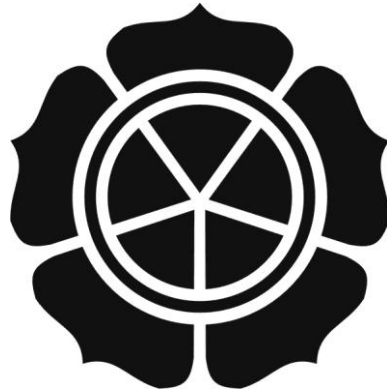


**IMPLEMENTASI ALGORITMA KRIPTOGRAFI ELGAMAL UNTUK
KEAMANAN PENGIRIMAN EMAIL BERBASIS JAVA**

SKRIPSI



disusun oleh

Muhammad Agus Mahardika

12.11.6083

**JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2016**

**IMPLEMENTASI ALGORITMA KRIPTOGRAFI ELGAMAL UNTUK
KEAMANAN PENGIRIMAN EMAIL BERBASIS JAVA**

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai derajat Sarjana S1
pada jurusan Teknik Informatika



disusun oleh

Muhammad Agus Mahardika

12.11.6083

**JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2016**

PERSETUJUAN

SKRIPSI

**IMPLEMENTASI ALGORITMA KRIPTOGRAFI ELGAMAL UNTUK
KEAMANAN PENGIRIMAN EMAIL BERBASIS JAVA**

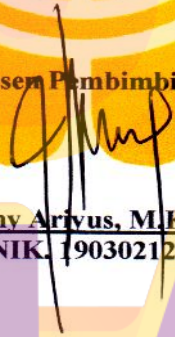
yang disusun oleh

Muhammad Agus Mahardika

12.11.6083

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 14 September 2015

Dosen Pembimbing,


Dony Ariyus, M.Kom
NIK. 190302128

PENGESAHAN

SKRIPSI

**IMPLEMENTASI ALGORITMA KIRPTOGRAFI ELGAMAL UNTUK
KEAMANAN PENGIRIMAN EMAIL BERBASIS JAVA**

yang disusun oleh

Muhammad Agus Mahardika

12.11.6083

telah dipertahankan di depan Dewan Penguji
pada tanggal 15 Januari 2016

Susunan Dewan Penguji

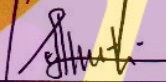
Nama Penguji

Kusnawi, S.Kom., M. Eng
NIK. 190302112

Dony Ariyus, M.Kom
NIK. 190302128

Erni Seniwati, M.Cs
NIK. 190302231

Tanda Tangan



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 28 Januari 2016

KETUA SEMIK AMIKOM YOGYAKARTA

Prof. Dr. M. Suyanto, M.M.
NIK. 190302001



PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

Yogyakarta, 28 Januari 2016



Muhammad Agus Mahardika

NIM. 12.11.6083

MOTTO

“Sebuah tekad yang kuat pasti akan mendapat keberhasilan yang tak ternilai harganya”

“Kita tidak akan bisa sampai puncak gunung jika tidak melangkah sedikit demi sedikit melewati medan yang sulit.”

Jadilah pribadi diri sendiri, jangan pernah meniru pribadi orang lain karena setiap manusia punya prinsip masing-masing.



PERSEMBAHAN

Dengan mengucapkan Alhamdulillah sebagai rasa syukur kepada ALLAH SWT serta junjungan nabi Muhammad SAW yang selalu memberikan rahmat-Nya sehingga skripsi ini dapat selesai. Adapun karya ini penulis persembahkan kepada :

1. Kedua orang tua yang senantiasa memberikan doa dan semangat dalam mengerjakan skripsi ini hingga proses ujian skripsi.
2. Pak Dony Ariyus selaku dosen pembimbing yang terus memberikan motivasi dan masukan dari apa yang telah penulis buat.
3. Kekasih tercinta Astri Kusuma Werdyani yang selalu memberikan semangat, doa dan motivasinya.
4. Mas Fuad yang selalu memberikan arahan arahan serta trik-triknya saat berperang didalam ruang sidang seperti apa.
5. Teman-teman 12-S1TI-05 yang selalu menanyakan “Sampai Mena Skripsinya?”. Pertanyaan-pertanyaan itulah yang membuat dan membangkitkan semangat penulis dalam menyusun laporan skripsi ini.
6. Sahabat Anggi, Irko, Gilang yang kocak-kocak. Kalian semua baik banget tapi aku lebih baik dari kalian tentunya. Next trip kita ke Lombok ya Guyss !! salam sukses semua buat kalian.
7. Aji, Fitrah, Ilham Mubarog kalian juga temen yang baik. Selalu membantu jika penulis membutuhkan kalian.

KATA PENGANTAR

Puji syukur penulis panjatkan kepada ALLAH SWT yang telah memberikan rahmat dan hidayah-Nya, sehingga penulis telah berikan kemudahan dan kekuatan dalam menyelesaikan skripsi yang berjudul **“IMPLEMENTASI ALGORITMA KRIPTOGRAFI ELGAMAL UNTUK KEAMANAN PENGIRIMAN EMAIL BERBASIS JAVA”** sesuai yang diharapkan, penulis dapat menyelesaikan skripsi yang merupakan matakuliah dan wajib ditempuh sebagai salah satu syarat menyelesaikan program sarjana pada STMIK AMIKOM Yogyakarta.

Dalam penulisan laporan skripsi ini penulis banyak mendapat bantuan dari berbagai pihak, untuk itu penulis menyampaikan rasa hormat dan terimakasih kepada :

1. Bapak Prof. Dr .M. Suyanto, M.M. selaku ketua STMIK AMIKOM Yogyakarta
2. Bapak Sudarmawan, M.T. selaku ketua Jurusan Teknik Informatika STMIK AMIKOM Yogyakarta.
3. Bapak Dony Ariyus, M. Kom. selaku dosen pembimbing.
4. Kedua orang tua yang telah memberikan semangat serta dukungan untuk menjalani kuliah serta menyelesaikan skripsi.
5. Teman-teman serta semua pihak yang telah banyak membantu dalam penyelesaian skripsi ini.

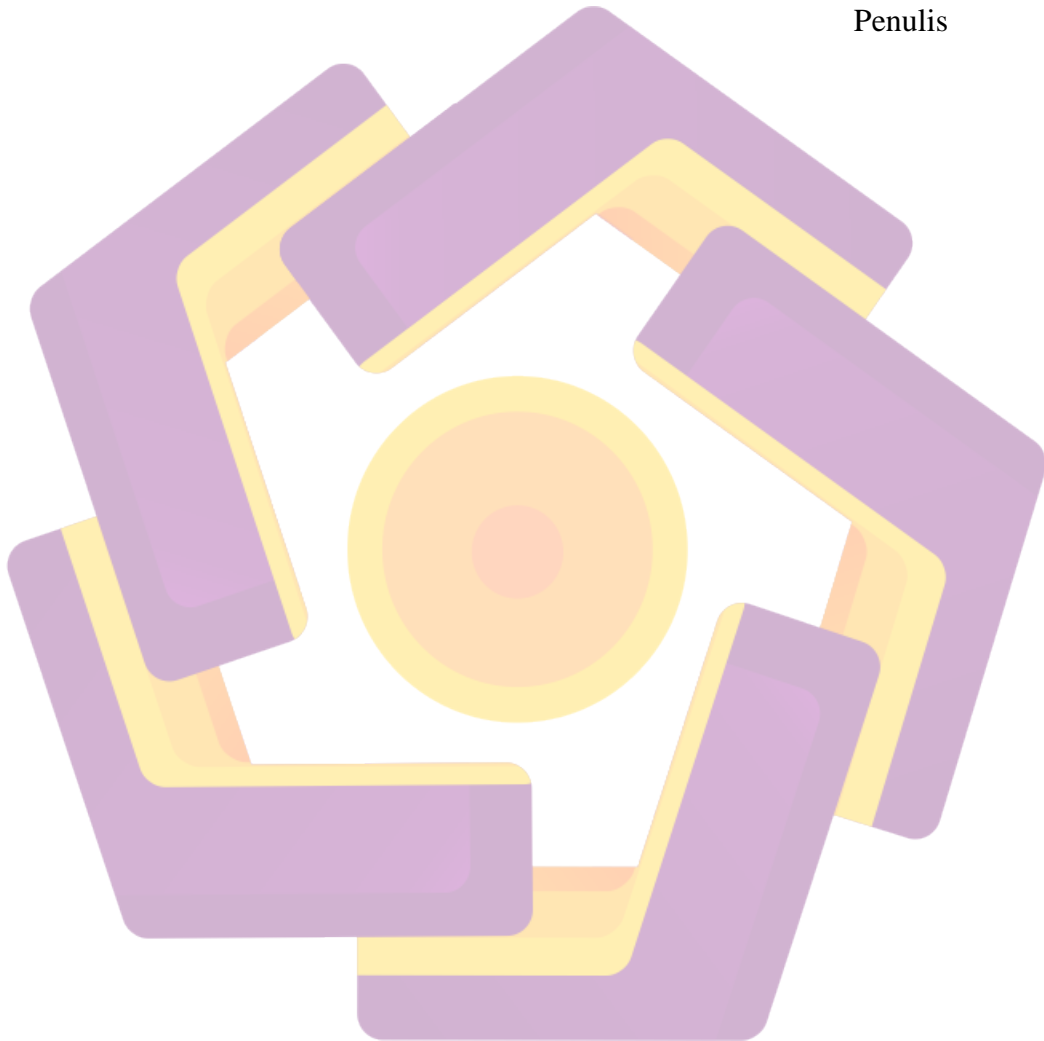
Penulis menyadari bahwa penyusunan skripsi ini masih jauh dari sempurna, dikarenakan keterbatasan pengetahuan dan pengalaman penulis.

Penulis menerima kritik dan saran dari pembaca guna perbaiki pada masa mendatang. Semoga skripsi ini dapat bermanfaat bagi kita semua.

Yogyakarta, 28 Januari 2016



Penulis



DAFTAR ISI

JUDUL.....	I
PERSETUJUAN.....	II
PENGESAHAN	III
PERNYATAAN.....	IV
MOTTO.....	V
PERSEMBAHAN	VI
KATA PENGANTAR.....	VII
DAFTAR ISI.....	IX
DAFTAR TABEL	XIII
DAFTAR GAMBAR.....	XV
INTISARI.....	XIX
<i>ABSTRACT</i>	XX
BAB I PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah	4
1.3 Batasan Masalah.....	4
1.4 Maksud dan Tujuan Penelitian	5
1.4.1 Internal.....	5
1.4.2 Eksternal	6
1.5 Manfaat Penelitian.....	6
1.6 Metode Penelitian	7
1.6.1 Metode Pengumpulan Data	7
1.6.2 Metode Analisis.....	8
1.6.3 Metode Perancangan.....	8

1.7	Sistematika Penulisan.....	8
BAB II LANDASAN TEORI.....		10
2.1	Tinjauan Pustaka	10
2.2	Kriptografi	11
2.2.1	Sejarah Kriptografi	11
2.2.2	Pengertian Kriptografi	11
2.2.3	Tujuan Kriptografi.....	12
2.2.4	Komponen Sistem Kriptografi	13
2.3	Jenis Algoritma Kriptografi.....	15
2.4	ELGamal.....	16
2.4.1	Pembangkit Kunci ELGamal.....	17
2.4.2	Enkripsi dan Dekripsi ELGamal	18
2.4.3	Kelebihan Algoritma ELGamal.....	18
2.5	<i>Email</i>	19
2.5.1	Kelebihan <i>Email</i>	19
2.5.2	Cara Kerja <i>Email</i>	20
2.5.3	Simple Mail Transfer Protocol (SMTP).....	21
2.5.4	Post Office Protocol version 3.....	22
2.6	File Document	23
2.6.1	Sejarah Microsoft Office	23
2.7	Java.....	24
2.7.1	Sejarah Java.....	24
2.7.2	Pengertian Java.....	25
2.7.3	Perkembangan Teknologi Java.....	25
2.7.4	Java Mail	26
2.8	Netbeans Integrated Development Environment (NetBeans IDE).....	27
2.9	MySQL.....	27
2.10	UML (<i>Unified Modeling Language</i>)	28

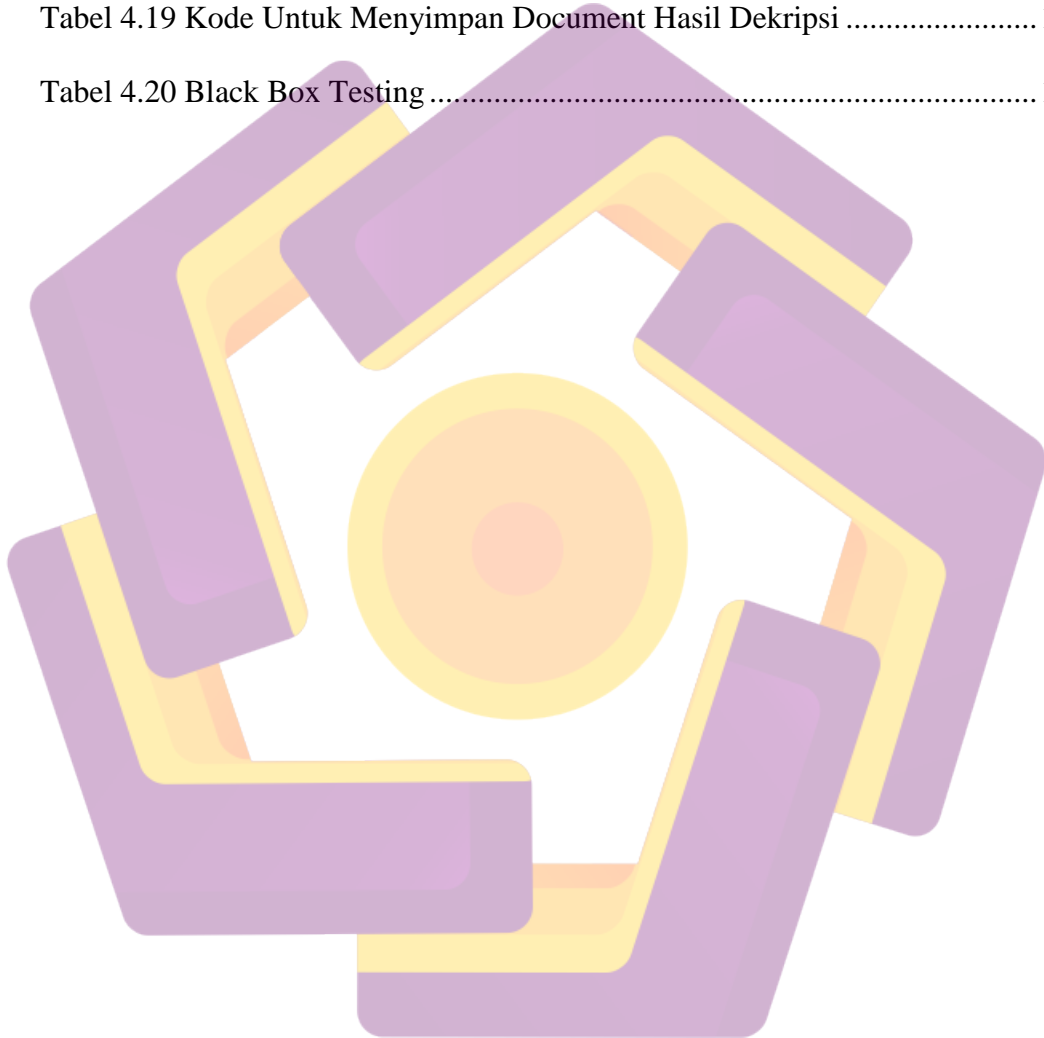
2.10.1	Pengenalan UML.....	28
2.10.2	Konsep Dasar UML.....	28
2.11	Bagan Alur (<i>flowchart</i>).....	32
2.12	Metode SWOT.....	34
2.12.1	Kekuatan.....	34
2.12.2	Kelemahan.....	35
2.12.3	Peluang.....	35
2.12.4	Ancaman.....	35
BAB III METODE PENELITIAN.....		36
3.1	Gambaran Umum Aplikasi.....	36
3.2	Kelemahan Sistem lama.....	38
3.3	Model Aplikasi Baru.....	38
3.4	Analisis SWOT.....	39
3.4.1	Kekuatan (<i>Strengths</i>).....	39
3.4.2	Kelemahan (<i>Weakness</i>).....	39
3.4.3	Peluang (<i>Opportunities</i>).....	40
3.4.4	Ancaman (<i>Threats</i>).....	40
3.5	Analisis Kebutuhan Sistem.....	41
3.5.1	Analisis Kebutuhan Fungsional.....	41
3.5.2	Analisis Kebutuhan Non-Fungsional.....	42
3.5.3	Analisis Kelayakan Sistem.....	44
3.6	Perancangan Algoritma.....	44
3.6.1	Proses Pembetulan Kunci.....	45
3.6.2	Proses Enkripsi.....	55
3.6.3	Proses Dekripsi.....	57
3.7	Perancangan Sistem.....	58
3.7.1	Perancangan UML.....	58
3.7.2	Perancangan Flowchart.....	75
3.7.3	Perancangan GUI (<i>Graphical User Interface</i>).....	79

BAB IV HASIL DAN PEMBAHASAN.....	92
4.1 Implementasi	92
4.1.1 Implementasi Algoritma ElGamal.....	92
4.1.2 Implementasi JavaMail.....	95
4.1.3 Implementasi Register dan Login.....	97
4.1.4 Implementasi Interface	99
4.2 Pembahasan	108
4.2.1 Kode Program.....	108
4.3 Pengujian Program	120
4.3.1 Pengujian Black Box Testing	120
4.3.2 White Box Testing.....	144
BAB V PENUTUP	149
5.1 Kesimpulan.....	149
5.2 Saran	149
DAFTAR PUSTAKA.....	151

DAFTAR TABEL

Tabel 2.1 Simbol-simbol Use Case Diagram	29
Tabel 2.2 Simbol-simbol Activity diagram	30
Tabel 2.3 sSimbol-simbol Seauence diagram	31
Tabel 2.4 Simbol-simbol <i>Class Diagram</i>	31
Tabel 2.5 Simbol Flowchart	33
Tabel 3.1 Matriks SWOT	40
Tabel 3.2 Perhitungan $a^2 \bmod p$ dan $a^q \bmod p$	54
Tabel 3.3 Konversi Karakter ke Kode ASCII	56
Tabel 3.4 Enkripsi plainteks ke chiperteks	56
Tabel 3.5 Dekripsi Chiperteks ke Plainteks	57
Tabel 4.1 Kode Class Pembangkit Kunci	92
Tabel 4.2 Kode Class Enkripsi Pesan	94
Tabel 4.3 Kode Class Dekripsi Pesan	94
Tabel 4.4 Kode Class Kirim Pesan <i>Email</i>	95
Tabel 4.5 Kode Class Terima Pesan <i>Email</i>	96
Tabel 4.6 Kode Class Register	97
Tabel 4.7 Kode Class Login	98
Tabel 4.8 Kode Untuk Mebangkitkan Kunci Public dan Private	108
Tabel 4.9 Kode Untuk Menyimpan Kunci Public dan Private	109
Tabel 4.10 Kode Untuk Mengenkripsi Pesan	110
Tabel 4.11 Kode Untuk Mengirim Pesan	111
Tabel 4.12 Kode Untuk Menerima Pesan	113
Tabel 4.13 Kode Untuk Mendekripsi Pesan	114

Tabel 4.14 Kode Untuk Membuka Document.....	115
Tabel 4.15 Kode Untuk Mengenkripsi Document.....	115
Tabel 4.16 Kode Untuk Menyimpan Document	117
Tabel 4.17 Kode Untuk Membuka Document Hasil Enkripsi.....	118
Tabel 4.18 Kode Untuk Mendekripsi Document.....	118
Tabel 4.19 Kode Untuk Menyimpan Document Hasil Dekripsi	119
Tabel 4.20 Black Box Testing	143



DAFTAR GAMBAR

Gambar 2.1 Sistem Kriptografi dengan Kunci Publik ELGamal	17
Gambar 2.2 Sistem Kerja <i>email</i>	21
Gambar 3.1 Sistem Pengiriman <i>Email</i> Tanpa Kriptografi	37
Gambar 3.2 Sistem Pengiriman <i>Email</i> Menggunakan Kriptografi.....	37
Gambar 3.3 Use Case Diagram	59
Gambar 3.4 Activity Diagram Register	59
Gambar 3.5 Activity Diagram Login.....	60
Gambar 3.6 Activity Diagram Informasi.....	60
Gambar 3.7 Activity Diagram Tulis Pesan.....	61
Gambar 3.8 Activity Diagram Pembangkit Kunci	62
Gambar 3.9 Activity Diagram Pesan Masuk	63
Gambar 3.10 Activity Diagram Enkripsi Dokumen.....	64
Gambar 3.11 Activity Diagram Dekripsi Dokumen.....	65
Gambar 3.12 Class Diagram.....	66
Gambar 3.13 Sequence Diagram Register.....	67
Gambar 3.14 Sequence Diagram Login	68
Gambar 3.15 Sequence Diagram Informasi	68
Gambar 3.16 Sequence Diagram Menulis Pesan.....	69
Gambar 3.17 Sequence Diagram Membangkitkan Kunci	69
Gambar 3.18 Sequence Diagram Mengenkripsi Pesan	70
Gambar 3.19 Sequence Diagram Mengirim Pesan.....	71
Gambar 3.20 Sequence Diagram Membuka Pesan Masuk.....	72
Gambar 3.21 Sequence Diagram Mendekripsi Pesan	73

Gambar 3.22 Sequence Diagram Enkripsi Document.....	74
Gambar 3.23 Sequence Diagram Mendekripsi Document	74
Gambar 3.24 <i>Flowchart</i> Halaman Awal (<i>Register, Login, dan Informasi</i>).....	75
Gambar 3.25 <i>Flowchart</i> Tulis Pesan dan Enkripsi Pesan	76
Gambar 3.26 <i>Flowchart</i> Pesan Masuk dan Dekripsi Pesan.....	77
Gambar 3.27 <i>Flowchart</i> Pembangkitan Kunci	78
Gambar 3.28 <i>Flowchart</i> Enkripsi dan Dekripsi Document	79
Gambar 3.29 Tampilan Menu Awal.....	80
Gambar 3.30 Tampilan Login	81
Gambar 3.31 Tampilan Register.....	81
Gambar 3.32 Tampilan Berhasil Register	82
Gambar 3.33 Tampilan Informasi	83
Gambar 3.34 Tampilan Menu Awal.....	84
Gambar 3.35 Tampilan Tulis Pesan	85
Gambar 3.36 Tampilan Masukkan Prima.....	86
Gambar 3.37 Tampilan Masukkan Alpha.....	86
Gambar 3.38 Tampilan Masukkan Beta	87
Gambar 3.39 Tampilan Pesan Masuk.....	88
Gambar 3.40 Tampilan Masukkan Prima Dekripsi.....	89
Gambar 3.41 Tampilan Masukkan Delta Dekripsi	89
Gambar 3.42 Tampilan Pembangkit Kunci	90
Gambar 3.43 Tampilan Enkripsi Document.....	90
Gambar 3.44 Tampilan Dekripsi Document.....	91
Gambar 4.1 Halaman Menu Awal.....	100

Gambar 4.2 Halaman Register.....	100
Gambar 4.3 Halaman Login	101
Gambar 4.4 Halaman Information.....	102
Gambar 4.5 Halaman Menu Utama.....	103
Gambar 4.6 Halaman Tulis Pesan dan Enkripsi Pesan.....	104
Gambar 4.7 Halaman Pesan Masuk dan Dekripsi	105
Gambar 4.8 Halaman Pembangkit Kunci	106
Gambar 4.9 Halaman Enkripsi Document.....	107
Gambar 4.10 Halaman Dekripsi Document	107
Gambar 4.11 Menuju Halaman Pembangkit Kunci	121
Gambar 4.12 Kunci Berhasil dibuat	122
Gambar 4.13 Menyimpan Kunci Publik.....	122
Gambar 4.14 Kunci Private Tersimpan	123
Gambar 4.15 Menuju Halaman Tulis Pesan	124
Gambar 4.16 Memasukkan Alpha(a)	125
Gambar 4.17 Memasukkan Beta(b).....	126
Gambar 4.18 Memasukkan Prima(p)	127
Gambar 4.19 Pesan Terenkripsi	128
Gambar 4.20 Pesan Terkirim.....	129
Gambar 4.21 Menuju Halaman Pesan Masuk	130
Gambar 4.22 Menuju Halaman Pesan Masuk	131
Gambar 4.23 Memasukkan Prima (p)	132
Gambar 4.24 Memasukkan Delta (d)	133
Gambar 4.25 Dekripsi Pesan Berhasil.....	134

Gambar 4.26 Menuju Halaman Enkripsi Document	135
Gambar 4.27 Membuka Document	136
Gambar 4.28 Memasukkan Prima	136
Gambar 4.29 Memasukkan Alpha	137
Gambar 4.30 Memasukkan Beta	137
Gambar 4.31 File Enkripsi Tersimpan	138
Gambar 4.32 Hasil Enkripsi Document.....	138
Gambar 4.33 Menuju Halaman Dekripsi Document.....	139
Gambar 4.34 Open Document Terenkripsi.....	140
Gambar 4.35 Masukkan Prima Dekripsi Document.....	140
Gambar 4.36 Masukkan d Dekripsi Document	140
Gambar 4.37 File Dekripsi Tersimpan	141
Gambar 4.38 Hasil Dekripsi Document	142
Gambar 4.39 Runtime Error	145
Gambar 4.40 Memilih Menu My Account	146
Gambar 4.41 Memilih Menu Sign-in dan Security	147
Gambar 4.42 Mengaktifkan Allow less secure apps	148

INTISARI

Kejahatan dalam dunia maya merupakan hal yang sangat merugikan baik bagi pengguna Internet maupun penyedia jasa Internet. Teknologi yang saat ini berkembang pesat justru membuat *cybercrime* menjadi lebih agresif dalam melakukan tindak kejahatan terutama di dunia maya. Kita tidak menyadari bahwa kehidupan kita sekarang banyak dilingkupi oleh *kriptografi*. Mulai dari percakapan telpon genggam, akses Internet, sampai aktivitas transaksi di ATM telah menggunakan *kriptografi*.

Kriptografi juga digunakan dalam proses pengiriman *Email*. Dengan menggunakan metode Enkripsi ELGamal, diharapkan proses pengiriman *email* melalui aplikasi JAVA menjadi lebih secure. Serangan *Main- In – The – Middle* merupakan ancaman besar terhadap pencurian informasi dari sebuah *email*. Salah satu algoritma yang digunakan untuk *Enkripsi* dan dibahas dalam Tugas Akhir ini adalah algoritma ELGamal dan akan diimplementasikan pada program JAVA.

Penggunaan kriptografi akan sangat membantu memberikan keamanan informasi *email* kita. Walaupun *attacker Main – In – The – Middle* berhasil mendapatkan teks yang kita kirim namun informasi tersebut sudah terenkripsi sebelumnya. Selain itu, proses enkripsi pada plainteks yang sama diperoleh ciperteks yang berbeda-beda, namun pada proses dekripsi diperoleh plainteks yang sama. Sehingga, membuat *email* menjadi lebih secure dibanding sebelumnya.

Kata Kunci: Kriptografi, *email*, ELGamal, Java, Main In The Middle

ABSTRACT

Crime in cyberspace is very harmful both for Internet users and Internet service providers. The technology that is currently growing rapidly makes cybercrime has become more aggressive in committing crimes, especially in cyberspace. We do not realize that our lives are now covered by at cryptography. Ranging from mobile phone conversations, Internet access, through the activity of ATM transactions have been using cryptography.

Cryptography is also used in the process of sending email. By using ElGamal encryption method, it is expected the process of sending email through JAVA applications become more secure. Attacked main- In - The - Middle poses a major threat to the theft of information from an email. One of the algorithms used for encryption and discussed in this final project is the ElGamal algorithm, and will be implemented in the JAVA program.

The use of cryptography will greatly help provide security information email us. Although the attacker Main - In - The - Middle managed to get the text that we send, but the information is encrypted before. Additionally, the encryption process at the same plaintext obtained ciphertexts different, but at the same decrypted plaintext obtained. So, making the the mail is more secure than before.

Keyword: Cryptography, email, ElGamal, Java, Main In The Middle

