

BAB I

PENDAHULUAN

1.1 Latar Belakang Penelitian

Perkembangan teknologi menjadi pemicu untuk berpikir lebih maju, dengan demikian manusia menginginkan segala sesuatu dilaksanakan dengan cepat dan tepat. Teknologi informasi merupakan teknologi yang dibangun dengan basis utama teknologi komputer. Untuk mempermudah kegiatan transaksional sehari-hari, perkembangan teknologi informasi memberikan dampak besar pada kebiasaan penggunaan *Website*.

Universitas Muhammadiyah Sukabumi memiliki 51 Ormawa yang di mana setiap oramawa memiliki program kerja wajib tahunan salah satunya pemilihan ketua ormawa. Ada beberapa pemilihan ketua ormawa diantaranya pemilihan Presiden Mahasiswa, pemilihan Gubernur Fakultas, pemilihan ketua himpunan dan pemilihan ketua UKM. Pemilu ketua ormawa yang diikuti oleh seluruh mahasiswa universitas muhammadiyah secara serentak adalah pemilihan Presiden Mahasiswa Universitas Muhammadiyah Sukabumi. Terhitung dari 2004 sampai dengan 2017 pelaksanaan pemillihan Presiden Mahasiswa Universitas Muhammadiyah Sukabumi telah dilaksanakan sebanyak 14 kali.

Berdasarkan data yang didapatkan dalam kurun waktu 2 tahun ke belakang, pada tahun 2016 dengan jumlah 3.200 mahasiswa aktif, jumlah partisipan atau suara masuk dari mahasiswa untuk pemilihan hanya 1.175 dipersentase 36.71% dari jumlah mahasiswa aktif. Kemudian pada tahun 2017 dengan jumlah 3.800 mahasiswa aktif, jumlah partisipan atau suara masuk dari mahasiswa untuk pemilihan hanya 1.436 dipersentase 37.78% dari jumlah mahasiswa aktif. Data tersebut didapatkan dari sistem pemilihan yang dilakukan secara konvensional dengan KPU (Komisi Pemilihan Umum) sebagai panitia pelaksananya. Pemilihan konvensional yaitu pemilihan yang

menggunakan kertas suara sebagai alat pemilihan, dengan cara mencoblos surat suara tersebut berdasarkan nomor urut atau pasangan calon di dalam bilik suara. Pemilihan dilaksanakan di kampus Universitas Muhammadiyah Sukabumi, yang tentunya menuntut pemilik hak suara datang ke kampus untuk menyalurkan suaranya.

Berdasarkan hal tersebut terdapat mahasiswa yang tidak menyalurkan suaranya dikarenakan berbagai alasan yang tidak memungkinkan untuk berpartisipasi. Saat pemilihan berlangsung, panitia bertugas menjadi penunjuk tata cara pemilihan. Salah satu tugas panitia adalah mendata mahasiswa aktif dengan cara meminta data ke setiap fakultas dan merekap data menggunakan bantuan Microsoft Excel. Hal tersebut membuat kesulitan dari kedua belah pihak yakni, mahasiswa yang ingin melakukan pemilihan harus mengantri dan menunggu datanya yang dicari dalam buku daftar mahasiswa, selain itu banyak juga mahasiswa yang tidak menyalurkan suara dengan alasan tidak ingin mengantri atau ada jam kuliah saat pemilihan berlangsung. Panitia penyelenggara pemilihan atau KPU mengalami kesulitan jika mahasiswa yang ingin melakukan pemilihan jumlahnya banyak dalam satu waktu. Hasil akhir pemilihan juga tidak segera diketahui oleh seluruh mahasiswa karena lamanya proses perhitungan data hasil pemilihan, dimana dalam proses perhitungan suara panitia harus memeriksa satu persatu surat suara untuk melihat sah atau tidaknya surat suara, karena hal ini untuk perhitungan suara ulang sangat sulit dilakukan karena pemeriksaan surat suara harus dimulai dari awal kembali. Dan kemungkinan ketidaksesuaian data jumlah pemilih, jumlah suara masuk dan jumlah suara tidak masuk. Hal ini sering dijadikan bahan perdebatan di akhir proses pemilihan antara masing-masing tim sukses pasangan calon Presma karena target mereka tidak tercapai.

Berdasarkan permasalahan tersebut, adapun usaha untuk mengurangi kendala-kendala di atas dari KPU adalah dengan menambah jumlah jam dan hari pemilihan serta penambahan panitia yang bertugas, namun solusi tersebut belum menunjukkan hasil yang signifikan. Pemilihan konvensional tersebut menggunakan anggaran dana

kampus yang cukup besar, karena harus membeli perlengkapan pemilu seperti membeli kertas, *print out* surat suara, dan peralatan yang dibutuhkan dalam pemilihan.

Kendala-kendala yang telah disampaikan, dibutuhkan suatu sistem pemilihan elektronik yang dapat mempermudah, mempercepat, meningkatkan jumlah pemilih pada pelaksanaan pemilihan Presiden Mahasiswa Universitas Muhammadiyah Sukabumi dan mengamankan data hasil suara pemilihan dengan menggunakan keamanan data berupa kriptografi . Kriptografi merupakan salah satu solusi atau metode pengamanan data yang tepat untuk menjaga kerahasiaan dan keaslian data, serta dapat meningkatkan aspek keamanan suatu data atau informasi. Metode ini bertujuan agar informasi yang bersifat rahasia tidak dapat diketahui atau di manfaatkan oleh orang atau pihak yang tidak bekepentingan. Kriptografi mendukung kebutuhan dua aspek keamanan informasi, yaitu perlindungan terhadap kerahasiaan data informasi dan perlindungan terhadap pemalsuan dan perubahan informasi yang diinginkan.

Untuk itu perlu adanya sistem pemilihan yang terbaru, dalam hal ini adalah pemanfaatan teknologi informasi berbasis *Website* sebagai pusat informasi dan penyimpanan data pemilihan elektronik. Proses pemilihan elektronik sama dengan proses pemilihan konvensional di mana satu mahasiswa memiliki satu kali hak pemilihan yang sah dengan menggunakan NIM (Nomor Induk Mahasiswa) yang dijadikan kata kunci sebagai acuan hak pemilihan dari mahasiswa.

Hasil dari pemilihan presiden mahasiswa Universitas Muhammadiyah Sukabumi yang berupa jumlah hasil suara dari seluruh mahasiswa yang melakukan pemilihan, data ini sangat penting untuk di jaga keamannya. Proses mengamankan data dapat di lakukan dengan menggunakan beberapa algoritma keamanan diantaranya menggunakan algoritma keamanan OTP (*One Time pad*) merupakan algoritma pengenkripsian data dan informasi yang relatif sederhana dan mudah digunakan namun cukup aman dalam menjamin kerahasiaan informasi atau data yang ingin dikirimkan, dan sistem OTP ini tiadk dapat di pecahkan karena merupakan algoritma

pengkripsian data dan informasi yang relatif sederhana dan mudah digunakan namun cukup aman dalam menjamin kerahasiaan informasi atau data yang ingin dikirimkan. Selain algoritma OTP (*One Time pad*) ada juga algoritma keamanan DES yang memiliki kelebihan yaitu memiliki struktur enkripsi dan dekripsi yang sama. Hanya saja dekripsi menggunakan kunci ronde dalam urutan terbalik. Dalam penerapan enkripsi DES sebuah iterasi (pengulangan) digunakan untuk mempersentasikan perhitungan teks tengah untuk setiap ronde.

Berdasarkan penelitian yang ada sebelumnya, pada sistem pemilihan ini menggunakan fungsi algoritma *Advanced Encrypt Standard* (AES) sebagai sistem keamanan data hasil *voting*. Algoritma *Advanced Encrypt Standard* (AES) Merupakan Algoritma *chiper* yang cukup aman untuk melindungi data atau informasi yang bersifat rahasia dan salah satu keamanan data yang penerepannya dalam sistem pemilihan ini memiliki 5 aspek yaitu : aspek kerahasiaan, aspek keutuhan data, aspek ketersediaan, aspek otentikasi, Algoritma AES adalah algoritma kriptografi yang dapat mengenkripsi dan mendekripsi data dengan panjang kunci yang bervariasi, yaitu 128 bit, 192 bit, dan 256 bit, pada 2017 telah dibuat aplikasi *E-voting* untuk pemilihan Presiden Mahasiswa Universitas Muhammadiyah Sukabumi. Namun tidak di lengkapi dengan sistem keamanan. Sehingga perlu adanya sistem keamanan.

Berdasarkan latar belakang masalah di atas, maka penulis bermaksud melakukan penelitian dengan judul **“Pemilihan Presiden Mahasiswa Berbasis Website dengan Menggunakan Keamanan Algoritma *Advanced Encrypt Standard* (AES) (Studi Kasus di Universitas Muhammadiyah Sukabumi)”**.

1.2 Identifikasi Masalah

Berdasarkan latar belakang masalah di atas maka permasalahan yang dapat dibahas meliputi:

1. Mahasiswa melakukan pemilihan di kampus dan antrian mahasiswa yang begitu banyak, sehingga memerlukan waktu yang lama sehingga mengurangi mahasiswa untuk menyalurkan hak suaranya.

2. Proses perhitungan suara menyita waktu yang cukup lama karena surat suara harus diperiksa satu persatu, serta sulitnya melakukan perhitungan ulang jika ada pihak yang tidak mempercayai hasil akhir, Jika pemilihan dilakukan secara elektronik berbasis *Website* tidak menutup kemungkinan kejahatan di dunia internet atau *Hacker* akan bermunculan yang akan mengetahui data rahasia dari sistem pemilihan ini.
3. Pemberian informasi jumlah pemilihan yang masih lambat karena diumumkan pada akhir pemilihan dan masih ada ketidak akuratan data pemilihan.
4. Menggunakan anggaran dana yang cukup besar karena harus membeli kertas dan *print out* surat suara yang begitu banyak.

1.3. Tujuan Penelitian

Berdasarkan identifikasi masalah di atas dapat dirumuskan tujuan penelitian ini yaitu sebagai berikut:

1. *Website* pemilihan Presiden Mahasiswa ini digunakan oleh seluruh mahasiswa aktif Universitas Muhammadiyah Sukabumi dan dilakukan dimana saja menggunakan *Website*.
2. Membantu petugas KPU dalam menghitung hasil pemilihan secara cepat dan mengurangi resiko tercadinya kecurangan, dengan mengamankan kerahasiaan data hasil suara dan perlindungan terhadap pemalsuan dan perubahan informasi yang diinginkan, dengan Algoritma AES (*Advanced Encrypt Standard*) sehingga data suara hasil pemilihan tidak dapat diketahui secara nominal angka atau di manfaatkan oleh orang atau pihak yang tidak bekepentingan.
3. Implementasi sistem berupa *Website* dibuat menggunakan Bahasa pemrograman PHP, serta memanfaatkan MySQLi sebagai basis data.
4. Mengurangi pengeluaran anggaran kampus, untuk melakukan pemilihan Presiden Mahasiswa ini.

1.4 Manfaat Penelitian

Berdasarkan penelitian ini manfaat yang akan dicapai adalah sebagai berikut.

1. Bagi Universitas Muhammadiyah Sukabumi
Menjadi inovasi baru dalam bidang teknologi berupa *Website* yang berfungsi secara *realtime*, dan mengurangi anggaran pengeluaran Kampus,
2. Bagi Komisi Pemilihan Umum
Untuk membantu kelancaran dan mempercepat kinerja KPU dalam proses pemilihan Presiden Mahasiswa di Universitas Muhammadiyah Sukabumi. Dengan Algoritma AES (*Advanced Encrypt Standard*) membantu pihak KPU mengamankan data hasil pemilihan.
3. Bagi Mahasiswa
Memudahkan mahasiswa untuk menyalurkan hak suaranya, karena dengan adanya *Website* Pemilu, mahasiswa bisa menyalurkan hak suara dimana dan kapan saja sesuai ketentuan yang berlaku.
4. Bagi Penulis
Agar penulis dapat mendalami pemrograman berbasis *Website* dan kriptografi khususnya kriptografi AES (*Advanced Encrypt Standard*) sehingga bisa menerapkan ilmu yang di dapat selama menempuh pendidikan di bangku kuliah dalam skripsi ini.

1.5 Batasan Masalah Penelitian

Untuk memudahkan dalam pembahasan masalah yang akan dibahas, maka batasan masalah pada penelitian ini adalah:

1. Mahasiswa melakukan Pemilihan Presiden Mahasiswa menggunakan *Website*. karena pemilihan dapat dilakukan dimana saja.
2. Mempercepat perhitungan suara, sehingga hasil pemilihan Presiden Mahasiswa dapat segera diketahui mahasiswa ketika waktu pemilihan ditutup, karena perhitungan suara dilakukan otomatis di dalam sistem, dan

keamanan data suara hasil pemilihan menggunakan algoritma AES (*Advanced Encrypt Standard*) 256 bit

3. Memberikan informasi jumlah pemilih, jumlah suara masuk dan jumlah suara yang tidak masuk secara akurat dan *up to date* pada pemilihan Presiden Mahasiswa. Karena semua informasi tersebut akan ditampilkan di dalam *Website*.
4. Mengurangi pengeluaran anggaran kampus, karena tidak harus mengeluarkan biaya untuk membeli perlengkapan dan peralatan kebutuhan dalam pemilihan ketua Ormawa.

1.6 Sistematika Penulisan

Uraian singkat pada masing-masing bab adalah sebagai berikut:

BAB I Pendahuluan

Membahas latar belakang masalah, identifikasi masalah, tujuan penelitian, manfaat penelitian, batasan penelitian dan sistematika penulisan.

BAB II Studi Pustaka

Memaparkan konsep umum diantaranya kajian islam yang terkait dan pengertian-pengertian yang terkait judul penelitian, memaparkan konsep analisis dan perancangan, bahasa pemrograman dan *tools* yang digunakan, konsep pengujian serta studi terdahulu yang terkait dengan penelitian yang didapat dari sumber-sumber yang digunakan sebagai panduan dalam penelitian dan penyusunan laporan

BAB III Metodologi Penelitian

Berisikan memaparkan langkah-langkah penelitian, pengumpulan data, analisis sistem, perancangan sistem, implementasi sistem, pengujian sistem serta menguraikan tempat dan waktu penelitian.

BAB IV Analisis dan Perancangan

Berisikan uraian tentang masalah apa saja yang dihadapi, bagaimana cara untuk mengatasi masalah, serta bagaimana perancangan program yang akan dibuat agar sesuai dengan kebutuhan.

BAB V Implementasi dan Pengujian

Berisikan implementasi dari hasil perancangan sistem dan menjelaskan jalannya proses pengujian sistem.

BAB VI Kesimpulan dan Saran

Berisikan kesimpulan yang didapat dari hasil penelitian dan saran agar ke depannya penelitian bisa dikembangkan kearah yang lebih baik.