SISTEM PENGKODEAN GABUNGAN AFFINE DAN MERKLE-HELLMAN

SKRIPSI

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

Oleh

Sindu Tri Guntoro
NIM 031810101015

JURUSAN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS JEMBER
2011

PERSEMBAHAN

Dengan menyebut nama Allah Yang Maha Pengasih dan Maha Penyayang serta sholawat kepada Nabi Muhammad SAW, dengan setulus hati kupersembahkan skripsi ini kepada :

1. Kedua orangtua tercinta, Ayahanda Sumiran dan Ibunda Demi Fatimah, yang telah memberikan segala cinta, kasih sayang, perhatian dan pengorbanan yang tiada henti, serta doa yang tak pernah putus dalam setiap langkah hidup ini;
2. Mbak Nenny, Mbak Herni, Mas Yusnar, Mas Yusuf yang memberi segala pengorbanan, perhatian, keceriaan dan doa yang selalu menyertai langkah ini, Mas Yusuf yang telah memberi masukan dan semangat dengan kasih. Ngalim, Syiro, Edi, Rosi, Shofi, Slamet, Zae, Ana, Nia yang telah memberikan semangat selama di kampus. Semoga cepet lulus ya!!!
3. Guru-guru sejak Taman Kanak-kanak hingga Perguruan Tinggi, yang telah memberikan ilmu dan membimbing dengan penuh kesabaran;
4. Almamater Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Jember.

MOTTO

Jangan putus asa. Mencoba itu, memang lambat. Dan, akan ada penghalang yang menghadang cita-cita itu. Maka, jangan pernah kalah olehnya.
(La Tahzan)

Tak ada rahasia untuk mencapai sukses. Sukses itu dapat terjadi karena persiapan, kerja keras, dan mau belajar dari kegagalan.
(General Colin Powell)

PERNYATAAN

Saya yang bertanda tangan dibawah ini :

nama : Sindu Tri Guntoro

NIM : 031810101015

menyatakan dengan sesungguhnya bahwa skripsi yang berjudul "Sistem Pengkodean Gabungan Affine dan Merkle-Hellman" adalah benar-benar hasil karya sendiri, kecuali jika disebutkan sumbernya dan belum pernah diajukan pada institusi manapun, serta bukan karya jiplakan. Saya bertanggungjawab atas keabsahan dan kebenaran isinya sesuai dengan sikap ilmiah yang dijunjung tinggi.

Demikian pernyataan ini saya buat dengan sebenarnya, tanpa adanya tekanan dan paksaan dari pihak manapun serta bersedia mendapat sanksi akademik jika ternyata di kemudian hari pernyataan ini tidak benar.

Jember, 10 Januari 2011
Yang menyatakan,

Sindu Tri Guntoro
NIM 031810101015

SKRIPSI

SISTEM PENGKODEAN GABUNGAN AFFINE DAN MERKLE-HELLMAN

Oleh

Sindu Tri Guntoro
NIM 031810101015

Pembimbing

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

Dosen Pembimbing Anggota : Ahmad Kamsyakawuni, S.Si.

PENGESAHAN

Skripsi berjudul "Sistem Pengkodean Gabungan Affine dan Merkle-Hellman" telah diuji dan disahkan pada :

hari :

tanggal :

tempat : Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Jember

Tim Penguji :

Ketua,	Sekretaris,
(Dosen Pembimbing Utama)	(Dosen Pembimbing Anggota)
Kiswara Agung Santoso, S.Si., M.Kom.	Ahmad Kamsyakawuni, S.Si.
NIP 197209071998031003	NIP 197211291998021001
Anggota I,	Anggota II,
Prof. Drs. Kusno, DEA., Ph.D.	Drs. Moh. Hasan, M.Sc., Ph.D.
NIP 196101081986021001	NIP 196404041988021001

Mengesahkan,
Dekan,

Prof. Drs. Kusno, DEA., Ph.D.
NIP 196101081986021001

RINGKASAN

Sistem Pengkodean Gabungan Affine dan Merkle-Hellman; Sindu Tri Guntoro, 031810101015; 2011: 47 halaman; Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Jember.

Kemajuan teknologi komputer membantu semua aspek kehidupan manusia, dari hal yang kecil sampai ke berbagai hal yang sangat rumit sekalipun. Jaringan komputer seperti LAN dan internet memungkinkan tersedianya informasi secara cepat. Masalah keamanan dan kerahasiaan data merupakan hal yang sangat penting dalam suatu organisasi maupun pribadi. Oleh karena itu, untuk mengatasi masalah ini dikembangkanlah cabang ilmu yang mempelajari tentang cara-cara pengamanan data atau dikenal dengan istilah Kriptografi. Salah satu metode kriptografi yang digunakan adalah Merkle-Hellman.

Masalah yang akan dikaji yaitu menggabungkan dua sistem pengkodean, antara pengkodean Affine dengan pengkodean Merkle-Hellman. Sistem pengkodean gabungan Affine dan Merkle-Hellman adalah sistem pengkodean yang memodifikasi pengkodean Affine dan pengkodean Merkle-Hellman yaitu pada kunci biner pada Merkle-Hellman dikalikan kunci x yang merupakan kunci Affine dan hasil enkripsinya dijumlahkan dengan kunci b yang merupakan kunci Affine.

Tujuan dari penulisan skripsi ini adalah menggabungkan sistem pengkodean Affine dan Merkle-Hellman, sehingga jumlah parameter dan jumlah langkah pada proses enkripsi maupun dekripsi lebih banyak dibandingkan dengan pengkodean Affine maupun Merkle-Hellman yang bertujuan guna mempersulit pembobolan pesan. Karena salah satu indikator suatu pengkodean lebih aman dibandingkan dengan yang lain adalah jumlah parameter pada proses dekripsi. Sehingga disimpulkan bahwa sistem pengkodean gabungan Affine dan Merkle-Hellman lebih aman dibandingkan dengan pengkodean Affine maupun pengkodean [illegible] Hellman.

PRAKATA

Puji syukur kehadirat Allah SWT atas segala rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul "Sistem Gabungan Pengkodean Affine Dan Merkle-Hellman". Skripsi ini disusun untuk memenuhi salah satu syarat untuk menyelesaikan 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 ingin menyampaikan terima kasih kepada :

1. Bapak Kiswara Agung Santoso, S.Si., M.Kom. dan Bapak Ahmad Kamsyakawuni, S.Si. Selaku Dosen Pembimbing yang telah meluangkan waktu, pikiran, dan perhatian dalam penulisan skripsi ini;
2. Bapak Prof. Drs. Kusno, DEA., Ph.D. dan Bapak Drs. Moh. Hasan, M.Sc., Ph.D., selaku Dosen Penguji yang telah memberikan segala masukan buat terselesainya skripsi ini;
3. Bapak Drs. Rusli Hidayat M.Sc., selaku Dosen Pembimbing Akademik yang telah membimbing selama menjadi mahasiswa;
4. keluarga besar di Kalimantan dan Banyuwangi yang selalu menyemangati tanpa lelah;
5. Ngalim, Andik, Syiro, Edi dan semua teman-teman angkatan 2003 semoga kebersamaannya akan tetap terjalin sampai kapanpun;
6. adik-adik angkatan yang selalu memberi semangat, terima kasih kepada kalian semua.

Penulis juga telah menerima segala kritik dan saran dari semua pihak demi kesempurnaan skripsi ini. Akhirnya penulis berharap, semoga skripsi ini dapat bermanfaat.

Jember, 10 Januari 2011 Penulis

DAFTAR ISI

Halaman

DAFTAR LAMPIRAN

Halaman

DAFTAR TABEL

Halaman

DAFTAR GAMBAR

Halaman