

Jurusan Teknik Informatika

Skripsi Sarjana Komputer

Semester Ganjil tahun 2000/2001

**PERANCANGAN KOMPRESI PADACRYPTOGRAPHY RSA
DALAM PENGAMANAN TRANSAKSI
E-COMMERCE**

Surya Wijaya 0331970178

Makmur 0331970801

Darman 0331970842

GT/04

Abstrak

Perkembangan E-commerce sangat ini sangat marak. Tanpa adanya jaminan keamanan maka transaksi tidak akan pernah terjadi. Untuk ini kami berusaha merancang algoritma enkripsi yang baik untuk mendukung Transaksi E-Commerce.

Dalam merancang algoritma enkripsi yang baik kami memilih algoritma enkripsi RSA sebagai algoritma dasar, dan kemudian kami memodifikasi algoritma RSA untuk mendapatkan algoritma yang lebih baik. Salah satu caranya adalah dengan teknik kompresi.

Dari penelitian algoritma modifikasi lebih baik daripada algoritma RSA sebelumnya, dari segi keamanan, ukuran data, serta waktu.

Untuk pengembangan berikutnya diharapkan ada yang menerapkan algoritma penulis untuk enkripsi text dan diharapkan ada yang mencoba membuat struktur data basenya agar dapat digunakan pada transaksi e-commerce *real time*.

Kata Kunci

Keamanan Data, RSA.

PRAKATA

Dengan segala Puji syukur kepada Tuhan Yang Maha Esa atas segala berkat karuniaNya yang telah diberikan kepada penulis, sehingga penulis dapat menyelesaikan Skripsi ini, dimana Skripsi merupakan salah satu syarat kelulusan pada jurusan Teknik Informatika untuk meraih gelar kesarjanaan dalam program jenjang pendidikan Strata-1 di Universitas Bina Nusantara.

Penulis menyadari sepenuhnya bahwa bentuk dari penulisan Skripsi ini tidak terlepas dari kekurangan-kekurangan yang ditimbulkan karena kemampuan, pengetahuan dan pengalaman penulis yang terbatas. Oleh karena itu saran dan kritik yang membangun dari para pembaca akan diterima dengan senang hati dan sebagai bahan pemikiran dan perbaikan di masa mendatang.

Penulis ingin mengucapkan terima kasih kepada banyak pihak yang membantu dalam penulisan skripsi ini. Ucapan terima kasih penulis hanturkan kepada :

- Ibu Ir. Th. Widia Soeryaningsih, MM., selaku Rektor Universitas Bina Nusantara.
- Bapak Ir. Sablin Yusuf, M.Sc, M.CompSc., selaku Ketua Jurusan Teknik Informatika.
- Bapak Gintoro, S.Kom., selaku pembimbing yang telah banyak membantu selama proses penulisan skripsi ini. Terima kasih atas segala ilmu, saran, dan masukan yang Bapak berikan selama ini kepada kami.

- Orang tua, saudara-saudari, dan teman-teman yang banyak memberikan dukungan.
- dan pihak-pihak yang tidak mungkin disebutkan satu persatu.

Akhir kata penulis berharap, semoga penulisan laporan ini bermanfaat bagi pembaca.

Jakarta, Januari 2001

Penulis

DAFTAR ISI

HALAMAN JUDUL LUAR	i
HALAMAN JUDUL DALAM	ii
PERYATAAN PERSETUJUAN	iii
ABSTRAK	iv
PRAKATA	vi
DAFTAR ISI	viii
DAFTAR GAMBAR	xv
DAFTAR TABEL	xviii
BAB 1 PENDAHULUAN	
1.1 Latar Belakang	1
1.2 Ruang Lingkup.....	4
1.3 Tujuan dan Manfaat	5
1.4 Metodologi Penelitian.....	6
1.5 Sistematika Penulisan	

BAB 2 LANDASAN TEORI

2.1	Internet	8
2.1.1	Sejarah Internet	8
2.1.2	Konsep Internet	9
2.1.3	Perkembangan Internet	11
2.2	Kemanan Internet	12
2.2.1	Aspek / servis dari <i>security</i>	12
2.2.1.1	Privacy / Confidentiality	12
2.2.1.2	Integrity	13
2.2.1.3	Authentication	14
2.2.1.4	Availability	15
2.2.1.5	Access Control	15
2.2.1.6	Non-Repudiation	15
2.2.2	Serangan terhadap Keamanan	16
2.2.3	Aplikasi Keamanan Internet	17
2.2.3.1	Secure Socket Layer(SSL)	18
2.2.3.2	Secure Electronic Transaction (SET)	19
2.3	Kompresi	21
2.3.1	Pengertian	21
2.3.2	Jenis-jenis kompresi	21
2.3.2.1	Huffman Coding	21

2.3.2.2	RLE (Run Length Encoding)	22
2.4	Kriptografi	23
2.4.1	Pengertian	23
2.4.2	Sejarah	24
2.4.3	Prinsip kerja Kriptografi	25
2.4.4	Penerapan Kriptografi	27
2.4.5	Jenis-jenis Algoritma Kriptografi	29
2.4.5.1	Algoritma <i>Secret Key</i>	30
2.4.5.1.1	Cara Kerja Algoritma <i>Secret key</i>	30
2.4.5.1.2	Jenis Algoritma <i>Secret key</i> ...	31
2.4.5.2	Algoritma Public Key	33
2.4.5.2.1	Cara Kerja Algoritma <i>Public key</i>	34
2.4.5.2.2	Jenis Algoritma <i>Public key</i> ...	35
2.4.6	Kriptanalisis (<i>cryptanalysis</i>) dan Serangan (<i>attack</i>) terhadap Kriptosistem	36
2.5	RSA	39
2.5.1	Sejarah RSA	39

2.5.2	Prinsip kerja Algoritma RSA	40
2.5.3	Pembuktian Algoritma RSA	41
2.5.4	Contoh Proses Enkripsi/Dekripsi RSA	42
2.5.5	Pengelolaan Kunci	43
2.5.5.1	Pendistribusian Kunci Umum	44
2.5.5.2	Penggunaan kunci umum untuk mendistribusikan <i>secret key</i>	45
2.5.6	Teori Angka (<i>Number Theory</i>)	46
2.5.6.1	Aritmetika Modular (<i>Modular Arithmetic</i>)	46
2.5.6.2	Bilangan Prima	48
2.5.6.3	Pembagi (<i>Divisor</i>)	48
2.5.6.4	Faktor Persekutuan Terbesar (<i>Greatest Common Divisor</i>)	49
2.5.6.5	<i>Invers modulo</i> dari sebuah bilangan	50
2.5.6.6	Teorema Fermat (Fermat's Theorem)	50
2.5.6.7	Fungsi Euler Totient - $\phi(n)$	51

BAB 3 ANALISIS DAN PERANCANGAN SISTEM

3.1	Latar Belakang Perancangan Sistem	51
3.2	Analisis Permasalahan	54

3.2.1	Kelemahan teknik RSA	54
3.2.2	Permasalahan pada penerapan RSA	55
3.3	Analisis Pemecahan Masalah	56
3.3.1	Solusi untuk kelemahan teknik RSA	56
3.3.1.1	Perancangan algoritma perhitungan yang baru pada teknik RSA	56
3.3.1.2	Penerapan teknik Kompresi	63
3.3.1.3	Contoh Penerapan Kompresi	65
3.3.2	Solusi permasalahan pada penerapan RSA	68
3.3.2.1	Penerapan Multi Key	69
3.3.2.2	Pemakaian VB6 DHTML dalam Client Side Scripting	70
3.4	Diagram Alir	71
3.5	Bagan Terstruktur	73
3.5.1	Bagan Tersruktur dari Aplikasi RSA di Client	73
3.5.2	Bagan Tersruktur dari Aplikasi RSA di Server	76
3.5.3	Bagan Terstruktur dari Hubungan Aplikasi RSA Client dan Server	79
3.6	Spesifikasi Rancangan	79
3.6.1	Spesifikasi Modul Untuk Aplikasi RSA di Server ...	79

3.6.2	Spesifikasi Modul Untuk Aplikasi RSA di Client ...	90
3.7	Tampilan Layar	104
3.7.1	Tampilan Layar di Client	105
3.7.2	Tampilan Layar di Server	106

BAB 4 IMPLEMENTASI & EVALUASI

4.1	Implementasi Sistem	107
4.1.1	Kebutuhan Hardware	107
4.1.2	Kebutuhan Software	108
4.1.3	Kebutuhan Jaringan	108
4.1.4	Kompilasi Software	109
4.1.5	Konfigurasi IIS (Internet Information System)	116
4.2	Evaluasi	126
4.2.1	Evaluasi di LAN	127
4.2.2	Evaluasi di WAN (Internet)	132
4.2.3	Evaluasi Ketahanan	136

BAB 5 KESIMPULAN & SARAN

5.1	Kesimpulan	138
5.2	Saran	139

DAFTAR PUSTAKA	140
RIWAYAT HIDUP	141
LAMPIRAN	144

DAFTAR GAMBAR

Gambar 2.1	Gambar Jaringan Internet	9
Gambar 2.2	Proses Transaksi Internet dengan SET	20
Gambar 2.3	Proses enkripsi dan dekripsi	26
Gambar 2.4	Proses enkripsi dan dekripsi dengan menggunakan kunci	27
Gambar 2.5	Algoritma <i>secret key</i> dengan kunci yang sama - E_K	31
Gambar 2.6	Algoritma <i>public key</i> dengan kunci yang berbeda	34
Gambar 3.1	Diagram Alir dari keseluruhan Proses	71-72
Gambar 3.2	Bagan Terstruktur dari aplikasi RSA di Client.....	73
Gambar 3.3	Bagan Terstruktur dari modul Encryption_Norm	74
Gambar 3.4	Bagan Terstruktur dari modul Encryption_Mod	75
Gambar 3.5	Bagan Terstruktur dari modul Encryption	76
Gambar 3.6	Bagan Terstruktur dari aplikasi RSA di Server	76
Gambar 3.7	Bagan Terstruktur dari Response_Norm	77
Gambar 3.8	Bagan Terstruktur dari Response_Mod	78
Gambar 3.9	Bagan Terstruktur dari modul ExponentialMod	78
Gambar 3.10	Bagan Terstruktur dari hubungan aplikasi RSA Client dan Server ..	79
Gambar 3.11	Tampilan Layar di Client	104
Gambar 3.12	Tampilan Layar untuk Response Normal RSA	105

Gambar 3.13	Tampilan Layar untuk Response Modified RSA	106
Gambar 4.1	Menu Utama	109
Gambar 4.2	Pemaketan Script	110
Gambar 4.3	Tipe Paket	111
Gambar 4.4	Direktori Paket	111
Gambar 4.5	Ketergantungan	112
Gambar 4.6	File Ikutan	112
Gambar 4.7	Penentuan Sumber	113
Gambar 4.8	Setting Keamanan	114
Gambar 4.9	Selesai	114
Gambar 4.10	Laporan	115
Gambar 4.11	Peletakan Paket	115
Gambar 4.12	Penentuan Paket	116
Gambar 4.13	Metode Peletakan	117
Gambar 4.14	Lokasi Peletakan	117
Gambar 4.15	Selesai	118
Gambar 4.16	Laporan	118
Gambar 4.17	Menu Run	119
Gambar 4.18	Console	120
Gambar 4.19	Console	120

Gambar 4.20	Menu Open	121
Gambar 4.21	IIS (Internet Information System)	121
Gambar 4.22	Wizard Pembentukan Virtual Directory	122
Gambar 4.23	Penentuan Direktori	122
Gambar 4.24	Penentuan Direktori	123
Gambar 4.25	Konfigurasi Izin Aktifitas	123
Gambar 4.26	Konfirmasi Selesai	124
Gambar 4.27	Console IIS	124
Gambar 4.28	Window Explorer	125
Gambar 4.29	Proses Kriptografi	126
Gambar 4.30	Grafik Perbandingan Peningkatan Ukuran Data	128
Gambar 4.31	Grafik Perbandingan Waktu Dekripsi LAN (1 Client)	129
Gambar 4.32	Grafik Perbandingan Waktu Dekripsi LAN (2 Client)	131
Gambar 4.33	Grafik Perbandingan Waktu Dekripsi WAN (1 Client)	133
Gambar 4.34	Grafik Perbandingan Waktu Dekripsi WAN (2 Client)	135

DAFTAR TABEL

Tabel 2.1	Sejarah Perkembangan Kriptografi (Stallings, 1996, p108)	24
Tabel 2.2	Perbandingan enkripsi <i>Conventional</i> dan <i>public key</i> (Stallings, 1995, p111).....	30
Tabel 2.3	Contoh Proses enkripsi dan dekripsi RSA	43
Tabel 3.1	Tabel Konversi pada algoritma Huffman Coding	65
Tabel 3.2	Tabel Konversi Run Length Encoding	67
Tabel 4.1	Perbandingan Waktu Kecepatan Enkripsi (detik) dan Ukuran Data (bytes) Proses Enkripsi Serta Waktu Kecepatan (detik) Dekripsi Algoritma RSA Pada Komputer Client (Workstation).....	127
Tabel 4.2	Perbandingan Waktu Kecepatan Interaksi (detik) dan Waktu Kecepatan (detik) Dekripsi Algoritma RSA dengan Menggunakan 2 Komputer (2 Client) pada Waktu Bersamaan	130
Tabel 4.3	Perbandingan Waktu Kecepatan Kirim (detik) dan Waktu Kecepatan (detik) Dekripsi Algoritma RSA pada Internet	132
Tabel 4.4	Perbandingan Waktu Kecepatan Interaksi (detik) dan Waktu Kecepatan (detik) Dekripsi Algoritma RSA dengan Menggunakan 2 Komputer (2 Client) di Internet pada Waktu Bersamaan	134

Tabel 4.5	Serangan terhadap Enkripsi Normal	137
Tabel 4.6	Serangan terhadap Enkripsi Modifikasi	137