BAB I

PENDAHULUAN

1.1 Latar Belakang

Masyarakat membutuhkan teknologi informasi karena kemajuan teknologi saat ini semakin pesat. Dengan munculnya internet, setiap orang dapat bertukar informasi, tetapi ini juga membuka peluang bagi setiap orang untuk terlibat dalam banyak kejahatan cyber.

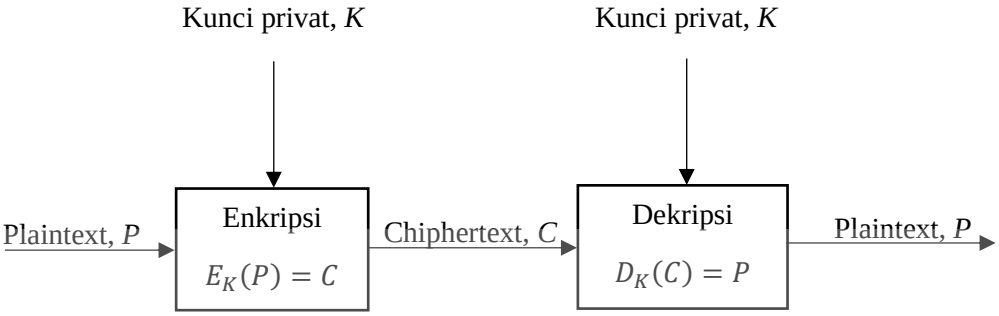
Keamanan data menjadi aspek yang sangat krusial. Setiap hari, jutaan informasi sensitif seperti data pribadi, transaksi keuangan, dan komunikasi rahasia dipertukarkan melalui jaringan internet. Kriptografi menjadi alat yang sangat penting untuk melindungi informasi ini dari akses yang tidak sah.

Kriptografi adalah bidang yang mempelajari teknik matematis yang berkaitan dengan aspek keamanan data seperti tingkat keyakinan, integritas, autentikasi entitas, dan autentikasi keaslian [1].

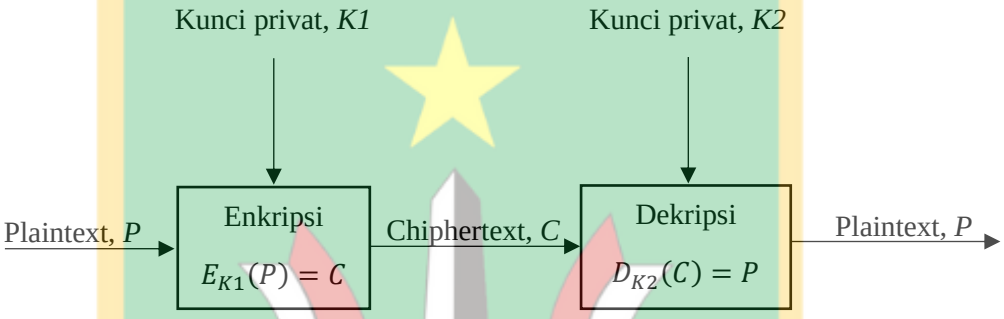
Dalam kriptografi, dua proses berbeda digunakan: enkripsi dan dekripsi. Tujuan utama enkripsi adalah untuk melindungi data digital yang disimpan di sistem komputer atau dikirim melalui internet atau jaringan komputer lainnya. Dekripsi adalah proses mengambil data atau teks yang dienkripsi dan mengubahnya kembali menjadi teks yang dapat dibaca dan dipahami oleh orang atau computer [2].

Gambar 1.1 Proses Enkripsi dan Dekripsi [3].

Algoritma kriptografi memerlukan kunci untuk melakukan enkripsi dan dekripsi. Algoritma kriptografi dikelompokan menjadi kelompok kunci simetri (*symmetric-key cryptography*) dan kelompok algoritma kriptografi kunci-nirsimetri (*asymmetric-key cryptography*) [4].



Gambar 1.2 Skema sistem kriptografi simetri, kunci enkripsi sama dengan kunci dekripsi [4].



Gambar 1.3 Dalam kriptografi nirsimetri, kunci enkripsi dan dekripsi berbeda. Kunci enkripsi bersifat publik, artinya tidak rahasia, sedangkan kunci dekripsi bersifat privat [4].

Jika persamaan matematis yang menjelaskan cara kerja algoritma kriptografi sangat kompleks sehingga tidak mungkin untuk dipecahkan secara analitik, algoritma kriptografi dianggap aman. Selain itu, waktu yang diperlukan untuk memecahkan chiperteks harus lebih lama daripada jumlah waktu yang diperlukan untuk menyimpan informasi tersebut [3]. Saat ini algoritma yang terkenal dengan tingkat keamanannya adalah RSA dan ECC. Penelitian tentang kedua algoritma ini sudah banyak dilakukan.

Menurut [5] tujuan dari setiap algoritma enkripsi dan dekripsi adalah untuk mempersulit serangan terhadap data sehingga transfer data dari pengirim ke penerima tidak terputus karena kita menjumpai banyak insiden yang melibatkan kejahatan dunia maya (kejahatan berorientasi komputer) yang menyerang data atau jaringan.

Sistem berdasarkan kurva ellips merupakan alternatif yang efektif terhadap sistem kriptografi RSA, karena melibatkan pendekatan matematika yang berbeda. Kriptografi kurva eliptik lebih disukai dalam penggunaan karena ini memerlukan ukuran kunci yang lebih kecil meskipun kompleksitas dalam matematika dibanding algoritma lainnya. Algoritma ECC lebih cepat dibanding RSA karena memerlukan lebih sedikit komputasi. ECC lebih menguntungkan dibanding RSA karena penggunaan memori yang rendah, konsumsi CPU yang rendah, dan ukuran kunci yang lebih pendek dibanding RSA [6][7][8][9].

Selanjutnya untuk keamanan ECC ini didasarkan pada masalah logaritma diskrit kurva eliptik, bukan masalah faktorisasi bilangan bulat. Semua karakteristik untuk memenuhi kebutuhan keamanan blokchain dipenuhi oleh ECC dibanding RSA. ECC adalah kriptografi yang menyediakan keamanan dan otentikasi data dengan bantuan komputasi serta kecepatan algoritma relatif baik. ECC keamanannya lebih besar dari RSA. ECC adalah sistem kriptografi kunci publik yang paling efisien, ini memberikan solusi keamanan tinggi yang tidak mempengaruhi kinerja. Saat ini, kurva ellips adalah satu-satunya metode yang memungkinkan peningkatan keamanan dengan ukuran kunci yang lebih kecil, yang mengurangi biaya pemrosesan. Dengan parameter yang lebih baik, ECC lebih efisien dalam hal operasional dan keamanan daripada RSA. Dibandingkan dengan sistem kriptografi kunci publik lain yang dikenal saat ini, skema kripto kurva elips menawarkan rasio keamanan per bit tertinggi [10][11][12][13][14][15][16][17].

Panjang kunci RSA yang lebih panjang menyebabkan algoritma yang paling tidak aman karena potensi serangan saluran samping. Pengoperasian di RSA relatif lebih cepat dibanding ECC tetapi dari segi keamanan ECC lebih kuat dibanding RSA. RSA cepat dalam enkripsi tetapi lambat dalam dekripsi, sedangkan ECC lambat dalam enkripsi tetapi cepat dalam dekripsi, secara keseluruhan ECC mengungguli RSA dalam hal kinerja dan keamanan [18][19][20].

Performa algoritma kriptografi sangat penting ketika digunakan dalam praktik. Waktu yang diperlukan untuk enkripsi dan dekripsi dapat berdampak pada efisiensi sistem secara keseluruhan, terutama untuk aplikasi yang membutuhkan pemrosesan data dalam waktu nyata.

Dalam hal menangani proses enkripsi dan dekripsi, setiap algoritma kriptografi pasti memiliki kelemahan dan kelebihan. Oleh karena itu, diperlukan analisis untuk performa, dan algoritma yang paling efisien memiliki ruang dan waktu yang paling sedikit. Ukuran masukan (input), yang menunjukkan jumlah data yang diproses, serta lamanya proses.

Kriptografi menggunakan banyak algoritma. Penelitian ini akan menggunakan algoritma RSA dan ECC, masing-masing dengan kemungkinan tingkat efisiensi yang berbeda; namun, kegagalan salah satu algoritma kriptografi dapat menyebabkan proses mengenkripsi dan mendekripsi menjadi lebih cepat. Hasil penelitian ini akan menganalisis perbandingan waktu enkripsi dan dekripsi antara algoritma ECC dan RSA, memberikan wawasan tentang kelebihan dan kekurangan masing-masing algoritma sehingga dapat membantu pengembangan sistem keamanan dalam memilih algoritma yang paling sesuai untuk kebutuhan aplikasi mereka.

1.2 Rumusan Masalah

Dengan demikian, rumusan masalah penelitian ini adalah:

1. Bagaimana perbandingan waktu enkripsi antara algoritma RSA dan ECC?
2. Bagaimana perbandingan waktu dekripsi antara algoritma RSA dan ECC?
3. Apa saja komponen yang memengaruhi kinerja enkripsi dan dekripsi algoritma RSA dan ECC?

1.3 Batasan Masalah

1. Penelitian ini lebih menekankan analisis daripada pembuatan aplikasi.
2. Data yang digunakan berupa karakter huruf latin dan diubah ke kode ASCII.

3. Panjang kunci yang berbeda mencakup 112-bit, 128-bit, 192-bit, 224-bit, 256-bit, 384-bit, 521-bit, 1024-bit, 2048-bit, 3072-bit, 4096-bit, 5120-bit, 6144-bit, 7680-bit, dan 15360-bit.
4. Pada tahap pengujian, dilakukan dengan menggunakan algoritma RSA dan ECC untuk memperoleh waktu enkripsi dan dekripsi.
5. Pada tahap analisis, hasil waktu enkripsi dan dekripsi RSA dan ECC dibandingkan, dan kemudian dilakukan analisis tingkat efisiensi.

1.4 Tujuan Penelitian

1. Menganalisis perbandingan waktu enkripsi dan dekripsi algoritma RSA dan ECC.
2. Menganalisis efisiensi kedua algoritma dalam hal waktu dan kecepatan proses enkripsi dan dekripsi dalam berbagai ukuran kunci untuk memahami keunggulan dan kelemahan masing-masing algoritma.
3. Menganalisis bagaimana performa waktu enkripsi dan dekripsi dari RSA dan ECC berubah seiring dengan peningkatan jumlah ukuran data yang dienkripsi atau didekripsi.
4. Menganalisis efektivitas penggunaan kunci untuk kedua algoritma.
5. Mengenali komponen yang memengaruhi kinerja enkripsi dan dekripsi algoritma RSA dan ECC.
6. Mengukur dan membandingkan kecepatan waktu enkripsi dan dekripsi dari algoritma RSA dan ECC untuk menilai kinerja masing-masing algoritma dalam situasi yang sama dan dengan ukuran kunci yang berbeda.
7. Menentukan algoritma mana yang lebih sesuai untuk berbagai aplikasi, terutama yang memerlukan efisiensi tinggi dan kinerja optimal.
8. Mengevaluasi bagaimana variasi ukuran kunci pada RSA dan ECC mempengaruhi waktu enkripsi dan dekripsi.

1.5 Manfaat Penelitian

Diharapkan bahwa penelitian ini akan bermanfaat untuk hal-hal berikut:

1. Membantu pengembang dan peneliti dalam memilih algoritma kriptografi yang paling efisien sesuai kebutuhan aplikasi mereka.
2. Menyediakan data yang berguna untuk pengembang perangkat lunak dalam memilih algoritma kriptografi yang sesuai berdasarkan kinerja, kebutuhan aplikasi, eksperimen dan pengembangan teknologi baru.
3. Menyediakan panduan untuk memilih algoritma yang optimal untuk perangkat keras yang berbeda.
4. Menyediakan studi kasus yang relevan untuk program pendidikan di bidang kriptografi.
5. Menyediakan sumber daya untuk penelitian mahasiswa dan proyek akademis di bidang kriptografi.
6. Membantu dalam merancang sistem yang dapat mengatasi serangan kriptografi seperti serangan waktu.
7. Memberikan informasi yang mendalam tentang kinerja algoritma, yang dapat digunakan untuk menetapkan kebijakan keamanan dan standar di organisasi atau industri.
8. Mendukung penelitian lebih lanjut dan inovasi dalam kriptografi dengan memberikan wawasan tentang kelebihan dan keterbatasan algoritma RSA dan ECC.
9. Mendukung pemilihan algoritma yang memberikan perlindungan terhadap serangan kuantum di masa depan.
10. Mendukung pengembangan teknik enkripsi yang lebih cepat dan aman di masa depan.
11. Mendukung evaluasi algoritma untuk sertifikasi keamanan dari badan standarisasi.