BAB I
PENDAHULUAN

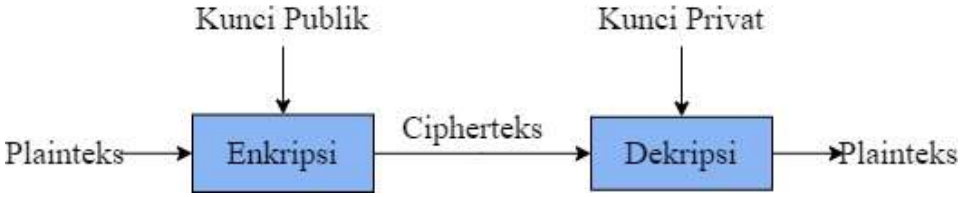
1.1. Latar Belakang

E-voting adalah kegiatan penyelenggaraan pemungutan suara elektronik secara digital, yang dimulai dari proses pendaftaran, pelaksanaan, penghitungan sampai dengan pengiriman hasil perolehan suara. E-voting telah menjadi topik populer diseluruh dunia, termasuk di Indonesia. Di era digital saat ini, sudah ada beberapa negara yang menggunakan e-voting sebagai media pemungutan suara dalam pemilihan presiden atau ketua organisasi (Hermawati, 2023). E-voting dikenal secara luas oleh masyarakat adalah Pemilu (Pemilihan Umum) atau Pilkada (Pemilihan Daerah), namun e-voting yang dikenal dengan skala kecil digunakan untuk pemilihan presiden atau ketua organisasi internal kampus dan perguruan tinggi lainnya (Angriani, 2019). E-voting memiliki kelebihan dalam pemilihan suara, menggunakan e-voting dapat mempercepat proses pemilihan, mengurangi biaya pemilihan dan meningkatkan akurasi dengan tepat dalam proses pemilihan (Yafi et al., 2023). E-voting juga memudahkan pemilih untuk menggunakan hak pilihnya tanpa harus menunggu antrian yang lama (Pramadipta, 2024).

Namun, sistem e-voting memiliki permasalahan atau tantangan, terutama dalam segi keamanan dan kerahasiaan data. Karena e-voting yang sifat sistemnya online, sistem tersebut rentan terhadap serangan *cyber* yang dapat memanipulasi dan membocorkan data. Oleh karena itu, pentingnya menerapkan keamanan pada sistem aplikasi e-voting guna melindungi dari serangan *cyber* (Hermawati, 2023). Keamanan merupakan aspek penting dalam melindungi sebuah sistem, karena tanpa keamanan, sistem akan menjadi target *cyber* untuk merentas data sistem tersebut. Dengan keamanan, data aplikasi e-voting tidak akan bisa direntas oleh pihak yang tidak bertanggung jawab atau *cyber* (Silalahi and Sindar, 2020). Untuk memastikan bahwa data sistem tersebut aman, maka diperlukan metode yang dapat digunakan untuk mengatasi permasalahan tersebut (Fatonah, 2022). Salah satu metode yang dapat digunakan untuk mengatasi permasalahan tersebut adalah metode kriptografi (Hermawati, 2023).

Kriptografi adalah metode yang bergerak dibidang teknologi informasi untuk mengamankan data yang bersifat pribadi atau rahasia (Ungkawa et al., 2021). Kriptografi memiliki dua jenis algoritma, yaitu algoritma simetris dan algoritma asimetris. Algoritma simetris adalah metode kriptografi yang menggunakan satu kunci yang sama untuk melakukan enkripsi dan dekripsi, sedangkan algoritma asimetris adalah metode kriptografi dengan menggunakan dua kunci yang berbeda untuk mengenkripsi maupun dekripsi (Arif and Nurokhman, 2023). Contoh algoritma simetris, yaitu *Data Encryption Standard (DES)*, *Advanced Encryption Standard (AES)* dan lainnya, algoritma asimetris, yaitu *Rivest Shamir Adleman (RSA)*, *Digital Signature Algorithm (DSA)* dan lainnya (Fatonah & Mulyana, 2022). Algoritma asimetris mempunyai keunggulan dari tingkat keamanan yang baik, karena menggunakan dua kunci untuk enkripsi dan dekripsi (Kasus et al., 2021).

Berikut adalah gambar proses enkripsi dan dekripsi algoritma asimetris



Gambar 1. 1 Proses Algoritma Asimetris

Dalam hal ini, peneliti menggunakan algoritma RSA sebagai metode pengamanan data dalam database pada sistem aplikasi e-voting tersebut. Pada tahun 1977 Algoritma RSA dikembangkan oleh tiga orang peneliti dari *MIT (Massachussets Institute of Technology)* yaitu Ron Rivest, Adi Shamir dan Leonard Adleman, yang dimana nama algoritma RSA adalah inisial dari nama belakang ketiga peneliti tersebut (Rizki and Ariyani, 2021). Pengertian lain algoritma RSA adalah teknik kriptografi menggunakan kunci yang berbeda untuk melakukan enkripsi dan dekripsi. Kunci untuk melakukan enkripsi disebut dengan kunci publik, sedangkan kunci untuk melakukan dekripsi disebut dengan kunci privat (Liana et al., 2023). Menurut Munir (2023) RSA akan aman jika modulus n cukup besar jika panjang n hanya 256 bit atau kurang, dapat difaktorkan dalam beberapa jam saja dengan sebuah komputer/*PC* dan jika Panjang n adalah 512 bit atau kurang, dapat difaktorkan dengan beberapa ratus komputer. Saat inipanjang kunci RSA yang aman adalah 2048 bit. Dalam proses perhitungan algoritma RSA terdapat tiga tahapan, yaitu pembangkitan kunci *(generate key),* enkripsi *(encryption)* dan deskripsi *(description)* (Dairi, 2022).

1.1.1. Tahapan Pembangkitan kunci

1. Pilih dua bilangan prima yang besar p dan q. Nilai p dan q bersifat rahasia (privat)
2. Hitung nilai $n = p \times q$. Nilai n tidak dirahasiakan sebaiknya $p \neq q$. Karena jika $p = q$ maka $n = p2$ sehingga p didapatkan dengan akar pangkat dua dari n
3. Menghitung $\varphi(n) = (p-1)(q-1)$
4. Memilih kunci publik yang disebut e, relatif prima terhadap φ, artinya faktor pembagi keduanya adalah 1, yang disebut secara matematika $gcd\ (e, \varphi) = 1$
5. Menghitung kunci privat (dekripsi) menggunakan rumus $e.d\ mod\ n = 1$
6. Maka hasil pembentukan kunci publik dan kunci privat adalah (e, n) untuk kunci publik dan (d, n) untuk kunci privat.
7. Nilai n tidak bersifat rahasia karena diperlukan pada saat perhitungan proses ekripsi dan deskripsi.

1.1.2. Tahapan Enkripsi

1. Masukan nilai hasil plainteks.
2. Konversi dalam bentuk UTF-8
3. Masukan kunci publik (e, n)
4. Lakukan perhitungan dengan rumus $C = M^e\ mod\ n$
5. Menemukan cipherteks.

1.1.3. Tahapan Dekripsi

1. Masukan pesan cipherteks yang telah ditemukan.
2. Masukan kunci privat (d, n)
3. Lakukan perhitungan dengan rumus $P = C^d\ mod\ n$
4. Konversi dalam bentuk UTF-8
5. Menemukan hasil deskripsi.

Menggunakan algoritma RSA cukup aman karena algoritma tersebut menggunakan konsep matematika yang menghitung bilangan besar sebagai faktor prima semakin besar angka prima, semakin baik keamanan data terhadap sistem tersebut (Setiawan, 2023).

Penelitian mengenai aplikasi e-voting sudah pernah dilakukan pada penelitian sebelumnya. Menurut penelitian sebelumnya yang dilakukan oleh Setiawan (2023), algoritma RSA dapat mengembangkan sistem e-voting dengan aman dan efektif. RSA yang merupakan algoritma kriptografi

yang terkenal memberikan perlindungan yang kuat terhadap data yang dikirimkan dan disimpan dalam database. Penelitian yang dilakukan oleh Anggoro (2019) membangun sistem keamanan menggunakan algoritma RSA guna menjamin kerahasiaan data hasil pemilihan. Hasil penelitian menunjukkan bahwa algoritma RSA efektif dalam menjaga kerahasiaan data pemilihan pada aplikasi e-voting. Penelitian sebelumnya yang dilakukan oleh Susanto (2022) berhasil mengembangkan aplikasi keamanan pesan teks yang efektif dengan menggunakan algoritma RSA. Penelitian ini memberikan solusi yang aman dan praktis untuk melindungi kerahasiaan pesan teks yang dikirim melalui SMS. Penelitian yang dilakukan oleh Hasbulloh (2022) berhasil mengembangkan dan menerapkan sistem e-voting berbasis web menggunakan algoritma RSA. Sistem ini dirancang untuk meningkatkan keamanan dan efisiensi dalam pemilihan organisasi ikatan pondok pesantren Smart-SIPKOTREN. Didukung oleh penelitian Putra (2021), kombinasi kedua algoritma RSA dan base64 dapat meningkatkan keamanan dan kerahasian data yang lebih terjamin. Kombinasi kedua algoritma tersebut memberikan lapisan tambahan yang signifikan, menjadikan sistem e-voting lebih tahan terhadap berbagai serangan *cyber*.

Berdasarkan pembahasan latar belakang tersebut, penelitian membahas tentang kerentanan data dalam database terhadap aplikasi e-voting dan menerapkan metode kriptografi dengan algoritma RSA untuk mengatasi kerentanan tersebut. Algoritma RSA digunakan untuk melindungi keamanan dan kerahasian data dalam database pada aplikasi e-voting. Dengan menerapkan algoritma RSA, data akan dienkripsi menggunakan kunci publik sebelum dikirim dan hanya dapat didekripsi oleh penerima yang memiliki kunci privat.

1.2 Rumusan Masalah

Berdasarkan penjabaran pada latar belakang diatas, rumusan masalah pada penelitian ini adalah bagaimana mengamankan data suara dalam database pada sistem aplikasi e-voting dengan menerapkan metode kriptografi dengan algoritma RSA.

1.3 Tujuan Penelitian

Tujuan dari penelitian ini menerapkan metode kriptografi dengan algoritma RSA sebagai perlindungan keamanan dan kerahasiaan data suara dalam database pada sistem aplikasi e-voting.

1.4 Manfaat Penelitian

Manfaat dari penelitian ini adalah (i) Meningkatkan keamanan data suara dalam database pada sistem aplikasi e-voting dengan menggunakan kriptografi algoritma RSA. (ii) Meningkatkan kepercayaan *user* bahwa aplikasi e-voting aman untuk digunakan.