BAB I
PENDAHULUAN

1.1 Latar Belakang

Di era teknologi informasi seperti sekarang ini, masalah keamanan data merupakan aspek yang sangat penting, baik bagi individu, perusahaan maupun negara. Bagi negara, aspek kemanan data ini, terutama dalam transmisi data, menjadi kunci kesuksesan dan kekuatan militer negara tersebut, terutama dalam perang. Transmisi data yang tidak aman dapat menyebabkan data tersebut jatuh ke tangan musuh yang berakibat fatal dan dapat mengubah jalannya perang. Bagi perusahaan, keamanan data menjadi penting dikarenakan banyak data perusahaan yang sifatnya rahasia. Apabila data rahasia ini jatuh ke tangan kompetitor, perusahaan dapat mengalami kerugian yang besar.

Untuk mengatasi masalah-masalah terkait keamanan data tersebut, diperlukan ilmu kriptografi. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek-aspek keamanan informasi seperti kerahasiaan dan keaslian data, autentikasi entitas, dan autentikasi sumber data. Dalam kehidupan sehari-hari, kriptografi telah secara umum digunakan, misalnya *end-to-end encryption* pada pesan *Whatsapp*, transaksi dengan kartu cerdas, *e-commerce* melalui internet, dan lain sebagainya. Teknik-teknik matematika yang digunakan dalam kriptografi antara lain teori bilangan, teori grup dan teori ring.

Algoritma kriptografi terbagi menjadi algoritma kriptografi simetris dan algoritma kriptografi asimetris atau kriptografi kunci publik. Algoritma kriptografi simetris adalah algoritma kriptografi yang kunci dekripsinya dapat diperoleh dengan mudah dari kunci enkripsinya, sedangkan algoritma kriptografi asimetris atau algoritma kriptografi kunci publik adalah algoritma kriptografi yang menggunakan dua kunci yang berbeda dalam proses enkripsi dan dekripsi (Buchmann, 2004). Saat ini, algoritma kriptografi asimetris yang banyak digunakan adalah algoritma kriptosistem RSA, algoritma kriptosistem ElGamal, dan algoritma-algoritma kriptografi *Elliptic Curve* (ECC) seperti *Elliptic Curve Integrated Encryption Scheme* (ECIES) dan ECC ElGamal.

Kriptosistem RSA ditemukan oleh tiga orang peneliti dari Massachusetts Institute of Technology (MIT) yaitu Ron Rivest, Adi Shamir dan Leonard Adleman pada tahun 1977. Keamanan kriptosistem RSA didasarkan pada tingkat kesulitan untuk memfaktorkan suatu bilangan menjadi dua buah bilangan prima. Masalah pemfaktoran ini sangat sulit dipecahkan. Pada saat ini, bilangan modulus RSA terbesar yang sudah berhasil dipecahkan berukuran 768-bit, yang berhasil dipecahkan oleh Thorsten Kleinjung, Kazumaro Aoki, Jens Franke, Arjen Lenstra, Emmanuel Thomè, Joppe Bos, Pierrick Gaudry, Alexander Kruppa, Peter Montgomery, Dag Arne Osvik, Herman te Riele, Andrey Timofeev dan Paul Zimmerman pada tahun 2009 (Kleinjung, T. dkk, 2010). Oleh karena itu, pada saat ini, bilangan sepanjang 1024-bit sampai 4096-bit masih dianggap aman dalam artian belum dapat difaktorkan. Kelemahan dari algoritma ini adalah karena besarnya bilangan yang dibutuhkan (1024-bit ~ 4096-bit), maka proses enkripsi dan dekripsi menggunakan algoritma ini membutuhkan waktu lama, terutama untuk data yang berukuran besar.

Elliptic Curve Cryptography (ECC) ditemukan pada tahun 1985 oleh Neal Koblitz dan Victor Miller. ECC menggunakan grup siklik berupa himpunan titik pada kurva eliptik di bawah operasi penjumlahan titik. Sifat siklik dari grup ini memungkinkan untuk melakukan operasi-operasi kriptografi seperti enkripsi dan dekripsi *plaintext*. Kelebihan dari ECC adalah penggunaan kunci yang lebih kecil daripada algoritma kriptografi RSA. Sebagai contoh, 160-bit ECC memiliki tingkat keamanan yang setara dengan RSA 1024-bit. Hal ini dikarenakan untuk memecahkan kunci yang dipakai dalam ECC, kriptanalis harus terlebih dahulu menyelesaikan *Elliptic Curve Discrete Logarithm Problem* (ECDLP) yang dikenal lebih sulit daripada memecahkan pemfaktoran suatu bilangan menjadi dua bilangan prima pada algoritma RSA. Contoh kriptosistem yang termasuk ke dalam ECC adalah ECC ElGamal, *Elliptic Curve Integrated Encryption Scheme* dan *Simplified Elliptic Curve Integrated Encryption Scheme* (Hankerson, Menezes, & Vanstone, 2004).

Simplified Elliptic Curve Integrated Encryption Scheme (S-ECIES) merupakan penyederhanaan dari kriptosistem *Elliptic Curve Integrated Encryption Scheme* (ECIES). Algoritma ini dikenal lebih mudah

diimplementasikan daripada ECC ElGamal karena *plaintext* hanya "disembunyikan" ke dalam titik-titik pada kurva eliptik dengan cara dioperasikan dengan titik pada kurva eliptik (*masking*), tidak seperti ECC ElGamal dimana *plaintext* dipetakan pada titik-titik pada kurva eliptik (*mapping*). Hal ini menyebabkan algoritma S-ECIES lebih cepat dan lebih mudah diimplementasikan dibandingkan ECC ElGamal karena tidak membutuhkan algoritma pemetaan *plaintext* pada titik.

Oleh karena itu, dalam penelitian ini, peneliti akan melakukan pengembangan kriptosistem RSA dan S-ECIES dengan menggabungkan kedua kriptosistem tersebut dan dalam implementasinya, penulis membuat sebuah program komputer menggunakan bahasa pemrograman Python versi 3.5 untuk memudahkan proses enkripsi dan dekripsinya.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah di atas, peneliti mengajukan beberapa rumusan masalah sebagai berikut:

1. Bagaimana konsep dan algoritma penggabungan kriptosistem S-ECIES dan kriptosistem RSA?
2. Bagaimana implementasi penggabungan kriptosistem S-ECIES dan kriptosistem RSA dalam bentuk program komputer?

1.3 Tujuan Penelitian

Tujuan yang hendak dicapai dalam penelitian ini adalah:

1. Mengembangkan kriptosistem baru hasil penggabungan kriptosistem S-ECIES dan kriptosistem RSA.
2. Mengimplementasikan penggabungan kriptosistem S-ECIES dan RSA ke dalam sebuah program komputer.

1.4 Manfaat Penelitian

Manfaat yang hendak dicapai dari penelitian ini adalah:

1. Memberikan sumbangsih kepada masyarakat pada umumnya dan dunia kriptografi pada khususnya tentang pengembangan kriptosistem S-ECIES dan RSA dengan mengembangkan kedua kriptosistem tersebut.
2. Dalam penelitian ini dikembangkan sebuah aplikasi yang bertujuan untuk membantu proses pembangkitan kunci, enkripsi dan dekripsi pada kriptosistem gabungan S-ECIES dan RSA.

1.5 Batasan Masalah

Dalam penelitian ini, penulis merumuskan batasan masalah sebagai berikut:

1. *Plaintext* yang digunakan dalam model pengembangan merupakan teks alfanumerik.
2. *Ciphertext* berupa larik yang berisi bilangan bulat hasil proses enkripsi yang kemudian disimpan sebagai *file object* Python.
3. Kurva eliptik yang digunakan dalam model pengembangan adalah kurva eliptik pada lapangan bilangan prima.
4. Kriptosistem S-ECIES yang digunakan menggunakan kurva eliptik pada bilangan prima 256-bit yang dirumuskan oleh *National Institute of Standards and Technology* (NIST *Curve* P-256).
5. Kriptosistem RSA yang digunakan menggunakan modulus 2048-bit.

1.6 Sistematika Penulisan

BAB I PENDAHULUAN

Bab pendahuluan berisi uraian latar belakang, rumusan masalah, tujuan penelitian, batasan masalah, manfaat penelitian dan sistematika penulisan.

BAB II LANDASAN PENELITIAN

Bab ini membahas teori-teori dasar dan konsep yang mendukung masalah yang akan dikaji. Akan dipaparkan teori dan konsep pada bidang matematika, khususnya mengenai teori bilangan, teori grup, teori ring, kriptosistem RSA, *Elliptic Curve Cryptography*, dan kriptosistem S-ECIES.

BAB III METODE PENELITIAN

Bab ini menjelaskan desain penelitian yang direncanakan dari perumusan masalah, model dasar, pengembangan model dasar, konstruksi program, validasi hingga kesimpulan.

BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Bab ini memuat hasil penelitian mengenai kriptosistem gabungan S-ECIES dan RSA. Pada bab ini, dijelaskan konsep dan algoritma kriptosistem S-ECIES, konsep dan penggabungan kriptosistem S-ECIES dan RSA serta implementasinya dalam program komputer.

BAB V SIMPULAN DAN SARAN

Bab penutup menyajikan kesimpulan-kesimpulan yang diambil dari seluruh uraian bab-bab sebelumnya, serta saran-saran dari hasil yang didapat.