BAB I

PENDAHULUAN

1.1 Latar Belakang

Indonesia merupakan negara yang menggunakan demokrasi sebagai sistem pemerintahannya. Salah satu pelaksanaan sistem demokrasi di Indonesia adalah dengan cara pemilihan pemimpin melalui voting. Voting dilaksanakan dari mulai skala besar yaitu untuk pemilihan presiden/wakil presiden, kepala daerah dan wakil-wakil rakyat. Pada skala kecil, terdapat pemilihan ketua BEM dalam suatu universitas, ketua rukun tetangga, dan lainnya. Pada voting, terdapat beberapa prosedur dan persyaratan yang harus dipenuhi oleh pemilih maupun penyelenggara. Oleh karena itu, voting membutuhkan regulasi dan prosedur agar lebih menjamin kerahasiaan serta bagaimana hasil penghitungan suara dapat berlangsung jujur dan transparan (Pratama & Pertiwi, 2022).

Memasuki era digital dan pesatnya perkembangan teknologi, keberadaan teknologi saat ini semakin maju dan terjangkau untuk mempermudah manusia dalam melakukan berbagai kegiatan (Sitorus & Antonieta, 2021). Bersamaan dengan itu terdapat salah satu cara pemilihan yang dikolaborasikan dengan perkembangan teknologi yaitu *e-voting*. Menurut Setiawan, dkk. (2023), Pemungutan suara elektronik (*e-voting*) secara umum dipahami sebagai penggunaan teknologi informasi dalam pemungutan suara, khususnya pemungutan suara elektronik, untuk mengurangi biaya pemilihan dan mempercepat pengumpulan data. Menurut Fikriansyah (2021), penggunaan teknologi dalam melakukan voting dapat menjadi alternatif baru dalam melaksanakan voting agar lebih efektif dan efisien. Dengan berbagai keuntungan yang ada, *e-voting* dapat dijadikan pilihan untuk menggantikan praktek voting tradisional.

Salah satu komponen penting dalam *e*-voting adalah keamanan dan kerahasiaan data karena penggunaan *e-voting* juga menimbulkan beberapa resiko, seperti kerentanan terhadap serangan *cyber* dan masalah integritas data (Yafi dkk., 2023). Sistem keamanan *e-voting* harus memiliki keamanan yang sama seperti pada voting biasa (Fikriansyah, 2021). Keamanan dan kerahasiaan data dapat dicapai dengan berbagai teknik kriptografi. Menurut Hidayatulloh, dkk. (2023), kriptografi

adalah cabang ilmu yang mempelajari beberapa teknik komputasi yang berkaitan dengan aspek keamanan informasi guna menjaga kerahasiaan pesan. Kriptografi sendiri tidak lepas dari berbagai protokol-protokol di dalamnya. Menurut (Menezes, Oorschot, & Vanstone, 1996), protokol dalam kriptografi adalah algoritma terdistribusi yang ditentukan oleh urutan langkah-langkah secara tepat dalam menentukan tindakan dari dua entitas atau lebih demi tujuan keamanan. Sedangkan algoritma merupakan seperangkat instruksi atau logika yang terbatas, ditulis untuk menyelesaikan tugas tertentu yang telah ditentukan sebelumnya (Putri dkk. 2022).

Kriptografi berasal dari kata *cryptos* (rahasia) dan *graphein* (tulisan). Jadi secara harfiah kriptografi berarti tulisan rahasia. Kriptografi pertama kali digunakan pada 1900 SM yang ditemukan berupa tulisan menggunakan aksara Mesir kuno yang tidak standar. Selanjutnya kriptografi terbagi menjadi dua yaitu kriptografi klasik dan kriptografi modern. Menurut Susanti (2020), kriptografi klasik merupakan kriptografi yang digunakan pada zaman dahulu dan hanya melakukan pengacakan pada huruf A-Z saja, sedangkan kriptografi modern merupakan perbaikan yang mengacu pada kriptografi klasik dengan memiliki berbagai macam algoritma yang dimaksudkan untuk mengamankan informasi yang dikirim melalui jaringan komputer. Kriptografi modern dibagi menjadi dua berdasarkan sifat kuncinya, yaitu kriptografi kunci-simetri dan kriptografi kunci publik.

Salah satu algoritma dari kriptografi kunci-simetri adalah *Advanced Encryption Standard* atau AES. Algoritma AES ditetapkan oleh *National Institute of Standards and Technology* (NIST) pada tahun 2000 sebagai pemenang sayembara untuk menentukan algoritma kriptografi standar yang baru yang diimplementasikan oleh Joan Daeman dan Vincent Rijmen. AES termasuk kepada jenis algoritma kriptografi yang bersifat simetri dan *block cipher*. Algoritma AES dipilih berdasarkan aspek keamanan AES banyak digunakan saat ini karena jauh lebih kuat daripada DES dan *triple* DES (Putri, dkk., 2023).algoritma, efisiensi, fleksibilitas, dan kebutuhan memori (Munir, 2019).

Pada kriptografi modern dikenal adanya fungsi *hash*. Fungsi *hash* adalah fungsi satu arah atau tidak pada yang berguna dalam pengecekan keaslian atau integritas suatu pesan yang dapat memiliki masukan random dan diubah menjadi nilai *hash* yang berukuran tetap (Harianja, 2024). Dalam fungsi *hash* satu arah

pesan dapat dibuat menjadi nilai *hash* namun tidak dapat dikembalikan. Salah satu fungsi *hash* adalah *Secure Hash Algorithm* atau SHA. Jenis SHA yang belum ditemukan kolisi atau nilai *hash* yang sama dari nilai awal yang berbeda hingga saat ini adalah SHA-256 (Az-Zahra, Marwati, & Sispiyati, 2024). SHA-256 merupakan fungsi *hash* satu arah (*One-Way Function*) versi SHA dengan ukuran *digest* sebesar 256 bit pada versi SHA-2 yang dirancang oleh *The National Institute of Standards and Technology* (NIST) pada tahun 2002. SHA-256 memiliki keamanan yang lebih dibandingkan SHA-1 karena SHA-256 belum berhasil diretas.

Pada penelitian sebelumnya oleh Fikriansyah (2021), algoritma kriptografi Elgamal yang merupakan kriptografi kunci asimetris digunakan untuk mengamankan data *e-voting*. Pada penelitian ini digunakan AES-256 karena AES-256 merupakan algoritma kunci simetris yang memiliki kecepatan komputasi lebih tinggi dibandingkan dengan algoritma kunci asimetris (Hajar, 2022). AES-256 juga telah diadopsi secara luas sebagai standar enkripsi oleh berbagai institusi dan organisasi di seluruh dunia yang menegaskan keandalannya dalam praktik keamanan modern. Kelebihan-kelebihan ini menjadikan AES-256 sebagai pilihan yang lebih tepat untuk aplikasi *e-voting* yang membutuhkan proses enkripsi dan dekripsi data secara cepat dan aman.

Berdasarkan latar belakang tersebut, penelitian ini akan merancang protokol dan *e-voting* berbasis aplikasi menggunakan algoritma AES-256 dan SHA-256. Algoritma AES-256 akan digunakan untuk merahasiakan data pilihan suara dan algoritma SHA-256 akan digunakan untuk mengecek keabsahan pada proses *login* dan proses verifikasi suara.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, masalah yang dibahas dalam penelitian ini adalah sebagai berikut.

1. Bagaimana skema aplikasi *e-voting* menggunakan algoritma AES-256 dan SHA-256?
2. Bagaimana konstruksi program aplikasi *e-voting* menggunakan algoritma AES-256 dan SHA-256?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah, tujuan dari skripsi ini adalah sebagai berikut.

1. Merancang protokol *e-voting* berbasis aplikasi menggunakan algoritma AES-256 dan SHA-256.
2. Mengonstruksi program aplikasi *e-voting* menggunakan algoritma AES-256 dan SHA-256.

1.4 Manfaat Penelitian

Berdasarkan tujuan penelitian, manfaat dari skripsi ini adalah sebagai berikut.

1. Manfaat teoritis dari penelitian ini adalah mengimplementasi teori grup, teori ring, dan juga lapangan *galois* (*galois field*) dalam AES-256 dan SHA-256 pada aplikasi *e-voting*.
2. Manfaat praktis dari penelitian ini adalah program aplikasi *e-voting* berbasis AES-256 dan SHA-256 yang dapat digunakan sebagai sarana pelaksanaan voting yang aman.