****

**IMPLEMENTASI ALGORITMA RIVEST CHIPER 6 UNTUK KRIPTOGRAFI PESAN CHATTING BERBASIS MOBILE**

Dwi Setiawan

*Program Studi Informatika,Fakultas Teknologi Informasi dan Elektro
Universitas Teknologi Yogykarta*

*Jl. Ringroad Utara Jombor Sleman Yogyakarta*

*E-mail :* *dwisetiawan206@gmail.com*

**ABSTRAK**

*Telepon seluler merupakan salah satu alat komunikasi yang saat ini paling banyak digunakan. Salah satu fitur pada telepon seluler berbasis android yaitu chatting. Sudah banyak aplikasi chatting pada android namun hanya beberapa yang menyertakan kriptografi langsung oleh pengguna aplikasi . Proses kriptografi pada pesan chat yang diterima maupun dikirim dibuat pada penelitian ini. Pada proyek penelitian ini proses kriptografi menggunakan algoritma RC6. Algortma RC6 merupakan algoritma kriptografi yang cukup aman dan memilki performa tinggi dan memiliki kelebihan waktu enkripsi dan dekripsi yang cenderung cepat. Pada proyek penelitian ini aplikasi yang dibangun memiliki fungsi enkripsi dan dekripsi. Enkripsi dimaksudkan untuk menyamarkan dan melindungi informasi sedangkan dekripsi dimaksudkan untuk mengembalikan pesan seperti semula agar dapat dibaca oleh penerima. Pada proses enkripsi dan dekripsi diperlukan kunci untuk mengacak dan mengembalikan isi pesan. Kunci tersebut didapat ketika pengirim dan penerima berstemu sebelumnya bisa juga mengirim kunci melalui aplikasi tetapi kunci yang dikirim akan segera dihapus oleh aplikasi dimaksudkan agar orang lain tidak mengetahui kunci untuk membuka pesan.*

**Kata kunci** : *Kriptografi, Chatting, RC6.*

1. **PENDAHULUAN**
	1. **Latar Belakang**

Telepon selular merupakan alat komunikasi yang sudah dipakai oleh sebagian besar orang di dunia. Salah satu telepon selular yang saat ini populer adalah telepon seluler berbasis android. Platform android sudah dibekali fitur-fitur yang banyak sekali seperti pemutar multi media, game, layanan internet dan lain sebagainya. Fitur yang paling banyak digunakan pada android yaitu chat atau *chatting.* Fitur *chatting* sangat berperan penting untuk mengirim pesan ataupun bertukar informasi.

*Chatting* adalah adalah suatu pesan instant ataupun *instant messaging* di sebuah teknologi jaringan komputer yang mengijinkan pemakainya untuk mengirimkan pesan ke pengguna lain yang tersambung dalam sebuah jaringan komputer ataupun internet. *Chatting* sangat populer saat ini diantaranya karena sangat murah dalam berkomunikasi dan penggunanya dapat bebas mengirim pesan ketika terhubung dengan internet. Untuk beberapa orang yang memiliki jabatan dan peran penting disuatu pemerintahan seperti pegawai bank atau bahkan presiden tentunya berkomunikasi melalui chat harus berhati-hati karena bisa saja informasi penting diketahui oleh pihak ketiga. Hal ini tentu membahayakan jika pesan yang dikirim bersifat pribadi atau informasi penting yang tidak boleh diketahui pihak lain, sehingga dalam hal ini perlu adanya proses pengamanan pesan yang dikirim maupun yang diterima salah satu metode yang dapat digunakan yaitu dengan kriptografi.

Kriptografi adalah cabang ilmu yang mempelajari bagaimana cara menjaga data atau pesan tetap aman saat dikirimkan dari pengirim ke penerima, metode pengamanan sebuah data atau informasi dengan kriptografi sudah banyak digunakan salah satu metode kriptografi adalah Rivest Chiper 6(RC 6). Algoritma ini hamper sama dengan RC5 tetapi memiliki beberapa kelebihan dalam mengamankan data.

Berdasarkan uraian diatas, pada penelitian ini penulis akan mengimplementasikan algoritma rivest chiper 6 untuk pengamanan sebuah pesan chat pada platform android.

* 1. **Rumusan Masalah**

Berdasarkan latar belakang diatas maka didapatkan rumusan masalah adalah bagaimana merancang aplikasi yang mampu melakukan enkripsi dan dekripsi pada pesan *chatting* menggunakan algoritma Rivest Code 6 berbasis mobile

* 1. **Batasan Masalah**

Batasan masalah yang akan dikaji dalam penelitian ini mencakup batasan-batasan sebagai berikut :

* + - * 1. Perancangan aplikasi menggunakan algoritma Rivest Code 6 untuk enkripsi maupun dekripsi pesan.
				2. Aplikasi yang dirancang hanya untuk telepon seluler berbasis android.
				3. Pengirim ataupun penerima pesan harus memiliki kunci yang sama.
				4. Pengguna harus sama-sama menggunakan aplikasi ini
				5. Pesan yang dikirim hanya berupa teks.
				6. Aplikasi tidak dapat mengirim ataupun menerima gambar.
				7. Aplikasi yang dibangun tidak diperuntukan untuk banyak user.
				8. Pesan yang masuk tidak akan memberikan notifikasi.
				9. Kontak pada aplikasi merupakan semua user yang menggunakan aplikasi.
	1. **Tujuan Penelitian**

Adapun tujuan penelitian ini adalah untuk membuat aplikasi keamanan Membantu seseorang dalam mengamankan sebuah pesan .

* 1. **Manfaat Penelitian**

Adapun manfaat dilakukanya penelitian ini yaitu diharapkan membantu dalam mengamankan pesan yang dikirim atau chat yang dikirim pada ponsel android untuk menghindari adanya pencurian informasi yang bersifat pribadi ataupun rahasia.

1. **LANDASAN TEORI**
	1. **Kajian Hasil Penelitian**

Penelitian oleh Akhir dan Dalimunthe (2015) tentang perancangan dan implementasi aplikasi chatting menggunakan android. Penelitian tersebut membahas tentang pemodelan sistem, analisis, dan desain sistem dalam pembuatan aplikasi chatting. Pembuatan aplikasi pada proyek tersebut menggunakan Eclipse dan MySQL sebagai database. Adapun manfaat penelitian tersebut yaitu memberi kemudahan bagi pengguna android dalam mengirimkan pesan.

Penelitian yang dilakuan oleh Zulham, dkk (2014) tentang keamanan email dengan kriptografi menggunakan algoritma Rivest Code 6 (RC6). Untuk memenuhi persyaratan AES yang diantaranya adalah kemampuan untuk beroprasi pada mode blok128 bit. Jika besar blok 128 bit langsung dipaksakan untuk diimplementasikan dengan algoritma RC5,maka akan dibutuhkan register kerja 64 bit. Hasil dari penelitian tersebut adalah sebuah aplikasi berbasis android yang mampu mengirim dan menerima pesan melalui email, aplikasi tersebut menggunakan algoritma RC6 sehinnga tingkat keamanan lebih terjamin, karena algoritma RC6 menggunakan algoritma blok chiper dengan 4 register sehingga lebih sulit untuk dipecahkan keamannya .

Penelitian oleh Indra (2014) dalam penelitianya tentang enkripsi pesan SMS berbasis android untuk mempertimbangkan solusi *encrypted end to end* dengan melakukan enkripsi terhadap pesan SMS. Enkripsi adalah proses mengubah suatu pesan asli yang biasa disebut *plaintext* menjadi sebuah sandi atau kode yang tidak terbaca yang biasa disebut *chipertext* dan untuk mengembalikanya diperlukan proses dekripsi. Hasil dari penelitian tersebut adalah sebuah aplikasi android yang mampu mengenkripsi pesan SMS .Namun aplikasi tersebut belum dapat mengirimkan langsung kunci enkripsi dan kunci dekripsinya bersamaan pesan teks.

Peneletian yang dilakukan Harsh dan Ravindra (2012) tentang analisis kinerja algoritma enkripsi RC6, Twofish, dan Rijindael. Pengujian ketiga algoritma tersebut atas dasar waktu efesiensi dalam melakukan enkripsi, pemanfaata sumberdaya dan pemanfaatan memori. Twofish dan Rijndael memiliki struktur yang sama dalam melakukan enkripsi dan dekripsi, sedangkan RC6 berbeda dalam penelitian tersebut ketiga algoritma telah dievaluasi pada kunci 128 bit,192 bit dan 256 bit. Hasil dari penelitian tersebut menujukan algoritma RC6 adalah algoritma block chipper yang lebih cepat dan lebh sederhana daripada Twofish dan Rijndael. RC6 sangat lebih unggul dimana tingkat enkripsi yang tinggi sementara Rijndael lebih unggul pada memori.

Penelitian yang dilakukan oleh Igor (2007) dalam penelitiannya mengenai perbandingan algoritma RC6 dengan algoritma Rijndael. *Data Encryption Standard* (DES) telah menjadi standar algoritma enkripsi sejak lama.Namun seiring dengan perjalanan waktu, semakin lama standar ini semakin tidak aman dan mudah untuk diserang. Oleh sebab itulah *National Institute of Standards and Technology* (NIST) mengusulkan pembentukan standar baru yang diberi nama *Advanced Encryption* *Standard* (AES). Dalam perlombaan memperebutkan kandidat AES yang baru, terpilihlah algoritma Rijndael sebagai pemenang, dan dinobatkan sebagai standar algoritma enkripsi yang baru berdasarkan pemungutan suara. Namun NIST sendiri menyatakan pada putaran final bahwa setiap algoritma yang dipertandingkan memiliki kelebihan dan kekurangan masing-masing, dan tidak ada satupun algoritma yang jauh lebih baik daripada algoritma lainnya.Maka pada penelitian yang dilakukan peneliti tersebut, dilakukan perbandingan algoritma RC6 sebagai salah satu finalis AES pada putaran final dengan algoritma Rijndael yang dinobatkan sebagai AES dengan melihat dimana kelemahan, kemiripan dan kelebihan algoritma RC6 sebagai kandidat AES bila dibandingkan dengan algoritma Rijndael beserta implementasi pada algoritmanya. Hasil dari penelitian tersebut yaitu RC6 memiliki kelebihan dalam bidang data dependent dalam enkripsinya dibandingkan Rijndael, Kode untuk RC6 lebih sederhana dibandingkan dengan Rijndael,RC6 juga tidak menghabiskan penggunaan memori yang banyak bila diterapkan ke dalam smart card dan Untuk urusan keamanan, kedua algoritma ini masih bekerja dalam performa yang sangat baik.

* 1. **Dasar Teori**
		1. **Kriptografi**

Menurut Ariyus (2008) dalam bukunya “Pengantar Ilmu Kriptografi”, kriptografi *(cryptografi)* berasal dari bahasa yunani yaitu *cryptos* artinya rahasia dan *graphein* artinya tulisan. Jadi kriptografi berarti tulisan rahasia. Secara istilah kriptografi didefinisikan sebagai ilmu sekaligus seni untuk menjaga kerahasiaan pesan (data atau informasi) yang mempunyai arti atau nilai, dengan menyamarkan atau mengacak menjadi bentuk yang tidak dimengerti menggunakan algoritma tertentu.

Dalam ilmu kriptografi suatu pesan yang akan dirahasiakan atau disandikan disebut dengan *plaintext*, sedangkan pesan yang telah disandikan sehingga tidak memiliki nilai dan arti lagi dengan tujuan agar pesan tidak dapat dibaca oleh pihak yang tidak berhak disebut *chipertext*. Dalam ilmu kriptografi juga terdapat istilah enkripsi dan deskripsi. Enkripsi merupakan proses menjadikan *plaintext* menjadi *chipertext* dengan menggunakan algoritma tertentu. Sedangkan proses mengembalikan *chipertext* menjadi *plaintext* disebut deskripsi.

* + 1. **Rivest Chiper 6**

Menurut Ariyus (2008) RC6 merupakan algoritma yang merupakan keturunan dari RC5 yang juga merupakan kandidat AES (*Advanced Encryption Standard*). Pada mulanya, perancangan RC6 diawali ketika RC5 dianggap dapat dijadikan kandidat untuk mengikuti kompetisi pemilihan AES. Modifikasi kemudian dibuat untuk meningkatkan keamanan dan performa dan juga untuk dapat memenuhi persyaratan AES.

RC6 dirancang untuk menghilangkan segala ketidakamanan yang ditemukan pada RC5, karena analisis pada RC5 menunjukkan bahwa ternyata jumlah rotasi yang terjadi pada RC5 tidak sepenuhnya bergantung pada data yang terdapat dalam blok. Selain itu, serangan kriptanalisis diferensial juga ternyata dapat menembus keamanan yang ditawarkan RC5.

RC6 juga dirancang untuk memenuhi persyaratan AES yang diantaranya adalah kemampuan untuk beroperasi pada mode blok 128 bit. Jika besar blok 128 bit langsung dipaksakan untuk diimplementasikan dengan algoritma RC5, maka akan dibutuhkan register kerja 64 bit. Spesifikasi arsitektur dan bahasa yang menjadi tempat implementasi algoritma yang ditentukan oleh AES belum mendukung pengoperasian 64 bit yang efisien. Oleh karena itu, daripada menggunakan 2 register 64 bit seperti pada RC5, RC6 menggunakan 4 register 32 bit. Karena menggunakan 4 register maka akan terdapat 2 operasi rotasi pada setiap *half-round* yang ada, dan juga akan lebih banyak bit-bit yang akan digunakan untuk mempengaruhi banyaknya bit yang dirotasi.

RC6 seperti juga RC5 mengeksploitasi penggunaan operasi-operasi primitif yang diimplementasikan secara efisien dalam prosesor-prosesor modern. RC6 juga selain menggunakan ketiga operasi primitif yang digunakan dalam RC5, juga menggunakan operasi perkalian 32-bit yang telah diimplementasikan secara efisien dalam prosesor modern saat ini. Primitif operasi perkalian ini sangat efektif dalam menghasilkan efek “*diffusion*” atau penyebaran yang tentu saja mengakibatkan RC6 lebih aman daripada RC5. Operasi perkalian ini digunakan untuk menghitung jumlah bit yang dirotasi sehingga konsep *data-dependent rotations* dapat dengan lebih sempurna diimplementasikan .

1. Algoritma

Algoritma RC6 seperti juga RC5 merupakan algoritma *cipher* yang terparameterisasi. RC6 secara tepat ditulis sebagai: 5

**RC6 – w / r / b**

Nilai parameter w, r, dan b menyatakan hal yang sama seperti yang ditunjukkan dalam algoritma RC5. Algoritma RC6 yang dipakai sebagai kandidat AES adalah RC6-32/20/b, yang berarti ukuran *word* 32 bit, jumlah ronde 20 kali, dengan panjang kunci b ditentukan pengguna.

1. Key Expansion Algorithm

Algoritma untuk membangkitkan kunci internal sama seperti pada RC5. Nilai konstanta Pw dan Qw yang digunakan juga sama, tetapi ukuran array S tidak sama dengan yang seperti RC5. Ukuran t dari array S dalam RC6 adalah t = 2(r+2), yang berarti terdapat lebih banyak kunci internal yang dibangkitkan daripada jumlah kunci internal RC5. Berikut algoritmanya:

S[0] = Pw

fori = 1 to (2r + 3) do

S[i] = S[i – 1] + Qw

i = 0

j = 0

A = 0

B = 0

for3 × max(c, (2r + 4)) times do

S[i] = (S[i] + A + B) <<< 3

A = S[i]

L[i] = (L[j] + A + B) <<< 3

B = L[i]

i = (i + 1) mod (2r+4)

j = (j + 1) mod c

1. Algoritma Enkripsi

Fungsi enkripsi menerima input 1 blok plaintext yang terbagi dalam 4 register yang masing-masing berupa w-bit word, yaitu A, B, C, dan D. Ciphertext hasil proses terbagi dan disimpan dalam A, B, C, dan D. Dalam proses enkripsi diperlukan tabel kunci S yang dianggap telah didapat dari proses sebelumnya.

Secara lebih detail, proses enkripsi dengan RC6 dapat dibagi dalam beberapa langkah. Dalam penjelasan berikut, notasi (A,B,C,D) = (B,C,D,A) berarti adalah operasi assignment yang dilakukan paralel (bersamaan) untuk setiap elemen di ruas kanan ke ruas kiri yang berkorespondensi. Langkah-langkahnya adalah sebagai berikut:

1. Mula-mula lakukan *half-round loop* yang seperti pada RC5:

**for**i = 1 **to** r **do**

A = ((AB) <<< B) + S[i] ⊕

(A,B) = (B,A)

1. Lakukan dua proses RC5 secara paralel, yang satu untuk register A, B dan yang lain untuk register C, D.

fori = 1 to r do

A = ((AB) <<< B) + S[2i] ⊕

C = ((CD) <<< D) + S[2i+1] ⊕

(A,B) = (B,A)

(C,D) = (D,C)

1. Pada tahap pertukaran, daripada menukar A dengan B, dan C dengan D, lakukan permutasi antar keempat register (A,B,C,D) = (B,C,D,A), sehingga komputasi AB bercampur dengan komputasi CD.

fori = 1 to r do

A = ((AB) <<< B) + S[2i] ⊕

C = ((CD) <<< D) + S[2i+1] ⊕

(A,B,C,D) = (B,C,D,A)

1. Campurkan komputasi AB dengan CD lebih jauh, yaitu dengan mempertukarkan kedua nilai yang menyatakan jumlah rotasi pada masing-masing komputasi.

fori = 1 to r do

A = ((A⊕B) <<< D) + S[2i]

C = ((C⊕D) <<< B) + S[2i+1]

(A,B,C,D) = (B,C,D,A)

1. Daripada menggunakan nilai B dan D secara langsung, RC6 menggunakan hasil transformasi kedua register ini. Hal ini dilakukan untuk tidak mengulangi masalah rotasi seperti pada RC5 di mana tidak seluruh bit dalam data yang berpengaruh dalam rotasi. Oleh karena itu, fungsi transformasi yang dipilih harus dapat memanfaatkan seluruh bit di dalam data untuk mengatur jumlah bit yang dirotasikan. Fungsi yang dipilih adalah *f(x) = x(2x + 1) (mod 2w)* yang kemudian diikuti dengan

rotasi ke kiri sebanyak 5 bit. Transformasi ini terpilih karena fungsi f(x) yang merupakan fungsi satu-ke-satu memiliki bit-bit orde atas yang menentukan jumlah rotasi yang akan digunakan yang sangat bergantung pada x.

fori = 1 to r do

p = (B × (2B + 1)) <<< 5

q = (D × (2D + 1)) <<< 5

A = ((A⊕p) <<< q) + S[2i]

C = ((C⊕q) <<< p) + S[2i+1]

(A,B,C,D) = (B,C,D,A)

1. Setelah *loop* di atas selesai, akan terdapat hasil di mana *plaintext* bisa menunjukkan bagian input ronde pertama dalam enkripsi dan *ciphertext* bisa menunjukkan bagian input ronde terakhir dalam enkripsi. Oleh karena itu perlu ditambahkan langkah-langkah di awal dan di akhir *loop* untuk menyamarkan hubungan ini. Sehingga, terbentuklah algoritma enkripsi RC6 yang sebagai berikut:

B = B + S[0]

D = D + S[1]

fori = 1 to r do

p = (B × (2B + 1)) <<< 5

q = (D × (2D + 1)) <<< 5

A = ((A⊕p) <<< q) + S[2i]

C = ((C⊕q) <<< p) + S[2i+1]

(A,B,C,D) = (B,C,D,A)

A = A + S[2r + 2]

C = C + S[2r + 3]

Perlu diketahui juga, dalam varian baru RC6 jumlah rotasi ke kiri yang mengikuti fungsi kuadrat bukan 5 bit tetapi adalah 2log(w) bit.

1. Algoritma Deskripsi

Sama seperti pada RC5, algoritma dekripsi RC6 juga merupakan penurunan dari algoritma enkripsi. Algoritmanya sebagai berikut:

C = C – S[2r + 3]

A = A – S[2r + 2]

**for**i = r **downto** 1 **do**

(A,B,C,D) = (D,A,B,C)

p = (D × (2D + 1)) <<< 5

q = (B × (2B + 1)) <<< 5

C = ((C – S[2i + 1]) >>> q)p ⊕

A = ((A – S[2i]) >>> p)q ⊕

D = D – S[1]

B = B – S[0]

* + 1. **Chatting**

Menurut Brilianto Ricky (2008) [chatting adalah](http://www.pengertianahli.com/2015/01/pengertian-chatting-apa-itu-chatting.html) percakapan dua orang atau lebih secara *realtime* melalui [jaringan internet.](http://www.pengertianahli.com/2013/11/pengertian-internet-terupdate.html) Chatting merupakan salah satu fasilitas yang ditawarkan oleh internet pada penggunanya untuk berkomunikasi langsung lewat percakapan. Cara chatting yang lebih umum dikenal adalah dengan cara mengetikkan pesan pada layar dan akan dibalas dengan bentuk pesan kembali, seperti cara mengirimkan [SMS.](http://id.wikipedia.org/wiki/SMS) Namun, chatting di internet tidak terbatas pada jumlah karakter sehingga pengguna dapat menulis pesan cukup panjang. Dengan perkembangan program atau [software](http://www.pengertianahli.com/2013/10/pengertian-software-perangkat-lunak.html) yang ditawarkan saat ini, pengguna internet sudah dapat ber-chatting dengan berbicara dan mengirimkan gambar kepada teman chatting di tempat lain. Misalnya, teknologi Yahoo Messanger yang memberikan fasilitas chatting untuk saling bertatap muka melalui sebuah kamera kecil. Namun, kamera ini harus dimiliki oleh pengguna internet jika ingin memanfaatkan fasilitas tersebut. Jadi, saat ini pengguna internet dapat ber-chatting melalui tulisan, suara, atau bertatap muka. Yang harus diingat bahwa semua fasilitas bisa digunakan jika teman chatting juga memiliki fasilitas yang sama.

* + 1. **Android**

Menurut Nazrudin Safaat (2012 : 1). 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.

1. **METODOLOGI PENELITIAN**

Dalam metode penelitian ini terdapat beberapa tahap untuk menyelesaikan penelitian ini, diantaranya :

## Pengumpulan Data

Pengumpulan data merupakan sebuah metode atau cara untuk mendapatkan sebuah informasi yang akan digunakan untuk pembangunan sebuah sistem. Pada tahap pengumpulan data ini terdapat beberapa hal yang harus dilakukan untuk membangun sebuah sistem, diantaranya adalah sebagai berikut :

1. Observasi

Observasi merupakan salah satu teknik pengumpulan data yang cukup efektif untuk mempelajari sistem baru. Observasi adalah pengamatan langsung suatu kegiatan yang sedang berjalan dan data yang diperlukan untuk memenuhi kebutuhan sistem yang akan dibuat.

1. Wawancara

Pengumpulan data dilakukan dengan menggunakan metode wawancara dilakukan dengan tujuan mendapatkan data-data yang dapat diolah secara mendalam dari mengubah teks biasa *(plain text)* menjadi text yang sudah dienkripsi *(chipper text).* Dalam wawancara ini dilakukan dengan Bapak Tri Widodo, M.Kom, yang mana beliau fokus di bidang kriptografi atau keamanan data. Wawancara ini dilakukan untuk mendapatkan informasi data untuk mengenkripsi teks menggunakan mtode RC6.

1. Studi Pustaka

Pengumpulan data dilakukan dengan cara membaca buku-buku yang berkaitan dengan penelitian, mencari refrensi dari internet dan dokumentasi lain yang berhubungan dengan penelitian. Buku yang digunakan sebagai refrensi salah satunya adalah buku “Pengantar Ilmu Kriptografi” pengarang Dony Ariyus tahun cetak 2008 dan beberapa buku dan refrensi lainya yang dijadikan acuan untuk menyusun laporan ini.

## Analisis

 Pengumpulan data dilakukan dengan cara membaca buku-buku yang berkaitan dengan penelitian, mencari refrensi dari internet dan dokumentasi lain yang berhubungan dengan penelitian. Buku yang digunakan sebagai refrensi salah satunya adalah buku “Pengantar Ilmu Kriptografi” pengarang Dony Ariyus tahun cetak 2008 dan beberapa buku dan refrensi lainya yang dijadikan acuan untuk menyusun laporan ini.

## Desain Sistem

Desain sistem dapat didefinisikan sebagai tahap setelah analisis dari siklus pengembangan sistem. Pendefinisian dari kebutuhan-kebutuhan fungsional dan persiapan untuk rancang bangun implementasi menggambarkan bagaiman suatu sistem dibangun**.**

1. Perancangan Sistem

Perancangan sistem akan dilakukan menggunakan UML (*Unified Modeling Language*). UML merupakan suatu bahasa visual untuk untuk pemodelan dan komunikasi mengenai sebuah sistem dengan menggunakan diagram dan teks-teks pendukung. UML hanya berfungsi untuk melakukan pemodelan. Jadi penggunaan UML tidak terbatas pada metodologi tertentu, meskipun pada kenyataannya UML paling banyak digunakan pada metodologi berorientasi objek.

1. Perancangan Basis Data

Perancangan basis data digunakan untuk menjelaskan hubungan antar data berdasarkan objek-objek dasar data yang memiliki hubungan antar relasi. Dalam hal ini desain basis data digunakan untuk memodelkan struktur data, dan untuk menggambarkannya digunakan beberapa notasi dal symbol, perancangan basis data dalam penelitian ini penulis menggunakan *software* EDraw.

1. Perancangan Interface

Perancangan *interface* untuk aplikasi *chatting* akan dibuat dengan beberapa form untuk menggambarkan tampilan aplikasi yang akan dibangun, perancangan *interface* dalam penelitian ini penulis menggunakan *software* balsamic mockup.

## Implementasi Sistem

Tahap ini adalah tahap implementasi dari perancangan yang sudah dibuat sebelumnya, menggunakan pemrograman berbasis m*obile* android.

1. **HASIL DAN PEMBAHASAN**
	1. **Analisa Sistem**

Sistem yang dibangun merupakan sebuah aplikasi kirim pesan melalui internet (*chatting)* berbasis mobile dengan menyisipkan algoritma rivest chipper 6 (RC6) dalam mengirim ataupun membuka pesan. Algoritma rivest chipper digunakan untuk mengenkripsi pesan yang kirim dengan menggunakan kunci (*key*) sehingga pesan berubah menjadi sebuah pesan yang tidak dapat dibaca oleh orang lain, selanjutnya pesan tersebut dikirim. Algoritma rivest chipper 6 (RC6) juga digunakan untuk mendekripsi pesan untuk melihat pesan asli penerima pesan harus memasukkan kunci yang sama pada saat pengirim mengenkripsi pesan.

* 1. **Analisa Kebutuhan Sistem**

Analisa kebutuhan sistem dilakukan untuk membangun sistem yang sesuai dengan kebutuhan yang diinginkan. Proses analisa sistem adalah proses yang harus dilakukan sebelum implementasi algoritma Rivest Chiper 6 (RC6) kedalam aplikasi chatting di android, sehingga proses pembuatan perangkat lunak menjadi lebih terstruktur. Analisa kebutuhan sistem mencakup tentang *software, hardware* yang diperlukan dalam pembuatan sistem.

1. Kebutuhan Perangakat Keras

Perangkat keras yang digunakan penulis dalam pembuatan aplikasi ini adalah sebagai berikut :

Komputer **:**

* + - * 1. Processor AMD A8-7410 APU with Radeon R5 Graphics (4 CPUs) ~2.2 GHz
				2. RAM 8 GB
				3. VGA AMD Radeon R5 Graphics
				4. Hardisk 500 GB

SmarthPhone **:**

* + - * 1. Device : Xiaomi mi 4c
				2. CPU : Hexa-core Max 1.8Ghz
				3. RAM : 2GB
				4. Android OS :Lollipop
1. Kebutuhan Perangkat Lunak

Perangkat lunak yang digunakan dalam pembuatan aplikasi ini yaitu sebagai berikut :

* + - * 1. Sistem operasi Windows 10 Pro 64 bit
				2. Android SDK
				3. Sublime
				4. Xampp
				5. Postman
				6. Android Studio
	1. **Analisa Pengembangan Sistem**

Pada tahap analisa pengembangan sistem dibuat sebuah rancangan dari aplikasi yang akan dibuat dengan menggunakan *Unified Modeling Language* (UML). Dalam tahap ini akan diberikan perincian tentang desain *input*, desain *output*, desain basis data, desain proses dan desain *interface* dari sistem yang akan dibangun .

* 1. **Rancangan Sistem**

Menurut Rossa dan Salahuddin (2016) UML merupakan bahasa visual untuk pemodelan dan komunikasi mengenai sebuah sistem dengan menggunakan diagram dan teks-teks pendukung. UML hanya berfungsi untuk melakukan pemodelan. Jadi penggunaan UML tidak terbatas pada metodologi tertentu, meskipun pada kenyataannya UML paling banyak digunakan pada metodologi berorientasi objek.

### Use Case Diagram

Use case diagram bertujuan untuk 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. Use case diagram untuk sistem yang akan dibangun terlihat pada Gambar 4.2.



*Gambar 4.1 : Use case diagram*

### Class Diagram

Berikut adalah class diagram untuk menggambarkan skema database yaitu table-tabel yang akan dibuat dalam database ditunjukkan pada Gambar 4.3.



*Gambar 4.2 : Class Diagram*

### Activity Diagram

Diagram aktivitas atau *activity diagram* menggambarkan *workflow* (aliran kerja) atau aktivitas dari sebuah sistem atau proses bisnis atau menu yang ada pada perangkat lunak.

### Sequence Diagram

Diagram sekuen atau *sequence diagram* menggambarkan kelakuan objek pada *use case* dengan mendeskripsikan waktu hidup objek dan *message* yang dikirimkan dan diterima antar objek. *Sequence diagram* untuk aplikasi chatting dengan RC6 digambarkan sebagi berikut :

1. Sequence Diagram Kirim Pesan

*Sequence diagram* kirim pesan menggambarkan bagaimana pengguna aplikasi dapat mengirim pesan, untuk dapat mengirim pesan pengguna aplikasi harus masuk ke menu utama lalu memilih menu tulis pesan. Setelah menulis pesan, proses selanjutnya diminta kunci untuk mengenkripsi pesan pada fungsi RC6 dan mengenkripsi pesan yang ditulis. Setelah pesan selesai dienkripsi maka hasil enkripsi akan tampil pada fungsi tulis pesandan kemudian pesan dapat dikirim dan pengirim dapat status pengiriman. Berikut adalah *sequence diagram* kirim pesan terlihat pada Gambar 4.5.



*Gambar 4.3 : Sequence diagram kirim pesan*

1. Sequence Diagram Buka Pesan

*Sequence diagram* buka pesan menggambarkan bagaimana pengguna aplikasi dapat membuka pesan yang kirim oleh pengirim pesan. Setelah masuk menu utama pengguna aplikasi masuk ke menu *inbox* lalu memilih pesan yang akan dibuka dan sistem meminta pengguna aplikasi memasukkan kunci yang sama dengan kunci enkripsi pada fungsi RC6, setelah penerima pesan memasukkan kunci maka sistem melakukan dekripsi yang kemudian hasil pesan akam tampil di isi pesan yang dapat dibaca oleh penerima. Sequence diagram buka pesan terlihat pada Gambar 4.6



*Gambar 4.4 : Sequence diagram buka pesan*

* 1. **Implementasi**

Implementasi dari proses analisis dan perancangan yang telah dilakukan pada bab sebelumnya. Implementasi bertujuan untuk menjelaskan *source code* dalam membangun aplikasi ,cara kerja aplikasi, bagaimana aplikasi berjalan. Pada tahap implementasi ini menghasilkan sebuah aplikasi mobile android untuk mengenkripsi dan mendekripsi pesan menggunakan algoritma RC6, untuk menggunakan aplikasi ini pengguna harus mendaftarkan diri atau registrasi untuk dapat masuk. Proses enkripsi dan dekripsi pesan memerlukan key yang sudah diketahui oleh pengirim dan penerima sebelumnya key ini dapat berubah-ubah sesuai pengirim dan penerima kehendaki. Pengirim dan penerima harus merahasiakan key supaya nantinya pesan tidak dapat didekripsi oleh pihak ketiga. *key* ini nantinya untuk menyamarkan pesan yang dikirim dan mengembalikan pesan yang disamarkan menjadi pesan asli yang dapat dibaca oleh penerima.

### Halaman Inbox

Tampilan halaman Menu Inbox akan muncul ketika user telah login. Halaman menu inbox berisi pesan yang masuk.Pesan yang masuk akan di *filter* sesuai dengan tanggal dan jam yang baru masuk sehingga pesan yang baru masuk akan muncul dipaling atas di list inbox (pesan masuk). Pada layout ini diatasnya terdapat navigation bar *inbox, outbox, friends* dan *about* untuk menuju ke layout selanjutnya. Pada layout ini juga terdapat *floating action button* yang terdapat di paling bawah layout *floating action button* ini digunakan untuk menuju ke menu tulis pesan. Tampilan halaman utama dijelaskan pada gambar 4.5



*Gambar 4.5 : Halaman Inbox*

### Halaman Outbox

Tampilan menu *outbox* berisi pesan yang dikirim oleh user, untuk menandai user berada pada menu *outbox* pada *navigation bar* terdapat garis bawah pada icon *outbox*. Tampilan menu *outbox* dijelaskan pada gambar 4.6.



*Gambar 4.7 : Halaman Outbox*

### Halaman Kontak

Tampilan menu kontak berisi daftar pengguna aplikasi yang menggunakan aplikasi pesan terenkripsi ini. Semua user pada aplikasi ini dapat mengirim dan menerima pesan dari siapapun. Tampilan menu kontak dijelaskan pada gambar 4.8.



*Gambar 4.8 : Halaman Kontak*

### Halaman Kunci

Tampilan menu kunci berisi kunci yang masuk kepada penerima pesan untuk membuka pesan yang terenkripsi, kunci yang dikirim akan dihapus aplikasi dalam waktu 10 menit. Tampilan menu kunci dijelaskan pada gambar 4.8.



*Gambar 4.9 : Halaman Kunci*

### Halaman Kirim Pesan

Tampilan kirim pesan akan muncul ketika pengguna aplikasi *klik floating action button* pada layout *inbox*. Halaman kirim pesan digunakan untuk mengirim pesan terenkripsi. Untuk mengirim pesan pengguna aplikasi diminta untuk memilih tujuan user yang akan dikirim pesan, kemudian mengisi pesan yang akan dikirim dan memasukkan *key* untuk mengenkripsi pesan *key* ini nantinya digunakan untuk membuka pesan, kemudian klik *encrypt* maka pesan akan terenkripsi dan klik tombol kirim untuk mengirim pesan. Halaman kirim pesan dijelaskan pada gambar 4.10.



*Gambar 4.10 : Halaman Kirim Pesan*

### Halaman Buka Pesan

Halaman buka pesan digunakan untuk membuka pesan yang sudah dikirim oleh pengirim. Halaman buka pesan akan muncul ketika list pesan masuk diklik maka akan membuka pesan sesuai pesan yang dipilih. Pada halaman buka pesan penerima diminta untuk memasukkan *key* untuk mendekripsi pesan ketika *key* yang dimasukkan salah maka pesan didekripsi tidak sesuai pesan asli, ketika *key* yang dimasukkan benar maka pesan terenkripsi akan didekripsi sesuai pesan aslinya. Halaman buka pesan dijelaskan pada gambar 4.11.



*Gambar 4.11 : Halaman Buka Pesan*

1. **PENUTUP**
	1. **Kesimpulan**

Berdasarkan penelitian dengan mengimplementasikan algoritma rivest chipper 6 pada pesan chatting berbasis mobile dapat ditarik kesimpulan sebagai berikut :

* + - * 1. Aplikasi dikembangkan menggunakan tool android studio dan database MySQl dan postman untuk uji JSON.
				2. Aplikasi yang telah dibangun sudah dapat mengenkripsi pesan.
				3. Aplikasi yang telah dibangun sudah dapat mendekripsi pesan dengan tepat sesuai pesan yang dikirim.
				4. Aplikasi yang telah dibangun sudah dapat mengirim dan menerima pesan.
				5. Aplikasi yang telah dibangun sudah dapat menampilkan kontak.
	1. **Saran**

Adapun saran untuk peneliti selanjutnya adalah sebagai berikut :

* + - * 1. Profil user sebaiknya ditambahkan foto dengan tujuan user lebih mudah dikenali.
				2. Menambahkan notifikasi ketika pesan masuk.
				3. Sebaiknya menggunakan database firebase karena lebih realtime ketika mengirim dan menerima pesan.

**DAFTAR PUSTAKA**

Ariyus, D. (2008). *Pengantar Ilmu Kriptografi.* Yogyakarta: Penerbit Andi.

Akhir, L.T. & Dalimunthe, I.A. (2015).Perancangan dan Pembuatan Aplikasi Mobile Chatting Berbasis Android. Poloteknik Negeri Medan. Medan.

Bonny, I. Perbandingan Algoritma RC6 dengan Rijndael pada AES. Jurusan Teknik Informatika ITB, Bandung.

Indra, M. (2014). Implementasi Algoritma RC6 Untuk Dekripsi dan Enkripsi SMS Berbasis Android. STMIK AMIKOM. Yogyakarta.

Ricky, B. (2008). Paduan Praktis Internet. Jakarta : Puspa Swara.

Rosa, A., & Shalahudin, M. (2016). *Rekayasa Perangkat Lunak Terstruktur dan Berorientasi Objek*. Bandung: Penerbit Informatika.

Safaat, N.H. (2015). *Berbagai Implementasi dan Pengembangan Aplikasi Berbasis Android.* Bandung: Informatika Bandung.

Supardi,Y. (2012). *Sistem Operasi Andal Android.* Jakarta: Elex Media Komputindo.

Verma, H.K. & Singh, R.K., *Performance Analysis of RC6, Twofish and Rijndael Block Cipher Algorithm*s. India: International Journal of Computer Applications (0975 – 8887),Volume 42– No.16.

Zulham, M., Kurniawan ,H., & Rahmad ,I.F. (2014). Perancangan Aplikasi Keamanan Data Email Menggunakan Algoritma Enkripsi RC6 Berbasi Android. STMIK Potensi Utama. Medan. Indonesia.