BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi mempermudah keterbukaan terhadap akses data dan informasi, salah satunya adalah media komunikasi sebagai perantara distribusi dan penyampaian pesan jarak jauh. Salah satu implementasinya adalah email yang saat ini sering digunakan sebagai media komunikasi jarak jauh. Tetapi akhir-akhir ini sering terjadi permasalahan kasus *cyber*, di antaranya adalah pemalsuan email (*spoofing*), disalahgunakan untuk menyebarkan spam, digunakan para peretas sebagai media menyebarkan *malware*, peretasan email (*man in the middle attack*), dan beberapa kasus lainnya. Kita ambil contoh ketika kita membuat akun *market place* seperti Shopee atau Go-jek atau Grab, kita diminta untuk mengaitkan akun tersebut dengan akun email yang kita miliki dan setelah itu wajib menyetujui syarat-syarat yang di mana kita biasanya langsung mencentangnya atau menyetujuinya tanpa harus membaca apa isi syarat-syarat tersebut. Ternyata di dalam syarat-syarat tersebut salah satunya berisi terkait pihak ketiga atau pemilik perusahan tersebut dapat melihat isi pesan mail kita. Ini mengindikasian bahwa isi pesan email dapat dilihat oleh orang lain dan tidak aman. Oleh karena itu, pada saat melakukan pengiriman atau penerimaan email diperlukan perhatian terhadap aspek keamanan yaitu, kerahasiaan (*confidentiality*), integritas (*integrity*), memastikan (*authentication*), dan penyangkalan (*non-repudiation*) (Agustina & Kurniati, 2009).

Sudah seharusnya informasi yang disampaikan melalui perantara email terjamin keamanannya pada saat didistribusikan dan disimpan di media penyimpanan baik publik maupun privat. Terlebih lagi isi dari email tersebut bersifat penting dan rahasia seperti hasil pemilihan umum atau perintah kerja. Zulfikar dkk. (2019) mengatakan beberapa email *service* seperti Google dan Yahoo pernah mengalami kasus keamanan, sehingga protokol yang digunakan saat itu diubah dari HTTP menjadi HTTPs, tetapi proses memuat data menjadi lebih lama dikarenakan HTTPs memerlukan proses lebih seperti otentikasi dan semacamnya untuk perizinan koneksi. Dengan kata lain email *service* lebih memperhatikan keamanan akun pengguna untuk meningkatkan keamanan dari email. Akan tetapi masih terdapat celah peretasan terhadap isi dari email itu sendiri, peretas mungkin saja akan meretas *mail server* dan melakukan penyadapan pada email yang menjadi sasaran.

Dari permasalahan yang ada maka diperlukan langkah antisipasi berupa meningkatkan keamanan pada data dan informasi. Salah satunya adalah dengan menerapkan kriptografi untuk menjaga keaslian dan kerahasiaan informasi dalam bentuk email.

Kriptografi adalah seni melindungi informasi yang dikirimkan agar terhindar dari gangguan, di sisi lain kriptanalisis adalah seni memecahkan sandi rahasia dan membaca informasi, atau menggantinya

dengan informasi yang berbeda. Kriptografi dan kriptanalisis adalah istilah dalam kriptologi (Cameron, 2003). Dalam proses penyamaran pesan digunakan kunci kriptografi, yaitu kunci simetri dan kunci asimetri. Kriptografi simetris menggunakan kunci yang sama (kunci simetris) untuk melakukan proses enkripsi dan dekripsi. Kriptografi asimetris menggunakan kunci yang berbeda untuk proses enkripsi (menggunakan kunci publik) dan dekripsi (menggunakan kunci privat). Kedua teknik tersebut memiliki keunggulan dan kekurangan masing-masing yang diukur berdasarkan durasi enkripsi, durasi dekripsi, tingkat perubahan yang dihasilkan, entropi, dan jumlah bit yang dibutuhkan untuk pengkodean secara optimal. Kriptografi asimetris dapat dikatakan lebih aman dari simetris, dikarenakan menggunakan dua kunci yang berbeda dan ukuran kunci yang ditawarkan relatif lebih panjang bisa mencapai 1024 bit. Di sisi lain, untuk kecepatan proses enkripsi dan dekripsi lebih unggul kriptografi simetris dan penggunaan memorinya pun relatif lebih rendah dengan nilai terendah 9,38 KB (Zulfikar, 2019).

Salah satu teknik kriptografi asimetris yaitu *Elliptic Curve Cryptography* (ECC). ECC dicetuskan oleh Neal Koblitz dan Victor S. Miller pada tahun 1985. Seiring dengan perkembangan ECC, ditemukan suatu teknik lain yang memiliki keamanan yang sama dengan ECC yaitu *Hyperelliptic Curve Cryptography* (HCC) (Tumbur, 2014). Kriptografi asimetris ini sulit sekali diretas dikarenakan adanya masalah *Elliptic Curve Discrete Logarithm Problem* (ECDLP). Masalahnya adalah ketika diberikan dua buah titik eliptik P dan Q lalu cari integer k sedemikian sehingga Q=kP. Secara komputasi sulit mencari k, jika k bilangan yang besar. Dalam hal ini k adalah logaritma diskrit dari Q dengan basis P.Pada algoritma ECC, Q adalah kunci public, k adalah kunci privat, dan P sembarang titik pada kurva eliptik. ECC memiliki perluasan sistem kriptografi. Salah satu perluasaannya adalah *Elliptic Curve Diffie Hellman* (ECDH). ECDH adalah sebuah protokol perjanjian kunci yang memungkinkan dua pihak pengirim dan penerima, yang pada awalnya masing-masing memiliki kurva eliptik dan titik kurva Q yang sama (kunci publik), membuat kunci rahasia bersama melalui saluran yang tidak aman. Kunci rahasia ini (atau kunci simetri) digunakan untuk enkripsi pesan asli (plainteks) atau dekripsi pesan chiperteks. Algoritma ECDH merupakan salah satu solusi yang aman untuk membuat kunci simetri yang nantinya digunakan untuk mengenkripsi atau dekripsi pesan email. Oleh karena itu, diperlukan program aplikasi pengirim email untuk menjaga keaslian dan kerahasian pesan email dengan menggunakan algoritma ECDH serta mempermudah proses pembangkitan kunci, enkripsi, dekripsi, dan pengiriman email.

Berikut beberapa kajian terdahulu yang membahas ECC dan email. Sihotang (2017) memaparkan salah satu perluasan ECC yaitu S-ECIES setelah itu menggabungkannya dengan kriptosistem RSA untuk mempersulit kriptanalis dalam melakukan kriptanalisis karena dibutuhkan dua algoritma dengan kompleksitas. Zahra (2020) memaparkan bagaimana penggabungan algoritma ECC dengan kriptografi visual untuk meningkatkan keamanan data (dalam hal ini data berupa gambar) agar tidak mudah diretas

oleh kriptanalisis. Sobari (2017) menerapkan enkripsi Caesar Cipher untuk aplikasi pengiriman email yang menggunakan delphi untuk meningkatkan keamanan email.

Berdasarkan pemaparan di atas maka penulis tertarik untuk melakukan penelitian terkait Aplikasi Pengiriman Email Menggunakan Enkripsi *Elliptic Curve Diffie Hellman*.

1.2 Rumusan Masalah

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

1. Bagaimana skema pengiriman email menggunakan enkripsi ECDH?
2. Bagaimana konstruksi program aplikasi pengiriman email menggunakan enkripsi ECDH?

1.3 Batasan Masalah

Dalam penelitian ini diperlukan batasan masalah sebagai berikut:

1. Pesan yang digunakan dalam aplikasi pengiriman email berupa *text* alfanumerik.
2. Proses enkripsi atau dekripsi menggunakan algoritma ECC dengan menggunakan algoritma pertukaran kunci, yaitu algoritma ECDH.

1.4 Tujuan Penelitian

Tujuan yang hendak dicapai dalam penelitian ini adalah:

1. Merancang sistem ECDH untuk enkripsi email.
2. Membuat aplikasi pengiriman email dengan algoritma ECDH.

1.5 Manfaat

Manfaat yang hendak dicapai dari penelitian ini:

1. Manfaat Teoritis

Mengembangkan skema enkripsi email menggunakan ECDH.

2. Manfaat Praktis

Mempermudah pengguna untuk melakukan pengiriman email serta untuk mengamankan pesan email.

1.6 Sistematika Penulisan

Penelitian ini terdiri dari lima bab, yaitu:

1. BAB I PENDAHULUAN

   Bab pendahuluan berisi mengenai latarbelakang, rumusan masalah, tujuan, batasan masalah, manfaat, dan sistematika penulisan.
2. BAB II LANDASAN TEORI

Bab ini membahas teori-teori dasar dan konsep yang membantu menyelesaikan masalah yang akan dikaji. Teori-teori dasar dan konsep pada bidang matematika tersebut meliputi teori bilangan, teori grup,teori ring, ECDH, dan ECC.

3. BAB III METODOLOGI PENELITIAN

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

4. BAB IV PEMBAHASAN DAN HASIL

   Bab ini memuat hasil penelitian mengenai implementasi pengiriman pesan email pada aplikasi pengirim email. Pada bab ini ,dijelaskan konsep dan algoritma ECDH pada skema pengiriman email menggunakan enkripsi yang menerapkan algoritma *Elliptic Curve Diffie Hellman* serta implementasinya dalam program komputer.

5. BAB V KESIMPULAN DAN SARAN

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