one time pad* (OTP) untuk mengamankan pesan teks?
3. Bagaimana merancang aplikasi pengamanan pesan teks berbasis *android*?

Batasan masalah dalam penelitian ini adalah Panjang kunci harus sama dengan panjang *plainteks* yang akan dienkripsikan, Batas maksimal ukuran *plainteks* 128 karakter dalam bentuk abjad, angka, dan simbol, aplikasi ini dapat berjalan minimal di sistem operasi versi *Android* 2.3, dan dalam merancang sistem menggunakan *software eclipse*. Manfaat dari penelitian ini adalah memberikan pengamanan pesan pada teks secara rahasia dapat mencegah pihak ketiga yang ingin dengan sengaja memonitor aktivitas pesan yang dikirimkan, terutama bagi para

pebisnis maupun individual yang tidak ingin informasi pentingnya bocor, Mencegah pencurian dan penyalahgunaan pesan teks pada ponsel agar tidak bisa dilihat oleh orang lain.

METODE PENELITIAN

Metode penelitian adalah susunan tahapan-tahapan yang akan dikerjakan oleh peneliti mulai dari perumusan masalah sampai penarikankesimpulan, dan membentuk sebuah diagram alur yang sistematis [3]. Metodologi penelitian ini digunakan sebagai acuan peneliti dalam pelaksanaan penelitian agar hasil yang didapat tidak sesuai dari tujuan yang telah ditentukan sebelumnya.

Metode penelitian ini terdiri dari :

1. Studi literatur
   Metode ini dilaksanakan melakukan studi yang relavan serta buku-buku maupun artikel-artikel yang didapatkan baik di perpustakaan ataupun melalui daring.
2. Analisa
   Dalam menganalisa dijelaskan objek-objek yang terlibat dalam domain masalah yaitu pesan SMS dan pengamanan SMS dan bagaimana interaksi terjadi antara objek tersebut, Objek dalam analisa adalah objek dari perspektif dunia nyata yang bakal diimplementasikan oleh bahasa pemograman.
3. Perancangan
   Merancang sistem atau aplikasi pengamanan pesan SMS berbasis android sebelum dilakukan implementasi dengan menggunakan algoritma One Time Pad untuk teknik pengamanan.
4. Implementasi
   Dalam implementasi ini maka dilakukan pengujian dan pengetesan terhadap hasil rancangan.

LANDASAN TEORI

3.1. Keamanan

Keamanan data telah menjadi bagian dari pengembangan teknologi informasi mengingat bahwa berjuta-juta bit informasi telah dipertukarkan dalam jaringan komputer terutama di internet. Masalah keamanan data dapat diklasifikasi ke dalam beberapa dimensi[4]. Sebuah situs yang menggeluti bidang komersial misalnya harus memenuhi persyaratan berikut ini:

1. ***Secrecy***: kategori kemanan yang meliputi perlindungan data/informasi dari akses oleh pihak-pihak yang tidak berhak serta menjaga masalah keaslian (autentik) dari sumber data/informasi. Masalah *secrecy* juga berhubungan dengan proses enkripsi-dekripsi serta proses autentikasi.
2. ***Integrity***: kategori keamanan data yang menjamin bahwa data tidak ada gangguan selama proses *transfer* dari sumber ke tujuan melalui saluran komunikasi. masalah *integrity* berkaitan dengan perlindungan data dari penyusup yang berusaha masuk ke sumber data, atau menyusup ke dalam jaringan data, dengan tujuan untuk mengubah dan merusak, termasuk virus yang bisa menghancurkan data juga akan menjadi bagian dari sebuah *integrity*.
3. ***Availability***: kategori keamanan data yang mempertahankan sumber informasi agar selalu siap sedia dan aktif dalam melayani para pengguna. Masalah *availability* juga berkaitan dengan usaha untuk melindungi server dari gangguan yang menyebabkan *server* bermasalah memberi pelayanan.

3.2. Kriptografi

Kata kriptografi berasal dari bahasa Yunani, "*kryptós*" artinya *"secret"* (rahasia) sedangakan "*graphein*" artinya "*writing"* (tulisan). Jadi, kriptografi berarti *"secret writing*" (tulisan rahasia). Beberapa defenisi dari kriptografi telah dikembangkan di dalam berbagai *literatur*. Kriptografi adalah sebuah ilmu dan seni dalam menjaga kerahasian sebuah pesan dengan cara menyandikan ke dalam bentuk yang sulit dimengerti maknanya. Defenisi ini cocok digunakan untuk menjaga keamanan komunikasi seperti komunikasi di kalangan militer, diplomat, atau mata-mata. Saat ini kriptografi lebih dari sekedar *privacy,* tetapi juga demi tujuan data *integrity, authentication,* dan *non-repudiation*. Cara unik yang mungkin berbeda pada setiap pelaku kriptografi sehingga setiap menulis sebuah pesan rahasia harus mempunyai nilai estetika tersendiri. Kriptografi berkembang dan menjadi sebuah seni dalam merahasiakan pesan (kata "*graphy*" di dalam "*cryptography*" sangat menyiratkan sebuah kegiatan dalam bidang seni. Kriptografi dapat diformulasikan secara matematis sehingga melahirkan sebuah metode yang formal[5], [6].

Dalam kriptografi sering menemukan berbagai istilah atau *terminology*. Beberapa istilah yang harus diketahui yaitu :

1. Pesan, plaintext, dan cipherteks
   Pesan (*message*) adalah data atau informasi yang dapat dibaca juga dimengerti maknanya oleh umum. Nama lain untuk pesan adalah *plaintext* atau teks nyata. Agar pesan tidak dapat lagi dibaca atau dimengerti maknanya oleh orang lain yang tidak ada kepentingan, maka pesan harus disandikan ke bentuk pesan lain yang tidak

dipahami. Bentuk pesan yang sudah tersandi disebut *cipherteks (ciphertext*) atau kriptogram *(cryptogram). Cipherteks* wajib harus dapat ditransformasikan kembali ke bentuk plaintext semula agar dapat diterima dan bisa dibaca.

2. Pengirim dan penerima
   Komunikasi data akan melibatkan pertukaran pesan antara dua objek. Pengirim adalah objek yang mengirim pesan kepada objek lainnya. Penerima adalah objek yang akan menerima pesan. Pengirim tentu akan menginginkan pesan terkirim secara aman, dimana pengirim yakin bahwa pihak lain tidak dapat membaca isi pesan yang akan dikirimkannya. Solusinya adalah dengan cara merubah pesan asli atau menyandikan pesan menjadi *cipherteks.*
3. Enkripsi dan dekripsi
   Proses penyandian plainteks menjadi sebuah *cipherteks* disebut *enkripsi (encryption).* Sedangkan proses mengembalikan *cipherteks* menjadi pesan asli atau *plainteks* disebut proses *dekripsi (decryption)*.
4. Cipher dan kunci
   Cipher yaitu aturan atau metode untuk melakukan enkripsi dan dekripsi, harus menggunakan fungsi matematika dalam proses enkripsi dan juga proses dekripsi. Beberapa cipher akan memerlukan algoritma yang tidak sama dalam *enciphering* dan deciphering. Konsep matematis yang mendasari sebuah algoritma kriptografi adalah tentang relasi antara dua buah himpunan yang berisi elemen plainteks dan himpunan yang berisi *cipherteks*. Enkripsi dan dekripsi merupakan fungsi yang memetakan elemen-elemen tersebut antara dua himpunan tersebut.
   Misalkan P menyatakan plainteks dan C menyatakan *cipherteks*, maka fungsi enkripsi E memetakan P ke C.
   E(P) = C
   Dan fungsi dekripsi D memetakan C ke P
   D(C) = P
   Berhubung proses enkripsi yang kemudian didekripsi yakni mengembalikan pesan ke pesan semula, maka kesamaan berikut harus benar, D(E(P)) = P Kriptografi akan mengatasi masalah keamanan data dengan menggunakan sebuah kunci, dalam hal ini algoritma tidak saatnya dirahasiakan lagi, tetapi kuncinya wajib dan harus tetap dijaga kerahasiaannya. Kunci *(key*) adalah sebuah parameter yang digunakan untuk transformasi *enciphering* dan deciphering[4][7]. Kunci biasanya berbentuk string atau deretan bilangan. Dengan menggunakan variabel K, maka fungsi enkripsi dan *dekripsi* dapat disajikan sebagai :
   $E_K(P)=C$ dan $D_K(C)=P$
   Dan kedua fungsi ini memenuhi
   $D_K(E_K(P))=P$ Keterangan :
   P = *plainteks*
   C = *cipherteks*
   K = kunci
   EK = proses enkripsi menggunakan kunci K
   DK = proses dekripsi menggunakan kunci K
5. Sistem kriptografi
   Membentuk sebuah sistem yang dinamakan system Kriptografi. Sistem kriptografi(*cryptosystem*) adalah kumpulan yang terdiri dari algoritma kriptografi, semua *plainteks* dan *cipherteks* yang mungkin, dan kunci. Di dalam kriptografi, *cipher* hanyalah salah satu komponen saja.
6. Penyadap
   Penyadap *(eavesdropper*) adalah orang yang berusaha mencoba menangkapdan mengambil pesan selama proses transmisi. Tujuan penyadap adalah tentu untuk mendapatkan semua informasi yang sebanyak-banyaknya mengenai sistem dan teknik kriptografi yang digunakan untuk berkomunikasi dengan maksud dan tujuan untuk memecahkan cipherteks.
   Nama lain penyadap : *enemy, adversary, intruder, interceptor, bad guy*.
7. Kriptanalisis dan kriptologi
   Kriptografi berkembang terus sehingga melahirkan bidang yang berlawanan yaitu *kriptanalisis. Kriptanalisis (cryptanalysis)* adalah sebuah ilmu dan seni untuk memecahkan *cipherteks* menjadi *plainteks* tanpa harus mengetahui kunci yang digunakan. Jika seorang kriptografer *(cryptographer*) mentransformasikan sebuah *plainteks* menjadi cipherteks dengan suatu algoritma dan kunci maka sebaliknya sudah pasti seorang kriptanalis berusaha untuk memecahkan *cipherteks* tersebut dengan tujuan menemukan plainteks atau kunci. Kriptologi (*cryptology*) adalah bidang ilmu dan studi mengenai kriptografi dan kriptanalisis. Baik kriptografi maupun kriptanalisis adalah objek yang saling berkaitan. (Munir, 2006:8)

3.3. Algoritma One Time Pad

Kriptografer sering disebut bahwa cipher yang dirancang tidak akan dapat dipecahkan. Saat ini sudah banyak terlihat bahwa *cipher subsititusi* (dengan segala versinya) dan cipher

transposisi pada akhirnya dapat dipecahkan juga. Kasus Queen Mary pada abad 18 dan Enigma pada PD II adalah pelajaran betapa klain *unbreakable cipher* sangat mudah dipatahkan[8].

Algoritma kriptografi sempurna aman dan tidak dapat dipecahkan adalah one time pad, secara matematis Shannon telah membuktikan bahwa OTP sulit dan tergolong tidak dapat dipecahkan. OTP ditemukan di tahun 1917 oleh Vernam dengan menggunakan deretan karakter-karakter kunci yang berisi huruf-huruf yang tersusun secara acak. Satu pad hanya boleh digunakan sekali (*one-time*) saja untuk mengenkripsi pesan, setelah itu pad yang telah digunakan wajibdan harus dihancurkan supaya tidak dapat dipakai kembali untuk mengenkripsi pesan lainnya. Aturan enkripsi yang digunakan sama persis seperti pada algoritma *Vigenere cipher*. Pengirim pesan menggunakan setiap karakter kunci untuk mengenkripsikan satu karakter plainteks. Enkripsi dapat dinyatakan sebagai penjumlahan modulo 26 dari satu karakter plainteks dengan satu karakter kunci one time pad [2].

$C1 = (p1+k1) \bmod 26$ . . . . . (I)

Yang dalam hal ini , *P1* adalah planteks ke-i, k*1* adalah huruf kunci ke-i. Panjang kunci harus dan wajibsama dengan panjang plainteks, untuk menjaga tidak ada kebutuhan mengulang penggunaan kunci selama proses enkripsi. Setelah sipengirim mengenkripsikan pesannya dengan kunci, pengirim wajib menghancurkan kunci tersebut. Penerima pesan menggunakan kunci yang sama untuk mendekripsikan karakter-karakter cipherteks menjadi karakter-karakter plainteks dengan persamaan.

$P1 = (c1+k1) \bmod 26$ . . . . . (II)

Meskipun OTP merupakan cipher yang aman, namun faktanya OTP tidak sering digunakan secara universal dalam sebuah aplikasi kriptografi sebagai satu-satunya sistem cipher yang tidak dapat dipecahkan (hanya sedikit sistem komunikasi yang menggunakan metode OTP). Alasan mengapa OTP tidak sering digunakan adalah segi kepraktisan, yaitu:

1. Disebabkan panjang kunci harus sama dengan panjang pesannya, maka OTP hanya cocok untuk pesan berukuran skala kecil. Semakin besar ukuran pesan maka sudah pasti semakin besar pula ukuran kuncinya. Pada aplikasi kriptografi dalam mengenkripsikan data yang tersimpan, timbul masalah dalam penyimpanann kunci pada aplikasi kriptografi untuk komunikasi pesan, dan akan timbul masalah dalam pendistribusian kunci.
2. Disebabkan kunci yang dibangkitkan secara acak, maka tidak mungkin pengirim dan penerima membangkitkan kunci yang sama secara bersamaa dan secara simultan. Jadi, salah seorang dari mereka harus membangkitkan kunci lalu mengirimkannya ke pihak penerima.

Kerena kerahasiaan kunci sebuah pesan harus dijamin, maka perlu ada perlindungan selama proses pengiriman kunci. Jika hanya ada satu saluran komunikasi maka pengirim dan penerima pesan membutuhkan barisan kunci yang lain untuk melindungi kunci lain.

ANALISA DAN PEMBAHASAN

4.1. Analisa

Analisa masalah bertujuan untuk menguraikan dan menyelesaikan permasalahan yang ada pada sistem aplikasi. Analisis ini diperlukan sebagai dasar bagi tahapan perancangan sistem. Analisis sistem meliputi identifikasi permasalahan, analisis sistem, analisis kriptografi, analisis proses *enkripsi*, analisis proses *dekripsi.*

Aplikasi Kriptografi SMS digunakan dalam pengiriman pesan baik secara pesan yang terenkripsi ataupun pesan yang tidak terenkripsi. Dalam mengirim sebuah pesan yang terenkripsi, maka aplikasi ini harus mengenkripsi terlebih dahulu sebauh pesan menjadi *chipertext* kemudian dikirim ke penerima dan penerima melakukan proses dekripsi pesan yang diterima menjadi *plainteks.* Untuk memudahkan operasionalnya huruf-huruf harus diterjemahkan dulu ke dalam angka 1 sampai 26 dengan A = 1; B = 2; dst sampai Z = 26 agar bisa melakukan perhitungan aljabarnya berupa bilangan modulus 26.

Metode enkripsi *one-time pad* memiliki sifta yaitu dimana kunci yang digunakan hanya akan diketahui oleh pengirim dan penerima informasi / pesan saja, kunci yang dibuat dengan menggunakan PRNG (*Pseudo-Random Number Generator*) adalah bersifat acak, meskipun keadaan proses pembuatan kunci boleh diketahui, juga panjang kunci yang wajib sama dengan panjang pesan, dan kunci hanya digunakan untuk satu kali proses *enkripsi.*

4.2. Pembahasan

One Time Pad termasuk dalam kelompok kriptografi simestri. *One-time pad* (*pad* = kertas bloknot) berisi deretan karakter-karakter kunci yang dibangkitkan secara acak. *Cipher* ini diimplementasikan melalui sebuah kunci yang terdiri dari sekumpulan *random* karakter-karakter yang tidak berulang. Setiap huruf kunci dijumlahkan *modulo* 26 dengan huruf

pada *plaintext.* Pada *One Time Pad*, panjang *stream* karakter kunci sama dengan panjang pesan. Aslinya, satu buah *one time pad* adalah sebuah pita (*tape*) yang berisi barisan karakter-karakter kunci. Satu *pad* hanya digunakan sekali (*one time*) saja untuk mengenkripsi pesan, setelah itu pad yang telah digunakan dihancurkan supaya tidak dipakai kembali untuk *mengenkripsi* pesan yang lain.

Enkripsi dapat digambarkan sebagai penjumlahan *modulo* 26 dari satu karakter plainteks dengan satu karakter kunci *one time pad*. Setelah pengirim mengenkripsikan pesan dengan *one time pad*, ia menghancurkan *one time pad* tersebut (makanya disebut satu kali pakai atau *one time*). Penerima pesan menggunakan one time pad yang sama untuk mendekripsikan karakter-karakter *cipherteks* menjadi karakter-karakter plaintek dengan persamaan.

Deretan Abjad
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
0 1 2 3 4 5 6 7 8 9 10 11 12
13 14 15 16 17 18 19 20 21 22 23 24
25

a. Proses Enkripsi Pesan SMS

Dalam proses enkripsi pesan teks dalam One Time Pad, *cipherteks* diperoleh dengan melakukan penjumlahan modulo 26 dari satu bit *plainteks* dengan satu bit kunci, seperti terlihat pada rumus :

Ci= (pi+ki) mod 26

Dimana :
Ci= cipherteks
Pi = plainteks
Ki = kunci

Sebagai contoh *enkripsi*, untuk *plainteks* IQBAL BATUBARA dengan kata kunci BATUBARAIQBAL akan menghasilkan *cipherteks* sebagai berikut :

Plainteks : IQBALBATUBARA
Kunci : BATUBARAIQBAL
Cipherteks : JQUUMBRTCRBRL

Yang mana diperoleh sebagai berikut (A = 0, B = 1, ..., Z = 25) :

(I +B) mod 26 = J
(Q+A) mod 26 = Q
(B+T) mod 26 = U
(A+U) mod 26 = U
(L+B) mod 26 = M
(B+A) mod 26 = B
(A+R) mod 26 = R
(T+A) mod 26 = T
(U+I) mod 26 = C
(B+Q) mod 26 = R
(A+B) mod 26 = B
(R+A) mod 26 = R
(A+L) mod 26 = L

b. Proses Deskripsi Pesan SMS

Sedangkan dalam proses *dekripsi*, untuk mendapatkan kembali *plainteks*, diperoleh dengan melakukan penjumlahan modulo 26 dari satu bit *cipherteks* dengan satu bit kunci:
Pi= (Ci-ki) mod 26

Contoh proses dekripsi, untuk *cipherteks* JQUUMBRTCRBRL dengan kata kunci BATUBARAIQBAL adalah sebagai berikut :

Cipherteks : JQUUMBRTCRBRL
Kunci : BATUBARAIQBAL
Plainteks : IQBALBATUBARA

Yang mana diperoleh sebagai berikut (A = 0, B = 1, ..., Z = 25) :

(J-B) mod 26 = I
(Q-A) mod 26 = Q
(U-T) mod 26 = B
(U-U) mod 26 = A
(M-B) mod 26 = L
(B-A) mod 26 = B
(R-R) mod 26 = A
(T-A) mod 26 = T
(C-I) mod 26 = U
(R-Q) mod 26 = B
(B-B) mod 26 = A
(R-A) mod 26 = R
(L-L) mod 26 = A

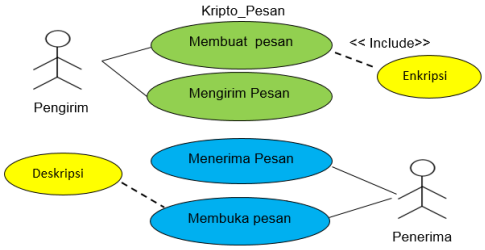
3.3 Perancangan Aplikasi

Perancangan akan dimulai setelah tahap analisis terhadap sistem selesai dilakukan. Perancangan dapat didenifisikan sebagai penggambaran, perencanaan dan pembuatan sketsa atau pengaturan dari beberapa elemen yang terpisah ke dalam satu kesatuan yang utuh dan berfungsi. Alat bantu yang digunakan untuk menggambarkan perancangan sistem secara umum yang akan dibangun. Untuk menjelaskan bagaimana suatu masukan diproses pada sistem maka digunakan spesifikasi proses dan kamus data untuk mengetahui aliran data yang mengalir pada sistem. Perancangan logika perangkat lunak yang dibangun menggunakan alat bantu perancangan system yaitu *Unified Modelling Language (UML)* dimana diagram yang digunakan antara lain *Use Case Diagram* dan *Activity Diagram*. Rancangan *Use Case Diagram* dan *Activity Diagram* dari perangkat lunak.

a. Use Case Diagram

Use case diagram merupakan salah satu diagram UML yang digunakan untuk menjelaskan setiap case yang dapat dijalankan oleh seorang User atau Aktor. *Use Case diagram* dibuat untuk memvisualisasikan /

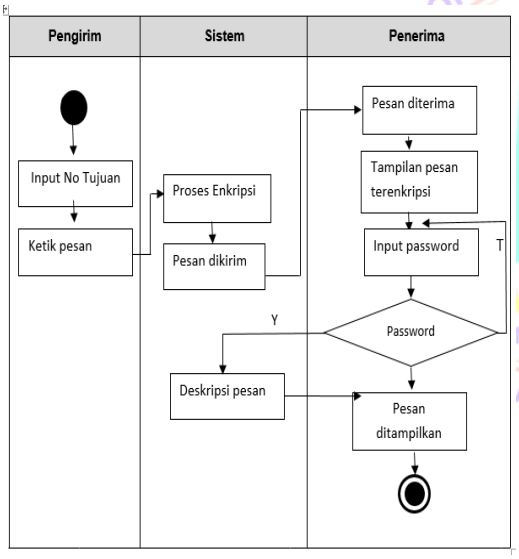
menggambarkan hubungan antara *Actor* dan *Use Case*. *Use Case diagram* mempresentasikan kegunaan atau fungsi-fungsi sistem dari perspektif pengguna. Use case diagram dari aplikasi yang akan dibangun digambarkan sebagai berikut ini.



Gambar 1: Use Case Diagram

b. *Activity* Diagram

Activity diagram merupakan salah satu diagram UML yang digunakan untuk menjelaskan urutan langkah yang dapat dilakukan dalam menjalankan perangkat lunak. *Activity* diagram dari aplikasi yang akan dibangun digambarkan sebagai berikut :



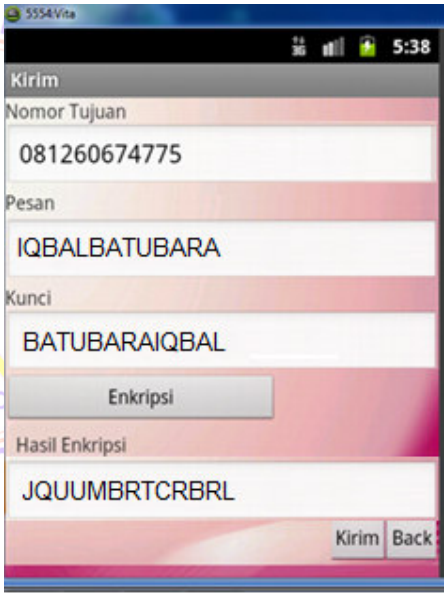
Gambar 2 : Activity Diagram

Aplikasi *enkripsi* dan *deskripsi* menggunakan algoritma *One Time Pad* (OTP) untuk proses. Berikut hasil dari implementasi program keseluruhan:

1. *Form Menu* Utama
   Form menu utama berfungsi untuk menampilkan semua pilihan yang ada pada aplikasi. Adapun implementasi *form menu* utama pada aplikasi *enkripsi* dan *deskripsi* ini adalah sebagai berikut:

Gambar 3 Tampilan Menu Utama

2. *Form Enkripsi* SMS
   Form enkripsi SMS sebagai fasilitas untuk mengenkripsi pesan SMS. Adapun implementasi *enkripsi* SMS adalah sebagai berikut:



Gambar 4 : Tampilan Form Enkripsi SMS

3. *Form Deskripsi* SMS
   Form deskripsi SMS sebagai fasilitas untuk mengdeskripsi pesan SMS dan menggembalikan pesan asli. Adapun implementasi *deskripsi* SMS adalah sebagai berikut:

Gambar 5: Tampilan Form Deskripsi SMS

KESIMPULAN

Setelah melakukan analisa dan pembahasan dari bab-bab sebelumnya maka pada akhir bab ini penulis dapat menyimpulkan bahwa dengan aplikasi *enkripsi* SMS dengan algoritma OTP dapat diambil kesimpulan:

1. Dengan adanya aplikasi ini, proses *enkripsi* dan *deskripsi* dapat memberikan kemudahan bagi pengguna dalam mengamankan pesan teks.
2. Algoritma One Time Pad (OTP) pada aplikasi pengamanan pesan teks dapat diterapkan sehingga proses *enkripsi* pesan SMS dapat lebih mudah.
3. Aplikasi *enkripsi* SMS berbasis *mobile android* dapat membantu pengguna mengenkripsikan pesan SMS sebelum dikirimkan.

DAFTAR PUSTAKA

[1] H. Saragih, G. Gusvita, B. Reza, D. Setiyadi, and R. Akbar, "Pengembangan Sistem Informasi Distribusi Informasi Sekolah Melalui Sms Gateway Dengan Zachman Framework," *J. Sist. Inf.*, vol. 8, no. 1, p. 32, 2013.

[2] L. Endah Pratiwi, R. Marwati, and I. Yusnitha, "PROGRAM APLIKASI KRIPTOGRAFI PENYANDIAN ONE TIME PAD MENGGUNAKAN SANDI VIGENERE."

[3] R. A.S and M. Shalahuddin, *Rekayasa Perangkat Lunak Terstruktur dan Berorentasi Objek*. Bandung: Informatika Bandung, 2016.

[4] D. Ariyus, "Kriptografi keamanan data dan komunikasi," *Yogyakarta Graha Ilmu*, 2006.

[5] R. Munir, "Kriptografi," *Inform. Bandung*, 2006.

[6] T. Limbong and P. D. P. Silitonga, "Testing the Classic Caesar Cipher Cryptography using of Matlab," *Int. J. Eng. Res. Technol.*, vol. 6, no. 2, pp. 175–178, 2017.

[7] B. Silaban and T. Limbong, "Aplikasi Pembelajaran Pengenalan Kriptografi Algoritma Affine Cipher Dan Vigenere Cipher Menggunakan Metode Computer Assisted Instruction," *Media Inf. Anal. dan Sist.*, vol. 2, no. 2, pp. 14–20, 2017.

[8] S. A. Sitorus and E. P. Malau, "Sistem Informasi Reservasi Hotel Pada GM. Marsaringar Balige Berbasis Android," *MEANS (Media Inf. Anal. dan Sist.*, vol. 2, no. 1, pp. 52–57, Jun. 2017.