PERANCANGAN APLIKASI KEAMANAN *CHATTING* MENGGUNAKAN METODE KRIPTOGRAFI *IMPROVED CAESAR CIPHER* BERBASIS MOBILE ANDROID

LAPORAN TUGAS AKHIR

Oleh :

AHMAD KHAIRU RAMDANI

03041481518029

JURUSAN TEKNIK ELEKTRO

FAKULTAS TEKNIK

UNIVERSITAS SRIWIJAYA

2017

LEMBAR PENGESAHAN

PERANCANGAN APLIKASI KEAMANAN *CHATTING* MENGGUNAKAN METODE KRIPTOGRAFI *IMPROVED CAESAR CIPHER* BERBASIS MOBILE ANDROID

SKRIPSI

Disusun Untuk Memenuhi Syarat Mendapatkan Gelar Sarjana Teknik
Pada Jurusan Teknik Elektro Fakultas Teknik
Universitas Sriwijaya

Oleh:
AHMAD KHAIRU RAMDANI
03041481518029

Palembang, Juli 2017

Mengetahui,

Ketua Jurusan Teknik Elektro	**Pembimbing Utama**
M.Abu Bakar Sidik,S.T.,M.Eng.,Ph.D	**Desi Windisari, ST., M. Eng**
NIP 197108141999031005	**NIP. 197812072008122001**

KEMENTERIAN RISET, TEKNOLOGI, DAN PENDIDIKAN TINGGI
UNIVERSITAS SRIWIJAYA
FAKULTAS TEKNIK KAMPUS PALEMBANG
JURUSAN TEKNIK ELEKTRO
Jln. Srijaya Negara Bukit Besar Palembang Kode Pos : 30139 Telp. (0711) 370178, 352870 Fax. (0711) 352870

BERITA ACARA UJIAN TUGAS AKHIR
JURUSAN TEKNIK ELEKTRO FAKULTAS TEKNIK UNSRI KAMPUS PALEMBANG
PERIODE SEMESTER GENAP TA 2016/2017 TANGGAL 26 JULI 2017

Nama : Ahmad Khairu Ramdani
Nim : 03091418151029
Judul Tugas Akhir : Perancangan Aplikasi Keamanan Chatting Menggunakan Metode Kriptografi Improved Caesar Cipher Berbasis Mobile Android
Pembimbing Utama : Desi Windisari., ST., M.Eng
Pembimbing Pembantu :

No	Perbaikan	Dosen	Tanda Tangan
1.	Penambahan Kesimpulan	Dr. H. Iwan Pahendra A.S.T., M.T	
2.	Jelaskan kunci, Hasting, Definisi karakter, Penjelasan "dinamis"	Puspa kurniasari. ST., M.T.	
3.	Tidak ada revisi	Abdul Haris Dalimunte ST, MTI	
4.			
5.			

Pembimbing Utama

(Desi Windisari., ST., M.Eng)
NIP. 197812072008122001

MOTTO

اللّٰهِ سَبِيْلِ فِى جَ خَرَ مَنْ ۚ فَهُوَ الْعِلْمِ طَلَبِ فِى

‘’Barang siapa keluar untuk mencari ilmu maka dia berada di jalan Allah ‘’
(HR.Turmudzi)

اُدَبُهُمْ حْسِنُوْا وَاَ اضُوْلاَدِضُكُمْ اَكْرِمُوْا

‘’Muliakanlah anak-anakmu dan baguskanlah pendidikan mereka’’.
(H.R.At-thabrani dan khatib)

Abstrak

PERANCANGAN APLIKASI KEAMANAN *CHATTING* MENGGUNAKAN METODE KRIPTOGRAFI *IMPROVED CAESAR CIPHER* BERBASIS MOBILE ANDROID

AHMAD KHAIRU RAMDANI
03041481518029

Keamanan sangat penting dalam segala aspek untuk melindungi data. Salah satu cara mengamankan informasi adalah menggunakan kriptografi. Kriptografi merupakan suatu metode yang dapat melakukan enkripsi dan dekripsi. Tujuan penelitian adalah untuk membuat aplikasi enkripsi dan dekripsi menggunakan algoritma *Improved Caesar Cipher* yang berguna untuk menjaga kerahasian teks dengan menggunakan gabungan algoritma *Caesar cipher* substitusi dan ROT13. Aplikasi ini berupa aplikasi chatting yang dapat mengenkripsikan teks dan hanya dapat di dekripsikan dengan memiliki kunci yang sama seperti kunci pengirim. Aplikasi ini dibuat untuk mengamankan informasi yang hanya boleh di ketahui oleh orang-orang tertentu. Berdasarkan dari hasil pengujian dengan menggunakan metode *blackbox* dalam menguji fungsional sistem dan pengujian enkripsi, aplikasi keamanan *Chat* menggunakan metode kriptografi *Improved Caesar Cipher* berbasis android dapat berjalan dengan baik dan telah sesuai dengan apa yang diharapkan.

Kata kunci—Kriptografi, Algoritma, Improved Caesar Cipher.

Abstrak

PERANCANGAN APLIKASI KEAMANAN *CHATTING* MENGGUNAKAN METODE KRIPTOGRAFI *IMPROVED CAESAR CIPHER* BERBASIS MOBILE ANDROID

AHMAD KHAIRU RAMDANI
03041481518029

Security is very important in all aspects to protect data.. one way of securing information is to use cryptography. Cryptography is a method that cav perform encryption and decryption. The purpose of research is to make encryption and decryption application using a Caesar Cipher Improved algorithms are useful for maintaining the confidentiality of text by using a combination of Caesar cipher substitution and ROT13 algorithms. This application is a chat app that can encrypt text and can only be decrypted by having the same key as the sender key. This app is created to secure information only to be known by certain people. Based on the test result using blackbox method in testing system functionality and encryption testing, chat application security using cryptography Caesar cipher improved method android based can run well and has been in accordance as expected.

Keywords— Cryptography, Algorithms, Improved Caesar Cipher.

KATA PENGANTAR

Puji syukur penulis ucapkan kehadiran Allah Yang Maha Kuasa atas rahmat dan hidayah yang telah dilimpahkan-Nya sehingga penulis dapat menyelesaikan laporan tugas akhir dengan judul **"PERANCANGAN APLIKASI KEAMANAN *CHATTING* MENGGUNAKAN METODE KRIPTOGRAFI *IMPROVED CAESAR CIPHER* BERBASIS MOBILE ANDROID".**

Adapun maksud penyusunan laporan tugas akhir ini adalah untuk memenuhi salah satu syarat dalam menyelesaikan pendidikan strata I pada Jurusan Teknik Elektro Program Studi Teknik Elektronika di Universitas Sriwijaya.

Penyelesaian laporan ini tak lepas dari kerjasama dan bantuan dari berbagai pihak yang telah memberikan bimbingan dan pengarahan kepada penulis dalam menyelesaikan laporan tugas akhir ini. Penulis juga mengucapkan terima kasih kepada pihak-pihak yang telah membantu dalam proses penyelesaian proposal ini, yaitu kepada :

1. Kedua Orang Tua, serta keluarga besar yang telah banyak membantu dan yang selalu memberikan dukungan serta doanya.
2. Cindy Triana Putri yang selalu membantu dan menyemangati
3. Bapak M.Abu Bakar Sidik,S.T.,M.Eng.,Ph.D., selaku Ketua Jurusan Teknik Elektro Universitas Sriwijaya.
4. Ibu Desi Windisari, ST., M. Eng., selaku Pembimbing Akademik sekaligus Pembimbing Tugas Akhir.
5. Seluruh Dosen dan staf-staf pada jurusan Teknik Elektro.
6. Teman-teman TTI (dari d3 ke s1) angkatan 2015 atas kebersamaannya.

Akhir kata penyusun mengharapkan semoga laporan tugas akhir ini dapat bermanfaat bagi semua dan semoga segala bantuan serta bimbingan yang penyusun dapatkan selama ini mendapatkan ridho ALLAH SWT, Amin.

Palembang, Juli 2017

Penulis

DAFTAR ISI

Halaman

DAFTAR TABEL

Halaman

DAFTAR GAMBAR

Halaman

BAB I

PENDAHULUAN

1.1. Latar Belakang

Aplikasi media sosial rata – rata memiliki fitur chat. Kita ambil contoh saja salah satu fasilitas Facebook yang paling sering di gunakan adalah chatting. Fasilitas chatting pada Facebook kini tak hanya ada pada web namun juga telah hadir pada perangkat bergerak yaitu bernama Facebook Messenger. Fasilitas Chatting Facebook sendiri merupakan fasilitas dimana dua atau sekelompok orang yang telah ditunjuk oleh pengguna yang menghendaki pengguna lain untuk dapat saling berkomunikasi. Dengan kata lain, data yang ditukar bersifat rahasia atau tidak untuk umum sehingga diperlukan adanya suatu skema dimana pengguna dapat berkomunikasi dengan obrolan secara aman.

Pengamanan data komunikasi dapat dilakukan salah satunya dengan Kriptografi. Kriptografi dapat diartikan sebagai teknik penyandian data. Kriptografi dibagi menjadi 2 proses utama yaitu enkripsi dan dekripsi. Enkripsi merupakan proses pengamanan suatu data dengan membuat data tersebut tidak dapat dibaca tanpa pengetahuan khusus. Sedangkan dekripsi adalah proses pengembalian data hasil enkripsi. Metode keamanan data atau kriptografi yang digunakan dalam penelitian ini adalah metode *Caesar Cipher*, metode ini digunakan oleh Julius Caesar untuk berkomunikasi dengan para panglimanya. Dalam kriptografi, *Caesar Cipher* dikenal dengan beberapa nama seperti: *Shift Cipher*, *Caesar's code* atau *Caesar shift*. *Caesar Cipher* merupakan teknik kriptografi yang paling sederhana dan banyak digunakan. *Cipher* ini berjenis *cipher* substitusi, dimana setiap huruf pada *plaintext*-nya digantikan dengan huruf lain yang tetap pada posisi alphabet.

Berdasarkan uraian singkat di atas maka penulis ingin membuat penelitian dengan judul "**PERANCANGAN APLIKASI KEAMANAN *CHATTING* MENGGUNAKAN METODE KRIPTOGRAFI *IMPROVED CAESAR CIPHER* BERBASIS MOBILE ANDROID**".

Metode keamanan data atau kriptografi yang digunakan dalam penelitian ini adalah metode *Caesar Cipher*, metode ini digunakan oleh Julius Caesar untuk berkomunikasi dengan para panglimanya. *Cipher* ini berjenis *cipher* substitusi, dimana setiap huruf pada *plaintext*-nya digantikan dengan huruf lain yang tetap pada posisi alphabet dan ROT 13 dimana jumlah alphabet di bagi menjadi 2 posisi.

1.2. Perumusan Masalah

Rumusan masalah dalam menyusun penelitian ini adalah bagaimana membuat aplikasi keamanan *chat* menggunakan metode kriptografi *Improved Caesar Cipher* pada sistem operasi mobile Android.

1.3. Batasan Masalah

Ruang lingkup penelitian dalam merancang perangkat lunak ini adalah :

1. Sistem keamanan *chat* ini dibatasi untuk teks.
2. Sistem keamanan teks *chat* ini membuat fungsi enkripsi dan deskripsi teks pada *chat* menggunakan algoritma *Improved Caesar Cipher*.
3. Sistem keamanan ini hanya diterapkan di perangkat mobile Android.

1.4. Tujuan Penelitian

Tujuan penelitian ini adalah :

1. Menghasilkan aplikasi keamanan *chatting* Menggunakan metode kriptografi *Improved Caesar Cipher* berbasis mobile Android.
2. Menghasilkan aplikasi yang dapat digunakan untuk pengiriman pesan dengan aman tanpa harus terbaca oleh orang lain menggunakan metode *Improve Caesar Cipher* pada sistem operasi mobile Android.

1.5. Sistematika Penulisan

Sistematika penulisan tugas akhir ini disusun sebagai berikut :

BAB I PENDAHULUAN

Pada bab ini berisikan gambaran umum penelitian yang dilakukan meliputi latar belakang masalah, rumusan masalah, tujuan penelitian, batasan masalah, dan sistematika penulisan yang merupakan panduan dalam penyusunan landasan teori.

BAB II TINJAUAN PUSTAKA

Pada bab ini menjelaskan dan membahas teori – teori yang berkaitan dengan sistem yang dibangun, beserta referensinya yang akan menjadi acuan dalam menyelesaikan penelitian ini.

BAB III METODE PENELITIAN

Pada bab ketiga ini akan menjelaskan metode-metode analisa data, yang digunakan untuk menganalisa data pada tugas akhir ini. Metode yang mencakup dalam tugas akhir ini adalah metode RUP

BAB IV HASIL DAN PEMBAHASAN

Pada bab ini akan membahas hasil yang didapat selama penelitian, proses pembuatan apliaksi menggunakan aplikasi eclipse, masalah yang didapat selama penelitian serta menggambarkan kelemahan serta kelebihan perangakat lunak yang dibangun.

BAB V KESIMPULAN DAN SARAN

Pada bab kelima ini berisikan kesimpulan dari analisa pada bab keempat dan saran untuk penelitian selanjutnya.

BAB II

TINJAUAN PUSTAKA

2.1 Teori Pendukung

2.1.1 Kriptografi

Kriptografi adalah bidang ilmu yang sangat penting keberadaannya untuk menjaga kerahasiaan dan keamanan suatu informasi dan data. Kriptografi (*Cryptography*) berasal dari bahasa Yunani : "*cryptos*" artinya "*secret*" (rahasia), sedangkan "*graphien*" artinya "*writing*" (tulisan). Jadi, kriptografi (*Cryptography*) berarti "*secret writing*" (tulisan rahasia)". (Munir, 2006:2).

2.1.2 *Chat* (Pesan Obrolan)

Dalam internet, *chatting* adalah obrolan kepada orang lain yang menggunakan *internet* dalam waktu yang bersamaan. Biasanya, obrolan ini merupakan pertukaran pesan teks yang membutukan sebuah *server* sebagai penyedia layanan dan sejumlah pengguna untuk terlibat dalam *chatting* tersebut. *Chatting* dapat dilakukan dengan menggunakan suara (*voice chat*) atau suara dan video. (Bagus, 2013:3)

2.1.3 Karakter

Menurut Kamus Besar Bahasa Indonesia dalam komputer karakter adalah huruf, angka, ruang dan simbol khusus yang dapat dimunculkan pada layar dengan *keyboard* (papan ketik). Contoh karakter dapat berupa huruf, angka, ruang (spasi) dan symbol-simbol seperti !, @, #, $, %, ^, &, *, (,), _, +, = dan lain sebagainya.

2.1.4 Android

Android adalah sebuah sistem operasi telepon selular atau perangkat mobile dan *computer tablet* layar sentuh berbasis linux. (Kasman, 2013:2).

Android adalah sebuah sistem operasi untuk perangkat mobile berbasis Linux yang mencakup sistem operasi, *middleware* dan aplikasi. Android menyediakan *platform* terbuka bagi para pengembang untuk menciptakan aplikasi mereka (Safaat, 2014:1).

Gambar 2.1 Gambar Logo Android

2.1.5 Metode *Caesar Chipper*

Caesar Cipher merupakan penyandian yang di pakai oleh Julius Caesar ketika mengirim pesan ke pasukannya aga tidak bisa di baca oleh orang lain kecuali orang terpercayanya, metode ini ialah metode sederhana untuk kriptografi, dengan mengganti huruf dengan beberapa huruf di sebelahnya sehingga informasi menjadi acak.

2.1.6 UML

UML (*Unified Modelling Language*) adalah salah standar bahasa yang banyak di dunia industri untuk mendefinisikan *requirement*, membuat analisis dan *desain*, serta menggambarkan arsitektur dalam pemrograman berorientasi objek. (Rosa, 2013:133).

Unified Modeling Language (UML) adalah suatu bahasa standar untuk menulis cetak biru *software*. UML bisa digunakan untuk visualisasi, spesifikasi, konstruksi, dan dokumentasi artifak-artifak sistem *software-intensive*. Dengan kata lain, seperti arsitek

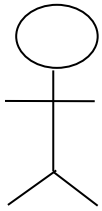
bangunan membuat cetak biru untuk digunakan oleh perusahaan konstruksi, arsitek *software* membuat diagram-diagram UML untuk membantu *software developer* membangun *software*. Bila anda memahami kosa kata UML (elemen-elemen gambar diagram dan maknanya), anda dapat dengan mudah memahami dan mengspesifikasi sistem dan menjelaskan desain sistem tersebut ke orang lain. (Pressman 2010: 841)

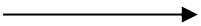
2.1.6.1 Use Case

Use case atau *use case diagram* merupakan pemodelan untuk kelakuan (*behavior*) sistem informasi yang akan dibuat. *Use case* mendeskripsikan sebuah interaksi antara satu atau lebih aktor dengan sistem informasi yang akan dibuat. Secara kasar, *use case* digunakan untuk mengetahui fungsi apa saja yang ada di dalam sebuah sistem informasi dan siapa saja yang berhak menggunakan fungsi-fungsi itu. Syarat penamaan pada *use case* adalah nama didefinisikan sesederhana mungkin dan dapat dipahami. Ada dua hal utama pada *use case* yaitu pendefinisian apa yang disebut aktor dan *use case.*

1. Aktor merupakan orang, proses, atau sistem lain yang berinteraksi dengan sistem informasi yang akan dibuat diluar sistem informasi yang akan dibuat itu sendiri, jadi walaupun simbol dari aktor adalah gambar orang, tapi aktor belum tentu merupakan orang.
2 *Use case* merupakan fungsionalitas yang disediakan sistem sebagai unit-unit yang saling bertukar pesan antar unit atau aktor (Rosa, 2013:155).

Tabel 2.1 Simbol-simbol yang Ada pada *Use Case* Diagram

Nama/Simbol	Keterangan
Use Case **nama use**	Fungsionalitas yang disediakan sistem sebagai unit-unit yang saling bertukar pesan antar unit atau aktor; biasanya dinyatakan dengan menggunakan kata kerja di awal frase nama *use case*.
Aktor (*actor*)  **nama actor**	Orang, proses, atau sistem lain yang berinteraksi dengan sistem informasi yang akan dibuat di luar sistem, jadi walaupun simbol dari aktor adalah gambar orang, tapi aktor belum tentu merupakan orang.
Asosiasi (*association*) ———————	Komunikasi antara aktor dan *use case* yang berpartisipasi pada *use case* atau *use case* memiliki interaksi dengan aktor.

Nama/Simbol	Keterangan
Ekstensi (*extend*)	Relasi *use case* tambahan ke sebuah *use case* dimana *use case* yang ditambahkan dapat berdiri sendiri walau tanpa *use case* tambahan.
Generalisasi (*generalization*) 	Hubungan generalisasi dan spesialisasi (umum-khusus) antara dua buah *use case* dimana fungsi yang satu adalah fungsi yang lebih umum dari lainnya.

Sumber: (Rosa dan Shalahuddin, 2013)

2.1.6.2 Class Diagram

Diagram kelas atau *class diagram* menggambarkan struktur sistem dari segi pendefinisian kelas-kelas yang akan dibuat untuk membangun sistem. Kelas memilki apa yang disebut atribut dan metode atau operasi.

1. Atribut merupakan variabel-variabel yang dimiliki oleh suatu kelas.
2. Operasi

Diagram kelas dibuat agar pembuat program atau *programmer* membuat kelas-kelas sesuai rancangan di dalam diagram kelas agar antar dokumentasi perancangan dan perangkat lunak sinkron. Susunan struktur kelas yang baik pada diagram kelas sebaiknya memiliki jenis-jenis kelas berikut:

1. Kelas *main*

Kelas yang memiliki fungsi awal dieksekusi ketika sistem dijalankan.

2. Kelas yang menangani tampilan sistem (*view*)

   Kelas yang mendefinisikan dan mengatur tampilan ke pemakai.

3. Kelas yang diambil dari pendefinisian *use case* (*controller*)

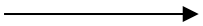
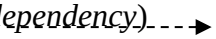
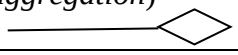
Kelas yang menangani fungsi-fungsi yang harus ada diambil dari pendefinisian *use case*, kelas ini biasanya disebut dengan kelas proses yang menangani proses bisnis pada perangkat lunak.

4. Kelas yang diambil dari pendefinisian data (model)

Kelas yang digunakan untuk memegang atau membungkus data menjadi sebuah kesatuan yang diambil maupun yang akan disimpan ke basisdata. Semua tabel yang dibuat di basisdata dapat dijadikan kelas, namun untuk tabel dari hasil relasi atau atribut *multivalue* pada ERD dapat dijadikan kelas tersendiri dapat juga tidak asalkan pengaksesannya dapat dipertanggungjawabkan atau tetap ada di dalam perancangan kelas (Rosa, 2013:141-142).

Tabel 2.2 Simbol-simbol yang Ada pada *Class* Diagram

Nama/Simbol	**Keterangan**
Kelas **nama_kelas** +atribut +operasi()	Kelas pada struktur sistem.

Antarmuka (*interface*)  **nama** **interface**	Sama dengan konsep *interface* dalam pemrograman berorientasi objek.
Asosiasi (*association*) 	Relasi antar kelas dengan makna umum, asosiasi biasanya juga disertai dengan *multiplicity*.
Generalisasi (*generalization*) 	Relasi antar kelas dengan makna generalisasi spesialisasi (umum-khusus).
Kebergantungan (*dependency*) 	Relasi antar kelas dengan makna kebergantungan antar kelas.
Agregasi (*aggregation*) 	Relasi antar kelas dengan makna semua bagian (*whole-part*).

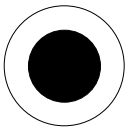
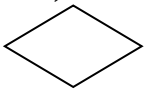
Sumber: (Rosa dan Shalahuddin, 2013)

2.1.6.3 Actvity Diagram

Diagram aktifitas atau *activity diagram* menggambarkan *workflow* (aliran kerja) atau aktifitas dari sebuah sistem atau proses bisnis atau menu yang ada pada perangkat lunak. Yang perlu diperhatikan disini adalah bahwa diagram aktifitas menggambarkan aktifitas sistem bukan apa yang dilakukan aktor, jadi aktifitas yang dapat dilakukan oleh sistem. Diagram aktifitas juga banyak digunakan untuk mendefinisikan hal-hal berikut:

1. Rancangan proses bisnis dimana setiap urutan aktifitas yang digambarkan merupakan proses bisnis sistem yang didefinisikan.
2. Urutan atau pengelompokan tampilan dari sistem atau *user interface* dimana setiap aktifitas dianggap memiliki sebuah rancangan antarmuka tampilan.
3. Rancangan pengujian dimana setiap aktifitas dianggap memerlukan sebuah pengujian yang perlu didefinisikan kasus ujinya.
4. Rancangan menu yang ditampilkan pada perangkat lunak (Rosa, 2013:161-162).

Tabel 2.3 Simbol-simbol yang Ada pada *Activity Diagram*

Nama/Simbol	**Keterangan**
Status Awal 	Status awal aktifitas sistem, sebuah diagram aktifitas memiliki sebuah status awal.
Status Akhir 	Status akhir yang dilakukan sistem, sebuah diagram aktifitas memiliki sebuah status akhir.
Aktifitas 	Aktifitas yang dilakukan sistem, aktifitas biasanya diawali dengan kata kerja.
Percabangan (*decision*) 	Asosiasi percabangan dimana jika ada pilihan aktifitas lebih dari satu.

Nama/Simbol	Keterangan
Penggabungan (*join*) 	Asosiasi penggabungan dimana lebih dari satu aktifitas digabungkan menjadi satu.

Sumber: (Rosa dan Shalahuddin, 2013)

2.1.6.4 *Sequence Diagram*

Diagram sekuen menggambarkan kelakuan objek pada *use case* dengan mendeskripsikan waktu hidup objek dan *message* yang dikirimkan dan diterima antar objek. Oleh karena itu untuk menggambar diagram sekuen maka harus diketahui objek-objek yang terlibat dalam sebuah *use case* beserta metode-metode yang dimiliki kelas yang diinstanisasi menjadi objek itu. Membuat diagram sekuen juga dibutuhkan untuk melihat skenario yang ada pada *use case*. Banyaknya diagram sekuen yang harus digambar adalah minimal sebanyak pendefinisian *use case* yang memiliki proses sendiri atau yang penting semua *use case* yang telah didefinisikan interaksi jalannya pesan sudah dicakup pada diagram sekuen sehingga semakin banyak *use case* yang didefinisikan maka diagram sekuen yang harus dibuat juga semakin banyak (Rosa, 2013:161-162).

Tabel 2.4 Simbol-simbol yang Ada pada *Sequence Diagram*

Nama/Simbol	**Keterangan**
Aktor  **nama actor**	Orang, proses, atau sistem lain yang berinteraksi dengan sistem informasi yang akan dibuat di luar sistem, jadi walaupun simbol dari aktor adalah gambar orang, tapi aktor belum tentu merupakan orang.
Objek 	Objek adalah menyatakan objek yang berinteraksi dengan pesan.
Garis Hidup *(Lifeline)*	Garis hidup (*lifeline*) adalah menyatakan kehidupan suatu objek.
Waktu Aktif 	Waktu aktif yaitu menyatakan objek dalam keadaan aktif dan berinteraksi, semua yang terhubung dengan waktu aktif ini adalah sebuah tahapan yang dilakukan didalamnya.

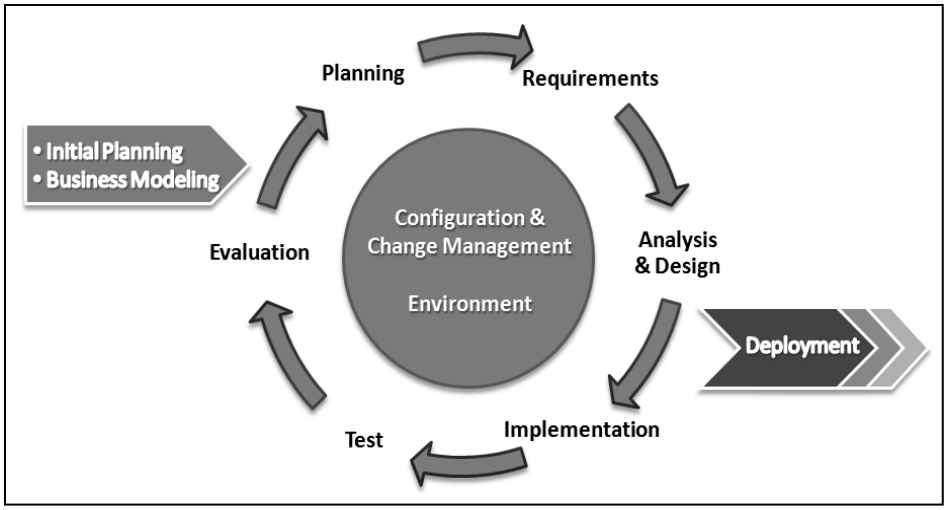
Nama/Simbol	**Keterangan**
Pesan tipe *create* <<*create*>>	Menyatakan suatu objek membuat objek yang lain, arah panah mengarah pada objek yang dibuat.
Pesan tipe *call* 1:nama_metode( )	Menyatakan suatu objek memanggil operasi/metode yang ada pada objek lain atau dirinya sendiri.
Pesan tipe *send* 1 : masukan	Menyatakan bahwa suatu objek mengirimkan data/masukan/informasi ke objek lainnya, arah panah megarah pada objek yang dikirim.
Pesan tipe *return* 1 : keluaran	Menyatakan bahwa suatu objek yang telah menjalankan suatu operasi atau metode menghasilkan suatu kembalian ke objek tertentu, arah panah mengarah pada objek yang menerima kembalian.
Pesan tipe *destroy* <<destroy>>	Menyatakan suatu objek mengakhiri hidup objek yang lain, arah panah mengarah pada objek yang diakhiri, sebaiknya jika ada *create* maka ada *destroy*.

Sumber: (Rosa dan Shalahuddin, 2013)

BAB III
METODOLOGI

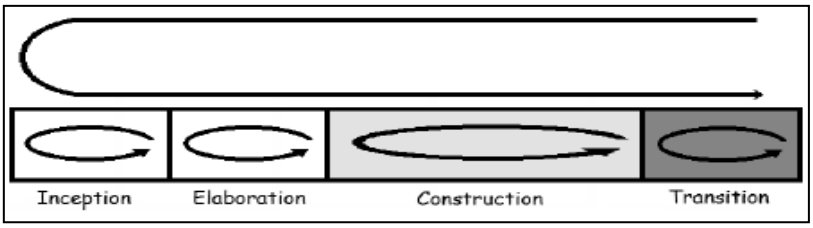
3.1 Metodologi RUP (*Rational Unifed Process*)

Proses penggulangan/iteratif pada RUP secara global dapat dilihat pada gambar berikut:



Gambar 3.1 Proses *Iterative* RUP

Pada metodelogi ini berisi tahapan sebagai berikut:



Gambar 3.2 Metodologi Perancangan

3.2 Input dan Output Tahapan *Rational Unifed Process*

Agar pembuatan sistem menjadi terarah, tahapan pengerjaan sistem akan dijelaskan melalui tabel dibawah ini.

Tabel 3.1. Tahapan Pengerjaan Keamanan Chat Menggunakan Caesar Cipher

KEGIATAN	INPUT	OUTPUT
***Inception* (permulaan)**	Langkah-langkah yang penulis lakukan pada tahap ini adalah analisa sistem. Tahap analisa ini dengan menggunakan teknik analisa SWOT.	Document data hasil analisa, dan Document SWOT untuk pengembangan aplikasi.
***Elaboration* (perluasan/perencanaan)**	Langkah-langkah yang dilakukan penulis pada tahap ini meliputi: perancangan database, perancangan alur sistem yang akan dibuat, perancangan antar muka.	Dokumen hasil rancangan dan User Interface.
***Construction* (konstruksi)**	Langkah-langkah yang dilakukan penulis pada tahap ini meliputi: pembuatan tampilan (*layout*) pada program dan pembuatan kode program.	Sistem aplikasi yang siap untuk di testing

KEGIATAN	INPUT	OUTPUT
***Transition* (transisi)**	Langkah-langkah yang dilakukan penulis pada tahap ini meliputi: pengujian program aplikasi dan instalasi program aplikasi yang telah dibuat ke perangkat mobile Android.	Sistem aplikasi yang dapat diimplementasikan pada mobile android.

3.3 Kebutuhan Sistem

1. **Perangkat Keras**

   Perangkat keras yang dibutuhkan untuk mendukung proses perancangan, dan pengoperasian aplikasi ini, yaitu:

   a. Perangkat untuk pembuatan program dan server :

      Personal Computer (PC) Dengan spesifikasi sebagai berikut :

      1. *Processor* Core i3,
      2. *Ram* 2 GB *Memory DDR3*
      3. *Harddisk* 500GB.

   b. Perangkat untuk pengguna :

      1. Smartphone Android 2.3.

2. Perangkat Lunak dan Bahasa Pemrograman

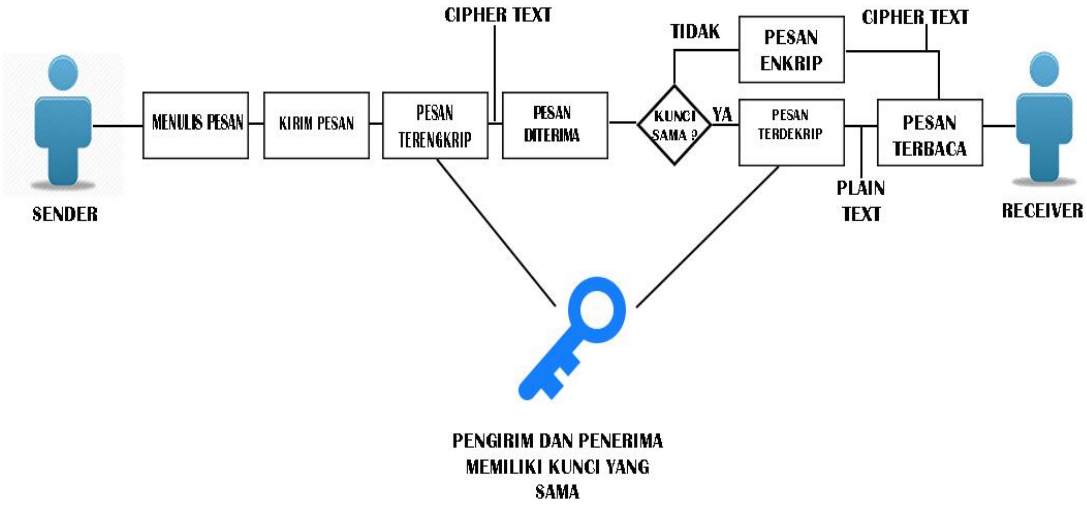
Perangkat lunak yang dibutuhkan untuk mendukung proses perancangan, dan pengoperasian aplikasi ini, yaitu:

Tabel 3.2 Perangkat Lunak (Software) Aplikasi

PERANGKAT LUNAK (SOFTWARE)		
NAMA SOFTWARE	**JENIS SOFTWARE**	**KEGUNAAN**
Eclipse	IDE Google (Integrated Development Environtment)	Sebagai aplikasi untuk melakukan pembuatan, pengembangan, dan menjalankan program.
Java	Back End	Bahasa yang dipakai untuk membuat aplikasi.
Sistem Operasi Android	Operating Sistem	Sistem operasi yang berguna sebagai platform di sisi pengguna.
Star UML	Design	Salah satu software untuk mendesign diagram aplikasi.
Dreamwheaver	Back End	Aplikasi untuk pembuatan syntax yang berfungsi sebagai penghubung antara aplikasi dan server
Xampp	Database	Aplikasi untuk mengolah database

3.4 Proses enkripsi dan dekripsi

Gambaran umum untuk proses pertukaran informasi mengunakan metode kriptografi *Caesar cipher improved* seperti gambar di bawah ini :

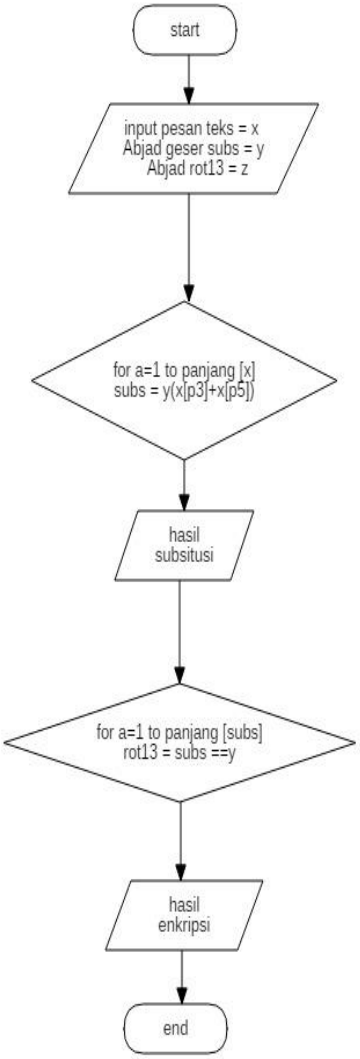


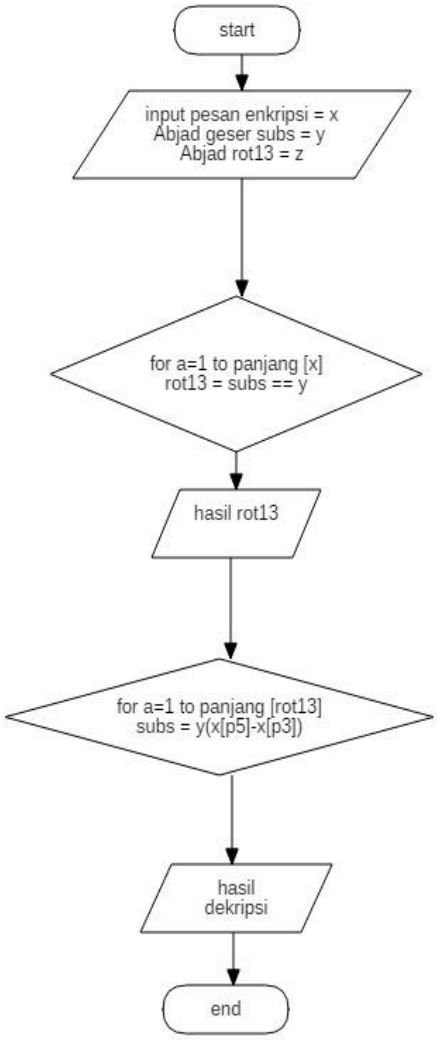
Gambar 3.3 gambaran umum proses bertukar informasi

Untuk rancangan proses enkripsi pengirim pertama-tama login ke dalam aplikasi kemudian masuk ke menu kunci untuk membuat kunci yang sama dengan si penerima, kunci disini berupa teks yang sama antara si pengirim dan penerima, berbeda dengan *plainteks* yang akan di enkrip maupun *ciphertext* yang akan di dekrip, kemudian pengirim masuk ke menu kontak dan memilih id penerima yang akan dikirimkan informasi, karena aplikasi ini akan mengirimkan informasi berdasarkan id pengguna, aplikasi secara otomatis akan masuk ke menu kirim dan baca pesan, kemudian pengirim menuliskan informasi yang di inginkan dan tekan pilihan “kirim”, pesan akan terkirim ke id si penerima, proses enkripsi akan dimulai ketika pegguna menekan pilihan kirim tersebut. Untuk proses enkripsi dapat dilihat dari gambar 3.4.

Untuk rancangan proses dekripsi pesan yang terkirim akan masuk ke id penerima, penerima harus login terlebih dahulu ke dalam aplikasi dan langsung masuk ke menu pesan masuk, informasi yang dikirim dari id pengirim akan muncul di menu pesan masuk tersebut, ketika si penerima membuka pesan dari id pengirim, informasi yang terenkripsi tadi secara otomatis

telah terdekripsi jika penerima telah mengatur kunci yang sama di menu kunci. Untuk proses dekripsi dapat dilihat dari gambar 3.5.





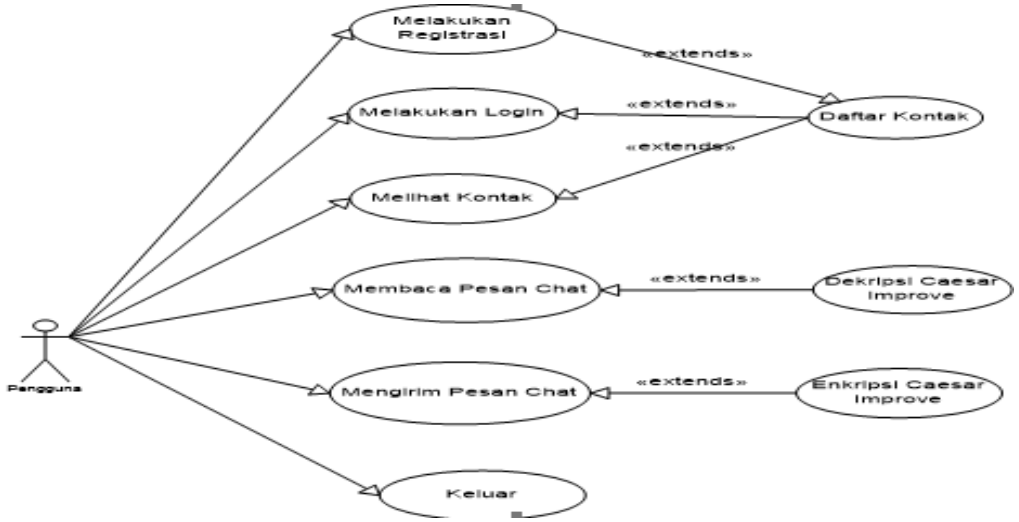
Gambar 3.4 Flowchart Enkripsi Gambar 3.5 Flowchart Dekripsi

3.5 Desain Sistem

Dalam mendesain bentuk sistem pada aplikasi keamanan *Chat* menggunakan metode kriptografi *Improved Caesar Cipher* pada sistem operasi mobile Android ini digunakan *tools* UML yang mengilustrasikan sistem yang akan dikembangkan dalam bentuk *usecase diagram*.

3.5.1 Usecase

Pada usecase aplikasi keamanan *chat* menggunakan metode kriptografi *improved caesar cipher* berbasis mobile android hanya memiliki 1 (satu) actor yang dapat bertindak sebagai penerima dan pengirim.



Gambar 3.6 Usecase User

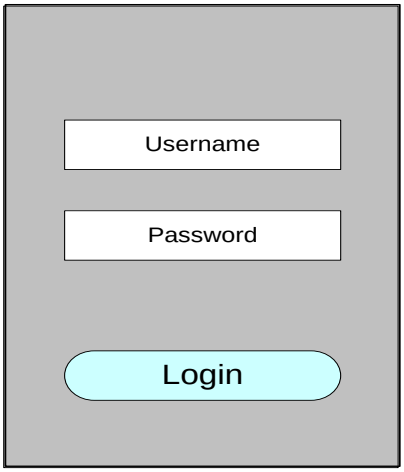
Tabel 3.3 Dekripsi Usecase Sistem keamanan Chatt

No.	Usecase	Dekripsi
1.	Melakukan Registrasi	Halaman Untuk Mendaftar ke Aplikasi Untuk Bisa Memanfaatkan Aplikasi Tersebut
2.	Melakukan Login	Halaman Untuk Masuk Ke Aplikasi
3.	Melihat Kontak	Halaman Untuk Melihat Daftar Kontak Yang Terdaftar
4.	Membaca Pesan *Chat*	Halaman untuk membaca *chat* enkripsi yang di dekripsikan terlebih dahulu
5.	Mengirim Pesan *Chat*	Halaman untuk mengirim *Chat* yang di enskripsikan terlebih dahulu
6.	Keluar	Untuk keluar dari aplikasi

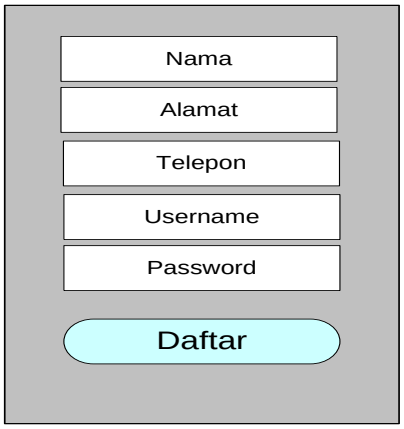
3.6 Perancangan User Interface

3.6.1 Perancangan Interface Aplikasi Android

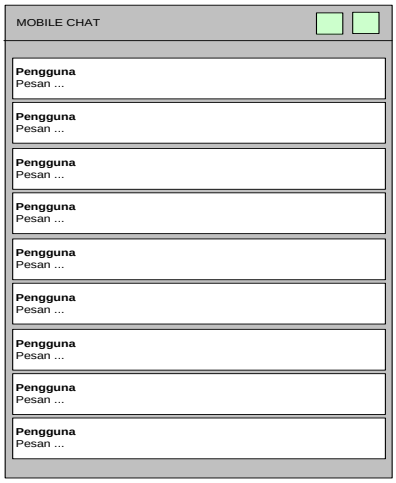
Dibawah ini perancangan awal aplikasi keamanan *Cha*t :



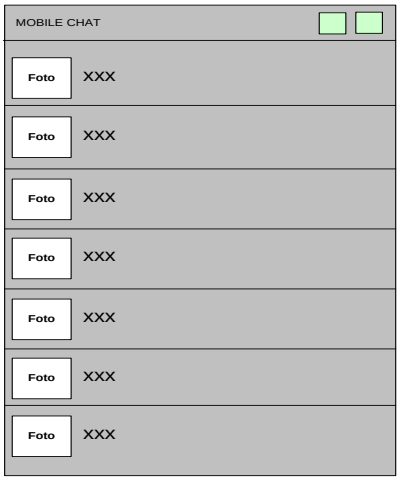
Gambar 3.7 Tampilan *Form Login*



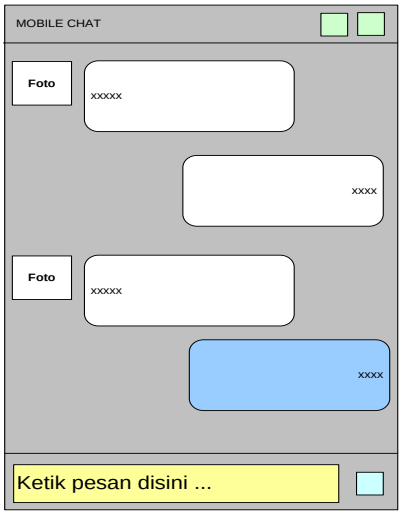
Gambar 3.8 Tampilan *Form Registrasi*



Gambar 3.9 Tampilan *Form* Utama



Gambar 3.10 Tampilan *Form* Kontak



Gambar 3.11 Tampilan *Form* Kirim dan Baca Pesan

PENUTUP

5.1 Kesimpulan

Dari perancangan sistem aplikasi keamanan *Chat* menggunakan metode kriptografi *Improved Caesar Cipher* pada sistem operasi mobile Android yang dilakukan pada penelitianini, maka dapat diambil kesimpulan sebagai berikut:

1. Program aplikasi yang telah dilakukan hanya mengenkripsi plainteks dalam penerapan pesan teks pada perangkat mobile smartphone.
2. Kata kunci dan panjang kunci dibuat dinamis (karakter kunci bisa berupa angka, huruf maupun simbol) sehingga pengirim pesan chat dapat merubah kata kunci sesuai dengan keinginan mereka.

5.2 Saran

Sistem yang penulis telah kembangkan belumlah sempurna seperti yang diharapkan dikarenakan keterbatasan pengetahuan dan waktu. Adapun saran penulis untuk pengembangan sistem ini adalah :

1. sistem pada aplikas ini dapat dikembangkan pada perangkat mobile yang menggunakan sistem operasi lain seperti QNX, symbian, windows phone, dan iOS.
2. Sistem di kemudian hari dapat mengenkripsi data berupa foto dan file dengan cara mengabungkan metode kriptografi yang dapat mengengkripsi data berupa foto dan file seperti *Hill Cipher* maupun yang lainnya.

DAFTAR PUSTAKA

Ahmad, Dharma Kasman(2013).*Kolaborasi Dahsyat Android Dengan PHP dan MySQL*.Yogyakarta: Penerbit Lokomedia.

A.S., Rosa dan Shalahuddin, M. 2013. *Rekayasa Perangkat Lunak Terstruktur Dan Berorientasi Objek. Informatika*. Bandung.

Nazruddin Safaat H. 2012. Android Pemrograman Aplikasi Mobile Smartphone dan Tablet PC Berbasis Android. Bandung : Informatika.

Pressman, Roger S. 2010. "Software Engineering : A Practitioner's Approach, 7th edition". McGraw-Hill, New York.

Munir, Rinaldi, 2006, Diktat Kuliah Kriptografi, Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung, Bandung.