BAB I
PENDAHULUAN

1.1 Latar Belakang

Seiring dengan kemajuan teknologi yang begitu pesat, pertukaran informasi pun terjadi dengan cepat dan masif. Percepatan pertukaran informasi ini diimbangi dengan transformasi media informasi dari cetak menjadi digital, atau dikenal dengan istilah digitalisasi. Digitalisasi memungkinkan suatu informasi untuk dapat diakses dengan lebih mudah oleh siapa pun, kapan pun, dan di mana pun. Kondisi ini membuat masalah keamanan informasi menjadi sebuah isu penting dan memerlukan penanganan yang tepat untuk melindunginya dari pihak asing atau kejadian yang tidak diinginkan.

Salah satu bentuk perlindungan terhadap informasi adalah dengan melakukan autentikasi pada pihak yang ingin mengaksesnya. Proses autentikasi akan memverifikasi bahwa pengakses adalah pihak yang memiliki otoritas atas informasi yang akan diakses. Proses auntentikasi dilakukan dengan mengikuti protokol atau rangkaian aturan tertentu. Jika protokol autentikasi berhasil dilaksanakan hingga selesai, maka pengakses akan diberi kewenangan atas informasi yang diinginkan.

Protokol autentikasi yang umum dijumpai adalah penggunaan *username* dan *password* saat melakukan *log-in* ke sebuah akun. *Username* merupakan identitas akun dan digunakan penyedia layanan (*server*) untuk mencari akun yang sesuai. Sedangkan *password* bersifat rahasia dan digunakan sebagai bentuk autentikasi oleh *server* terhadap pengguna (*user)*. Dengan cara ini, *user* diberi otoritas untuk mengakses akun jika *user* menggunakan *username* dan *password* yang benar.

Namun, penggunaan *password* sebagai bentuk autentikasi terhadap *user* juga memiliki kendala. Salah satu kendala yang dihadapi adalah mengenai bocornya *username* dan *password* sebuah akun. Sebagai contoh kasus, survei yang dilakukan Cisco di kawasan Asia pada tahun 2020 menemukan adanya 81% kasus kebocoran data yang terjadi terkait dengan *password* yang dibobol oleh *hacker*, kemudian dijual di *dark web* atau digunakan sendiri (Naufal, 2020). Selain itu,

pada tahun 2021 terdapat kejahatan siber yang membocorkan 3,2 juta alamat *email* beserta *password* pengguna (Ikhsan, 2021). Adanya kebocoran *username* dan *password* ini menimbulkan kejahatan siber lainnya di mana pihak asing yang mengetahui *username* dan *password* orang lain melakukan *log-in* seolah ia adalah pemilik akun yang asli. Saat *username* dan *password* yang digunakan sesuai, maka *server* akan mengenali pihak asing sebagai *user* asli dan memberikan otoritas untuk mengakses akun terkait.

Untuk menanggulangi hal ini, maka dibutuhkan alternatif lain sebagai protokol autentikasi. Adapun tujuannya adalah agar pihak asing tetap tidak bisa mengakses akun meskipun ia mengetahui *username* dan *password* yang digunakan oleh *user* asli. Protokol yang dapat diterapkan adalah *Two Way Challenge-Response Protocol*. Dalam protokol ini, *server* memberikan tantangan (*challenge*) kepada *user*, kemudian *user* memberikan jawaban (*response*) kepada *server*. Protokol ini mengautentikasi keaslian *user* melalui kebenaran dari jawaban yang diberikan oleh *user*.

Pemberian *challenge* dan *response* bisa dilakukan mengikuti Algoritma *Elliptic Curve Diffie Hellman*. Aspek yang dimanfaatkan yaitu kegunaan Algoritma *Elliptic Curve Diffie Hellman* untuk pertukaran kunci simetri. Pada protokol ini, *server* akan selalu membangkitkan bilangan acak, sehingga *challenge* yang diterima *user* akan berbeda tiap kali melakukan *log-in*. Akibatnya, *response* yang diberikan *user* juga akan berbeda-beda tiap waktunya. Dengan demikian, meskipun ada pihak asing yang mengetahui jawaban *user* saat ini, *response* tersebut belum tentu dapat digunakan pada saat *log-in* berikutnya. Munir (2019) menyatakan bahwa Algoritma *Elliptic Curve Diffie Hellman* memiliki keamanan yang tinggi didasarkan pada sulitnya pemecahan masalah logaritma diskrit. Meskipun begitu, dalam hal komputasi, perhitungan yang terlibat dalam Algoritma *Elliptic Curve Diffie Hellman* lebih efisien dan sederhana.

Untuk memudahkan pengaplikasian protokol autentikasi ini, maka dibuatlah sebuah program aplikasi menggunakan bahasa pemrograman Python. Bahasa pemrograman Python dipilih karena memiliki banyak *built-in library* yang dapat dengan mudah diterapkan dalam pemrograman untuk kriptografi. Selain itu, pada bahasa pemrograman Python, program aplikasi dapat dibuat berbasis *Graphical*

User Interface (GUI), sehingga lebih memudahkan *user* dalam menggunakan fitur-fitur yang ada pada program aplikasi.

Berikut beberapa kajian yang telah dilakukan seputar *Two Way Challenge-Response Protocol* dan Algoritma *Elliptic Curve Diffie Hellman*. Husain, dkk. (2019) menggunakan *Challenge-Response Authentication Protocol* sebagai penanggulangan atas *Sybil Attack*. Zahra (2021) menggunakan *Elliptic Curve Cryptography* pada kriptografi visual untuk gambar berwarna. Azizah (2020) menggabungkan *Elliptic Curve Cryptography* dan modifikasi *Hill Cipher* untuk meningkatkan keamanan pesan. Adapun Sitohang (2019) mengkaji salah satu kriptosistem yang termasuk *Elliptic Curve Cryptography* yaitu *Simplified Elliptic Curve Integrated Encryption Scheme* dan menggabungkannya dengan kriptosistem RSA. Selain itu, Rambonang (2015) menggunakan algoritma SHA-1 pada *Two Way Challenge-Response Protocol* untuk autentikasi klien pada transaksi berbasis web. Lalu Ferdinan (2021) membuat aplikasi pengiriman email menggunakan *Elliptic Curve Diffie Hellman* sebagai metode enkripsi.

Berdasarkan latar belakang di atas, maka penulis tertarik untuk melakukan penelitian terkait Implementasi Algoritma *Elliptic Curve Diffie Hellman* pada *Two Way Challenge-Response Protocol* sebagai protokol autentikasi untuk *user*. Aspek keterbaruan penelitian ini dibandingkan penelitian-penelitian sebelumnya terletak pada penggunaan Algoritma *Elliptic Curve Diffie Hellman* untuk proses pemberian *challenge* dan *response*.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, maka rumusan masalah pada penelitian ini adalah sebagai berikut:

1. Bagaimana protokol dan skema implementasi Algoritma *Elliptic Curve Diffie Hellman* pada *Two Way Challenge-Response Protocol*?
2. Bagaimana konstruksi program aplikasi autentikasi menggunakan *Two Way Challenge-Response Protocol* dan Algoritma *Elliptic Curve Diffie Hellman*?

1.3 Tujuan

Tujuan yang hendak dicapai dalam penelitian ini adalah:

1. Merancang protokol dan skema implementasi Algoritma *Elliptic Curve Diffie Hellman* pada *Two Way Challenge-Response Protocol*.
2. Mengkonstruksi program aplikasi autentikasi menggunakan *Two Way Challenge-Response Protocol* dan Algoritma *Elliptic Curve Diffie Hellman*.

1.4 Manfaat

Manfaat yang diharapkan dari penelitian ini yaitu:

1. Manfaat Teoritis

Penelitian ini diharapkan dapat mengembangkan protokol dan skema autentikasi *user* sebagai implementasi Algoritma *Elliptic Curve Diffie Hellman* pada *Two Way Challenge-Response Protocol*.

2. Manfaat Praktis

Secara praktis, penelitian ini menghasilkan *prototype* program autentikasi menggunakan bahasa pemrograman *Python,* dengan mengimplementasikan Algoritma *Elliptic Curve Diffie Hellman* pada *Two Way Challenge-Response Protocol*.