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 disetujuai 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	Tanda Tangan
Kusnawi, S.Kom., M. Eng **NIK. 190302112**	
Dony Ariyus, M.Kom **NIK. 190302128**	
Erni Seniwati, M.Cs **NIK. 190302231**	

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

KETUA STMIK 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 semngat dalam mengerjakan skripsi ini hingga proses ujian skripsi.
2. Pak Dony Ariyus selaku dosen pembingbing 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

DAFTAR TABEL

DAFTAR GAMBAR

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 chiperteks 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.Attactkted 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 chiperteks 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