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 berbasiskan 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 men-*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

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN