BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Teknologi internet saat ini memasuki era pertumbuhan yang sangat cepat. Internet telah memberikan pengaruh besar terhadap berbagai bidang kehidupan manusia seperti bidang Ekonomi, Pendidikan, Sosial, Kebudayaan dan lain-lain. Adanya program digitalisasi serta banyaknya aplikasi inovasi yang dapat mendorong kehidupan sehari-hari telah menggeser cara masyarakat melakukan suatu kegiatan menjadi digital atau *online*. Dengan maraknya kegiatan yang dilakukan secara *online*, semakin banyak pula data yang diunggah dan ditransmisikan melalui *internet*. Banyaknya data yang ditransmisikan melalui internet dapat menarik perhatian dari orang-orang yang memiliki kemampuan untuk melakukan kejahatan *online* seperti peretasan, pencurian data, penggunaan data pribadi secara ilegal, dan lain-lain.

E-commerce menjadi salah satu *website* yang paling banyak menjadi sasaran pencurian data pengguna. Berdasarkan data yang diperoleh dari IDNTimes, beberapa kasus pencurian data pengguna *e-commerce* antara lain, Pada 2019, 13 juta akun pengguna Bukalapak diretas oleh hacker asal Pakistan. Pada Juli 2020, Lembaga Riset Siber Indonesia Communication and Information System Security Research Center (CISSReC) menemukan bahwa ada orang yang membeli data 91 juta pengguna akun Tokopedia yang bocor beberapa pada Mei lalu dan mengedarkan tautan unduhannya melalui Facebook. Pada Oktober 2020, sebanyak 1,1 juta data pengguna supermarket online RedMart milik Lazada diretas. Banyak informasi pribadi yang diperjualbelikan seperti nama, nomor telepon, e-mail, alamat, password, hingga nomor kartu kredit pengguna RedMart[1].

Selain peretasan data, kejahatan digital lain yang sering terjadi adalah pemalsuan dokumen seperti dokumen kependudukan KTP, KK, Akte, dan lain-lain. Dalam data di Robinopsnal Bareskrim Polri menunjukkan 95 kejahatan terkait pemalsuan dokumen dan surat autentik. Bila dirata-ratakan, tujuh

kejahatan pemalsuan dokumen dan surat autentik ditangani Polri setiap hari. Data itu didapat mulai 1 sampai 12 Januari 2022[2].

Untuk menghindari berbagai jenis kejahatan digital seperti yang dijelaskan diatas, solusi yang dapat digunakan adalah dengan mengimplementasikan sistem keamanan menggunakan kriptografi. Dalam kehidupan sehari-hari kriptografi telah banyak digunakan untuk melindungi data pengguna. Contoh penggunaan kriptografi antara lain pada transaksi melalui Anjungan Tunai Mandiri (ATM), TV berbayar, Transaksi *E-Commerce*, Tandatangan Digital, dan lain-lain. Bentuk perlindungan yang dilakukan selama transaksi menggunakan mesin ATM adalah dengan mengenkripsikan PIN. Di sisi bank, PIN yang disimpan di dalam basis data juga dienkripsi.

Pada sistem TV berbayar, sinyal broadcast dienkripsi dengan kunci yang unik. Orang-orang yang berlangganan TV berbayar pada dasarnya membayar untuk mengetahui kunci tersebut. Pada transaksi *e-commerce* yang dilakukan melalui *web browser* dilengkapi dengan protokol SSL (*Secure Socket Layer*), protokol ini memfasilitasi penggunaan enkripsi untuk data yang rahasia dan membantu menjamin integritas informasi yang dipertukarkan antara *website* dan *web browser*. Tanda tangan digital berfungsi mirip dengan "sidik jari" digital. Tanda tangan digital, yang berbentuk pesan *barcode*, secara aman menghubungkan penandatangan dengan dokumen dalam transaksi yang direkam. Tanda tangan digital mengandalkan format yang diterima secara universal yang dikenal sebagai *Public Key Infrastructure* (PKI) untuk memastikan keamanan yang ditingkatkan[3].

Kriptografi merupakan ilmu yang mempelajari sebuah proses pengubahan informasi dari bentuk awal yang dapat dibaca oleh manusia menjadi bentuk yang tidak dapat dipahami secara langsung oleh manusia pada umumnya [4]. Kriptografi terbagi menjadi 3 jenis antara lain Algoritma kriptografi simetris, algoritma kriptografi asimetris, dan fungsi hash *(Hash Function)*[5]. Algoritma kriptografi simetris merupakan algoritma yang menggunakan satu kunci yang sama untuk melakukan proses enkripsi dan

proses dekripsi[5]. Penggunaan kunci yang sama dalam algoritma simetris membuat kerahasiaan kunci harus sangat dijaga, karena jika kunci dibocorkan maka setiap orang dapat melakukan proses dekripsi pesan dan dapat melihat isi pesan asli setelah dilakukan dekripsi[6].

Algoritma kriptografi asimetris atau dengan nama lain algoritma kriptografi kunci publik merupakan algoritma kriptografi yang menggunakan dua buah kunci yang berbeda untuk melakukan proses enkripsi dan dekripsi. Kunci ini selanjutnya disebut dengan kunci publik *(public key)* dan kunci privat (*private key*). Kunci publik merupakan kunci yang bersifat publik auat dapat dilihat, sedangkan kunci privat merupakan kunci yang hanya dimiliki oleh orang yang berhak, yaitu pengirim dan penerima[5]. Algoritma kriptografi asimetris RSA *(Rivest Shamir Adleman)*, ECC *(Elliptic Curve Cryptography)*, dan ElGamal merupakan beberapa algortima yang terkenal dan banyak digunakan dalam dunia kriptografi[6].

Fungsi Hash merupakan algoritma kriptografi yang tidak menggunakan kunci dalam proses pengubahan pesan*(unkeyed cryptosystem)*. Fungsi Hash mengubah sebuah pesan menjadi karakter acak yang memiliki karakteristik yang sama. Fungsi Hash dikenal juga dengan nama lain *"one-way function"*[7].

Dalam kriptografi, terdapat dua proses utama yaitu enkripsi dan dekripsi pesan. Pesan asli sebelum dilakukan proses enkripsi disebut dengn pesan biasa (*plaintext*), sedangkan pesan hasil enkripsi yang berupa susnan karakter acak disebut *ciphertext*[6]. Enkripsi merupakan prosses mengubah pesan asli menjadi ciphertext, sedangkan dekripsi merupakan proses pengembalian pesan dari ciphertext menjadi pesan asli yang dapat dibaca[6].

Pada algoritma kriptografi simetris, penggunaan kunci enkripsi dan dekripsi yang sama akam membuat waktu komputasi lebih sedikit jika dibandingkan dengan algoritma kriptografi asimetris. Waktu komputasi yang sedikit dapat menjadi solusi untuk sistem dengan kebutuhan distribusi data yang cepat. Masalah yang timbul dari algoritma kriptografi simetris adalah terdapat banyak pengguna yang melakukan pengiriman pesan, sehingga sistem

harus membuat kunci sebanyak jumlah pesan yang dikirim. Hal ini akan sangat kompleks dan merugikan dari sisi keamanan[8]. Pada algoritma kriptografi asimetris, keuntungan utamanya terletak pada enkripsi yang kuat dengan penggunaan 2 buah kunci sehingga dekripsi pesan menjadi sulit diprediksi oleh peretas [6].

Berdasarkan latar belakang diatas, dibutuhkan sebuah sistem keamanan yang memiliki tingkat keamanan tinggi agar dapat terhindar dari resiko peretasan data secara ilegal. Peneliti dalam penelitian ini akan melakukan penelitian dengan judul "**Analisis Perbandingan Kompleksitas Waktu Algoritma Kriptografi Asimetris (RSA, ECC, dan ElGamal) dalam Proses Enkripsi, Dekripsi, dan Tandatangan Digital**". Penelitian ini akan berfokus pada melakukan perbandingan antara tiga algoritma kriptografi asimetris yaitu RSA, ECC, dan ElGamal.

Pemilihan algoritma kriptografi asimetris didasarkan pada tingkat keamanan yang lebih tinggi dibandingkan dengan algoritma kriptografi simetris. Algoritma RSA, ECC, dan ElGamal dipilih karena merupakan algoritma asimetris yang paling banyak digunakan dan diteliti hingga saat ini. Analisis dalam penelitian ini merujuk pada klasifikasi data berupa waktu pembangkitan kunci untuk enkripsi dan dekripsi, waktu enkripsi, waktu dekripsi, waktu pembangkitan kunci untuk tanda tangan digital, serta waktu pembuatan tanda tangan digital. Parameter tersebut selanjutnya dapat digunakan untuk melakukan perhitungan kompleksitas waktu dari masing-masing algoritma. Perhitungan kompleksitas waktu bertujuan untuk mengetahui besaran waktu yang dibutuhkan suatu algoritma kriptografi untuk melakukan sebuah proses tanpa ada pengaruh atau interfensi dari luar seperti kecepatan prosesor dan *compiler*. Data tersebut selanjutnya dapat digunakan sebagai data penelitian dan dasar pembentukan kesimpulan.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, rumusan masalah yang muncul antara lain :

1. Bagaimana nilai perbandingan waktu atau kecepatan dari algoritma RSA, ECC dan ElGamal sesuai dengan parameter yang ditentukan?
2. Bagaimana nilai perbandingan kompleksitas waktu yang dihasilkan dari setiap algoritma?

1.3 Tujuan Penelitian

Tujuan penelitian dalam penelitian ini adalah :

1. Melakukan perbandingan waktu /kecepatan proses enkripsi, dekripsi, dan tandatangan digital menggunakan algoritma kriptografi asimetris yang meliputi RSA, ECC, dan ElGamal.
2. Melakukan perhitungan dan perbandingan nilai kompleksitas waktu dari proses enkripsi, dekripsi, dan tandatangan digital menggunakan algoritma kriptografi asimetris yang meliputi RSA, ECC, dan ElGamal.

1.4 Batasan Masalah

Untuk memfokuskan pembahasan dalam penelitian, maka beberapa batasan masalah yang digunakan dalam penelitian ini adalah :

1. Algoritma yang diuji dalam penelitian ini adalah algoritma kriptografi asimetris yang meliputi RSA, ECC, dan ElGamal.
2. Bahasa pemrograman yang digunakan adalah C++ dengan *library* yang digunakan untuk pembuatan sistem enkripsi dan dekripsi adalah NTL (*Number Theory Library*) dengan output aplikasi berupa *console*.
3. Parameter yang digunakan untuk melakukan perbandingan algoritma antara lain waktu pembangkitan kunci untuk enkripsi dan dekripsi, waktu enkripsi, waktu dekripsi, waktu pembangkitan kunci untuk tanda tangan digital, serta waktu pembuatan tanda tangan digital.

4. Nilai kompleksitas algoritma yang dihitung adalah kompleksitas waktu dengan kasus terburuk (*worst case*) yang disimbolkan dengan notasi O besar *(big-O).*
5. Kurva yang digunakan untuk pengujian algoritma ECC adalah curve P-192 dengan nilai Px dan Py sudah di *define*.
6. Panjang kunci yang dibandingkan untuk algoritma ECC, RSA dan ElGamal adalah 192 bit, serta tambahan untuk algoritma RSA dan Elgamal dengan panjang kunci 512 bit, dan 1024 bit.

1.5 Manfaat Penelitian

Manfaat yang diharapkan dari penelitian ini antara lain :

1. Manfaat bagi peneliti, dapat menerapkan ilmu tentang algoritma kriptografi dan mengimplementasikan serta menganalisis perbedaan antar setiap jenis kriptografi secara langsung.
2. Manfaat bagi akademik, diharapkan dapat menjadi perbadingan untuk penelitian yang serupa.
3. Manfaat bagi kalangan umum, diharapkan penelitian ini dapat bermanfaat dan dipertimbangkan untuk dikembangkan lebih lanjut untuk meningkatkan kualitas keamanan yang telah ada dan digunakan saat ini.
4. Manfaat bagi kalangan peneliti, diharapkan penelitian ini dapat dijadikan sebagai alternatif untuk mempertimbangkan penggunaan algoritma yang akan dikembangkan kedepannya.