ANALISIS DAN IMPLEMENTASI IDENTITY BASED ENCRYPTION BONEH FRANKLIN

Maman Abdurohman, Misioner Eman T. B., Andrian Rakhmatsyah
Jurusan Teknik Informatika, Sekolah Tinggi Teknologi Telkom Bandung
Jln. Telekomunikasi No. 1,Dayeuhkolot, Bandung, tlp/fax 022-7565931
E-mail: m_abdurohman@yahoo.com

ABSTRAKSI

Identity-Based Encryption memberikan 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 publik yang lebih mudah diingat. 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 Privat Key Generator untuk mendapatkan kunci privat dari kunci publik yang digunakan dan mendeteksi 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 ini berdasarkan konsep yang dikenalkan oleh Boneh dan Franklin. Paper ini berisi perancangan dan implementasi 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*

1. PENDAHULUAN

1.1 Latar Belakang

Identity-Based Encryption merupakan teknik enkripsi dengan menggunakan kunci asimetris dengan kelebihan kunci publik yang digunakan dapat berupa sembarang string. Enkripsi biasanya menggunakan kunci publik yang 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. Disamping itu dengan menggunakan Identity-Based Encryption, seseorang dapat mengirimkan email yang telah dienkripsi dengan kunci publik walaupun penerima belum mempunyai kunci privat sekalipun.

Permasalahan yang dibahas dalam paper ini adalah:

a. Bagaimana kemudahan penggunaan *Identity-Based Encryption* untuk pengamanan pengiriman informasi.
b. Bagaimana *Identity-Based Encryption* menghasilkan kunci yang dibutuhkan.
c. Bagaimana Identity-Based Encryption dapat menghilangkan kebutuhan sertifikat untuk autentikasi kunci publik.

1.2 Tujuan Pembahasan

Tujuan penulisan paper ini adalah:

a. Mempelajari dan mengaplikasikan *Identity-Based Encryption Boneh-Franklin*.
b. Analisis kecepatan enkripsi dan dekripsi dari *Identity-Based Encryption Boneh-Franklin* berdasarkan ukuran file yang akan di proses dan ukuran file cipher yang dihasilkan.

1.3 Metode Penyelesaian

Metode penyelesaian yang digunakan:

a. Studi Literatur: memecahkan rumusan permasalahan berdasarkan referensi.
b. Analisis masalah dan kebutuhan perangkat lunak yang akan dibangun.
c. Merancang pemecahan masalah berdasarkan hasil analisis yang didokumentasikan dalam suatu spesifikasi.
d. Implementasi : Tahap pembuatan perangkat lunak *Identity-Based Encryption Boneh-Franklin*.
e. Penyusunan laporan paper dan kesimpulan akhir.

2. DASAR TEORI

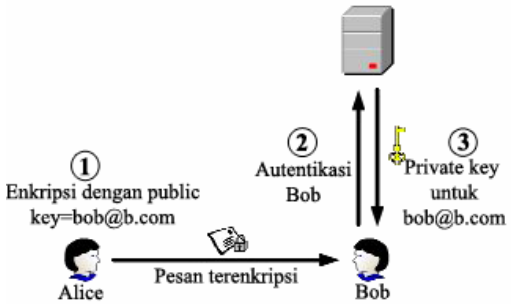
2.1 Konsep Dasar *Identity-Based Encryption (IBE)*

Konsep IBE ditemukan pada tahun 1984 oleh Adi Shamir dalam rangka mengatasi masalah autentikasi kunci publik. Idenya adalah untuk menghindari kebutuhan autentikasi dengan cara kunci publik yang digunakan berhubungkan langsung dengan identitas *user*. Kunci publik *user* dihasilkan langsung dari informasi publik yang tersedia yang dapat mengidentifikasikan *user* tersebut secara unik. Informasi ini disebut sebagai identitas digital *user*. Bergantung pada aplikasi, identitas ini dapat berupa nama *user*, nomor kartu identitas, nomer telepon, alamat *email*, atau

informasi yang mungkin lainnya. Dengan demikian, kunci publik *user* telah siap tersedia untuk siapapun yang mengetahui identitasnya sehingga tidak diperlukan lagi pencarian kunci pada basis data.

Pada sistem kunci publik konvensional, pasangan kunci dihasilkan dengan memilih secara acak sebuah kunci privat dan dengan menggunakan fungsi satu arah diperoleh kunci publik. Pada IBE, kunci publik ditentukan berdasarkan identitas *user*. Kemudian kunci privat harus dihasilkan dari kunci publik. Dalam hal ini, pembuatan kunci tidak dapat dilakukan oleh *user* sendiri. Apabila seorang *user* mengetahui bagaimana cara manghasilkan kunci privat yang bersesuaian dengan kunci publiknya, maka ia juga dapat membuat kunci privat untuk *user* lainnya. Oleh karena itu, diperlukan pihak ketiga yang disebut *Private Key Generator (PKG)*. Setelah melalui suatu prosedur autentikasi, PKG akan menghasilkan kunci privat user. PKG dapat melakukan ini dengan mengetahui suatu informasi rahasia yang disebut *master key*. Informasi yang tersedia untuk umum yang bersesuaian dengan *master key* disebut parameter sistem.

Dengan konsep IBE, Shamir telah membuat implementasi untuk *Identity-Based Signature*. Implementasi ini mirip dengan RSA yang cukup rumit. Di lain pihak, Shamir melihat bahwa teknik enkripsi RSA tidak dapat dikonversi ke teknik *Identity-Based Encryption.* Hal ini baru terpecahkan pada tahun 2001, dimana Boneh dan Franklin menemukan bahwa sifat *bilinear* dari *pairing* dapat digunakan untuk mengkonversikan teknik enkripsi ElGamal menjadi IBE dan berdasar pada kriptografi kurva elips. Pada saat yang sama, teknik IBE lainnya juga ditemukan oleh Cocks, yaitu berdasarkan residu kuadratis. Pada sistem IBE, Autentikasi dan pelaksanaan kebijaksanaan dilakukan melalui *centrally-administered server.*



Gambar 1. Teknik Identity-based Encryption

Dengan demikian. Kunci privat hanya perlu dihasilkan satu kali saja pada saat penerimaan pesan pertama. Komunikasi selanjutnya dapat di dekripsi dengan menggunakan kunci privat yang sama, sehingga dapat dilakukan ketika user sedang *offline*. *Offline* disini berarti, kedua entitas tidak perlu berhubungan dengan *key server* yang dalam hal ini adalah PKG.

2.2 Kriptosistem Kurva Elips (*Elliptic Curves Cryptosystem*)

Pada tahun 1985, Neil Koblitz dan Viktor Miller secara terpisah memproposalkan kriptosistem kurva elips (*Elliptic Curves Cryptosystem - ECC*) yang menggunakan masalah logaritma diskrit pada titik-titk kurva elips yang disebut dengan ECDLP (*Elliptic Curves Discrete Logarithm Problem*). Kriptosistem kurva ellips ini dapat digunakan pada beberepa keperluan seperti:

- Skeme enkripsi (ElGamal ECC)
- Tanda tangan digital (ECDSA – *Elliptic Curves Digital Signature*)
- Protokol pertukaran kunci (Diffie Hellman ECC)

Saat ini ada tiga macam sistem kriptografi kunci publik yang aman dan efisien yang dikelompokan berdasarkan permasalahan matematis, yaitu:

- Sistem Pemfaktoran Bilangan Integer (*Integer Factorization Systems*).
- Sistem Logaritma Diskrit (*Discrete Logarithm Systems*).
- Kriptosistem Kurva Elips (*Elliptic Curves Cryptosystem*).

2.3 Protokol Pertukaran Kunci Diffie – Hellman pada Kurva Elips

Diffie–Hellman pertama kali memperkenal-kan algoritma kunci publik pada tahun 1976. Algoritma ini memiliki keamanannya dari kesulitan menghitung logaritma diskrit dalan *finite field*, dibandingkan kemudahan dalam menghitung bentuk eksponensial dalam *finite field* yang sama. Algoritma ini dapat digunakan dalam mendistribusikan kunci publik yang dikenal dengan protokol pertukaran kunci.

Penjelasan protokol pertukaran kunci ini dapat diilustrasikan antara dua orang, misalkan saja **Alice** dan **Bob,** yang keduanya sepakat mengenai bilangan prima yang besar misalkan *n* dan *g* dimana *g* merupakan modulo *n*. Selanjutnya akan terdapat dua buah integer yang tidak dirahasiakan atau merupakan kunci publik dan dapat didistribusikan dalam saluran bebas. Proses berikutnya dijelaskan dalam tahapan-tahapan di bawah ini :

2.4 *Tate Pairing*

Pada kriptografi kurva elips, penentuan pasangan kunci (*key pair*) merupakan suatu hal yang penting untuk tetap menjaga kriteria-kriteria pada kriptografi kurva elips. *Tate pairing* diperkenalkan oleh Frey dan Ruck. Tate pairing digunakan untuk mencari pasangan kunci pada kurva elips, perhitungan untuk perhitungan untuk Tate Pairing ini adalah menggunakan algoritma Miller Tate pairing mempunyai sifat bilinear sebagai berikut:

$$e\left(a \cdot X, b \cdot Y\right) = e\left(X, Y\right)^{ab}$$

dimana a,b adalah bilangan integer dan X,Y adalah suatu titik pada kuva elips. Sistem Identity Based Encryption ini menggunakan sifat dari bilinear tersebut untuk menghasilkan kunci publik dan kunci privat yang sesuai.

Selain itu Tate Pairing juga mempunyai sifat non-degenerate, yang di sebut disini non-degenerate.

2.5 Fungsi Hash

Fungsi hash merupakan fungsi yang bersifat satu arah dimana jika kita memasukkan data, maka fungsi hash akan menghasilkan suatu "checksum" dari data tersebut. Keluaran dari fungsi hash merupakan Message Authenticated Code (MAC) atau biasa disebut dengan message digest.

2.6 AES (Advanced Encryption Standard)

AES (*Advanced Encryption Standard*) digunakan sebagai standar algoritma kriptografi yang terbaru. AES menggantikan DES (*Data Encryption Standar*) yang pada tahun 2002 sudah berakhir masa penggunaannya. DES juga dianggap tidak mampu lagi untuk menjawab tantangan perkembangan teknologi komunikasi yang sangat cepat. AES sendiri adalah algoritma kriptografi dengan menggunakan algoritma Rijndael yang dapat mengenkripsi dan mendekripsi blok data sepanjang 128 bit dengan panjang kunci 128 bit, 192 bit, atau 256 bit.

Pada Paper ini, fungsi AES ini digunakan untuk menyandikan pesan text yang digunakan dengan panjang kunci 192 bit. Operasi penyandian blok (*block cipher*) yang digunakan adalah mode operasi *Cipher Feedback (CFB)* (http://en.wikipedia.org/wiki/Cipher_feedback).

2.7 Identity Based Encryption Boneh Franklin

Skema IBE yang diperkenalkan oleh Boneh dan Franklin terdiri dari 4 algoritma utama, yaitu ***setup, extract, encrypt, decrypt***. Proses s*etup* dijalankan oleh PKG (*Private Key Generator*) untuk menghasilkan kunci *master* dan parameter sistem, proses *extract* juga dijalankan oleh PKG untuk menghasilkan kunci privat dari kunci publik entitas yang menggunakan sistem IBE. Sedangkan *encrypt* dan *decrypt* dijalankan oleh entitas yang menggunakan sistem IBE. *Sistem Identity Based Encryption Boneh Franklin (IBE-BF)* ini berdasar pada kriptografi kurva elips, persamaan kurva yang digunakan adalah:

$$E : y^2 = x^3 + 1$$

dan menggunakan sifat bilinear dari Tate Pairing pada pemetaan kurva elips untuk menghasilkan suatu pasangan kunci (W-RFID 05_2-3_Gibson.pdf), persamaan *Tate Pairing* pada sistem IBE-BF adalah:

$$\hat{e}(P,Q) = e\left(P, \varphi(x,y)\right) = e\left(P, (\omega x, y)\right)$$

dimana $\omega : x^3 = 1 \bmod p$

dan

$$\hat{e}(a \cdot P, b \cdot Q) = \hat{e}(P,Q)^{ab}$$

IBE-BF Setup

IBE-BF Setup dilakukan pada entitas server PKG (Private Key Generator). Perhitungan yang pertama kali dilakukan pada IBE-BF Setup yaitu penentuan bilangan prima p dan q yang memenuhi kondisi berikut:

- q>3
- p=2 mod 3 dan p=6q-1.

Setelah p dan q didapatkan, selanjutnya dilakukan perhitungan sebagai berikut.

1. Tentukan master key s yang hanya diketahui oleh PKG. $s \in Z_q^*$.
2. Tentukan parameter global yang akan dipublikasikan ke pengguna sistem IBE-BF yaitu:
   - Tentukan titik $P \in E(F_p)[q]$.
   - Tentukan $P_{PUB} = s \cdot P$
   - Tentukan $\omega : x^3 = 1$, dimana $x \neq 1$
   - Tentukan 4 fungsi hash, yaitu:
     - $H_1 : \{0,1\}^* \rightarrow F_p$.
     - $H_2 : F_{p^2} \rightarrow \{0,1\}^n$.
     - $H_3 : \{0,1\}^n \times \{0,1\}^n \rightarrow Z_q^*$
     - $H_4 : \{0,1\}^n \rightarrow \{0,1\}^n$
   - Tentukan ruang untuk cipher dan ruang untuk pesan.
     - $\mathbf{M} = \{0,1\}^n$
     - $\mathbf{C} = E(F_p) \times \{0,1\}^n$

IBE-BF Extract.

IBE-BF Extract dilakukan pada saat user ingin mendapatkan kunci privat dari kunci publik yang digunakan untuk mengenkripsi pesan yang di tujukan kepada user tersebut. Perhitungan ini juga dilakukan pada server PKG dan kunci privatnya dikirimkan ke user tersebut. Perhitungan yang dilakukan adalah sebagai berikut.

- $ID_y = \dfrac{p+q}{q} \cdot H_1(ID)$
- $ID_x = \left(ID_y{}^2 - 1\right)^{\frac{1}{3}}$
- $Q_{ID} = \left(ID_x, ID_y\right) \in E(F_p)[q]$
- $d_{ID} = s \cdot Q_{ID} \in E(F_p)[q]$

ID adalah string identitas yang digunakan sebagai kunci publik, H adalah fungsi hash yang di gunakan, d_{ID} adalah kunci privat dari kunci publik tersebut.

IBE-BF Encrypt.

Proses ini dilakukan pada saat pengirim ingin mengenkripsi pesan $M \in \mathbf{M}$ menjadi suatu cipher $C \in \mathbf{C}$ untuk di kirim ke penerima. Proses ini tidak perlu berhubungan dengan server PKG. Langkah-langkah pada proses ini adalah sebagai berikut:

- $ID_y = \frac{p+q}{q} \cdot H_1(ID)$.
- $ID_x = \left(ID_y{}^2 - 1\right)^{\frac{1}{3}}$.
- $Q_{ID} = \left(ID_x, ID_y\right) \in E\left(F_p\right)[q]$.
- Tentukan $\sigma \in \{0,1\}^n$.
- Hitung $r = H_3(\sigma, M)$.
- Hasil enkripsi adalah:
  $C = \left\langle rP, \sigma \oplus H_2\left(g_{ID}^r\right), M \oplus H_4(\sigma)\right\rangle$
  dimana $g_{ID} = \hat{e}\left(Q_{ID}, P_{PUB}\right) \in E_{p^2}$

IBE-BF Decrypt.

Proses ini dilakukan untuk mendekripsi cipher $C = \langle U, V, W\rangle$ yang diterima, sebelumnya penerima pesan harus telah mendapatkan kunci privatnya d_{ID} dari server PKG. Langkah-langkah pada proses ini adalah sebagai berikut:

Jika $U \notin E\left(F_p\right)[q]$, maka cipher tidak valid. Jika cipher adalah valid, maka lakukan perhitungan sebagai berikut:

o Tentukan
$V \oplus H_2\left(\hat{e}\left(d_{ID}, U\right)\right) = \sigma$.

- Tentukan $W \oplus H_4(\sigma) = M$
- Tentukan $r = H_3(\sigma, M)$. Jika $U \neq rP$, maka cipher tidak valid

Jika $U = rP$, maka keluaran adalah M dari hasil dekripsi cipher C.

3. PERANCANGAN DAN IMPLEMENTASI SISTEM IBE-BF

3.1 Proses Umum IBE-BF

Proses pada sistem *Identity Based Encryption Boneh Franklin* secara umum adalah sebagai berikut:

- *Setup*, yaitu penentuan parameter sistem dan *master key s* yang dijalankan oleh mesin PKG (*Private Key Generator*). Parameter sistem ini adalah berupa $params\left(p, q, PBITS, P, P_{pub}, \omega\right)$ dan dipublikasikan ke semua pemakai sistem IBE-BF.
- *Extract*, untuk mendapatkan kunci privat dari sistem IBE-BF sesuai dengan kunci publik yang digunakan yang pada sistem IBE-BF ini adalah alamat email.
- *Encrypt*, yaitu proses untuk mengenkripsi suatu pesan dengan menggunakan sistem IBE-BF berdasarkan parameter yang di hasilkan oleh PKG dan dengan menggunakan kunci publik yang sesuai.
- *Decrypt*, yaitu proses untuk mendekripsi pesan yang telah di enkripsi dengan menggunakan kunci privat yang telah di dapat kan dari proses *extract*.

3.2 Fungsi Hash

Pada sistem IBE-BF ini di butuh kan 4 fungsi hash, fungsi hash yang di gunakan pada Paper ini adalah SHS (*Secure Hash Standard*):

1. $H_1 : SHS(string)$, hash dilakukan sampai pada posisi string yang memiliki nilai kosong *string[i]=0*, dimana $i \geq 0$, keluaran dari hash ini adalah suatu titik pada sumbu y.
2. $H_2 : SHS(Q)$ hash dilakukan pada titik Q kurva $E\left(F_{p^2}\right)$ dengan panjang hash=n bit, dimana $n \geq 0$, keluaran dari hash ini adalah n. Pada Paper ini n yang digunakan adalah 160 bit.
3. $H_3 : SHS\left(x_1, x_2\right)$, keluaran dari hash ini adalah hasil hash dari x_1 dan x_2 dengan panjang hash adalah n byte.
4. $H_4 : SHS\left(y\right)$, keluaran dari hash ini adalah hasil hash dari y dengan panjang hash adalah n bit.

Pada sistem IBE-BF, masukan adalah berupa string identitas (ID), sehingga di butuhkan suatu fungsi untuk mengubah ID tersebut menjadi suatu titik pada kurva elips yaitu dengan cara mengkonversikan string identitas menjadi suatu bilangan *integer* yang kemudian bilangan integer tersebut menjadi suatu titik pada kurva elips.

3.3 MapToPoint.

Konversi string identitas (*ID*) menjadi suatu bilangan *integer* adalah dengan menggunakan suatu *hash*. *Hash* adalah suatu fungsi matematika yang mengkonversikan suatu pesan dengan panjang yang tidak tetap menjadi suatu kumpulan digit dengan panjang yang tetap (*fixed-length string*). Pada Paper ini, algoritma yang digunakan untuk fungsi *hash* tersebut adalah SHS.

Kondisi *MapToPoint* adalah sebagai berikut:

Persamaan kurva elips adalah $y^2 = x^3 + 1$, $H_1 = SHS(ID)$ merupakan fungsi *hash* yang digunakan, *p* adalah bilangan prima, Q_{ID} adalah titik hasil konversi *string* identitas pada kurva elips. Maka algoritma dari MapToPoint dapat dituliskan sebagai berikut:

1. $y_0 = SHS(ID)$.
2. $x_0 = \left(y_0{}^2 - 1\right)^{\frac{1}{3}} \bmod p$.
3. $Q_{ID} = (x_0, y_0)$

3.4 Tate Pairing.

Terdapat titik yang unik pada kurva elips dari pasangan kunci yang sesuai dengan pasangan kunci lawan (lawan kunci publik adalah kunci privat, dan sebaliknya). Penentuan kunci lawan ini dapat dicari dengan menggunakan algoritma Tate pairing dengan masukan adalah P_{PUB}, Q_{ID} dan keluarannya adalah $g_{ID} = e(P_{PUB}, \omega Q_{ID}) = \hat{e}(P_{PUB}, Q_{ID})$, untuk implementasi Tate Pairing kurva elips pada Paper ini diambil dari Miracl 5.0.

4. PENGUJIAN DAN ANALISIS

4.1 Pengujian Fungsional.

Tujuan utama dari sistem kriptografi ada menyandikan suatu pesan text yang dapat dibaca isi dari pesan text tersebut menjadi suatu kode yang tidak dapat dibaca. Perangkat lunak yang di bangun harus dapat memenuhi tujuan utama tersebut, sehingga pada Penelitian ini dilakukan pengujian pada 5 jenis pesan text, yaitu file_1.txt, file_2.txt, file_3.txt, file_4.txt, file_5.txt. Perbandingan isi daripada pesan text asli dengan pesan text hasil dekripsi dilakukan dengan perintah "**comp** [*data1*] [*data2*]" pada menu *command prompt* Microsoft Windows XP Profesional Service Pack 2.

4.2 Perbandingan Ukuran File.

Pada aplikasi Penelitian ini, mode operasi yang di gunakan untuk mengenkripsi pesan text pada algoritma enkripsi AES adalah mode operasi CFB yang merupakan mode operasi *stream cipher*, sehingga hasil dari pesan text yang telah di enkripsi (*cipher-text*) tidak boleh lebih besar daripada pesan text aslinya. Berikut ini akan diberikan tabel pengujian terhadap beberapa hasil enkripsi dari beberapa pesan text.

Tabel 1. Hasil pengujian beberapa hasil enkripsi

File	*Ukuran text*	*Hasil dekripsi*	*Perbandingan*
file_1.txt	1,000 B	1,000 B	Sesuai
file_2.txt	5,000 B	5,000 B	Sesuai
file_3.txt	25,000 B	25,000 B	Sesuai
file_4.txt	125,000 B	125,000 B	Sesuai
file_5.txt	625,000 B	625,000 B	Sesuai

4.3. Perbandingan Ukuran File.

Pada penelitian ini, mode operasi yang di gunakan untuk mengenkripsi pesan text pada algoritma enkripsi AES adalah mode operasi CFB yang merupakan mode operasi *stream cipher*, sehingga hasil dari pesan text yang telah di enkripsi (*cipher-text*) tidak boleh lebih besar daripada pesan text aslinya. Berikut ini akan diberikan tabel pengujian terhadap beberapa hasil enkripsi dari beberapa pesan text.

File	*Ukuran pesan text*	*Hasil enkripsi*	*Perbedaan ukuran file*
File_1.txt	1,000 B	988 B	12 B
File_2.txt	5,000 B	4,940 B	60 B
File_3.txt	25,000 B	24,700 B	300 B
File_4.txt	125,000 B	123,500 B	1,500 B
File_5.txt	625,000 B	617,500 B	7,500 B

Data percobaan diatas: pesan text yang pertama berisi 12 pergantian baris dari suatu deretan karakter dalam 1 baris atau biasa disebut dengan baris baru untuk suatu deretan karakter. Pada percobaan ini, pesan text kedua, ketiga, keempat dan kelima mempunyai isi yang sama dengan pesan text pertama. Pesan text yang kedua merupakan 5 kali perulangan dari isi pesan text pertama, pesan text ketiga merupakan 5 kali perulangan dari pesan text kedua, pesan text keempat merupakan 5 kali perulangan pesan text yang ketiga, begitu juga dengan pesan text yang kelima yang juga merupakan 5 kali perulangan dari pesan text yang keempat.

Dari hasil percobaan diatas, dapat disimpulkan bahwa pada hasil enkripsi pesan text tidak lebih besar dari dari ukuran pesan text aslinya, bahkan lebih kecil karena pada hasil enkripsi pesan text, bit yang merepresentasikan baris baru tidak di ikut sertakan pada hasil enkripsi yang di decode dengan menggunakan pada mode operasi CFB.

4.3 Perbandingan Kecepatan Fungsi Aplikasi Terhadap Ukuran Pesan Text.

Hasil pengujian aplikasi pada bagian ini akan menghasilkan data-data pengujian pada fungsi enkripsi dan dekripsi. Pengujian dilakukan terhadap beberapa pesan text yaitu: (contoh ada di sower.pdf)

Keunggulan.

Keunggulan utama pada sistem IBE-BF adalah kesederhanaannya. Dengan menggunakan kunci publik yang mudah di ingat dan mudah untuk diketahui. Keunggulan IBE-BF secara rinci adalah sebagai berikut:

- Pengirim dapat mengenkripsi pesan ke penerima tanpa perlu adanya sertifikat karena kunci publik nya berupa identitas. Dengan demikian, IBE-BF telah menghilangkan kebutuhan akan sertifikat, sehingga IBE-BF

telah menghilangkan kompleksitas pada sistem PKI yang berhubungan dengan sertifikat.

- Pada saat pengirim akan mengenkripsi suatu pesan yang ditujukan kepada penerima, pengirim tetap dapat mengenkripsi pesan berdasarkan parameter sistem walaupun penerima belum pernah berhubungan dengan PKG karena penghasilan kunci privat untuk mendekripsi pesan tersebut hanya pada saat proses *extract*, dan hal ini tidak harus dilakukan pada saat yang sama dengan pengenkripsian.
- Kunci publik yang digunakan adalah sesuatu yang unik, dalam sistem IBE-BF ini yang digunakan adalah alamat email sehingga tidak dibutuhkan manajemen kunci.

Kelemahan.

Jika kunci privat di ketahui oleh seseorang yang tidak berkepentingan, maka orang tersebut dapat mendekripsi semua pesan yang telah di enkripsi dengan menggunakan kunci publik dari kunci privat yang di ketahui tersebut. Hal ini dapat diatasi dengan cara membuat tanggal kadaluarsa dari kunci privat tersebut. Pembuatan tanggal kadaluarsa ini akan mempengaruhi kinerja dari PKG. Sebagai contoh, jika pada kunci privat di masukkan tahun berlaku kunci privat tersebut, maka user akan membutuhkan kunci privat yang baru jika tahun pada kunci privat tersebut telah kadaluarsa. Semakin pendek jangka kadaluarsa dari kunci privat, maka akan semakin sering proses penghasilan kunci privat yang baru dilakukan sehingga akan semakin membebani PKG.

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Beberapa kesimpulan yang dapat diambil adalah sebagai berikut:

1. Metode *Identity-Based Encryption Boneh-Franklin* dapat dijadikan alternatif pada sistem kriptografi *asymetric*.
2. Besar file hasil enkripsi memiliki ukuran yang sama dengan file aslinya, beberapa lebih kecil.
3. Pengelolaan sistem kunci publik dengan IBE-BF lebih mudah diaplikasikan.

5.2 Saran

Beberapa saran untuk pengembangan sistem selanjutnya adalah sebagai berikut:

1. Sistem enkripsi IBE-BF masih memiliki kelemahan karena memungkinkan penyadapan informasi kunci publik.
2. Perlu dilakukan perbandingan dengan sistem enkripsi yang serupa.

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

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

[5] Evelyn, *Identity Based Encryption*, Departemen Teknik Elektro, Institut Teknologi Bandung, 2004.

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

[7] 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.

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

[9] 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.

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

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

[12] V. Miller, *Short program for function on curves*, Unpublished manuscript, 1986.