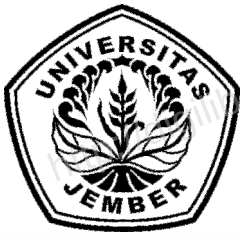
SISTEM PENGKODEAN *VIGENERE* DENGAN SUBSTITUSI INKREMENTAL TANPA BATAS

SKRIPSI

Oleh

Tutut Nisfatul Lailiyah
NIM 021810101079

JURUSAN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS JEMBER
2009



SISTEM PENGKODEAN *VIGENERE* DENGAN SUBSTITUSI INKREMENTAL TANPA BATAS

SKRIPSI

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

Oleh

Tutut Nisfatul Lailiyah
NIM 021810101079

JURUSAN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS JEMBER
2009

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 Taufiqurochman dan Ibunda Khomsatun Rosidah, serta nenek tercinta 'Ipoeh' 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 Noeng, Mas Sinyo, Mbak Ana, Mbak Rietha, Mas Gundhust, Mbak E'enk dan Adik Hafidz yang memberi segala pengorbanan, perhatian, keceriaan dan doa yang selalu menyertai langkah ini, Mas Budi yang telah menemani dalam suka dan duka serta memberikan semangat dengan cinta, kasih sayang dan pengorbanan. Deasy, Ochie', Wieta, Ana, dan Iim yang telah memberikan semangat selama di kampus;
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)

Penaklukan terbesar adalah pada saat kita berhasil menaklukkan diri kita sendiri.
(Toetoet)

PERNYATAAN

Saya yang bertanda tangan di bawah ini :

nama : Tutut Nisfatul Lailiyah

NIM : 021810101079

menyatakan dengan sesungguhnya bahwa skripsi yang berjudul *"Sistem Pengkodean Vigenere dengan Substitusi Inkremental Tanpa Batas"* adalah benar-benar hasil karya sendiri, kecuali jika 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 sebenarnya, tanpa adanya tekanan dan paksaan dari pihak manapun serta bersedia mendapat sanksi akademik jika ternyata dikemudian hari pernyataan ini tidak benar.

Jember, 13 Agustus 2009

Yang menyatakan,

Tutut Nisfatul Lailiyah

NIM 021810101079

SKRIPSI

SISTEM PENGKODEAN *VIGENERE* DENGAN SUBSTITUSI INKREMENTAL TANPA BATAS

Oleh

Tutut Nisfatul Lailiyah
NIM 021810101079

Pembimbing

Dosen Pembimbing Utama : Kiswara Agung Santosa, M.Kom

Dosen Pembimbing Anggota : Ahmad Kamsyakawuni, S.Si

PENGESAHAN

Skripsi berjudul *Sistem Pengkodean Vigenere dengan Substitusi Inkremental Tanpa Batas* 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,
Kiswara Agung Santoso, M.Kom. NIP 132 207 813	Ahmad Kamsyakawuni, S.Si. NIP 132 206 038
Anggota I,	Anggota II,
Prof. Drs. I Made Tirta, M.Sc, Ph.D. NIP. 131 474 500	Drs. Rusli Hidayat, MSc. NIP 132 048 321

Mengesahkan

Dekan FMIPA,

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

RINGKASAN

Sistem Pengkodean *Vigenere* dengan Substitusi Inkremental Tanpa Batas : Tutut Nisfatul Lailiyah; 021810101079; 2009; 30 halaman; Jurusan Matematika Fakultas MIPA Universitas Jember.

Kemajuan teknologi di bidang komputer memungkinkan ribuan orang yang menggunakan komputer terhubung dalam satu dunia maya yang dikenal sebagai *cyberspace* atau internet. Seiring kemajuan teknologi tersebut maka pengamanan terhadap data ratusan organisasi sangat mutlak diperlukan karena semakin canggih teknologi yang ada maka semakin canggih juga kejahatan yang mungkin terjadi. Metode pengamanan data yang banyak digunakan saat ini adalah kriptografi. Salah satu metode kriptografi klasik yang dapat digunakan adalah *Vigenere Cipher.*

Ciri khas dari *Vigenere Cipher* adalah pengulangan pada kuncinya sepanjang *Plaintext* apabila panjang kunci lebih pendek dari panjang *Plaintext*. Namun hal itu juga menjadi kelemahan *Vigenere Cipher* karena perulangan kunci yang pendek memungkinkan untuk sepotong *Plaintext* akan dienkripsikan menjadi *Ciphertext* yang sama. Untuk itu perlu penanganan khusus agar kunci tidak mudah ditebak.

Tujuan dari penulisan skripsi ini adalah untuk memodifikasi pengkodean *Vigenere* dengan menggunakan kunci substitusi inkremental tanpa batas. Kunci yang digunakan adalah penggabungan kunci *Vigenere* dengan kunci substitusi inkremental, kunci substitusi inkremental merupakan kunci yang berupa angka. Modifikasi yang dilakukan pada penelitian ini adalah pada proses inkrementalnya. Disini inkremental yang digunakan adalah inkremental tanpa batas yang didapatkan dari panjang *Plaintext*/*Ciphertext* dikurangi dengan kunci *Vigenere.* Angka kunci inkremental tanpa batas ini nantinya dikalikan dengan kunci *Vigenere* yang sudah dikonversikan ke angka, sehingga didapatkan kunci baru yang digunakan dalam proses enkripsi dan dekripsi. Kunci baru ini nantinya lebih sulit ditebak oleh kriptoanalis dibandingkan dengan kunci inkremental biasa yang merupakan pergeseran dari kunci *Vigenere*nya.

PRAKATA

Syukur Alhamdulillah penulis panjatkan kehadirat Allah SWT, penguasa alam semesta yang melimpahkan rahmat dan hidayah-Nya berupa kemampuan berpikir dan analisis, sehingga penulis dapat menyelesaikan skripsi yang berjudul *Sistem Pengkodean Vigenere dengan Substitusi Inkremental Tanpa Batas*, sebagai persyaratan akademis akhir pada perkuliahan Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Jember.

Keberhasilan penyusunan skripsi ini tidak lepas karena mendapatkan bimbingan, dorongan dan bantuan dari semua pihak yang selama ini telah memberikan motivasi kepada penulis. Oleh karena itu penulis menyampaikan penghargaan dan ucapan terima kasih kepada:

1. Kiswara Agung Santoso, M.Kom, selaku Dosen Pembimbing Utama dan Ahmad Kamsyakawuni, S.Si, selaku Dosen Pembimbing Anggota yang telah membimbing dan mengarahkan penulis;
2. Prof. Drs. I Made Tirta, MSc, Ph.D dan Drs. Rusli Hidayat, MSc, selaku Dosen Penguji yang telah memberikan masukan, saran dan kritik yang membangun dalam penulisan skripsi ini;
3. Agustina Pradjaningsih, S.Si, M.Si selaku Dosen Wali yang telah membimbing dan mengarahkan selama kegiatan perkuliahan dilakukan;
4. Bapak dan Ibu di Trenggalek sekeluarga yang telah memberikan dorongan dan do'anya demi terselesainya skripsi ini;
5. semua adik-adik angkatan 2003, 2004 dan 2005 yang telah memberikan dorongan semangat;
6. semua pihak yang tidak bisa disebutkan satu persatu.

Akhirnya, tiada usaha yang akan berhasil tanpa dimulai dari usaha yang kecil. Semoga skripsi ini dapat bermanfaat.

Jember, 13 Agustus 2009 Penulis

DAFTAR ISI

Halaman

DAFTAR TABEL

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR LAMPIRAN

Halaman

BAB 1. PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi di bidang komputer memungkinkan ribuan orang yang menggunakan komputer terhubung dalam satu dunia maya yang dikenal sebagai *cyberspace* atau internet. Begitu juga dengan ratusan organisasi seperti perusahaan, lembaga negara, lembaga keuangan, militer dan sebagainya. Seiring kemajuan teknologi tersebut maka pengamanan terhadap data ratusan organisasi itu sangat mutlak diperlukan karena semakin canggih teknologi yang ada maka semakin canggih juga kejahatan yang mungkin terjadi, termasuk kejahatan yang berkaitan dengan pencurian data. Oleh karena itu pengamanan data sangat diperlukan dalam dunia teknologi komunikasi. Metode yang dapat digunakan untuk mengamankan data adalah dengan Kriptografi dan Steganografi. Kriptografi merupakan ilmu yang digunakan untuk mengamankan data atau pesan dengan cara mengubahnya (disebut juga dengan enkripsi) menjadi data atau pesan lain dengan algoritma sandi tertentu sehingga tidak sembarang orang bisa mengetahui data atau pesan aslinya. Sementara itu, Steganografi merupakan ilmu yang juga digunakan untuk melindungi data atau pesan dengan cara menyelubunginya didalam data atau pesan lain.

Keunggulan Kriptografi dibandingkan Steganografi adalah teknik pada Kriptografi memiliki algoritma yang pasti dalam enkripsi dan dekripsi pesan. Pada Steganografi, biasanya lebih menggunakan kreativitas sehingga lebih bersifat sebagai sebuah seni. Oleh karena itu kriptografi semakin berkembang dan semakin banyak digunakan untuk menjaga keamanan data. Dalam kriptografi, data yang dikirimkan melalui jaringan akan disamarkan sedemikian rupa sehingga kalaupun data itu bisa dibaca maka tidak bisa dimengerti oleh pihak yang tidak berhak. Dalam kriptografi data yang dikirimkan dan belum mengalami penyandian dikenal dengan istilah *Plaintext*, dan setelah disamarkan dengan suatu cara penyandian maka *Plaintext* ini akan berubah menjadi *Ciphertext.* Untuk melakukan proses penyandian diperlukan adanya kunci. Kriptografi terbagi dalam dua metode yaitu metode kriptografi klasik