BAB 1

PENDAHULUAN

1.1 Latar Belakang

Seiring dengan perkembangan teknologi informasi secara tidak langsung dunia komunikasi juga ikut terpengaruh. Dengan adanya internet, komunikasi jarak jauh dapat dilakukan dengan cepat dan mudah. Akan tetapi internet tidak terlalu aman karena merupakan media komunikasi umum yang dapat digunakan oleh siapapun sehingga sangat rawan terjadi penyalahgunaan informasi oleh pihak-pihak yang tidak berhak mengetahui informasi tersebut. Oleh karena itu dibutuhkan sebuah metode yang dapat menjamin kerahasiaan dan keamanan data pada saat dikirimkan. Metode tersebut yaitu kriptografi. Kriptogafi adalah ilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas [1]. Kriptografi biasanya diimplementasikan untuk keperluan pengamanan data baik dalam bentuk teks (SMS), suara, gambar, maupun video. Berdasarkan kunci yang digunakan, kriptografi terbagi menjadi 2 jenis yaitu kriptografi simetri (kunci privat) dan kriptografi asimetri (kunci publik). Pada algoritma kriptografi simetris digunakan kunci yang sama untuk enkripsi dan dekripsi pesan. Karena yang digunakan adalah kunci yang sama, maka kunci yang digunakan oleh pengirim untuk enkripsi juga harus dikirimkan ke penerima untuk dekripsi pesan. Proses pertukaran kunci tersebut melewati jaringan yang tidak aman, maka diperlukan pengamanan untuk pertukaran kunci tersebut agar kunci tidak dapat diketahui oleh pihak – pihak yang tidak berhak.

Pada penelitian sebelumnya telah dilakukan penelitian mengenai algoritma ECDH [2] tetapi pada penelitian tersebut, terbatas hanya pada analisis perhitungan pembangkitan kunci bersama tidak diimplementasikan pada proses enkripsi dan dekripsi kunci serta tidak dilakukan pengujian performansi algoritma. Pada penelitian sebelumnya, juga telah diimplementasikan suatu sistem proses pertukaran kunci dengan menggunakan algoritma Diffie-Hellman [3] dan [4], hanya saja untuk tingkat kesulitan pemecahan kuncinya masih terbilang rendah.

Algoritma tersebut meningkatkan keamanan proses pertukaran kunci hanya saja menghasilkan ukuran kunci yang besar untuk sistem yang aman.

Oleh karena itu, penulis ingin mengimplementasikan pengenkripsian data suara dengan dilengkapi pengamanan proses pertukaran kunci dengan sistem kriptografi *elliptic curve* Diffie-Hellman untuk proses enkripsi dan dekripsi suara serta melakukan analisis mengenai performansi algoritma ECDH itu sendiri. Kriptografi kurva eliptik termasuk kedalam sistem kriptografi asimetris yang mendasarkan keamanannya pada permasalahan matematis kurva eliptik. 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 dekripsi. *Elliptic Curve Cryptography* (ECC) mempunyai keuntungan jika dibandingkan dengan kriptografi asimetris lainnya yaitu dalam hal ukuran panjang kunci yang lebih pendek tetapi memiliki tingkat keamanan yang sama. Sehingga kecepatannya lebih tinggi, konsumsi daya yang lebih rendah, adanya penghematan bandwith. Keuntungan keuntungan tersebut sangat berguna untuk aplikasi-aplikasi yang memiliki keterbatasan pada *bandwith*, kapasitas pemrosesan, ketersediaan sumber tenaga dan ruang.

Diffie-Hellman pertama kali memperkenalkan algoritma kunci publik pada tahun 1976 atas hasil kerja sama antara Whitfield Diffie dan Martin Hellman. Metode ini merupakan metode partikal pertama untuk menciptkan sebuah rahasia bersama antara dua belah pihak melalui sebuah jalur komunikasi yang tidak terjaga. Algoritma Diffie-Hellman ini memiliki keamanannya dari kesulitan menghitung algoritma diskrit dalam *finite field*, dibandingkan kemudahan dalam menghitung bentuk eksponensial dalam *finite field* yang sama. Algoritma ini dapat digunakan dalam mendistribusikan kunci publik yang dikenal dengan protocol pertukaran kunci.

Kriptografi kurva eliptik (*Elliptic Curve Cryptography*) menggunakan dua kunci yaitu kunci publik dan kunci privat. Kunci publik pada kriptografi adalah sebuah titik pada kurva eliptik dan kunci privatnya adalah sebuah angka random. Kunci publik diperoleh dengan melakukan operasi perkalian terhadap kunci privat dengan titik generator G pada kurva eliptik. Titik generator G digunakan untuk

melakukan pertukaran kunci DiffieHellman. Sehingga menjadi dasar untuk memilih pertukaran kunci Diffie-Hellman.

1.2 Rumusan Masalah

Untuk menjaga keutuhan data yang dikirimkan maka diperlukan sebuah sistem kriptografi. Namun karena sistem ini berjalan tidak selalu pada aplikasi yang memiliki *bandwidth*, kapasitas pemrosesan, ketersediaan sumber tenaga dan ruang yang besar, maka diperlukan sistem kriptografi dengan panjang kunci yang pendek tetapi tingkat kemanan yang tinggi. Ada beberapa masalah yang harus diselesaikan yaitu :

a. Bagaimana merancang dan mengimplementasikan suatu algoritma pertukaran kunci yang memiliki tingkat kesulitan pemecahan kunci yang tinggi dengan panjang kunci yang pendek?
b. Bagaimana performansi algoritma yang dirancang ?
c. Bagaimana pengaruh dari algoritma pertukaran kunci terhadap proses enkripsi suara dengan algoritma simetri?

1.3 Tujuan Penelitan

Tujuan dari pelaksanaan tugas akhir ini antara lain :

a. Merancang dan menganalisis proses pertukaran kunci publik Diffie-Hellman dengan proses enkripsi dan dekripsi kunci menggunakan kriptosistem kurva eliptik.
b. Mengetahui dan menganalisis kelebihan algoritma pertukaran kunci *Elliptic Curve* Diffie-Hellman dibanding algoritma Diffie-Hellman terkait dengan kesukaran pemecahan kunci dan waktu komputasi.
c. Menganalisis performansi algoritma *Elliptic Curve* Diffie-Hellman.
d. Menganalisis pengaruh penambahan algoritma pertukaran kunci *Elliptic Curve* Diffie-Hellman pada algoritma simetri AES untuk enkripsi dan dekripsi suara.

1.4 Batasan Masalah

Batasan masalah pada tugas akhir ini adalah :

a. Persamaan kurva eliptik yang digunakan dalam implementasi adalah kurva eliptik pada GF(p) (atau F_p) yaitu $y^2 = [x^3 + ax + b] \pmod p$.

b. Proses pertukaran kunci dilakukan oleh dua pihak dan diasumsikan kedua pihak memiliki sepasang kunci asimetri (*public key* dan *private key*).
c. Parameter performasi yang dihitung adalah waktu komputasi, koefisien korelasi, *avalanche effect*, tingkat kesukaran pemecahan kunci berdasarkan panjang kunci.
d. Proses pengamanan pertukaran kunci dilakukan untuk kunci enkripsi-dekripsi suara pada algoritma AES 128.

1.5 Metode Penelitian

Metode yang dilakukan di dalam pelaksanaan tugas akhir ini sebagai berikut :

1. Study literature

   Literatur dalam hal ini baik berupa buku, catatan, hasil penelitian, dan sumber-sumber elektronik di internet. Studi literatur ini ditujukan untuk mendapatkan referensi yang jelas dan tepat mengenai simulasi yang akan dibuat.

2. Tahap bimbingan

   Pada tahap ini dilakukan bimbingan dengan dosen pembimbing untuk memperbaiki kekurangan dan mendapatkan ide-ide baru untuk pelaksanaan tugas akhir ini.

3. Perancangan Sistem

   Merancang sistem yang akan dibuat, membuat diagram alir algoritma.

4. Realisasi Sistem

   Membuat sistem sesuai dengan perancangan yang telah dibuat sebelumnya.

5. Pengujian dan Analisis

   Pada tahap ini dilakukan pengujian pada sistem yang telah dibuat sesuai dengan perancangan kemudian dilakukan analisa terhadap hasil pengujian yang diperoleh.

1.6 Sistematika Penelitian

Pada pelaksanaan tugas akhir ini terdapat lima bab utama serta lampiran yang bertujuan untuk menunjang kelengkapan informasi pada pelakasanaan tugas akhir ini. Adapun lima bab utama pada tugas akhir ini adalah :

BAB I PENDAHULUAN

Pada Bab ini berisi uraian secara singkat mengenai latar belakang permasalahan, perumusan masalah, tujuan penelitian, pembatasan masalah penelitian, metodologi penelitian, sistematika penulisan, dan waktu pelaksanaan penelitian

BAB II DASAR TEORI

Bab ini berisi tentang teori dasar mengenai Kriptografi, Algoritma asimetrik, Kriptosistem kurva elips (*elliptic curves cryptosystem*), metode pertukaran kunci Diffie-Hellman, alogoritma simetri AES, parameter performansi serta teori dasar lain yang berkaitan dengn pelaksanaan tugas akhir ini.

BAB III PERANCANGAN SISTEM

Bab ini menjelaskan tentang perancangan sistem yang akan dibuat serta algoritma – algoritma kriptografi yang digunakan.

BAB IV PENGUJIAN SISTEM DAN ANALISIS HASIL

Bab ini menjelaskan beberapa hasil pengujian dan analisis dari simulasi yang telah dilakukan berdasarkan perancangan yang dilakukan.

BAB V PENUTUP

Bab ini berisi kesimpulan hasil simulasi dan analisis serta saran sebagai bentuk pengembangan perancangan yang lebih baik lagi