

Jurusan Teknik Informatika
Skripsi Sarjana Komputer
Semester VII tahun 2000/2001

ANALISIS DAN PERANCANGAN ALGORITMA ENKRIPSI
DALAM APLIKASI E-COMMERCE
(Studi Kasus : Ojolali.com)

Lenny Wongosari <0331970049>
Iwan Supandy <0331970139>
Edwin Sugianto <0331970338>

Kelas / Kelompok : Khusus / AS - 01

Abstrak

Salah satu faktor penting dalam *e-commerce* adalah keamanan data yang dikirim melalui jaringan komunikasi. Untuk menjamin keamanan pengiriman data tersebut, dilakukan pengacakan terhadap data-data yang akan dikirim, yang disebut sebagai teknik enkripsi. Melihat pentingnya enkripsi, khususnya dalam aplikasi berbasis internet, maka penulis bermaksud untuk mengembangkan algoritma enkripsi yang lebih baik dari algoritma yang ada saat ini.

Sebelum merancang algoritma enkripsi yang dibutuhkan, terlebih dahulu dilakukan analisis terhadap beberapa algoritma enkripsi, antara lain : algoritma *public key* (RSA) dan algoritma *symmetric key* (DES). Dari hasil analisis tersebut diperoleh keunggulan dan kelemahan dari masing-masing teknik, kemudian keunggulan dari masing-masing teknik tersebut dipadukan menjadi sebuah algoritma enkripsi baru, yang diberi nama algoritma ELI.

Evaluasi terhadap algoritma ELI dilakukan dengan membandingkannya dengan algoritma RSA, DES dan SOLITAIRE dari segi ukuran key dan jumlah perulangan yang dibutuhkan untuk memecahkan ciphertext menjadi plaintext serta waktu untuk *decipher* berdasarkan *dictionary attack*. Hasil yang diperoleh yaitu bahwa algoritma ELI yang memadukan operasi matematis dan operasi bit akan menghasilkan *cipher text* yang lebih bervariasi dibandingkan dengan algoritma yang hanya menggunakan perhitungan matematis saja. Sehingga untuk memecahkannya dibutuhkan *effort* yang lebih besar.

Kesimpulan yang dapat diambil dari penelitian ini adalah meskipun algoritma ELI terbukti lebih baik daripada algoritma RSA, DES, dan SOLITAIRE dengan ukuran key yang sama, tetapi kinerjanya masih dibatasi oleh kemampuan komputer saat ini yang hanya mampu menangani jumlah variabel sampai 64 bit.

Kata Kunci : enkripsi, *e-Commerce*, *public key*, *symmetric key*

PRAKATA

Puji syukur kami panjatkan kepada Tuhan Yang Maha Esa atas berkat-Nya sehingga kami dapat menyelesaikan penulisan skripsi dengan judul “Analisis dan Perancangan Algoritma Enkripsi dalam aplikasi e-Commerce”. Selain sebagai salah satu syarat utama untuk memperoleh gelar kesarjanaan di Fakultas Ilmu Komputer, Universitas Bina Nusantara, penulisan skripsi ini juga dimaksudkan untuk turut membantu perkembangan teknologi informasi, khususnya pengembangan teknik enkripsi.

Pada kesempatan ini kami ingin mengucapkan terima kasih yang sebesar-besarnya kepada :

1. Bapak Andreas Soegandi, S.Kom. selaku dosen pembimbing yang telah banyak memberikan bimbingan dan petunjuk-petunjuk yang berharga selama penyusunan skripsi ini.
2. Bapak Ir. Sablin Yusuf dan Bapak Yanuar Wahyudi, S.Kom. selaku Ketua dan Sekretaris Jurusan Teknik Informatika Universitas Bina Nusantara.
3. Bapak Akbar selaku Marketing Manager dari perusahaan Ojolali.com yang telah memberikan ijin dan membantu memberikan keterangan-keterangan pada saat kami melakukan survei ke perusahaan Ojolali.com
4. Dosen-dosen Universitas Bina Nusantara yang telah banyak membimbing kami saat menuntut ilmu di Universitas Bina Nusantara.
5. Orang tua dan anggota keluarga yang telah memberikan dukungan moril dan materiil dalam penyusunan skripsi ini.
6. Teman-teman sekalian yang telah membantu penyusunan skripsi ini.

Kami menyadari bahwa masih terdapat banyak kekurangan dalam skripsi ini, mengingat kemampuan kami yang terbatas. Segala saran dan kritikan yang membangun akan kami terima dengan senang hati demi diperolehnya suatu hasil yang lebih baik.

Akhir kata, kami mengharapkan skripsi ini dapat memberikan manfaat bagi pihak yang membutuhkannya.

Penulis

DAFTAR ISI

Halaman Judul Luar	i
Halaman Judul Dalam	ii
Halaman Persetujuan <i>Hardcover</i>	iii
Halaman Pernyataan Dewan Penguji	iv
Abstrak	vii
Prakata	viii
Daftar Isi	x
Daftar Tabel	xiv
Daftar Gambar	xv
Daftar Lampiran	xvii
BAB 1 PENDAHULUAN	
1.1 Latar Belakang	1
1.2 Ruang Lingkup	3
1.3 Tujuan dan Manfaat	4
1.4 Metodologi	4
1.5 Sistematika Penulisan	5
BAB 2 LANDASAN TEORI	
2.1 E-Commerce	7
2.2 Security dalam e-Commerce	8
2.3 Enkripsi dan Dekripsi	9

2.4 Kriptografi	10
2.5 Algoritma Kriptografi dan Teknik Hash	11
2.6 Algoritma RSA (Rhivest-Shamir-Adelman)	12
2.6.1 Penggunaan Algoritma RSA untuk Privacy dan Digital Signature	15
2.6.2 Implementasi RSA dalam SSL (Secure Socket Layer)	15
2.7 Algoritma DES (Data Encryption Standard)	17
2.7.1 Proses Enkripsi dengan Algoritma DES	19
2.7.2 Proses Dekripsi dengan Algoritma DES	25
2.8 Algoritma Solitaire	25
2.8.1 Enkripsi dengan Algoritma Solitaire	26
2.8.2 Dekripsi dengan Algoritma Solitaire	26
2.8.3 Menghasilkan Keystream Letters	26
2.8.4 Menentukan Key yang akan Digunakan	27

BAB 3 ANALISIS SISTEM

3.1 Gambaran Umum Perusahaan	29
3.1.1 Latar Belakang Perusahaan	29
3.1.2 Struktur Organisasi Perusahaan	31
3.1.3 Deskripsi Tugas dari Pihak yang Terkait	31
3.2 Analisa Sistem Penjualan	34
3.2.1 Proses Aliran Data pada Sistem Penjualan	34
3.2.2 Tampilan Layar	41
3.3 Analisa Kebutuhan Sistem Penjualan	43

3.4	Alternatif Kebutuhan Sistem Penjualan	46
BAB 4 RANCANGAN ALGORITMA YANG DIUSULKAN		
4.1	Usulan Algoritma Baru	48
4.1.1	Kriteria Penulis mengenai Security yang Memadai	48
4.1.2	Penjelasan mengenai Software Enkripsi yang Umum digunakan	49
4.2	Perbandingan Rancangan Algoritma dengan Algoritma yang Berjalan	50
4.3	Manfaat Rancangan Algoritma bagi Perusahaan	52
4.4	Penjelasan Rancangan Algoritma	54
4.4.1	Penjelasan Cara Kerja Algoritma beserta Cara Kerja masing-masing Modul	54
4.4.2	Pseudocode Algoritma	76
4.4.3	Tampilan Layar	85
4.4.4	Penjelasan Tampilan Layar	85
4.5	Perbandingan Antar Algoritma	87
4.5.1	Proses Perbandingan	87
4.5.2	Analisa Hasil Perbandingan	91
4.5.2.1	Teknik Jumlah Perulangan	91
4.5.2.2	Teknik Pengujian Waktu	96
4.5.2.3	Perbandingan Enkripsi Menggunakan Algoritma ELI dengan Algoritma RSA	99
4.5.3	Kesimpulan Analisis	101

4.6 Implementasi Algoritma terhadap Website Ojolali.com	101
4.6.1 Penjelasan Implementasi Algoritma	101
4.6.2 Proses Enkripsi Implementasi Algoritma	104
4.6.3 Analisa Perbandingan Waktu Enkripsi dan Transfer Data	106
Antara Algoritma ELI dan RSA	

BAB 5 KESIMPULAN DAN SARAN

5.1 Kesimpulan	108
----------------	-----

5.2 Saran	109
-----------	-----

DAFTAR PUSTAKA	110
-----------------------	-----

RIWAYAT HIDUP	112
----------------------	-----

LAMPIRAN-LAMPIRAN	L1
--------------------------	----

FOTOCOPY SURAT SURVEI	
------------------------------	--

DAFTAR TABEL

Tabel 2.1	Permutasi PC-1	19
Tabel 2.2	Jumlah shift left untuk setiap iterasi	20
Tabel 2.3	Permutasi PC-2	21
Tabel 2.4	Permutasi IP	22
Tabel 2.5	E-Bit selection table	22
Tabel 2.6	S-box yang pertama	23
Tabel 2.7	Permutasi P	24
Tabel 2.8	Permutasi IP^{-1}	25
Tabel 4.1	Perbandingan jumlah perulangan untuk masing-masing algoritma	93
Tabel 4.2	Perbandingan waktu dictionary attack untuk masing-masing algoritma	97
Tabel 4.3	Perbandingan cipher text algoritma RSA dengan algoritma ELI	100

DAFTAR GAMBAR

Gambar 2.1	Langkah-langkah untuk menghasilkan 16 subkey	20
Gambar 2.2	Fungsi f pada algoritma DES	24
Gambar 3.1	Struktur organisasi perusahaan	31
Gambar 3.2	Diagram Konteks dari Sistem Penjualan Ojolali.com	34
Gambar 3.3	Diagram Nol dari Sistem Penjualan Ojolali.com	35
Gambar 3.4	Diagram Rinci dari Proses 1.0	36
Gambar 3.5	Diagram Rinci dari Proses 2.0	37
Gambar 3.6	Diagram Rinci dari Proses 3.0	38
Gambar 3.7	Diagram Rinci dari Proses 4.0	39
Gambar 3.8	Layar pendaftaran anggota baru atau perubahan profil anggota	41
Gambar 3.9	Layar pembayaran dengan kartu kredit	42
Gambar 4.1	Blok diagram algoritma ELI	55
Gambar 4.2	Flowchart untuk modul isprime	56
Gambar 4.3	Flowchart untuk modul formcreate	57
Gambar 4.4	Flowchart untuk modul tofindd	59
Gambar 4.5	Flowchart untuk modul button3_click	60
Gambar 4.6	Flowchart untuk modul expmod	62
Gambar 4.7	Flowchart untuk modul pangkat	64
Gambar 4.8	Flowchart untuk modul dectobin	65
Gambar 4.9	Flowchart untuk modul bintodec	66
Gambar 4.10	Flowchart untuk modul xorshleft	67

Gambar 4.11	Flowchart untuk modul button1_click	68
Gambar 4.12	Flowchart untuk modul shrightxor	70
Gambar 4.13	Flowchart untuk modul button2_click	72
Gambar 4.14	Flowchart untuk modul button4_click	74
Gambar 4.15	Flowchart untuk modul button5_click	75

DAFTAR LAMPIRAN

1. Program ELI diimplementasikan dengan Borland Delphi 5.0	L1
2. Program simulasi enkripsi pada form pendaftaran sebagai bagian dari website Ojolali.com diimplementasikan dengan ASP, VBScript, HTML	
2.1. Algoritma <i>key generation</i> diimplementasikan dengan ASP	L8
2.2. Form pendaftaran beserta algoritma enkripsi	L10
2.3. Form hasil enkripsi diimplementasikan dengan ASP	L16
3. Tabel perbandingan jumlah perulangan tiap karakter studi kasus	L17
4. Tabel perbandingan waktu untuk setiap karakter studi kasus	L20