BAB I
PENDAHULUAN

1.1 Latar Belakang

Indonesia merupakan negara yang menerapkan sistem demokrasi yang memungkinkan rakyat untuk memilih langsung wakil-wakil atau kepala daerah melalui proses pemungutan suara. Dalam proses pemungutan suara, terdapat sejumlah kriteria yang harus dipenuhi oleh warga negara agar mereka berhak memberikan suara, dan negara memiliki kewajiban untuk menjaga hak-hak tersebut saat warga negara menyalurkan suara mereka.

Saat ini pemungutan suara di Indonesia masih menggunakan cara yang konvensional yaitu, dengan mencoblos kertas suara pada bilik yang ada di tempat pemungutan suara atau sering disebut dengan TPS. Pada pemungutan suara yang konvensional ini memiliki beberapa kelemahan seperti lamanya proses perhitungan suara, kurang akuratnya hasil perhitungan suara (faktor *human error*), tidak ada salinan kertas suara, sulitnya perhitungan kembali, serta besarnya anggaran yang dikeluarkan (Rokhman. 2011).

Seiring perkembangan teknologi, pemungutan suara kini memiliki teknik lain, yaitu *electronic voting. Electronic voting* merupakan suatu metode pengumpulan suara dengan menggunakan perangkat elektronik. *E-voting* memiliki beberapa kelebihan seperti mempercepat penghitungan suara, lebih akuratnya hasil penghitungan suara, menghemat biaya pengiriman suara, menghemat biaya pencetakan kerta suara, kertas suara dapat dibuat dalam beberapa versi bahasa, serta menyediakan akses informasi yang lebih banyak berkenaan dengan pilihan suara (Darmawan, dkk., 2014).

Di Indonesia *e-voting* masih jarang digunakan karena ada beberapa aspek yang belum terpenuhi seperti aksesibilitas, kepercayaan publik serta ketersediaan perangkat lunak. Selain itu, *e-voting* harus memenuhi asas pemilihan umum (pemilu) yaitu luber dan jurdil (Rokhman. 2011).

Proses pemungutan suara memerlukan prosedur yang dapat memastikan kerahasiaan dan keabsahan hasil pemilihan (Risnanto, 2017). Kerahasasiaan ini dapat dicapai dengan adanya kriptografi. Kriptografi merupakan ilmu yang

mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi (Menezes, dkk., 2018).

Untuk menangani masalah keamanan informasi telah diciptakan seperangkat protokol yang rumit. Sebagai sarana keamanan, kriptografi tidak dapat dipisahkan dari keberadaan protokol. Dalam konteks kriptografi, protokol merupakan rangkaian algoritma yang secara eksak diatur dalam urutan langkah-langkah untuk mengkoordinasikan tindakan antara dua entitas atau lebih dengan tujuan mencapai keamanan (Menezes, 1996). Sedangkan algoritma adalah urutan langkah-langkah untuk memecahkan suatu masalah. Pada penelitian yang dilakukan oleh Fikriansyah (2021) protokol yang digunakan merupakan protokol kritografi dan protokol tanda tangan digital.

Kriptografi sudah eksis sejak kurang lebih sekitar tahun 400 sebelum masehi yang digunakan oleh bangsa Yunani. Alat yang digunakan untuk menyembunyikan pesan kala itu disebut dengan *scytale*. Kriptografi menurut sejarahnya dibagi menjadi dua yaitu kriptografi klasik dan kriptografi modern. Kriptografi klasik pada umumnya bergantung pada penggunaan kunci simetris dan telah digunakan sebelum era komputerisasi, sementara kriptografi modern cenderung mengandalkan penggunaan kunci publik dan operasi komputerisasi yang berdasarkan sistem bilangan biner.

Salah satu algoritma kunci publik dalam kriptografi modern adalah Rivest Shamir Adleman (RSA). Algoritma ini ditemukan pada tahun 1976 oleh Ron Rivest, Adi Shamir, dan Len Adleman. Keamanan algoritma RSA ini bergantung pada kerumitan dalam menguraikan bilangan besar menjadi faktor-faktor prima.

Selain algoritma RSA, dalam kriptografi juga mengenal algoritma fungsi *Secure Hash Algorithm* (SHA). Fungsi *hash* merupakan fungsi yang *input* nya berupa *string* dengan panjang yang tidak ditentukan, kemudian mengubahnya menjadi *string* dengan panjang yang tetap. Fungsi *hash* memiliki beragam algoritma seperti SHA-0, SHA-1, SHA-256, serta SHA-512, untuk saat ini fungsi *hash* yang terkenal merupakan SHA-256.

Fikriansyah (2021) melakukan implementasi algoritma El Gamal dan SHA-256 pada aplikasi *e-voting* menggunakan bahasa pemrograman *python*. Pada penelitian tersebut diperoleh kesimpulan bahwa pengimplementasian antara kedua algoritma tersebut memiliki keamanan yang cukup tinggi dikarenakan El Gamal menggunakan bilangan acak prima yang bernilai cukup besar dan algoritma SHA-256 memiliki proses komputasi yang relatif baru dan rumit sehingga aman dalam penggunaannya.

Ridwan dkk. (2016) pada penelitiannya tentang rancang bangun *e-voting* dengan menggunakan keamanan algoritma Rivest Shamir Adleman (RSA) berbasis *WEB* dengan studi kasus pemilihan ketua BEM FMIPA. Pada penelitian tersebut diperoleh kesimpulan implementasi algoritma RSA pada *e-voting* berhasil menjaga integritas data hasil *voting* sehingga dapat diverifikasi bahwa hasil *e-voting* tidak mengalami perubahan selama proses pengiriman.

Berdasarkan pemaparan diatas, peneliti tertarik untuk mengimplentasikan algoritma RSA dan SHA-256 pada aplikasi *e-voting*. Algoritma RSA digunakan untuk proses merahasiakan pilihan suara sedangkan algoritma SHA-256 akan digunakan untuk proses keabsahan dari pilihan suara. Aplikasi ini akan berbasis *web* yang dibangun dengan bahasa pemrograman *Javascript*.

1.2 Rumusan Masalah

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

1. Bagaimana skema *e-voting* menggunakan SHA-256 dan algoritma RSA?
2. Bagaimana konstruksi aplikasi *e-voting* menggunakan SHA-256 dan algoritma RSA?
3. Bagaimana validasi aplikasi *e-voting* menggunakan SHA-256 dan algoritma RSA?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah di atas, tujuan pada penelitian ini sebagai berikut:

1. Merancang protokol *e-voting* menggunakan SHA-256 dan algoritma RSA.

2. Mengonstruksi aplikasi *e-voting* menggunakan SHA-256 dan algoritma RSA.
3. Memvalidasi aplikasi *e-voting* menggunakan SHA-256 dan algoritma RSA.

1.4 Manfaat Penelitian

Manfaat penelitian ini adalah:

1. Manfaat Teoritis

   Secara teoritis hasil dari penelitian ini bermanfaat bagi bidang kriptografi mengenai implementasi penggunaan algoritma SHA-256 dan RSA pada aplikasi *e-voting*.
2. Manfaat Praktis

   Secara praktis penelitian ini menghasilkan *prototype* aplikasi *e-voting* berbasis web yang menggunakan algoritma SHA-256 dan RSA sebagai sistem pengamanannya.