MODIFIKASI PENGKODEAN ELGAMAL MENGGUNAKAN DUA KUNCI PRIVAT DAN EMPAT KUNCI PUBLIK

SKRIPSI

Oleh

Arif Rahman
NIM 021810101016

JURUSAN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS JEMBER
2009

MODIFIKASI PENGKODEAN ELGAMAL MENGGUNAKAN DUA KUNCI PRIVAT DAN EMPAT KUNCI PUBLIK

SKRIPSI

diajukan guna melengkapi tugas akhir dan memenuhi salah satu syarat
untuk menyelesaikan Program Studi Matematika (S1)
dan mencapai gelar Sarjana Sains

Oleh

Arif Rahman
NIM 021810101016

JURUSAN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS JEMBER

2009

PERSEMBAHAN

Skripsi ini saya persembahkan untuk :

1. Ayahanda (H. Muhdar Juhri) dan Ibunda (Hj. Nur Ainiyah) yang senantiasa memberikan do'a restu dan bimbingan tiada hentinya. Skripsi ini sebagai wujud terimakasih, hormat dan bakti ananda atas pengorbanan selama ini;
2. Nur Azizah, Skg, istri tercinta, terima kasih atas semangat, nasehat, bimbingan, do'a, serta kasih sayang yang senantiasa diberikan;
3. M. Rohullah Maulana AL-Aziz, anak tersayang, bersamamu semangat dan keceriaan, kaulah harapan hidup;
4. Ayahanda (Ansyari) dan ibunda (Hatniyah) selaku mertua yang senantiasa memberikan semangat, dukungan dan do'a untuk ananda;
5. Kakak Dewi dan kakak Lisa, terimakasih atas dorongan dan perhatiannya.

MOTTO

Sesungguhnya sesudah kesulitan itu ada kemudahan,
maka apabila kamu telah selesai dari suatu urusan,
kerjakanlah dengan sungguh-sungguh urusan yang lain
(QS. Al Insyiroh: 94)

Kemenangan hanya dapat diraih dengan kesabaran
(HR. At-Tarmidzi)

PERNYATAAN

Saya yang bertanda tangan di bawah ini:

Nama : Arif Rahman

NIM : 021810101016

menyatakan dengan sesungguhnya bahwa karya tulis ilmiah yang berjudul: *Modifikasi Pengkodean ElGamal Menggunakan Dua Kunci Privat dan Empat Kunci Publik* adalah benar-benar hasil karya sendiri, kecuali jika dalam pengutipan substansi disebutkan sumbernya, dan belum pernah diajukan pada institusi manapun, serta bukan karya jiplakan. Saya bertanggung jawab atas keabsahan dan kebenaran isinya sesuai dengan sikap ilmiah yang harus dijunjung tinggi.

Demikian pernyataan ini saya buat dengan sebenar-benarnya, tanpa adanya tekanan dan paksaan dari pihak manapun serta bersedia mendapat sanksi akademik jika ternyata dikemudian hari pernyataan ini tidak benar.

Jember, 30 Juni 2009

Yang menyatakan,

Arif Rahman
NIM 021810101016

SKRIPSI

MODIFIKASI PENGKODEAN ELGAMAL MENGGUNAKAN DUA KUNCI PRIVAT DAN EMPAT KUNCI PUBLIK

Oleh

Arif Rahman
NIM 021810101016

Pembimbing

Dosen Pembimbing Utama : Drs. Moh. Hasan, M.Sc., PhD.

Dosen Pembimbing Anggota : Kiswara Agung Santoso, S.Si., M.Kom.

PENGESAHAN

Skripsi berjudul *Modifikasi Pengkodean ElGamal Menggunakan Dua Kunci Privat dan Empat Kunci Publik* telah diuji dan disahkan oleh Fakultas Matematika dan Ilmu Pengetahuan Alam (FMIPA) Universitas Jember pada:

Hari :

Tanggal :

Tempat : FMIPA Universitas Jember.

Tim Penguji

Ketua,	Sekretaris,
Drs. Moh. Hasan, M.Sc., Ph.D. NIP 131759844	Kiswara Agung Santoso, S.Si., M.Kom. NIP 132207813
Anggota I,	Anggota II,
Kristina Wijaya, S.Si., M.Si. NIP 132258180	Agustina Pradjaningsih, S.Si., M.Si. NIP 132257933

Mengesahkan

Dekan,

Prof. Drs. Kusno, DEA., Ph.D.
NIP. 131 592 357

RINGKASAN

Modifikasi Pengkodean ElGamal Menggunakan Dua Kunci Privat dan Empat Kunci Publik; Arif Rahman, 021810101016; 2009: 34 halaman; Jurusan Matematika Fakultas MIPA Universitas Jember.

Ketika suatu pesan ditransfer dari satu pihak ke pihak yang lain, ada kemungkinan bahwa pesan tersebut dapat diambil atau bahkan dimodifikasi oleh pihak-pihak yang tidak diinginkan. Dalam hal ini, kriptografi sangat berperan dalam menyandikan pesan. Pengkodean ElGamal merupakan salah satu jenis kriptografi. Penelitian ini berupaya untuk mendeskripsikan proses penyandian pesan dengan pengkodean ElGamal menggunakan 4 kunci publik dan 2 kunci privat (modifikasi pengkodean ElGamal).

Pada penelitian ini dijelaskan langkah-langkah kerja yang dilakukan, yaitu memodifikasi pengkodean ElGamal dan membuat simulasi modifikasi pengkodean ElGamal dengan Program Maple 9.5.

Modifikasi pengkodean ElGamal memiliki proses yang sama dengan pengkodean ElGamal biasa, yaitu pembentukan kunci, enkripsi dan dekripsi. Tetapi, modifikasi pengkodean ElGamal lebih aman daripada pengkodean ElGamal biasa karena mempunyai lebih banyak kemungkinan pemecahan kunci privat. Secara umum, semakin banyak elemen kunci yang digunakan pada pengkodean ElGamal maka semakin aman pemecahan kunci privat.

PRAKATA

Syukur Alhamdulillah kepada Allah SWT atas segala limpahan rahmat, karunia serta hidayah-Nya, sehingga penulis dapat menyelesaikan karya ilmiah yang berjudul *Modifikasi Pengkodean ElGamal Menggunakan Dua Kunci Privat dan Empat Kunci Publik.* Karya tulis ilmiah ini disusun untuk memenuhi syarat dalam menyelesaikan program pendidikan strata satu (S1) pada Jurusan Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Jember.

Penyusunan skripsi ini tidak lepas dari bantuan berbagai pihak, oleh karena itu penulis menyampaikan ucapan terimakasih yang tiada terhingga kepada:

1. Bapak Drs. Rusli Hidayat, M.Sc., selaku ketua Jurusan Matematika Fakultas MIPA Universitas Jember;
2. Bapak Drs. Moh. Hasan, M.Sc., Ph.D., selaku Dosen Pembimbing Utama dan Bapak Kiswara Agung Santoso, S.Si., M.Kom., selaku Dosen Pembimbing Anggota yang telah meluangkan waktu, pikiran dan perhatiannya guna memberikan bimbingan demi terselesaikannya penulisan skripsi ini;
3. Ibu Kristiana Wijaya, S.Si., M.Si., dan Ibu Agustina Pradjaningsih, S.Si., M.Si., selaku Dosen Penguji yang telah memberikan saran dan kritik demi kesempurnaan penulisan skripsi ini;
4. Ayahanda tercinta (H. Muhdar Juhri) dan Ibunda (Hj. Nur Ainiyah) atas segala cinta, kasih sayang, pengorbanan, dorongan dan do'a tiada henti;
5. Istri (Nur Azizah, Skg) dan anak (M. Rohullah Maulana AL-Aziz) yang selalu memberi semangat, keceriaan, perhatian, dorongan dan do'a tiada henti;
6. Teman-teman 2002, terima kasih atas do'a dan bantuan yang telah diberikan.

Penulis sadar bahwa skripsi ini belumlah sempurna, oleh karena itu saran dan kritikan yang membangun sangat diharapkan. Akhirnya penulis berharap agar skripsi ini dapat memberikan manfaat bagi pembaca.

Jember, 30 Juni 2009 Penulis

DAFTAR ISI

DAFTAR TABEL

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR ALGORITMA

Halaman

DAFTAR LAMPIRAN

Halaman