ANALISIS DAN IMPLEMENTASI IDENTITY BASED ENCRYPTION BONEH FRANKLIN

Misioner Eman Tb[1], -[2]

[1]Teknik Informatika, Fakultas Teknik Informatika, Universitas Telkom

Abstrak

Identity-Based Encryption memberikan kemudahan pada kriptografi dengan menggunakan sembarang string sebagai kunci publik. Pada kriptografi kunci publik, biasanya enkripsi menggunakan kunci publik yang rumit dan sulit diingat. Identity-Based Encryption menggunakan kunci yang lebih mudah di ingat. Kunci publik pada Identity-Based Encryption ini dapat berupa alamat email, nomor telepon, ataupun suatu kata. Dengan menggunakan metode ini, enkripsi dapat dilakukan sebelum mengetahui kunci privat dari pasangan kunci publik yang sesuai. Pada saat penerima menerima suatu pesan yang terenkripsi tersebut, penerima akan menghubungi Private Key Generator untuk mendapatkan kunci privat dari kunci publik yang digunakan dan mendekripsi pesan yang telah terenkripsi tersebut dengan menggunakan kunci privat yang didapat tersebut.

Identity Based Encryption yang dilakukan pada Tugas Akhir ini berdasar pada konsep yang dikenalkan oleh Boneh dan Franklin. Tugas Akhir ini berisi perancangan dan implementasi dari Identity Based Encryption Boneh Franklin dan perhitungan waktu terhadap fungsi-fungsi hasil implementasi dengan menggunakan perhitungan waktu pada sistem operasi.

Kata Kunci : Identity-Based Encryption, kunci publik, kunci privat, Private Key Generator.

Abstract

Identity Based Encryption facilitate is an easy way to cryptography by using arbitrary string as a public key. In the common public key cryptography, the encryption using a complicated public key and hard to remember. In the Identity Based Encryption, the public key can be email address, phone number or an arbitrary word. Using this method, the encryption can be done before pairing the public key and the private key. When the recipient recieve an encrypted message, the recipient have to contact the Private Key Generator to obtain his/ her private key and decrypt the encryped message using his/ her private key.

The Identity Based Encryption in this project is based on Boneh and Franklin method. An overview of the Identity Based Encryption Boneh Franklin implementation is given in this project and the duration measurement of this implementation using operating system high precision timer.

Keywords : Identity-Based Encryption, Public Key, Private Key, Private Key Generator.

BAB I
PENDAHULUAN

1.1 Latar Belakang

Identity-Based Encryption merupakan teknik enkripsi dengan menggunakan kunci asimetris yang mempunyai keistimewaan, yaitu kunci publik yang digunakan dapat berupa sembarang string. Biasanya, enkripsi menggunakan kunci publik yang rumit dan sulit diingat. *Identity-Based Encryption* menggunakan kunci yang lebih "user-friendly". Kunci publik pada *Identity-Based Encryption* ini dapat berupa alamat email, nomor telepon, ataupun suatu kalimat. Kelebihan lain dari teknik enkripsi ini yaitu tidak diperlukannya penentuan pasangan kunci sebelum melakukan enkripsi. Dengan menggunakan *Identity-Based Encryption*, seseorang dapat mengirimkan pesan yang telah dienkripsi dengan kunci publik walaupun penerima belum mempunyai bahkan belum pernah mendengar kunci privat sekalipun.

1.2 Perumusan Masalah

Adapun permasalahan yang ingin diangkat dalam penelitian tugas akhir ini adalah:

1. Bagaimana kemudahan penggunaan *Identity-Based Encryption* untuk pengamanan pengiriman informasi.
2. Bagaimana *Identity-Based Encryption* menghasilkan kunci yang dibutuhkan.
3. Bagaimana *Identity-Based Encryption* dapat menghilangkan kebutuhan sertifikat untuk kunci publik.

1.3 Tujuan Penelitian

Tujuan penelitian dari tugas akhir ini adalah:

1. Mempelajari kemudahan yang di hasilkan dengan menggunakan string identitas sebagai kunci publik dan mengimplementasikan sistem *Identity-Based Encryption Boneh-Franklin*.

2. Analisis kecepatan proses-proses pada sistem Identity Based Encryption Boneh Franklin dengan menggunakan perhitungan kecepatan proses berdasarkan waktu pada sistem operasi yang di gunakan serta analisis file hasil encode dan decode pesan text dengan menggunakan AES.

1.4 Batasan Masalah

Pembahasan masalah pada tugas akhir ini akan dibatasi pada ruang lingkup :

1. Tidak menganalisis secara matematis teknik *Identity-Based Encryption Boneh-Franklin*.
2. File yang digunakan untuk enkripsi adalah berupa file pesan text.
3. Fungsi hash, fungsi AES dan fungsi pairing yang digunakan pada kurva elips diambil dari implementasi yang telah ada dari MIRACL 5.0.
4. Implementasi perangkat lunak digunakan bahasa pemrograman Microsoft Visual C++ 6.0.

1.5 Metodologi Pemecahan Masalah

Metode yang digunakan dalam penyelesaian Tugas Akhir ini yaitu:

1. Studi Literatur

   Diperlukan untuk memecahkan rumusan permasalahan berdasarkan referensi dan mengumpulkan data yang berkaitan dengan perumusan masalah.
2. Analisis masalah dan kebutuhan perangkat lunak yang akan dibangun.
3. Merancang pemecahan masalah berdasarkan hasil analisis yang didokumentasikan dalam suatu spesifikasi.
4. Implementasi

   Tahap pembuatan perangkat lunak *Identity-Based Encryption Boneh-Franklin*.
5. Penyusunan laporan tugas akhir dan kesimpulan akhir.

1.6 Sistematika Penulisan

Tugas Akhir ini akan disusun dengan sistematika sebagai berikut :

Bab I Pendahuluan.

Bab ini memberikan gambaran secara garis besar tentang Tugas Akhir yang dilakukan penulis. Mencakup latar belakang pembuatan Tugas Akhir, perumusan masalah, pembatasan masalah, tujuan, metodologi pemecahan masalah dan sistematika penulisan.

Bab II Dasar Teori.

Bab ini menjelaskan seluruh teori yang menjadi landasan konseptual dan pendukung penyelesaian Tugas Akhir ini yaitu teori tentang mekanisme *Identity-Based Encryption Boneh-Franklin.*

Bab III Perancangan dan Implementasi Sistem *Identity Based Encryption*.

Menjelaskan tentang proses analisis masalah dan kebutuhan perangkat lunak. Berisi rancangan yang meliputi proses enkripsi dan dekripsi suatu pesan dengan menggunakan *Identity-Based Encryption Boneh-Franklin.*

Bab IV Pengujian dan Analisis.

Mengimplementasikan dan analisis dari proses enkripsi suatu pesan dengan menggunakan *Identity-Based Encryption Boneh-Franklin.*

Bab V Kesimpulan.

Bab ini berisi kesimpuan dari keseluruhan sistem yang dibuat serta saran yang berkaitan dengan aplikasi Tugas Akhir ini dan kemungkinan pengembangan selanjutnya.

BAB V
KESIMPULAN

5.1 Kesimpulan.

Adapun kesimpulan yang bisa diambil dari penelitian tugas akhir ini adalah sebagai berikut :

1. Pada sistem IBE-BF, memberikan kemudahan bagi pengguna sistem tersebut karena kemudahan dalam mengingat kunci publik yang digunakan.
2. Dengan menggunakan identitas sebagai kunci publik, maka sistem IBE-BF ini telah menghilangkan kebutuhan akan sertifikat kunci publik karena string tersebut merupakan identitas dari pengguna kunci publik sehingga pada saat akan melakukan enkripsi suatu pesan text dengan menggunakan kunci publik yang sesuai, pengguna sistem IBE-BF tidak perlu berkomunikasi dengan server key untuk melihat otentikasi dari kunci publik tersebut.
3. Hasil encode dari pesan text dengan menggunakan AES lebih kecil dari pesan text sebelum di encode sebesar jumlah baris baru pada pesan text.
4. Waktu yang di butuhkan untuk proses sistem ini relatif konstan sesuai dengan parameter kunci yang di gunakan dan penggunaan waktu disini adalah waktu proses pada sistem operasi yang digunakan untuk menjalankan aplikasi sistem IBE-BF.

5.2 Saran.

1. Untuk menghasilkan kunci privat dari setiap kunci publik, kunci master dari PKG mempunyai peran yang sangat penting sehingga keamanan dan keberadaan dari kunci master harus terjamin, karena jika kunci master diketahui oleh pihak yang tidak berkepentingan maka akan sangat berbahaya. Selain itu jika kunci master hilang, penghasilan kunci privat dari kunci publik tidak dapat dilakukan lagi.

2. Pengambilan kunci privat untuk kunci publik sesuai dilakukan dengan proses extract, pada proses ini, PKG akan mengirimkan kunci privat kepada pengguna sistem IBE-BF ini, sehingga dibutuhkan media pengiriman kunci privat yang aman.
3. Aplikasi yang dibangun hanya berupa implementasi berbasis perintah baris dan tidak bekerja pada jaringan internet sehingga aplikasi ini nantinya dapat di kembangkan menjadi aplikasi yang berguna untuk pemakaian sehari-hari seperti menanamkan aplikasi ini pada server email untuk pengamanan isi dari email.

DAFTAR PUSTAKA

[1] A. Menezes, P. Van Oorschot, S. Vanstone, "Handbook of Applied Cryptography: Chapter 8", CRC Press, 1996.

[2] Budi Rahardjo, Keamanan Sistem informasi Berbasis Internet, PT Insan Indonesia, Bandung, 2005.

[3] Certicom Research, "Standard for Efficient Cryptography: Sec 1: Elliptic Curve Cryptography", Certicom Corp., 2000.

[4] Clifford Cocks, "An Identity Based Encryption Scheme based on Quadratic Residues", Communications Electronics Security Group, Cheltenham, 2001.

[5] Dan Boneh, Matthew Franklin, "*Identity Based Encryption from Weil Pairing*", http://crypto.standard.edu/~dabo/papers/ibe.pdf, 2001.

[6] Evelyn, "Identity Based Encryption", Departemen Teknik Elektro, Institut Teknologi Bandung, 2004.

[7] Federal Information Processing Standards Publication 180-1, Secure Hash Standard, 1995.

[8] Gerhard Frey, Michael Muller, Hans-Georg Ruck, "The Tate Pairing and The Discrete Logarithm Applied to Ellipticc Curve Cryptosystems", Institute for Experimental Mathematics, University of Essen Ellernstr, Essen, 1998.

[9] G. M. Bertoni, L. Chen, P. Fragneto, K. A. Harrison, G. Pelosi, Computing Tate Pairing on Smartcards.

[10] http://en.wikipedia.org/wiki/Cipher_feedback

[11] Nana Juhana, "Implementasi Elliptic Curves Cryptosystem (ECC) pada Proses pertukaran Kunci Diffie Hellman dan Skema Enkripsi El Gamal", Pasca Sarjana Teknik Industri, Institut Teknologi Bandung, 2005.

[12] Steven Galbraith, "Supersingular Curve and the Tate Pairing", Royal Holloway University of London, http://www.isg.rhul.ac.ud/~sdg/.

[13] Tim Gibson, Securing Wireless Communications with Identity-based Encryption, Voltage Security.

[14] V. Miller, "Short program for function on curves", Unpublished manuscript, 1986.