IMPLEMENTASI KRIPTOSISTEM KURVA ELIPTIK DENGAN PERTUKARAN KUNCI DIFFIE-HELLMAN PADA DATA AUDIO DIGITAL

Anita Ahmad Kasim
Jurusan Matematika FMIPA UNTAD Kampus BumiTadulakoTondo Palu

Abstract

Technology not only allows information submitted in the form of text, but also in the form of images, audio or video. However, the use of digital audio data is not necessarily improves the security of the message. Various attack techniques emerged so others can know the confidential information contained in digital audio messages. One attempt to provide information that can be done is a cryptographic system or cryptosystem. In the elliptic curve equation are the values that can be used as a private key and public key to encrypt the data in this form of audio. Audio data will be processed on the secure encryption and decryption using elliptic curve cryptography with Diffie-Hellman key exchange. Parameters and variables contained in the curve equation would be calculated to determine the shared secret key to be used in both encryption and decryption process audio. The conditions before the encrypted audio data are audible. The result of encrypting the audio data to produce a new audio is not clear. Decryption process causes the data back to the original audio data so that the second audio data can be heard clearly. Attack man in the middle of this process can't decrypt the encrypted audio file. File decryption results may not be tuned so that the audio file will be secure and can only be heard by the user encryption and decryption that really has the right combination of keys that user actual encryption and decryption.

Keywords: Elliptical Curve Cryptosystem, encrypt, decrypt, Diffie-Hellman, digital audio.

I. Pendahuluan

Kemajuan teknologi memungkinkan informasi tidak hanya disampaikan dalam bentuk teks, tetapi juga dalam bentuk gambar, audio maupun video. Hampir seluruh data kini dikelola dalam bentuk data digital, termasuk audio yang dikenal dengan audio digital. Akan tetapi, penggunaan data audio digital belum tentu meningkatkan keamanan pesan tersebut. Berbagai teknik penyerangan muncul sehingga pihak yang tidak bertanggungjawab dapat mengetahui informasi rahasia yang terkandung dalam pesan audio digital. Salah satu upaya pengamanan informasi yang dapat dilakukan adalah sistem kriptografi atau kriptosistem.

Kriptografi merupakan ilmu untuk menyamarkan suatu pesan demi menjaga kerahasiaannya. Suatu pesan (*plain text*) harus melalui proses enkripsi terlebih dulu menjadi bentuk yang tidak berarti (*cipher text*) sebelum dikirimkan ke penerima yang berhak. Hanya pihak yang berhak yang dapat melakukan proses dekripsi, yaitu mengubah kembali *cipher text* menjadi *plain text* memakai suatu kunci yang rahasia. Kriptografi menganut prinsip kerahasiaan melalui ketidakjelasan (*secrecy through obscurity*).

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 sistem kriptografi kurva eliptik yang memiliki tingkat keamanan yang lebih tinggi. Untuk kepentingan keamanan audio digital diperlukan sebuah sistem yang dapat mengamankan data audio digital.

II. Landasan Teori

II.1 Kriptografi

Kriptografi (*cryptography*) berasal dari bahasa Yunani *cryptós* yang berarti rahasia dan *gráphein* yang berarti tulisan. Secara harfiah, kriptografi dapat diartikan sebagai tulisan yang dirahasiakan. Tujuannya adalah supaya tulisan tersebut tidak dapat diartikan oleh setiap orang. Tulisan yang dirahasiakan hanya orang-orang tertentu yang dapat mengartikan yaitu jika orang tersebut mengetahui cara menyembunyikan tulisan.

Menurut Schneier (1996) kriptografi adalah ilmu yang mempelajari bagaimana membuat suatu pesan yang dikirim dapat disampaikan kepada penerima dengan aman. Pesan asli yang dimengerti isinya/maknanya ini dinamakan *plaintext*. Pesan yang tidak dimengerti, yang merupakan hasil transformasi dari *plaintext*, disebut *ciphertext*. Stalling (1999) menyatakan bahwa suatu sistem kriptografi dapat diklasifikasikan kedalam 3 (tiga) dimensi yang independen, yaitu :

a. Operasi yang digunakan untuk mentransformasikan *plaintext* ke *cipertext*.
b. Kunci yang digunakan.
c. Cara pemrosesan *plaintext*.

Plaintext biasa disimbolkan sebagai M (*Message*) atau P (*Plaintext*), yang dapat berupa suatu aliran bit, berkas teks, berkas bitmap, berkas suara digital atau berkas video digital. M adalah data biner, sedangkan *ciphertext* biasanya disimbolkan sebagai C (*Ciphertext*), dan juga merupakan data biner (Schneier,1996).

Schneier (1996), jika enkripsi disimbolkan sebagai fungsi E (*Encryption*) dan dekripsi disimbolkan sebagai fungsi D (*Decryption*), maka dengan menggunakan notasi matematika, enkripsi dan dekripsi dapat ditulis pada persamaan 2.1 dan 2.2.

$$E(M) = C \qquad (2.1)$$

$$D(C) = M \qquad (2.2)$$

Proses enkripsi dan dekripsi pada *plaintext* dan *ciphertext* dapat dilihat pada Gambar 2.1.

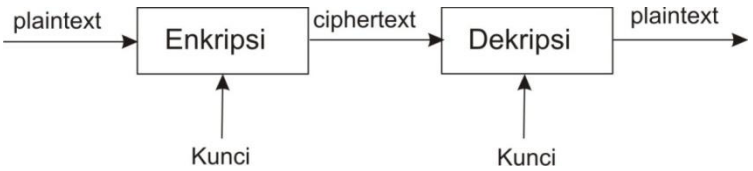
Gambar 2.1. : Proses Enkripsi dan Dekripsi

II.2 Algoritma dan Kunci

Kriptografi menggunakan kunci (*key*) untuk melakukan proses enkripsi dan dekripsi. Kunci (disimbolkan sebagai K) pada kriptografi berupa satu nilai dari sejumlah bilangan yang banyak jumlahnya. Dengan adanya penggunaan kunci, maka notasi matematika untuk fungsi enkripsi dan dekripsi dapat ditulis pada persmaan 2.3 dan 2.4. (Schneier, 1996)

$$E_K(M) = C \quad (2.3)$$

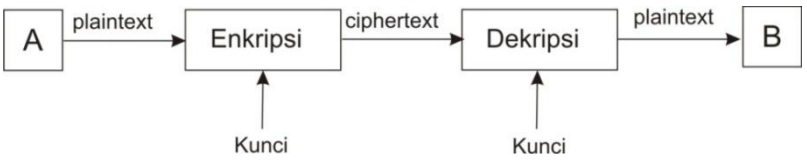
$$D_K(C) = M \quad (2.4)$$



Gambar 2.2: Enkripsi dan Dekripsi dengan Kunci

II.3 Kriptogarfi Kunci Simetrik (Algoritma Kunci Rahasia)

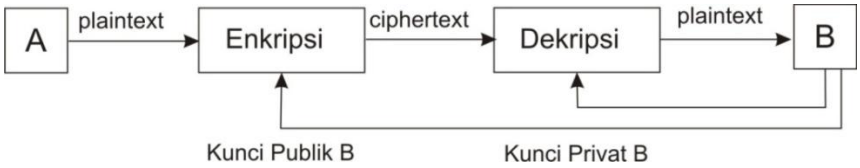
Kriptografi Kunci Simetrik adalah metode kriptografi dengan penggunaan kunci untuk membuat pesan yang disandikan sama dengan kunci yang dipakai untuk membuka pesan yang disandikan. Jadi pihak pengirim pesan dan pihak penerima pesan memiliki kunci yang sama. Kunci enkripsi sama dengan kunci dekripsi. (Schneier, 1996). Proses enkripsi dan dekripsi dengan kunci simetrik dapat dilihat pada gambar 2.3.



Gambar 2.3. : Proses enkripsi dan dekripsi dengan kunci simetrik

II.4 Kriptografi Kunci Asimetri (Kriptografi Kunci Publik)

Kriptografi Kunci Asimetrik adalah metode kriptografi dengan penggunaan kunci untuk membuat pesan yang disandikan berbeda dengan kunci yang dipakai untuk membuka pesan yang disandikan. Jadi pihak pengirim pesan dan pihak penerima pesan memiliki kunci yang berbeda. Kunci enkripsi tidak sama dengan kunci dekripsi. Kunci Asimetrik sering juga disebut kunci publik. Kriptografi kunci-publik menggunakan sepasang kunci, satu kunci untuk enkripsi dan satu kunci untuk dekripsi. Kunci untuk enkripsi bersifat publik (tidak rahasia) sehingga dinamakan kunci publik (*public key*), sedangkan kunci dekripsi bersifat rahasia sehingga dinamakan kunci rahasia (*private key* atau *secret key*). Gambaran Asimetrik dapat dilihat seperti gambar 2.4.



Gambar 2.4.:Proses enkripsi dan dekripsi dengan kunci asimetrik

II.5 Sistem Kriptografi Kurva Eliptik (*Elliptic Curves Cryptosystem*)

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

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

Salah satu sistem kriptografi kunci publik yang aman dan efisien berdasarkan permasalahan matematis, yaitu sistem kripto Kurva Eliptik (*Elliptic Curves Cryptosystem*). Pada sistem ini digunakan masalah logaritma diskrit kurva eliptik dengan menggunakan grup kurva eliptik. Struktur kurva eliptik digunakan sebagai grup operasi matematis untuk melangsungkan proses enkripsi dan deskripsi. Cara ini menyebabkan kesulitan menghitung k jika diketahui Q dan P dimana $Q = k\,P$. Sebelum memahami mengenai kurva eliptik diperlukan pemahaman mengenai beberapa konsep dasar matematika seperti aritmatika modular, kekongruenan dan lapangan berhingga.

II.6 Pertukaran Kunci Diffie Hellman pada Kriptosistem Kurva Eliptik

Implementasi sistem kripto kurva eliptik untuk protokol pertukaran kunci dapat dilakukan dengan menggunakan tahapan pada Diffie-Helman dengan mengubah parameter yang disesuaikan dengan persamaan kurva elips.

Misal diberikan kurva $E : y^2 = x^3 + 2x + 1$ dengan bilangan prima yang dipilih p=5, maka himpunan titik-titik pada kurva $E(Z_5)$ = {**(0,1), (1,3), (3,3), (3,2), (1,2), (0,4)**} yang berturut-turut diberi notasi P_1, P_2, P_3, P_4, P_5, P_6

1. **Alice** memilih kunci rahasia ***a***, misalkan ***a*** = 2 dan menghitung kunci publiknya yaitu :

   $P_{Alice} = a\,P_1 = 2\,P_1 = P_1 + P_1 = P_2 = (1,3)$

   Hasil kunci publik ini dikirm ke **Bob**

2. **Bob** memilih kunci rahasia ***b***, misalkan ***b*** = 3 dan menghitung kunci publiknya yaitu :

   $P_{Bob} = a\,P_1 = 3\,P_1 = P_1 + P_1 + P_1 = P_3 = (3,3)$

   Hasil kunci publik ini dikirm ke **Alice**

3. **Alice** dan **Bob** secara terpisah menghitung dari kunci publik yang diterima untuk menghasilkan kunci rahasia yang sama, yaitu :

   Alice : $S_{Alice\_Bob} = a\,P_{Bob} = 2\,P_3 = P_6 = (0,4)$

   Bob : $S_{Alice\_Bob} = a\,P_{Alice} = 3\,P_2 = P_6 = (0,4)$

II.7 Enkripsi dan Dekripsi Kriptografi Kurva Eliptik

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 Z_p, dan kunci publik pemakai lain Q =d*P. Kemudian dipilih suatu bilangan random k {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)

$$M' = [M \; . \; X(k*d*P)] \qquad (2.5)$$

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.

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,* lalu dihitung d*(k*P), dengan d adalah kunci rahasia yang dimasukkan oleh pemakai selanjutnya k*P berasal dari ciphertext. Satu buah blok data lalu dibaca (M'). Setelah itu dilakukan proses dekripsi untuk memperoleh M, dengan cara sebagai berikut:

$$M = [M' \; . \; X(d*(k*P))] \qquad (2.6)$$

Proses ini akan terus dilakukan selama data terenkripsi yang dibaca masih ada.

II.8 Gambaran Umum Sistem

Sistem kriptografi audio dengan kurva eliptik ini merupakan sebuah sistem yang mengimplementasikan elemen kurva eliptik dalam proses enkripsi dan proses dekripsi. Pada persamaan kurva eliptik terdapat nilai-nilai yang dapat digunakan sebagai kunci privat dan kunci publik untuk menyandikan sebuah data dalam hal ini berbentuk audio.

Data audio yang akan diamankan diproses pada proses enkripsi dan dekripsi menggunakan kriptografi kurva eliptik. Parameter dan variabel yang terdapat dalam persamaan kurva akan dihitung untuk menentukan kunci rahasia bersama yang akan digunakan pada kedua proses baik enkripsi maupun dekripsi audio.

III. Hasil Penelitian

Penggunaan parameter yang benar memungkinkan pengguna enkripsi dan dekripsi menghasilkan sebuah berkas yang terenkripsi yang dapat didengarkan kembali dengan proses

dekripsi. Dalam penelitian ini ukuran berkas dan waktu audio yang menjadi masukan dalam proses ini tidak berubah ketika berkas telah selesai dienkripsi.

Masukan parameter dan proses kunci yang benar dalam sistem ini menghasilkan proses enkripsi dan dekripsi audio berjalan dengan baik. Proses enkripsi akan menghasilkan berkas audio yang terenkripsi yang tidak dimungkinkan untuk didengarkan oleh orang-orang yang tidak berhak. Kondisi audio yang terenkripsi ketika didekpripsi dengan kunci privat dan proses kunci publik yang benar akan memungkinkan audio yang tidak bisa didengarkan dapat kembali ke audio semula. Kondisi audio sebelum dan sesudah proses enkripsi maupun dekripsi adalah:

- Sebelum dienkripsi: Audio terdengar jelas baik dalam format.
- Setelah dienkripsi: Audio terenkripsi sehingga tidak jelas terdengar dalam format mp3 suara terdengar gangguan noise yang mengganggu audio.
- Setelah didekripsi: Audio kembali terdengar jelas baik dalam format mp3.

Serangan yang akan muncul dalam sistem ini jika dalam proses kriptografi terdapat *man in the middle* dimana seseorang mengetahui salah satu kunci misalnya kunci publik. Maka dalam sistem ini tidak dapat melakukan dekripsi terhadap berkas audio yang dienkripsi. Berkas hasil dekripsi tetap tidak dapat didengarkan sehingga berkas audio akan aman dan hanya bias didengarkan oleh pengguna enkripsi maupun dekripsi yang benar-benar memiliki kombinasi kunci yang tepat yaitu pengguna enkripsi dan dekripsi yang sebenarnya.

IV. Kesimpulan dan Saran

IV.1 Kesimpulan

Kesimpulan yang diperoleh dalam penelitian implementasi sistem kriptografi kurva eliptik terhadap data audio digital terkompresi sebagai berikut:

1. Keadaan data audio .mp3 sebelum dienkripsi terdengar jelas. Hasil enkripsi pada data audio .mp3 dengan mengenkripsi header diawal blok data menghasilkan sebuah audio baru yang tidak terdengar .
2. Hasil enkripsi pada data audio .mp3 tanpa mengenkripsi header diawal blok data menghasilkan sebuah audio baru yang tidak jelas terdengar .
3. Proses dekripsi menyebabkan data kembali ke data audio semula sehingga data audio dapat terdengar dengan jelas.
4. Ukuran data dan waktu audio tidak mengalami perubahan dalam proses enkripsi maupun dekripsi.
5. Serangan *man in the middle* dalam proses ini tidak dapat melakukan dekripsi terhadap berkas audio yang dienkripsi. Berkas hasil dekripsi tetap tidak dapat didengarkan sehingga berkas audio akan aman dan hanya bias didengarkan oleh pengguna enkripsi maupun dekripsi yang benar-benar memiliki kombinasi kunci yang tepat yaitu pengguna enkripsi dan dekripsi yang sebenarnya.

IV.2 Saran

Saran dalam penelitian selanjutnya diharapakan dapat melakukan hal-hal sebagai berikut:

1. Penelitian untuk membahas lebih detail teknik kompresi audio sehingga dimungkinkan untuk membuat media player audio terenkripsi yang dapat membaca berkas audio terkompresi yang terenkripsi dengan lebih baik.
2. Penelitian ini belum dapat menampilkan error secara kuantitatif sehubungan dengan perhitungan signal audio. Perhitungan signal audio sebelum dan sesudah enkripsi dapat memperlihatkan adanya perubahan data audio secara lebih detail.
3. Ukuran berkas audio terkompresi yang relatif kecil memungkinkan penelitian lanjutan untuk mengimplementasikan kriptografi kurva elitik pada audio pada telepon selular.

V. Daftar Pustaka

1. Huang, X., Kawashima, R., Segawa N., 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
2. Lu,G.,1999, *Multimedia Database Management System*, Artech House, Boston, London
3. Muller, V., dan Paulus, S., 1998, *Elliptische Kurven Und Public Key Kryptographie*, Technische Universitat Darmstadt, Fachbereich Informatik, Darmstadt.
4. Shen, G., 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
5. 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
6. Schneier, B., 1996, *Applied Cryptography Protocols, Algorithm and Source code in C*, Second Edition, Willey Computer Publishing, John Willey & Sons, inc.
7. Shoup,V., 2008, *A Computational Introduction to Number Theory and Algebra*, Version 2, Cambridge University Press.
8. Stalling, W., 1999, *Cryptography and Network Security, Principal and Practice*, Second Edition, Prentice Hall, New Jersey
9. 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
10. Wahid, A., 2003, *Impelementasi audio security menggunakan Algoritma Data Encryption Standart (DES)*, Tesis S2 Ilmu Komputer Universitas Gadjah Mada, Jogjakarta

11. Zhang, Y., Cui, T., dan Tang, H., 2008, *A new secure e-mail scheme based on Elliptic Curve Cryptography Combined Public Key*, IFIP International Conference on Network and Parallel Computing, College of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing, China