# BAB I

# PENDAHULUAN

## 1.1 Latar Belakang

Sistem keamanan *e-voting* terus dikembangkan sehingga telah banyak negara yang menggunakan sistem *e-voting* sebagai pengganti sistem pemungutan suara manual yang lebih lambat dan rentan terhadap kecurangan. *E-voting* dapat menjanjikan hasil suara dapat diperoleh dengan cepat dan mudah, serta mengurangi kemungkinan kesalahan penghitungan suara. Negara Yang mengunakan sistem *e-voting* yaitu Brazil, India, Swiss dan Australia. Indonesia sendiri *e-voting* bertujuan untuk implementasi undang-undang ITE sehingga selaras dengan Undang-Undang Dasar Tahun 1945.[1]

Namun, sistem e-*voting* juga memiliki kesulitan tersendiri, terutama dalam hal keamanan informasi. Karena secara online, sistem *e-voting* dapat rentan terhadap serangan *cyber* dan kebocoran data. Oleh karena itu, penting untuk menjamin bahwa sistem *e-voting* yang digunakan aman dan terlindungi dari ancaman *siber*.

Keamanan merupakan aspek penting dari setiap sistem dan harus diberikan prioritas yang tinggi. Ketika keamanan diabaikan, sistem rentan terhadap berbagai serangan yang dapat mengancam integritasnya. Hal ini juga berlaku pada sistem *e-voting*. Untuk menjaga kerahasiaan data, terutama data pribadi yang hanya diketahui oleh pihak yang berwenang, perlindungan data dengan sistem keamanan yang unggul menjadi prioritas utama dari pengembang sistem. Agar *sistem e-voting* terlindungi dari serangan siber dan kecurangan, diperlukan penggunaan teknologi yang dapat meningkatkan keamanan informasi, salah satunya adalah *kriptografi.*

Secara umum, *Kriptografi* adalah seni dan bidang ilmu yang bertujuan untuk menjaga kerahasiaan pesan dengan menggunakan teknik yang memastikan bahwa data tidak dapat dibaca oleh orang yang tidak memiliki akses yang sah. Dalam konteks sistem *e-voting, kriptografi* digunakan untuk mengamankan data sensitif seperti identitas pemilih, suara yang diberikan, dan hasil pemilihan dari akses yang tidak diizinkan atau manipulasi.[2]

Penerapan *kriptografi* bertujuan untuk melindungi semua informasi yang tidak boleh diketahui oleh pihak yang tidak berwenang dengan cara mengenkripsinya. Selain itu, penggunaan *kriptografi* juga dapat meningkatkan kerahasiaan dalam komunikasi, karena pesan yang disampaikan menjadi sulit untuk dipahami oleh orang yang tidak memiliki kunci dekripsi yang tepat. Dengan adanya *kriptografi,* informasi tidak hanya disembunyikan, tetapi juga disamarkan sehingga tidak dapat diakses oleh individu yang tidak memiliki hak yang sah untuk mengaksesnya.

Pada penelitian ini *kriptografis* yang dipakai pada *e-voting* dalam membangun sistem keamanan menggunakan algoritma *simetris* yaitu algoritma *one time pad* dan *kriptografis* fungsi hash yang digunakan adalah SHA *256*. Kemudian diperkuat dengan sistem *fingerprint,* dimana saat pemilih melakukan login dan menentukan pilihannya menggunakan *fingerprint*.

Fungsi *hash* adalah fungsi matematika yang mengubah data *digital* apapun menjadi *string* keluaran dengan jumlah karakter tetap. *Hasting* adalah tindakan satu arah untuk mengubah data (disebut pesan) menjadi output (disebut *hash*). Fungsi *hash* adalah alat dasar *kriptografi* modern yang digunakan dalam keamanan informasi untuk meng*autentikasi* transaksi, pesan, tanda tangan *digital*. dan *integritas* data, karena memiliki beberapa sifat yang bertujuan mengamankan data Sehingga sesuai dengan yang dibutuhkan pada sistem *e-voting*. Pada penelitian ini digunakan algoritma SHA generasi kedua yaitu Algoritma *SHA-256* sebagai pelindung keamanan data sebab pada algoritma SHA generasi pertama atau SHA-1 masih rentan terhadap serangan tabrakan. Artinya, nilai *hash* yang sama dapat dihasilkan dari input yang berbeda, sehingga berpotensi memungkinkan penyerang membuat kata sandi satu kali yang valid untuk akses yang tidak sah.

Sementara algoritma *OTP* adalah password valid atau *verification code* yang hanya berlaku untuk sekali login atau transaksi. Kegunaan OTP adalah menghindari sejumlah kekurangan yang terkait dengan kata sandi *statis*. Berbeda dengan kata sandi *statis,* OTP tidak rentan terhadap serangan-serangan seperti serangan *replay.* Jadi meskipun penyusup yang sudah berhasil merekam OTP tidakakan dapat menggunakannya karena OTP tersebut sudah tidak lagi berlaku.

Berdasarkan data awal hasil *observasi* lapangan, di Desa Perupuk Kecamatan

Tanjung Pura Kabupaten Langkat dengan jumlah DPT pada pilkades sebanyak 2091 orang. Pada pilkades tahun 2022 di Desa Perupuk data pemilih di lima TPS yang hadir berjumlah 1.538 yang hadir dan yang tidak hadir berjumlah 553 orang. Pemungutan dan perhitungan suara pilkades di Desa Perupuk Kecamatan Tanjung Pura Kabupaten Langkat dilakukan dengan cara *konvensional* Pemilihan *konvensional* dapat menimbulkan berbagai masalah, baik dalam keamanan data juga memakan waktu serta memiliki biaya operasional yang banyak, namun masalah masalah ini dapat di minimalisasi dengan cara mengganti dengan sistem *E-voting*. *E-voting* adalah sistem pemungutan suara yang memanfaatkan teknologi informasi untuk memfasilitasi pemilih dalam memberikan suaranya dan untuk menghitung suara secara cepat dan akurat. Tujuan utamanya adalah untuk mempercepat dan mempermudah proses pemilihan, termasuk dalam pemilihan kepala desa (pilkades), dengan menggunakan perangkat elektronik seperti komputer. Berdasarkan pembahasan masalah di atas menjadi dasar untuk penulis menjalankan penelitian ini.

## 1.2 Rumusan Masalah

Berdasarkan uraian latar belakang di atas maka dirumuskan beberapa masalah, yaitu:

1. Bagaimana merancang sistem keamanan *e-voting* sehingga dapat menjamin kerahasiaan hasil pemungutan suara.
2. Apakah mungkin untuk mengembangkan sistem keamanan e-voting yang unggul dan dapat menjamin hasil pemungutan suara dengan menggunakan algoritma *one time pad* dan kriptografi fungsi *hash* SHA 256 yang selanjutnya dapat digunakan untuk penyelenggaraan pilkades di desa Paya Perupuk Kecamatan Tanjung Pura Kabupaten Langkat?
3. Apakah pada pengujian yang dilakukan terhadap sistem keamanan *e-voting* dalam penelitian ini memenuhi komponen komponen penting dari keamanan *e-voting*?

## 1.3 Batasan Masalah

Batasan masalah yang dibahas Pada Penelitian ini adalah :

1. Penelitian ini dimaksudkan untuk merancang sistem keamanan *e-voting* pada

pemilihan Kepala Desa di Desa Paya Perupuk Kecamatan Tanjung Pura Kabupaten Langkat.

2. Keamanan sistem *e-voting* yang dirancang dhanya untuk melindungi hasil pemungutan suara.
3. Algoritma yang dipakai untuk keamanan *e-voting* adalah dengan menerapkan fumgsi *hash SHA-256* dan algoritma *ome time pad.*

## 1.4 Tujuan Penelitian

Tujuan yang ingin dicapai dari penulisan tugas akhir ini adalah :

1. Merancang sistem *e-voting* yang unggul dari segi keamanan hasil pemungutan suara agar dapat digunakan pada pelaksanaan pilkades di desa Paya Perupuk Kecamatan Tanjung Pura Kabupaten Langkat, untuk mengurangi beberapa kelemahan dari sistem yang selama ini digunakan.
2. Menerapkan *kriptografi* fungsi *hash* SHA 256 dan algoritma *one time pad* dalam merancang keamanan *e-voting* untuk menghindari kecurangan dalam pelaksanaan pilkades Paya Perupuk Kecamatan Tanjung Pura Kabupaten Langkat.

## 1.5 Manfaat Penelitian

Adapun Manfaat yang ingin dicapai dari penelitian tugas akhir ini adalah sebagai berikut :

1. Hasil penelitian ini dapat memberikan gambaran mengenaiDesain Dan *Implementasi* Sistem Keamanan *E-voting* Menggunakan Fungsi *Hash Dan* Algoritma *One Time Pad.*
2. Dengan adanya sistem keamanan pada *E-voting,* kecurangan yang sering terjadi dalam pilkades dapat dihindari dan terdeteksi dengan cepat.
3. Hasil penelitian ini bisa dijadikan saran untuk pihak pemerintah, dan semua pihak yang terlibat mengenai Desain Dan Implementasi Sistem *E-voting.*