PERANCANGAN SISTEM KRIPTOGRAFI KURVA ELIPTIK PADA AUDIO DIGITAL TERKOMPRESI

Anita Ahmad Kasim[1]
[1]Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam
Universitas Tadulako, Email:nita.kasim@gmail.com

Abstrak

Penelitian ini bertujuan melakukan perancangan sisten kriptografi kurva eliptik pada data audio digital terkompresi sehingga diperoleh sebuah sistem kriptografi yang dapat melakukan proses enkripsi dan dekripsi berkas audio digital terkompresi. Data audio digital yang asli wav dan data audio terkompresi .mp3 akan dienkripsi menghasilkan berkas audio terenkripsi. Pengujian sistem dilakukan dengan memproses berkas pesan audio dalam sistem menggunakan parameter kurva eliptik. Parameter dan nilai field p akan diubah-ubah untuk mengetahui pengaruh sistem kriptografi kurva eliptik terhadap berkas audio terkompresi. Panjang berkas audio pun akan dibuat bervariasi, untuk melihat waktu yang dibutuhkan sistem untuk mengenkripsi berkas dengan panjang berkas yang berbeda-beda. Pengujian akan dilakukan terhadap 5 buah berkas terkompresi .mp3 yang berasal dari berkas .wav. Masing-masing berkas akan dienkripsi untuk melihat perubahan yang terjadi pada berkas ketika dienkripsi dalam sistem. Hasil yang diperoleh dalam penelitian ini aalah sebuah system yang mampu melakukan proses enkripsi dan dekripsi audio menggunakan proses kriptorafi kurva eliptik.

Kata Kunci: kriptografi, kurva elitik, audio digital terkompresi

I. Pendahuluan

Kompresi data dan sistem kriptografi memiliki peranan yang sangat penting untuk proses transmisi data dalam jaringan transmisi data publik melalui jaringan komputer. Menurut Sandoval dan Uribe (2005), kompresi dan kriptografi merupakan dua hal yang berlawanan, dimana proses kriptografi akan melakukan konversi data dari data yang dapat terbaca (*legible data*) menjadi data yang tak dapat terbaca (*illegible data*) melalui proses penyandian sedangkan proses kompresi melakukan pencarian bagian-bagian data yang ganda (redudansi) atau pola data yang dapat dihilangkan dengan tujuan untuk mengurangi ukuran data. Pemanfaatan proses kompresi dan sistem kriptografi secara benar akan bermanfaat untuk beberapa hal berikut:

a. Kompresi data sebelum dienkripsi akan mengurangi bagian data ganda (redudansi) yang dapat dieksploitasi oleh kriptanalisis.
b. Kompresi data dapat mempercepat proses enkripsi
c. Jika kompresi data ditransmisikan melalaui jaringan komputer maka penggunaan bandwidht akan berfungsi lebih baik.

Perkembangan penelitian dalam bidang kriptografi dan teknologi komputer membuat beberapa algoritma kunci asimetrik seperti RSA dan Diffe-Hellman menjadi tidak begitu aman.

Kemudian, melalui penelitian kriptografi berkembang sebuah kriptosistem kurva eliptik yang memiliki tingkat keamanan yang lebih tinggi. Untuk kepentingan keamanan audio digital diperlukan sebuah sistem yang dapat mengamankan data audio digital.

Untuk menemukan sebuah sistem kriptografi yang dapat mengamankan pesan dengan berkas audio maka perlu dilakukan sebuah penelitian mengenai implementasi kriptosistem kurva eliptik. Penelitian ini akan fokus pada proses enkripsi dan dekripsi kompresi data audio digital.

II. Tinjauan Pustaka

Penelitian mengenai sistem kriptografi pada audio dan beberapa implementasi kriptosistem kurva eliptik yang pernah dilakukan sebelumnya dilakukan oleh Wahid (2003), melakukan Impelementasi *audio security* menggunakan Algortiam *Data Encryption Standar* (*DES*). Proses enkripsi dan dekripsi pada audio dengan algoritma DES dimana data pesan di bagi menjadi dua blok pesan yang diproses dengan cara pertukaran blok pesan. Banyaknya jumlah pertukaran blok pesan menjadi *ciphertext*nya menjadikan kriptosistem ini sulit untuk dikriptanalisis.

Huang, dkk (2008), melakukan penelitian mengenai desain dan implementasi steganografi audio. Sistem ini membentuk sebuah model desain untuk bit-bit audio yang akan di enkripsi dalam skema steganografi. Teknik steganografi yang digunakan adalah *multi bit embedding process*.

Shen dan Zheng (2008), melaksanan penelitian tentang implementasi kurva eliptik dalam e-commerce. Dengan adanya perkembangan penelitian dalam bidang kriptografi yang cepat, kriptosistem kurva eliptik menjadi tren kriptografi publik di masa depan. Penelitian ini menggunakan *tools* berorientasi objek dengan membagi kriptosistem kurva eliptik menjadi beberapa layer yang setiap layernya akan berhubungan dengan *class-class* dalam sistem *e-commerce*. Kesimpulan yang diperoleh dalam penelitian ini adalah penggunaan kriptosistem kurva eliptik memberi keuntungan dalam hal kemudahan untuk pengembangan sistem *e-commerce* .

Sung, dkk (2007), melakukan penelitian implementasi kriptosistem kurva eliptik pada dokumen XML. Penelitian ini menggambarkan teknik kriptosistem kurva eliptik untuk menyandikan sebagian data yang dirahasiakan dalam dokumen XML. Hal ini akan menjamin keamanan sebuah data dokumen XML.

Mekanisme pertukaran kunci yang digunakan dalam penelitian ini adalah algoritma Diffie Hellman. Algoritma Diffie Hellman adalah sebuah metode untuk melakukan pertukaran kunci antar dua orang yang saling bertukar pesan rahasia. Algortima Diffie Hellman juga merupakan algortima untuk encoding dan decoding melalui pemrosesan kunci privat dan kunci publik.

III. Landasan Teori

Dalam proses enkripsi, pertama-tama dilakukan pembacaan suatu berkas kunci publik yang berisi kurva eliptik E. Suatu *titik* P yang berada pada E, suatu bilangan prima p $\in Z_p$, dan kunci publik pemakai lain Q =d*P. Kemudian dipilih suatu bilangan random k $\in${2,…,p-1} dihitung k*Q dan k*P, selanjutnya berkas data dibaca secara per blok (M) dan dienkripsi dengan cara : (Műller dan Paulus, 1998)

$$M' = [M \oplus X(k*d*P)] \quad (3.1)$$

Keterangan :

M = data yang akan dienkripsi

M' = blok data yang telah dienkripsi

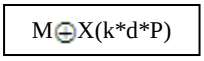
k = suatu bilangan random yang akan digunakan sebagai *kunci rahasia enkripsi* dengan k □ {2,…,p-1}

d = kunci publik dekripsi

P = suatu titik pada kurva $E_p(a,b)$

X(k*Q) = koordinat X untuk titik yang dihasilkan dari perkalian k*Q.

M di-xor-kan dengan absis titik yaitu k*Q, hasilnya berupa string yang lalu ditulis ke berkas. Hasil akhirnya secara sederhana dapat digambarkan pada Gambar 3.1.



M’

Gambar 3.1: Gambar Blok data yang telah dienkripsi

Keterangan :

k : *kunci rahasia enkripsi*

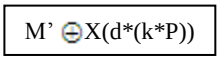
M’ : Data terenkripsi.

M : Data yang belum terenkripsi.

Proses ini akan terus dilakukan selama data yang dibaca masih ada. Dalam proses dekripsi, pertama-tama dilakukan pembacaan suatu berkas kunci publik yang berisi kurva eliptik E, suatu titik P yang berada pada E dan suatu lapangan bilangan prima p. Kemudian dibaca *ciphertext* seperti pada Gambar.3.9. Lalu dihitung d*(k*P), dengan d adalah kunci rahasia yang dimasukkan oleh pemakai dan k*P berasal dari ciphertext. Satu buah blok data lalu dibaca (M’). Setelah itu dilakukan proses dekripsi untuk memperoleh M, dengan cara sebagai berikut:

$$M = [M' \oplus X(d*(k*P))] \quad (3.2)$$

M’ di-xor-kan dengan absis titik yaitu d*(k*P) sehingga diperoleh suatu string. Hasilnya (M) lalu ditulis ke berkas. Hasil akhirnya secara sederhana dapat digambarkan pada Gambar 3.2.



M

Gambar 3.2:. Blok data yang telah didekripsi

Keterangan :

M’ : Data terenkripsi.

M : Blok data yang telah didekripsi

IV. Metodologi

Metode penelitian yang digunakan dalam mengimplementasi kriptosistem ini adalah sebagai berikut:

a. Studi Pustaka

Studi pustaka dilakukan untuk mengumpulkan data pustaka yang berhubungan dengan beberapa materi seperti skema kriptosistem kurva eliptik, teori mengenai proses enkripsi dan deksripsi dalam kriptosistem kurva eliptik serta teori mengenai teori kompresi data audio digital.

b. Analisa Sistem Dan Perancangan Sistem

Dalam analisa sistem dan perancangan sistem akan dilakukan pembahasan mengenai proses alur sistem yang di implementasikan dalam bentuk *Context Diagram* dan *Data Flow Diagram* (DFD) dalam beberapa level.

c. Implementasi Sistem

Implementasi sistem akan membahas mengenai gambaran sistem secara keselurahan meliputi pemrograman tiap modul yang ada dalam sistem.

d. Pengujian Sistem

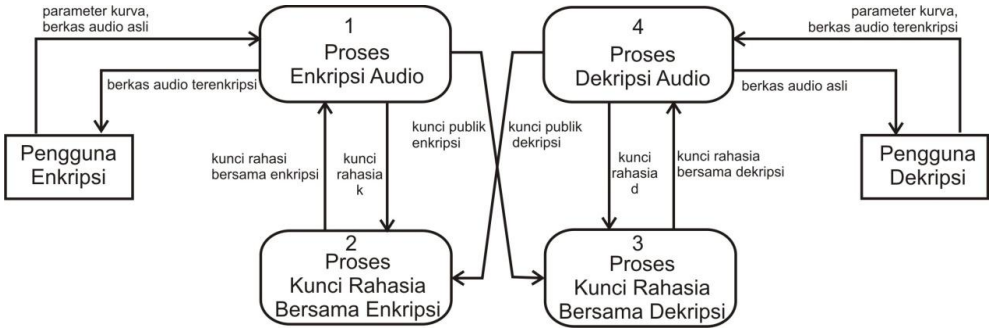
Pengujian sistem dilakukan guna mengetahui keakuratan sistem terhadap algoritma yang digunakan, sehingga bebas dari kesalahan baik secara logika dan secara sintaks programnya. Selanjutnya pengujian unjuk kerja sistem kriptografi terhadap keamanan pesan yang di enkripsi dan di dekripsi.

V. Perancangan Sistem

Proses aliran data dalam sistem audio audio kurva eliptik melibatkan sistem dengan pengguna sebagaimana yang digambarkan dalam diagram konteks sistem audio audio kurva eliptik pada gambar 5.1.

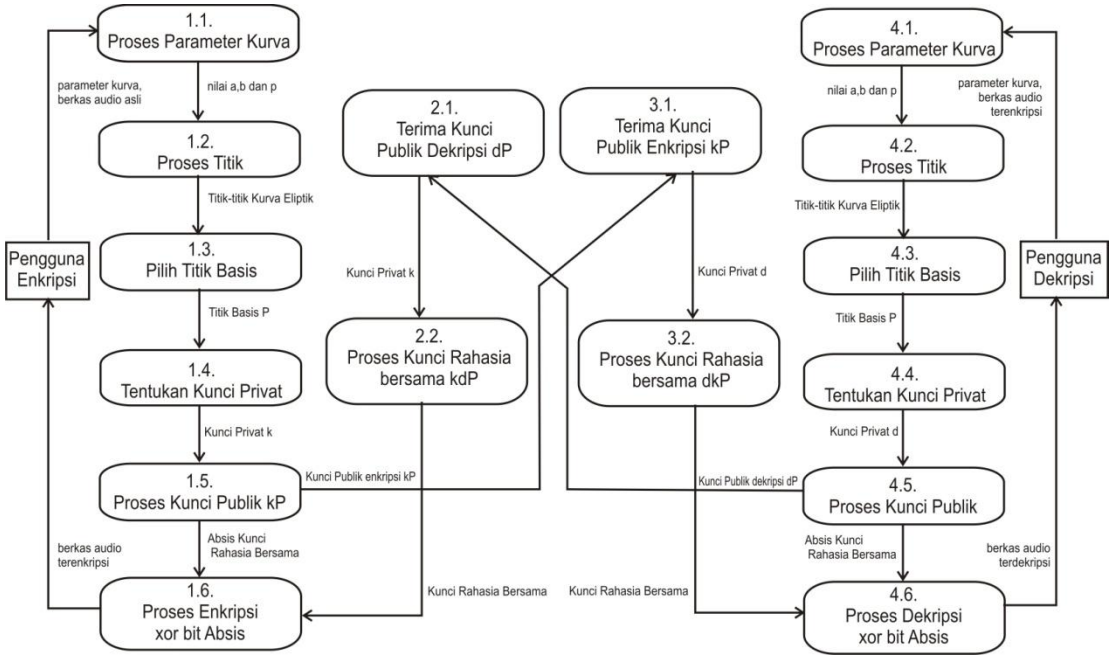
Gambar 5.1: Diagram Konteks Sistem Kriptografi Audio Terkompresi Kurva Eliptik

Proses aliran data pada level 1 ada empat proses yang akan dilakukan sistem yaitu proses enkripsi, proses dekripsi, proses kunci rahasia bersama . Kedua proses ini digambarkan pada gambar 5.2.



Gambar 5.2 : DFD Level 1 Sistem Kriptografi Audio Terkompresi Kurva Eliptik

Dalam proses enkripsi audio terdapat beberapa proses yang termasuk dalam DFD Level 2. Proses enkripsi audio meliputi proses enkripsi dan proses berkas hasil enkripsi ke berkas hasil. Aliran data pada level 2 digambarkan pada Gambar 5.3.



Gambar 5.3 : DFD Level 2 Sistem Kriptografi Audio Terkompresi Kurva Eliptik

Sistem ini memungkinkan pengguna melakukan enkripsi dan dekripsi terhadap berkas audio. Proses titik akan menghasilkan titik-titik yang akan digunakan pada proses enkripsi dan dejripsi. Proses dekripsi ini akan mengembalikan nilai-nilai audio ke nilai audio semula sehingga berkas audio akan kembali ke berkas yang asli.

Dalam proses Enkripsi dan dekripsi audio terdapat beberapa proses yang meliputi pemrosesan kunci privat dan publik serta proses enkripsi yang melibatkan titik pada kurva eliptik dan data nilai dari audio yang akan dienkripsi.

Proses dekripsi audio melakukan proses pengambilan titik dari hasil enkripsi dan memproses dekripsinya untuk mengembalikan nilai biner audio ke nilai data aslinya sehingga data audio kembali ke berkas aslinya.

VI. Hasil

Implementasi sistem dalam penelitian ini menghasilkan sebuah Sistem Kriptografi Audio Digital Terkompresi Kurva Eliptik. Sistem ini mampu melakukan proses enkripsi dan dekripsi terhadap data digital audio terkompresi. Data audio terkompresi .mp3 akan dienkripsi menghasilkan berkas audio terenkripsi. Pengujian sistem dilakukan dengan memproses berkas pesan audio dalam sistem menggunakan parameter kurva eliptik. Parameter dan nilai field p akan diubah-ubah untuk mengetahui pengaruh sistem kriptografi kurva eliptik terhadap berkas audio terkompresi. Panjang

berkas audio pun akan dibuat bervariasi, untuk melihat waktu yang dibutuhkan sistem untuk mengenkripsi berkas dengan panjang berkas yang berbeda-beda.

VII. Kesimpulan

Kesimpulan yang diperoleh dalam penelitian perancangan sistem kriptografi kurva eliptik terhadap data audio digital terkompresi menghasilkan sebuah sistem kriptografi yang mampu melakukan enkripsi dan dekripsi kurva eliptik dengan kemampuan memproses parameter kurva, memproses titik-titik pada kurva eliptik, memproses kunci publik serta memproses proses enkripsi dan dekripsi. Kemampuan yang dimiliki sistem mampu menghasilkan berkas audio terenkripsi yang tidak jelas terdengar tetapi dengan ukuran dan aktu audio yang mengalami perubahan. Proses dekripis dalam sistem dapat mengembalikan berkas audio ke dalam bentuk audio asli yang dapat terdengar bunyi pesan aslinya.

VIII. Daftar Pustaka

Huang, X., Kawashima, R., Segawa N., dan Abe, Y., 2008, *Design and implementation of synchronized audio-to-audio steganography scheme*, IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Iwate Prefectural University, Tokyo, Japan

Muller, V., dan Paulus, S., 1998, *Elliptische Kurven Und Public Key Kryptographie*, Technische Universitat Darmstadt, Fachbereich Informatik, Darmstadt.

Sandoval, MM., dan Uribe, CF., 2007, *A Hardware Architecture for Elliptic Curve Cryptography and Lossless Data Compression*, Proceedings of the 15th International Conference on Electronics, Communications and Computers (CONIELECOMP 2005), National Institute for Astrophysics, Optics and Electronics Computer Science Department, Mexico

Shen, G., dan Zheng, X., 2008, *Research on Implementation of Elliptic Curve Cryptosystem in E-Commerce*, IEEE International Symposium on Electronic Commerce and Security, University of Science and Technology, Beijing, China

Sung, KS., Ko, H., dan Seok Oh, H., 2007., *XML Document Encrypt Implementation using Elliptic Curve Cryptosystem*, IEEE International Conference on Convergence Information Technology, School of Engineering, Dept of Computer Science, Kyungwon University

Wahid, A., 2003, *Impelementasi audio security menggunakan Algoritma Data Encryption Standart (DES)*, Tesis S2 Ilmu Komputer Universitas Gadjah Mada, Jogjakarta