

**APLIKASI PENGIRIMAN TEKS VIA EMAIL YANG AMAN
DENGAN MENGGUNAKAN ALGORITMA RSA-CRT**



SKRIPSI

**Disusun Sebagai Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana Komputer
Departemen Ilmu Komputer / Informatika**

**Disusun oleh:
Samsul Ma'arif
J2F009018**

**DEPARTEMEN ILMU KOMPUTER/INFORMATIKA
FAKULTAS SAINS DAN MATEMATIKA
UNIVERSITAS DIPONEGORO**

2016

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Saya yang bertanda tangan di bawah ini :

Nama : Samsul Ma'arif

NIM : J2F009018

Judul : Aplikasi Pengiriman Teks via *Email* yang Aman dengan Menggunakan Algoritma RSA-CRT

Dengan ini saya menyatakan bahwa dalam tugas akhir/ skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan di dalam daftar pustaka.

Semarang, 10 Agustus 2016

Samsul Ma'arif

J2F009018

HALAMAN PENGESAHAN

Judul : Aplikasi Pengiriman Teks via *Email* yang Aman dengan Menggunakan Algoritma RSA-CRT

Nama : Samsul Ma'arif

NIM : J2F009018

Telah diujikan pada sidang tugas akhir pada tanggal 1 Juli 2016 dan dinyatakan lulus pada tanggal 1 Julii 2016.

Semarang, 10 Agustus 2016

Mengetahui,

Ketua Departemen Ilmu Komputer /
Informatika FSM UNDIP

Panitia Penguji Tugas Akhir
Ketua,

Ragil Saputra, S.Si, M.Cs

NIP. 19801021 200501 1 003

Nurdin Bahtiar, S.Si, M.T

NIP. 19790720 200312 1 002

HALAMAN PENGESAHAN

Judul : Aplikasi Pengiriman Teks via *Email* yang Aman dengan Menggunakan Algoritma
RSA-CRT

Nama : Samsul Ma'arif

NIM : J2F009018

Telah diujikan pada sidang tugas akhir pada tanggal 1 Juli 2016.

Semarang, 10 Agustus 2016

Pembimbing

Sukmawati Nur Endah, S.Si, M.Kom

NIP. 19780502 200501 2 002

ABSTRAK

Perkembangan teknologi yang sangat pesat membuat manusia semakin mudah dalam melakukan aktifitasnya sehari-hari contohnya pengiriman pesan via *email*. Namun dengan perkembangan teknologi juga membuat pengiriman pesan menjadi semakin tidak aman. Oleh karena itu dibutuhkan sebuah teknik untuk mengamankan pesan sehingga tidak terjadi perubahan pesan di tengah jalan oleh pihak ketiga, diantaranya dengan menggunakan kriptografi. Salah satu algoritma dalam kriptografi yang dapat berfungsi untuk mengamankan teks adalah algoritma RSA. Dalam perkembangannya proses RSA memiliki masalah saat melakukan proses dekripsinya, yaitu membutuhkan waktu yang relatif lama sehingga ditambahkan algoritma CRT (*Chinese Remainder Theorem*) untuk mempercepat waktu dekripsi. Pada penelitian ini mengimplementasikan algoritma RSA-CRT pada pengiriman teks via *email*. Penelitian ini menggunakan model proses *waterfall* yang diimplementasikan dengan menggunakan bahasa pemrograman MatLab. Berdasarkan hasil penelitian, algoritma RSA-CRT dapat diimplementasikan pada pengiriman sebuah pesan via *email*. Pada penelitian ini dapat disimpulkan bahwa kecepatan waktu algoritma RSA-CRT lebih cepat dibandingkan dengan algoritma RSA. Semakin besar parameter nilai n berdampak pada waktu proses dekripsinya begitu juga ukuran teksnya semakin besar.

Kata kunci : Kriptografi, Pengiriman Teks, algoritma RSA, algoritma CRT, algoritma RSA-CRT, *waterfall*, MatLab, *email*.

ABSTRACT

The rapid advancement of technology makes human easier to do their daily activities, such as sending messages via email. On the down side, the rapid advancement of technology also makes sending a message via email becomes insecure. Therefore, a technique for securing messages is needed, so that the message would not be changed by the third party in the middle of the line, which can be done by cryptography technique. One of the cryptography algorithm which could securing texts is RSA algorithm. On the progress, the RSA algorithm still having an issue when decrypting texts, where it needs relatively more time so it has to be added with CRT (*Chinese Remainder Theorem*) algorithm to fasten the decrypting process. This study implemented RSA-CRT algorithm for sending texts via *email*. This study used *waterfall* method as model process and MatLab as programming language. Based on this study, RSA-CRT algorithm could be implemented for securing the process of sending texts via *email*. This study concludes that the elapse time of RSA-CRT algorithm is faster than RSA algorithm. The bigger the parameter value of n , affected the time of decrypting process as well as the size of texts which also got bigger.

Keywords : Cryptography, Sending Texts, RSA algorithm, CRT algorithm, RSA-CRT algorithm, *waterfall*, MatLab, *email*.

KATA PENGANTAR

Segala puji penulis ucapkan kehadirat Allah SWT yang telah melimpahkan rahmat dan hidayah-Nya sehingga penulis dapat menyusun tugas akhir yang berjudul “**Aplikasi Pengiriman Teks via *Email* yang Aman dengan Menggunakan Algoritma RSA-CRT**” sehingga dapat memperoleh gelar Sarjana Strata Satu Departemen Ilmu Komputer/ Informatika pada Fakultas Sains dan Matematika Universitas Diponegoro.

Dalam penyusunan tugas akhir ini, penulis mendapat bantuan dan dukungan dari banyak pihak. Atas peran sertanya dalam membantu dalam penyelesaian tugas akhir ini, penulis ingin mengucapkan terima kasih kepada :

1. Prof. Dr. Widowati, S.Si, M.Si selaku Dekan Fakultas Sains dan Matematika Universitas Diponegoro.
2. Ragil Saputra, S.Si, M.Cs. selaku Ketua Departemen Ilmu Komputer/ Informatika FSM Undip
3. Sukmawati Nur Endah, S.Si M.Kom selaku dosen pembimbing yang telah membimbing dan mengarahkan Penulis dalam menyelesaikan tugas akhir ini.
4. Bapak Helmie Arif Wibawa, S.Si, M.Cs. selaku Koordinator Tugas Akhir Departemen Ilmu Komputer / Informatika.
5. Semua pihak yang telah membantu kelancaran dalam pelaksanaan tugas akhir ini yang tidak dapat penulis sebutkan satu per satu.

Penulis menyadari bahwa masih banyak kekurangan dalam penyusunan laporan tugas akhir ini, untuk itu penulis mohon maaf dan mengharapkan saran serta kritik yang membangun dari pembaca.

Semoga laporan tugas akhir ini dapat bermanfaat bagi pengembangan ilmu dan pengetahuan, khususnya pada bidang komputer.

Semarang, 10 Agustus 2016

Samsul Ma'arif

DAFTAR ISI

HALAMAN PERNYATAAN KEASLIAN SKRIPSI.....	ii
HALAMAN PENGESAHAN	iii
HALAMAN PENGESAHAN	iv
ABSTRAK	v
ABSTRACT	vi
KATA PENGANTAR.....	vii
DAFTAR ISI	viii
DAFTAR GAMBAR.....	x
DAFTAR TABEL	xii
DAFTAR ALGORITMA	xiii
BAB I PENDAHULUAN	1
1.1. Latar Belakang.....	1
1.2. Rumusan Masalah.....	3
1.3. Tujuan Dan Manfaat	3
1.4. Ruang Lingkup	3
1.5. Sistematika Penulisan	4
BAB II TINJAUAN PUSTAKA	6
2.1. Kriptografi	6
2.2. Faktor Persekutuan Terbesar	9
2.3. Algoritma <i>Extended Euclid</i>	11
2.4. Invers	12
2.5. Algoritma Fast Modular Exponentiation	14
2.6. Algoritma RSA	15
2.5.1. Pembangkit Kunci RSA	17
2.5.2. Enkripsi RSA.....	18
2.5.3. Dekripsi RSA.....	19
2.6. Algoritma <i>Chinese Remainder Theorem</i> (CRT).....	20
2.7. Algoritma RSA Dengan CRT (RSA-CRT)	21
2.7.1. Pembangkit Kunci RSA-CRT	22
2.7.2. Enkripsi RSA-CRT.....	22

2.7.3. Dekripsi RSA-CRT	22
2.8. <i>Structured Programming</i>	23
2.8.1. <i>Flowchart</i>	23
2.8.2. Pemodelan Fungsional.....	24
2.9. Model Proses <i>Waterfall</i>	26
BAB III <i>COMMUNICATION, PLANNING DAN MODELING</i>	28
3.1. <i>Communication</i>	28
3.1.1. <i>Project Initiation</i>	28
3.1.1. <i>Requirement Gathering</i>	29
3.2. <i>Planning</i>	30
3.3. <i>Modelling System</i>	31
3.3.1. Analisis	31
3.3.2. Desain	34
BAB IV CONSTRUCTION.....	44
4.1. Implementasi.....	44
4.1.1. Lingkungan Implementasi Sistem	44
4.1.2. Implementasi Fungsional.....	44
4.1.3. Implementasi Antarmuka	45
4.2. Pengujian Perangkat Lunak	49
4.2.1. Pengujian Fungsional Sistem	49
4.2.2. Pengujian Manual Algoritma RSA-CRT.....	49
4.2.3. Pengujian Perbandingan Algoritma RSA-CRT.....	57
4.2.4. Pengujian Ukuran Teks	58
BAB V KESIMPULAN DAN SARAN	59
5.1. Kesimpulan	59
5.2. Saran	59
DAFTAR PUSTAKA.....	60
LAMPIRAN – LAMPIRAN	62

DAFTAR GAMBAR

Gambar 2.1	Sistem Kriptografi Konvensional	7
Gambar 2.2	Kriptografi Kunci Simetri	7
Gambar 2.3	Kriptografi Kunci Asimetri.....	8
Gambar 2.4	Proses Enkripsi.....	8
Gambar 2.5	Proses Dekripsi	8
Gambar 2.6	Algoritma RSA	16
Gambar 2.7	Model Proses <i>Waterfall</i>	26
Gambar 3.1	Arsitektur Aplikasi Pengiriman Teks via <i>Email</i> yang Aman dengan Menggunakan Algoritma RSA-CRT	29
Gambar 3.2	<i>Context Diagram</i> Aplikasi Pengiriman Teks via <i>Email</i> yang Aman dengan Menggunakan Algoritma RSA-CRT	32
Gambar 3.3	DFD Level 1 Aplikasi Pengiriman Teks via <i>Email</i> yang Aman dengan Menggunakan Algoritma RSA-CRT	33
Gambar 3.4	DFD Level 2 Aplikasi Pengiriman Teks via <i>Email</i> yang Aman dengan Menggunakan Algoritma RSA-CRT	33
Gambar 3.5	Alur Proses Pembangkit Kunci	36
Gambar 3.6	Alur Proses Mencari Nilai n dan $\phi(n)$	36
Gambar 3.7	Alur Proses Mencari Nilai e dan Nilai d	37
Gambar 3.8	Alur Proses Mencari Nilai dP , dQ dan $qInv$	37
Gambar 3.9	Alur Proses Mengirim Pesan via <i>Email</i>	38
Gambar 3.10	Alur Proses Enkripsi Pesan	38
Gambar 3.11	Alur Proses Dekripsi Pesan.....	39
Gambar 3.12	Antarmuka <i>Main</i> pada Aplikasi Pengiriman Teks via <i>Email</i> yang Aman dengan Menggunakan Algoritma RSA-CRT.....	41
Gambar 3.13	Antarmuka Pembangkit Kunci pada Aplikasi Pengiriman Teks via <i>Email</i> yang Aman dengan Menggunakan Algoritma RSA-CRT	41
Gambar 3.14	Antarmuka Mengirim Pesan pada Aplikasi Pengiriman Teks yang Aman dengan Menggunakan Algoritma RSA-CRT via <i>Email</i>	42

Gambar 3.15	Antarmuka Dekripsi pada Aplikasi Pengiriman Teks yang Aman dengan Menggunakan Algoritma RSA-CRT via <i>Email</i>	42
Gambar 3.16	Antarmuka Bantuan pada Aplikasi Pengiriman Teks yang Aman dengan Menggunakan Algoritma RSA-CRT via <i>Email</i>	43
Gambar 4.1	Tampilan Halaman <i>Main</i>	46
Gambar 4.2	Tampilan Halaman Pembangkit Kunci.....	47
Gambar 4.3	Tampilan Halaman Mengirim Pesan	47
Gambar 4.4	Tampilan Halaman Dekripsi	48
Gambar 4.5	Tampilan Halaman Bantuan	48
Gambar 4.6	Tampilan Hasil Pembangkit Kunci Aplikasi Pengiriman Teks via <i>Email</i> Menggunakan Algoritma RSA-CRT	51
Gambar 4.7	Tampilan Hasil Enkripsi Pesan Aplikasi Pengiriman Teks via <i>Email</i> Menggunakan Algoritma RSA-CRT	54
Gambar 4.8	Tampilan Hasil Dekripsi Pesan Aplikasi Pengiriman Teks via <i>Email</i> Menggunakan Algoritma RSA-CRT	57

DAFTAR TABEL

Tabel 2.1 Contoh menentukan gcd dari 120 dan 56	10
Tabel 2.2 Contoh menentukan gcd dari 100 dan 85	11
Tabel 2.3 Invers perkalian 11 pada Z_{45}	13
Tabel 2.4 Ketentuan <i>Binary</i>	14
Tabel 2.5 Pembuktian gcd dari 1456 dan 83 adalah 1	17
Tabel 2.6 Invers Perkalian 77 pada Z_{480}	18
Tabel 2.7 Program <i>Flowchart</i>	23
Tabel 2.8 Notasi DFD	25
Tabel 3.1 Tabel Kebutuhan Fungsional	30
Tabel 3.2 Tabel Kebutuhan Non Fungsional	30
Tabel 4.1 Rencana Pengujian Fungsional Sistem.....	49
Tabel 4.2 Pembuktian gcd dari 616 dan 81 adalah 1	50
Tabel 4.3 Invers Perkalian 81 terhadap Z_{616}	50
Tabel 4.4 Invers Perkalian 23 terhadap Z_{29}	51
Tabel 4.5 Perubahan Teks Menjadi Nilai ASCII.....	52
Tabel 4.6 Hasil Enkripsi RSA-CRT	53
Tabel 4.7 Hasil Dekripsi RSA-CRT	55
Tabel 4.8 Mengubah ASCII ke Bentuk Karakter Asli.....	56
Tabel 4.9 Pengujian Algoritma RSA-CRT	58
Tabel 4.10 Tabel Pengujian Ukuran Teks	59

DAFTAR ALGORITMA

Algoritma 2.1. Algoritma <i>Greatest common divisor</i> ($\gcd(a, b)$)	10
Algoritma 2.2. <i>Extended Euclid</i> $\gcd(a, b)$	11

BAB I

PENDAHULUAN

Bab ini berisi latar belakang, rumusan masalah, tujuan dan manfaat, ruang lingkup dan sistematika penulisan tugas akhir mengenai Aplikasi Pengiriman Teks yang Aman dengan Menggunakan Algoritma RSA-CRT via *Email*.

1.1. Latar Belakang

Perkembangan teknologi yang sangat pesat dan dilengkapi dengan adanya internet membuat manusia semakin mudah dalam melakukan aktifitasnya sehari-hari. Salah satu contohnya adalah pengiriman sebuah pesan. Pengiriman sebuah pesan dengan bentuk surat dan dikirim menggunakan pos akan membutuhkan waktu yang lama. Sedangkan jika menggunakan *electronic messaging (email)*, pengiriman data, dokumen maupun gambar bisa diterima dalam hitungan detik. Namun dengan kemajuan teknologi tersebut juga membuat pengiriman pesan menjadi lebih tidak aman. Untuk meningkatkan keamanan dalam pengiriman pesan, dibutuhkan sebuah ilmu atau metode yang bisa menjaga pesan terkirim dengan aman kepada penerima yang dituju, dan tidak terjadi perubahan pesan di tengah jalan oleh pihak ketiga. Ilmu tersebut lebih dikenal dengan sebutan kriptografi.

Dalam kamus bahasa Inggris Oxford diberikan pengertian kriptografi sebagai berikut:

“Sebuah teknik rahasia dalam penulisan, dengan karakter khusus, dengan menggunakan huruf dan karakter di luar bentuk aslinya, atau dengan metode-metode lain yang hanya dapat dipahami oleh pihak - pihak yang memproses kunci, juga semua hal yang ditulis dengan cara seperti ini.” Jadi, secara umum dapat diartikan sebagai seni menulis atau memecahkan cipher (Talbot & Welsh, 2006). Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data serta otentikasi (Menezes, et al., 1996). Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga. Kriptografi memiliki banyak sekali algoritma yang digunakan untuk

mengamankan pesan, salah satu algoritma kriptografi yang paling sering digunakan saat ini adalah RSA.

RSA merupakan algoritma kunci publik yang diambil dari nama penemunya yaitu Rivest-Shamir-Adleman. RSA merupakan salah satu jenis algoritma dalam sistem kriptografi asimetris dimana penggunaan kunci berbeda saat enkripsi dan dekripsi. Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor primanya. RSA terbukti secara matematika memiliki keamanan yang tinggi akibat bersandar pada persoalan faktorisasi yang sampai saat ini belum ada algoritma faktorisasi yang efisien (Sadikin, 2012).

Penelitian tentang keamanan RSA pernah dilakukan oleh Zainal Arifin yang berjudul “Studi Kasus Penggunaan Algoritma RSA Sebagai Algoritma Kriptografi yang Aman”. Kesimpulan dari penelitian tersebut adalah algoritma RSA merupakan salah satu solusi yang baik untuk mengatasi masalah keamanan dan kerahasiaan data yang pada umumnya diterapkan dalam pengiriman dan penyimpanan data melalui media elektronik (Arifin, 2009). Dalam penelitian yang lain yang berjudul “Pengamanan Pengiriman Pesan Via SMS dengan Algoritma RSA Berbasis Android” juga menyimpulkan bahwa validitas pesan yang akan dikirim setelah melakukan proses enkripsi dan dekripsi adalah 100% sehingga untuk keamanan pengiriman data terjamin aman (Alvianto & Darmaji, 2015). Berdasarkan dua penelitian tersebut RSA memiliki keamanan yang cukup handal.

Namun dalam proses dekripsi, RSA membutuhkan waktu yang lama karena prosesnya melibatkan bilangan-bilangan besar sehingga untuk mempercepat dekripsi RSA digunakan metode tambahan CRT (*Chinese Remainder Theorem*). Terbukti Algoritma RSA-CRT memiliki komputasi yang lebih singkat daripada Algoritma RSA biasa, yaitu sekitar 4 kali lebih cepat (Sadikin, 2012). Beberapa penelitian dengan tema RSA-CRT telah banyak dilakukan diantaranya oleh Stevens Jethefer dengan judul “Studi dan Perbandingan Mengenai Metode Perkalian *Montgomery* dan *Chinese Remainder Theorem* (CRT) dalam Mempercepat Dekripsi RSA” dengan hasil RSA-CRT memiliki performa yang lebih baik dibanding RSA konvensional (Jethefer, 2006). Ada juga penelitian oleh Ashari Arief yang berjudul “Implementasi Algoritma Kriptografi RSA - CRT pada Aplikasi *Instant Messaging*” dengan hasil bahwa Algoritma RSA-CRT memiliki kecepatan proses dekripsi dua kali lipat lebih cepat dibandingkan dengan dekripsi Algoritma RSA biasa (Arief, 2016). Selain itu

juga ada penelitian oleh Muhamad Reza Firdaus Zen dengan judul “Algoritma Kriptografi Kunci-publik RSA menggunakan *Chinese Remainder Theorem*” dengan hasil RSA-CRT memiliki keuntungan dalam kecepatan proses bila dibandingkan dengan Algoritma RSA standar (Zen, 2008).

Berdasarkan penjelasan di atas, maka pada penelitian ini membuat sebuah aplikasi yang menerapkan Algoritma RSA-CRT untuk mengamankan data teks yang kemudian dikirim via *email*. Setelah itu dibandingkan apakah Algoritma RSA-CRT memiliki kecepatan komputasi yang lebih baik dibandingkan dengan Algoritma RSA biasa.

1.2. Rumusan Masalah

Berdasarkan uraian pada latar belakang, maka rumusan masalah yang diangkat pada tugas akhir ini adalah bagaimana membuat Aplikasi Pengiriman Teks via *Email* yang Aman dengan Menggunakan Algoritma RSA-CRT yang nantinya dibandingkan dengan Algoritma RSA biasa apakah Algoritma RSA-CRT memiliki komputasi yang lebih baik dari pada Algoritma RSA biasa.

1.3. Tujuan Dan Manfaat

Tujuan yang ingin dicapai dalam penelitian tugas akhir ini adalah

1. Menghasilkan Aplikasi Pengiriman Teks via *Email* yang Aman dengan Menggunakan Algoritma RSA-CRT.
2. Ingin mengetahui apakah Algoritma RSA-CRT memiliki kecepatan komputasi yang lebih baik dibanding dengan Algoritma RSA biasa.

Manfaat yang diharapkan dari penelitian ini adalah untuk meningkatkan keamanan data atau informasi yang berupa teks pada saat menggunakan *email* dengan sebuah algoritma yang memiliki waktu proses dekripsi yang paling cepat.

1.4. Ruang Lingkup

Ruang lingkup dalam pembuatan Aplikasi Pengiriman Teks via *Email* yang Aman dengan Menggunakan Algoritma RSA-CRT dalam penelitian ini adalah sebagai berikut :

1. Data berupa teks dan tidak memiliki jeda “*enter*”.
2. Bilangan prima p dan q yang dapat diproses oleh aplikasi ini antara 2 byte sampai 4 byte dengan nilai p dan q tidak boleh sama.

3. Nilai e adalah sembarang nilai 1 digit sampai 8 byte dan nilai n (hasil kali dari nilai p dan q) adalah 8 byte atau dibawahnya.
4. Penerima dan pengirim pesan menggunakan nilai p, q dan e yang sama.
5. Aplikasi dibangun menggunakan bahasa pemrograman *Matlab*.
6. Aplikasi yang dibuat berbasis *desktop* dan membutuhkan *email* yang masih aktif.
7. Model pengembangan perangkat lunak menggunakan model proses *waterfall*.

1.5. Sistematika Penulisan

Sistematika penulisan yang digunakan dalam tugas akhir ini terbagi dalam beberapa pokok bahasan, yaitu :

BAB I PENDAHULUAN

Bab ini berisi latar belakang, rumusan masalah, tujuan dan manfaat, ruang lingkup dan sistematika penulisan tugas akhir mengenai Aplikasi Pengiriman Teks via *Email* yang Aman dengan Menggunakan Algoritma RSA-CRT.

BAB II TINJAUAN PUSTAKA

Bab ini memaparkan studi pustaka yang berhubungan dengan topik tugas akhir mengenai Aplikasi Pengiriman Teks via *Email* yang Aman dengan Menggunakan Algoritma RSA-CRT. Pustaka yang digunakan dalam penyusunan tugas akhir ini meliputi Kriptografi, Faktor Persekutuan Terbesar, *Extended Euclid*, Invers, Algoritma RSA, *Chinese Remainder Theorem* (CRT), RSA Dengan CRT (RSA-CRT), *Structured Programming* dan Model Proses *Waterfall*.

BAB III COMMUNICATION, PLANNING DAN MODELING

Bab ini menjelaskan mengenai pembahasan tahapan dari model *waterfall* yang meliputi tahap *Communication*, *Planning* dan *Modeling* dari Aplikasi Pengiriman Teks via *Email* yang Aman dengan Menggunakan Algoritma RSA-CRT.

BAB IV CONSTRUCTION

Bab ini menjelaskan mengenai pembahasan dua tahapan akhir dari model *waterfall* yang meliputi tahap implementasi (*code*) dan pengujian

(*test*) dari Aplikasi Pengiriman Teks via *Email* yang Aman dengan Menggunakan Algoritma RSA-CRT.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi tentang kesimpulan dari hasil pembuatan Aplikasi Pengiriman Teks via *Email* yang Aman dengan Menggunakan Algoritma RSA-CRT dan saran-saran untuk pengembangan selanjutnya.