BAB I

PENDAHULUAN

1.1. Latar Belakang

Perkembangan dunia teknologi informasi dan komunikasi (TIK) yang pesat mengubah aktivitas manusia menjadi lebih mudah. Dalam hal berkomunikasi, sekarang masyarakat bisa berkomunikasi jarak jauh dengan menggunakan telepon maupun media internet. Dalam hal perbankan, masyarakat dimudahkan dalam hal bertransaksi dengan adanya *ATM* maupun *e-banking*.

Begitu pula dalam bidang politik, dengan adanya perkembangan dunia TIK, hal ini dapat membuat sistem voting konvensional berubah menjadi sistem voting yang menggunakan teknologi komputer atau yang sering disebut dengan *electronic voting* (*e-voting*). Terdapat banyak keuntungan dari sistem *e-voting* dibandingkan dengan sistem voting konvensional, yaitu proses penghitungan suara menggunakan komputer sehingga proses menjadi lebih cepat dan akurat. Proses tersebut menyebabkan berkurangnya waktu penghitungan dan mengurangi kekhawatiran terjadinya kesalahan yang dilakukan oleh manusia. Selain itu, dengan menggunakan sistem *e-voting* ini biaya pelaksanaan *e-voting* dapat dikurangi karena tidak menggunakan bahan satu kali pakai seperti kertas sebagai media pemilihan dan juga tidak memerlukan biaya pendistribusian kertas suara.

Perkembangan internet yang pesat, menjadikan internet mudah digunakan dan dijangkau oleh semua orang. Namun hal tersebut membawa dampak bagi keamanan informasi maupun pesan yang menggunakan internet. Informasi menjadi sangat rentan untuk diketahui, diambil, dan dimanipulasi oleh pihak-pihak yang tidak berkepentingan.

Dalam *e-voting*, masalah keamanan juga merupakan masalah mendasar yang tidak bisa dilupakan. Selain masalah keamanan yang tidak bisa dijamin,

terdapat masalah lain untuk penerapan e-voting di Indonesia, yaitu infrastruktur yang belum merata dan masih banyak masyarakat yang gagap teknologi (Rahman,2012).

Ada 4 (empat) persyaratan agar system *e-voting* dapat dipercaya oleh masyarakat yaitu *secure* (aman/terjamin), *accurate* (akurat), *re-countable* (dapat dihitung kembali), dan *accessible* (kemudahan untuk mengakses) (Oriez, 2004). Salah satu syarat tersebut yaitu *secure* terkait dengan keamanan informasi selama pelaksanaan *e-voting* (Agustina & Kurniati, 2009).

Untuk memenuhi aspek-aspek keamanan informasi pada sistem, diperlukan metode yang dapat menjaga keamana informasi tersebut. Metode yang dimaksud adalah kriptografi. Terdapat beberapa protokol kriptografi yang digunakan untuk sistem *e-voting* yang dijelaskan oleh Scheiner (1996). Protokol tersebut adalah *Single Central Facility* dan *Two Central Facilities*.

Pada penelitian kali ini, sistem *e-voting* menggunakan protokol *Two Central Facilites*. Pada penelitian sebelumnya, Janga Shireesha dan So-In Chakchai (2005) menjelaskan bahwa protokol Two Central Facilities yang dimodifikasi memenuhi semua persyaratan online voting yang aman. Dan untuk menjaga keamanan data pada saat pengiriman, penelitian kali ini juga menambahkan penggunaan dua algoritma kriptografi sebagai kombinasi keamanan dari sistem *e-voting*.

Algoritma pertama yang digunakan adalah algoritma simetris, yaitu AES. Penggunaan algoritma AES ini karena memiliki tingkat keamanan yang cukup tinggi. Hal ini berdasarkan penelitian yang dilakukan oleh A. Raji Reddy (2011) yang menyatakan bahwa AES memiliki keamanan yang lebih tinggi dari MARS. Dan juga berdasarkan penelitian dari M.Anand Kumar (2012) yang melakukan penelitian tentang efisiensi dari algoritma Blowfish dan AES. M. Anand Kumar menjelaskan bahwa pada saat sistem membutuhkan keamanan yang tinggi, AES dapat digunakan dibandingkan Blowfish yang memiliki performa yang lebih bagus namun tingkat keamanannya masih dibawah AES. Namun terdapat kekhawatiran dalam proses pendistribusian kunci dari algoritma AES. Karena jika kunci tersebut diketahui oleh pihak lain, maka pihak tersebut bisa mengetahui data

yang dikirimkan.

Untuk algoritma kedua, digunakan algoritma asimetris, yaitu algoritma RSA. Seperti yang dijelaskan Evgeny (2009), Algortima RSA memiliki keamanan yang lebih tinggi dari algoritma simetris namun membutuhkan waktu yang lama dalam pengerjaan prosesnya.

Untuk menutupi kekurangan masing-masing algoritma, maka algoritma RSA hanya digunakan untuk mengirimkan kunci dari algoritma AES secara aman. Sedangkan algoritma AES digunakan untuk proses enkripsi dan dekripsi terhadap data yang dikirimkan, seperti yang dilakukan oleh Palanisamy (2011).

Pada penelitian yang dilakukan Dan DuFeu dan Jon Haris (2001), Janga Shireesha dan So-In Chakchai (2005) dan Wardhani (2009), algoritma yang digunakan adalah RSA dan *Blowfish*. Sehingga masih memiliki tingkat keamanan yang lebih rendah dibandingkan dengan menggunakan algoritma AES dan RSA.

Kombinasi algoritma AES dan RSA telah digunakan pada penelitian yang dilakukan oleh Erick Priyanggodo, Alfian Prayanta, dan Fitrah (2012), namun penelitian yang dilakukan adalah pengecekan pengaruh kombinasi AES dan RSA terhadap *running time* pada saat pengiriman hasil suara ke CTF. Sedangkan pada penelitian kali ini, penelitian dilakukan untuk melihat pengaruh kombinasi algoritma AES dan RSA terhadap sistem e-voting berdasarkan tujuan kriptografi.

Jadi pada penelitian kali ini, sistem *e-voting* dibuat dengan menggunakan protokol Two Central Facilities, dengan menggunakan algoritma AES untuk enkripsi data yang dikirimkan dan algoritma RSA untuk enkripsi kunci dari algoritma AES. Selain itu, pada penelitian kali ini AES juga digunakan untuk proses enkripsi terhadap data yang disimpan ke dalam database. Hal tersebut dilakukan untuk mencegah pencurian maupun pengubahan informasi di dalam database oleh pihak yang tidak bertanggung jawab yang melakukan pengaksesan ke dalam database secara langsung.

1.2. Rumusan Masalah

Rumusah masalah dalam penelitian ini adalah :

1. Bagaimana peran protokol Two Central Facilities dalam memenuhi kriteria yang harus dimiliki sistem *e-voting* yang dijelaskan oleh Scheiner.
2. Bagaimanakah pengaruh algoritma AES dan RSA pada sistem e-voting berdasarkan tujuan kriptografi, yaitu *confidentially* (kerahasiaan), *data* integrity (integritas data), *authentication* (autentikasi), dan *non*-repudiation (nir-penyangkalan).

1.3. Batasan Masalah

Batasan masalah yang diteliti antara lain adalah :

1. Sistem ini difokuskan pada proses pemungutan suara berlangsung.
2. Protokol yang digunakan adalah *Two Central Facilities* yang dikembangkan oleh Dan Dufeu dan Jon Harris.
3. Algoritma kriptografi yang digunakan adalah AES dan RSA.

1.4. Tujuan Penelitian

Sejalan dengan permasalah yang telah dirumuskan, maka tujuan yang ingin dicapai pada penelitian ini adalah :

1. Membangun sistem *e-voting* menggunakan protokol *Two Central Facilities* yang sesuai dengan kriteria yang harus dimiliki sistem *e-voting.*
2. Implementasi algoritma AES dan RSA pada sistem e-voting dan pengaruhnya terhadap sistem secara keseluruhan berdasarkan tujuan kriptografi, yaitu *confidentially* (kerahasiaan), *data integrity* (integritas data), *authentication* (autentikasi), dan *non-repudiation*

(nir-penyangkalan).

1.5. Sistematika Penulisan

Dalam penyusunan skripsi ini, sistematika penulisan dibagi menjadi beberapa bab sebagai berikut:

BAB I PENDAHULUAN

Bab ini menguraikan tentang latar belakang masalah, rumusan masalah, maksud dan tujuan, batasan masalah, metode penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini memaparkan beberapa teori yang mendukung dalam pembuatan perangkat lunak seperti, *E-Voting*, Kriptografi, Algoritma RSA, Algoritma AES, protokol, protokol *Two Central Facilities*, *CLA, dan CTF*.

BAB III METODOLOGI PENELITIAN

Bab ini merupakan penjabaran dari implementasi algoritma RSA dan AES pada sistem *e-voting* yang menggunakan protokol *Two Central Facilities*. Mencakup analisis, dan desain model sistem.

BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Pada bab ini akan dibahas secara mendalam mengenai hal-hal yang dilakukan selama penelitian berlangsung, mulai dari proses modifkasi protokol *Two Central Facilities*, pembangunan perangkat lunak, hingga proses pengujian protokol *Two Central Facilities* dan algoritma AES dan RSA yang akan digunakan untuk menjawab apa yang sudah dirumuskan dalam rumusan masalah.

BAB V KESIMPULAN DAN SARAN

Pada bab ini berisi tentang kesimpulan dari BAB IV dan saran yang diajukan agar dapat menjadi bahan pertimbangan untuk rekomendasi penelitian selanjutnya.