KEAMANAN SISTEM DATABASE APLIKASI E-VOTING MENGGUNAKAN METODE KRIPTOGRAFI ALGORITMA RSA *(Rivest Shamir Adleman)*

SKRIPSI

Diajukan oleh:
Dery Dinata
2011102441185

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS MUHAMMADIYAH KALIMANTAN TIMUR
JULI 2024

KEAMANAN SISTEM DATABASE APLIKASI E-VOTING MENGGUNAKAN METODE KRIPTOGRAFI ALGORITMA RSA *(Rivest Shamir Adleman)*

SKRIPSI

Diajukan Sebagai Salah Satu Persyaratan Untuk Memperoleh Gelar Sarjana Komputer Teknik Informatika Sains dan Teknologi Universitas Muhammadiyah Kalimantan Timur

Diajukan oleh:
Dery Dinata
2011102441185

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS MUHAMMADIYAH KALIMANTAN TIMUR
JULI 2024

LEMBAR PERSETUJUAN

KEAMANAN SISTEM DATABASE APLIKASI E-VOTING MENGGUNAKAN METODE KRIPTOGRAFI ALGORITMA RSA *(Rivest Shamir Adleman)*

TUGAS AKHIR/SKRIPSI/TESIS/DISERTASI

Diajukan oleh:

Dery Dinata
2011102441185

Disetujui untuk diujikan
Pada tanggal 30 Juni 2024

Pembimbing

Sayekti Harits Suryawan, S.Kom, M.Kom
NIDN. 1119048901

Mengetahui,
Koordinator Tugas Akhir/Skripsi/Tesis/Disertasi

Abdul Rahim, S.Kom., M.Cs
NIDN. 1115039601

LEMBAR PENGESAHAN

KEAMANAN SISTEM DATABASE APLIKASI E-VOTING MENGGUNAKAN METODE KRIPTOGRAFI ALGORITMA RSA *(Rivest Shamir Adleman)*

SKRIPSI

Diajukan oleh:
Dery Dinata
2011102441185

Diseminarkan dan Diujikan
Pada 08 Juli 2024

Penguji I	Penguji II
Muhammad Taufiq Sumadi, S.Tr.Kom., M.Tr.Kom	**Savekti Harits Suryawan, S.Kom, M.Kom**
NIDN. 1111089501	**NIDN. 1119048901**

Mengetahui,
Ketua
Program Studi Teknik Informatika

Arbansyah, S.Kom., M.TI
NIDN. 1118019203

PERNYATAAN KEASLIAN PENELITIAN

Saya yang bertanda tangan dibawah ini:

Nama	: Dery Dinata
NIM	: 2011102441185
Program Studi	: Teknik Informatika
Judul Penelitian	: KEAMANAN SISTEM DATABASE APLIKASI E-VOTING MENGGUNAKAN METODE RSA *(Rivest Shamir Adleman)*

Menyatakan bahwa tugas skripsi yang saya tulis ini benar-benar hasil karya saya sendiri, dan bukan merupakan hasil plagiasi/falsifikasi/fabrikasi baik sebagian atau seluruhnya. Atas pernyataan ini, saya siap menanggung risiko atau sanksi yang dijatuhkan kepada saya apabila kemudian ditemukan adanya pelanggaran terhadap etika keilmuan dalam tugas skripsi saya ini, atau klaim dari pihak lain terhadap keaslian karya saya ini.

Samarinda, 30 Juni 2024
Yang membuat pernyataan

Dery Dinata
NIM: 2011102441185

ABSTRAK

E-voting adalah pemungutan suara elektronik yang mencakup seluruh proses pemilihan, mulai dari pendaftaran hingga pengiriman hasil suara. Di Universitas Muhammadiyah Kalimantan Timur (UMKT), e-voting telah diterapkan untuk pemilihan ketua dan wakil organisasi internal kampus, termasuk Badan Eksekutif Mahasiswa (BEM). Meskipun e-voting memiliki kelebihan dalam mempercepat proses pemilihan, mengurangi biaya, dan meningkatkan akurasi, sistem ini rentan terhadap serangan siber yang mengancam keamanan dan kerahasiaan data suara. Oleh karena itu, diperlukan langkah-langkah keamanan yang efektif untuk melindungi sistem e-voting. Penelitian ini bertujuan untuk meningkatkan keamanan data suara dalam sistem e-voting di UMKT menggunakan metode kriptografi algoritma RSA. Algoritma RSA menggunakan kunci publik untuk enkripsi dan kunci privat untuk dekripsi, memastikan data suara terenkripsi tidak dapat diakses tanpa melalui proses dekripsi. Metode penelitian mix method digunakan, menggabungkan pendekatan kuantitatif eksperimental dan studi kasus kualitatif. Wawancara dilakukan dengan narasumber terkait untuk mendapatkan data yang sesuai dengan kebutuhan pengguna. Hasil penelitian menunjukkan bahwa penerapan algoritma RSA berhasil meningkatkan keamanan data suara dengan mengenkripsi data sensitif, mencegah akses tidak sah dan manipulasi data. Pengujian fungsional menunjukkan bahwa sistem berhasil mengenkripsi dan mendekripsi data dengan benar. Pengujian sistem juga menunjukkan bahwa setiap perubahan tidak sah pada data pemungutan suara di database terdeteksi dan ditolak oleh sistem. Implementasi algoritma RSA ini meningkatkan kepercayaan pengguna terhadap sistem e-voting di UMKT, karena data suara dilindungi dengan baik.

Kata Kunci: E-voting, Keamanan data, Kriptografi, Algoritma RSA, Enkripsi, Dekripsi, Serangan siber, Universitas Muhammadiyah Kalimantan Timur.

ABSTARACT

E-voting is an electronic voting process that encompasses the entire election process, from registration to the transmission of voting results. At Universitas Muhammadiyah Kalimantan Timur (UMKT), e-voting has been implemented for the election of internal campus organization leaders, including the Student Executive Board (BEM). Despite its advantages in speeding up elections, reducing costs, and improving accuracy, e-voting systems are vulnerable to cyber attacks that threaten the security and confidentiality of voting data. Therefore, effective security measures are necessary to protect e-voting systems. This research aims to enhance the security of voting data within the e-voting system at UMKT using the RSA cryptographic algorithm. The RSA algorithm utilizes a public key for encryption and a private key for decryption, ensuring that encrypted voting data cannot be accessed without decryption. A mixed-method research approach combining quantitative experimental methods and qualitative case studies was employed. Interviews with relevant stakeholders were conducted to gather data pertinent to user needs. The research findings indicate that implementing the RSA algorithm successfully enhances the security of voting data by encrypting sensitive information and preventing unauthorized access and data manipulation. Functional testing demonstrates that the system encrypts and decrypts data accurately. System testing also reveals that any unauthorized changes to voting data in the database are detected and rejected. The implementation of the RSA algorithm enhances user confidence in the e-voting system at UMKT, ensuring robust protection of voting data.

Keywords: *E-voting, Data security, Cryptography, RSA algorithm, Encryption, Decryption, Cyber attacks, Universitas Muhammadiyah Kalimantan Timur.*

PRAKATA

Assalamualaikum Wr. Wb

Dengan nama Allah Yang Maha Pengasih dan Penyayang, segala puji hanya bagi-Nya. Shalawat serta salam semoga tercurahkan kepada Rasulullah Muhammad SAW, yang telah membawa petunjuk serta rahmat bagi seluruh alam. Prakata ini dibuat sebagai ungkapan terima kasih dan penghargaan yang tulus dari penulis kepada semua pihak dalam penyelesaian skripsi ini, sehingga Peniliti dapat menyelesaikan skripsi ini dengan judul "Keamanan Sistem Database Aplikasi E-Voting Menggunakan Metode Kriptografi Algoritma Rsa *(Rivest Shamir Adleman)*". Penulis menyadari bahwa penulisan dan penyusunan skripsi ini dapat terselesaikan karena dukungan, bantuan, bimbingan, nasehat dan doa. Untuk itu penulis menyampaikan terimakasih kepada Bapak Sayekti Harits Suryawan, S.Kom, M.Kom yang telah membimbing penulis dalam penyusunan skripsi ini dan terimakasih sebesar-besarnya kepada:

1. Kepada orang tua tersayang dan tercinta Bapak Asrul Sani, S.Pd dan Ibu Normaningsih yang selalu ada setiap saat dari saya kecil hingga dewasa yang tiada henti memberikan kasih sayang, dukungan serta doa yang selalu mereka berikan sehingga skripsi dapat selesai.
2. Kakak dan Adik tercinta yang selalu memberikan dukungan, doa dan semangat positifnya sehingga penelitian skripsi dapat selesai.
3. Bapak Muhammad Taufiq Sumadi, S.Tr.Kom., M.Tr.Kom selaku dosen penguji yang telah memberikan masukan, saran dan arahan dalam proses menyelesaikan skripsi ini.
4. Dr. Muhammad Musiyam, M.T, selaku Rektor Unversitas Muhammadiyah Kalimantan Timur
5. Bapak Arbansyah, S.Kom., M.TI selaku ketua Program Studi S1 Teknik Informatika
6. Seluruh Bapak dan Ibu Dosen Program Studi Teknik Infromatika Universitas Muhammadiyah Kalimantan Timur.
7. Sahabat dan teman-teman saya semuanya yang selalu memberikan dukungan dan semangat dalam menjalani proses menyelesaikan skripsi ini.

Penulis menyadari bahwa penelitian ini masih jauh dari kesempurnaan, oleh karena itu segala saran dan kritik membangun sangat kami harapkan guna perbaikan di masa yang akan datang.

Waalaikumsalam Wr. Wb

Samarinda, Juli 2024

Peyusun

Dery Dinata

2011102441185

DAFTAR ISI

DAFTAR TABEL

Tabel **Halaman**

DAFTAR GAMBAR

Gambar **Halaman**

DAFTAR LAMPIRAN

Lampiran **Halaman**

BAB I
PENDAHULUAN

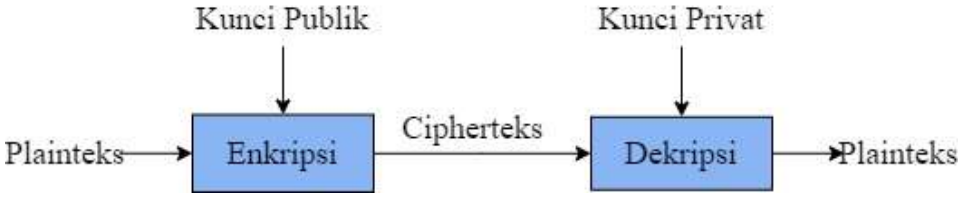
1.1. Latar Belakang

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.

BAB II
METODOLOGI

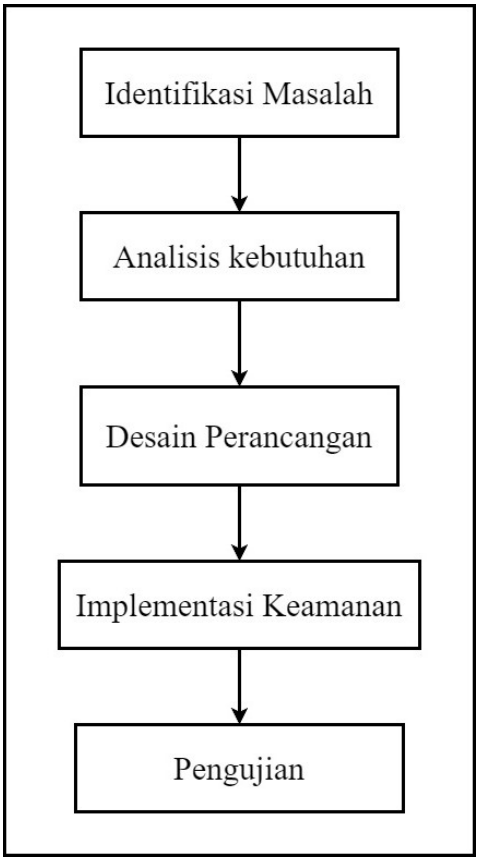
2.1 Jenis Penelitian

Dalam penelitian ini peneliti menggunakan jenis penelitian *mix method,* yaitu gabungan antara penelitian kuantitatif dan kualitatif. Penelitian kuantitatif dengan pendekatan eksperimental untuk membuat sistem keamanan data suara dalam database sistem aplikasi e-voting menggunakan algoritma RSA. Melalui eksperimen ini, peneliti melakukan pengujian dengan skenario pengujian. Penelitian kualitatif dengan mengambil studi kasus di lembaga pendidikan perguruan tinggi dengan melakukan wawancara bersama narasumber yang terkait untuk mendapatkan data yang sesuai dengan kebutuhan *user*, serta untuk mengidentifikasi kendala dan tantangan yang dihadapi dalam menerapkan sistem tersebut. Dengan penggabungan penelitian ini, dapat memberikan wawasan tentang mengimplementasikan keamanan data suara dengan algoritma RSA dalam sistem aplikasi e-voting.

2.2. Diagram Alur Penelitian

Tahapan penelitian merupakan langkah atau gambaran untuk membuat alur penelitian, mulai dari mengidentifikasi masalah, implementasi hingga sampai dengan selesai.

Berikut adalah diagram alur penelitian yang dapat dilihat pada gambar 2.1 dibawah.



Gambar 2. 1 Diagram Alur

2.2.1. Identifikasi Masalah

Penelitian bertujuan untuk mengatasi masalah keamanan data yang sering terjadi pada sistem aplikasi e-voting. Permasalahan yang sudah terjadi seperti halnya serangan *cyber* untuk memanipulasi

data pada sistem tersebut. Dalam mengidentifikasi masalah peneliti melakuakan studi literatur dengan membaca, mempelajari dan mengumpulkan jurnal-jurnal serta referensi lainnya untuk mendapatkan informasi dalam mengatasi permasalahan tersebut. Hasil dari permasalahan yang sudah terjadi adalah dari segi integritas keamanan dan kerahasiaan data yang rentan terhadap manipulasi oleh pihak yang tidak bertanggung jawab.

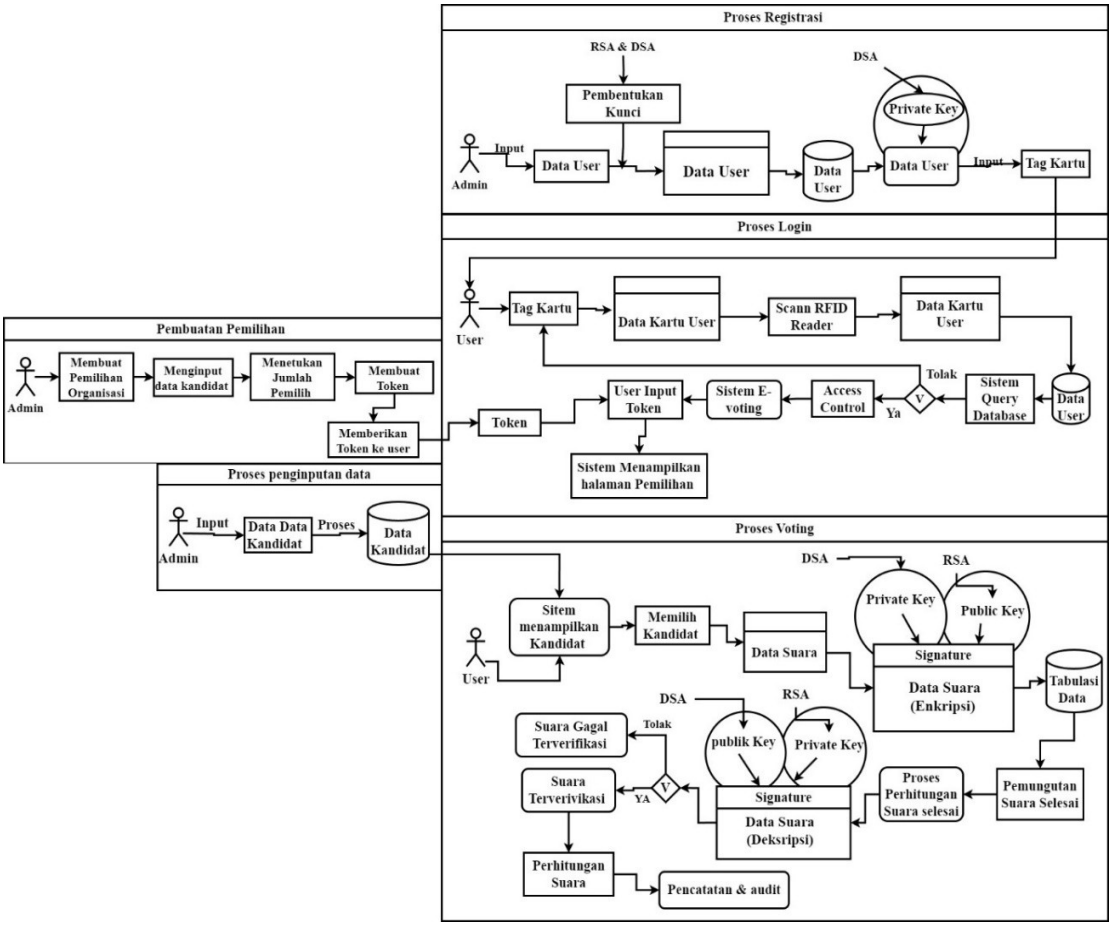
2.2.2. Analisis Kebutuhan

Setelah mengidentifikasi masalah peneliti melakukan wawancara kepada mahasiswa Universitas Muhammadiyah Kalimantan Timur. Wawancara ini bertujuan untuk memperoleh pemahaman apa yang harus dipenuhi dalam sistem e-voting tersebut, termasuk kebutuhan pengguna, fitur-fitur keamanan, dan kebutuhan lainya yang diperlukan.

2.2.3. Desain Perancangan

Setelah melakukan analisis kebutuhaan selanjutnya melakukan desain perancangan. Tahap ini peneliti membuat desain alur pengamanan data suara pada sistem e-voting menggunakan algoritma RSA. Desain ini mencakup pembuatan kunci publik dan kunci privat, implementasi mekanisme enkripsi dan dekripsi dalam menyimpan dan memproses data suara dalam database serta verifikasi.

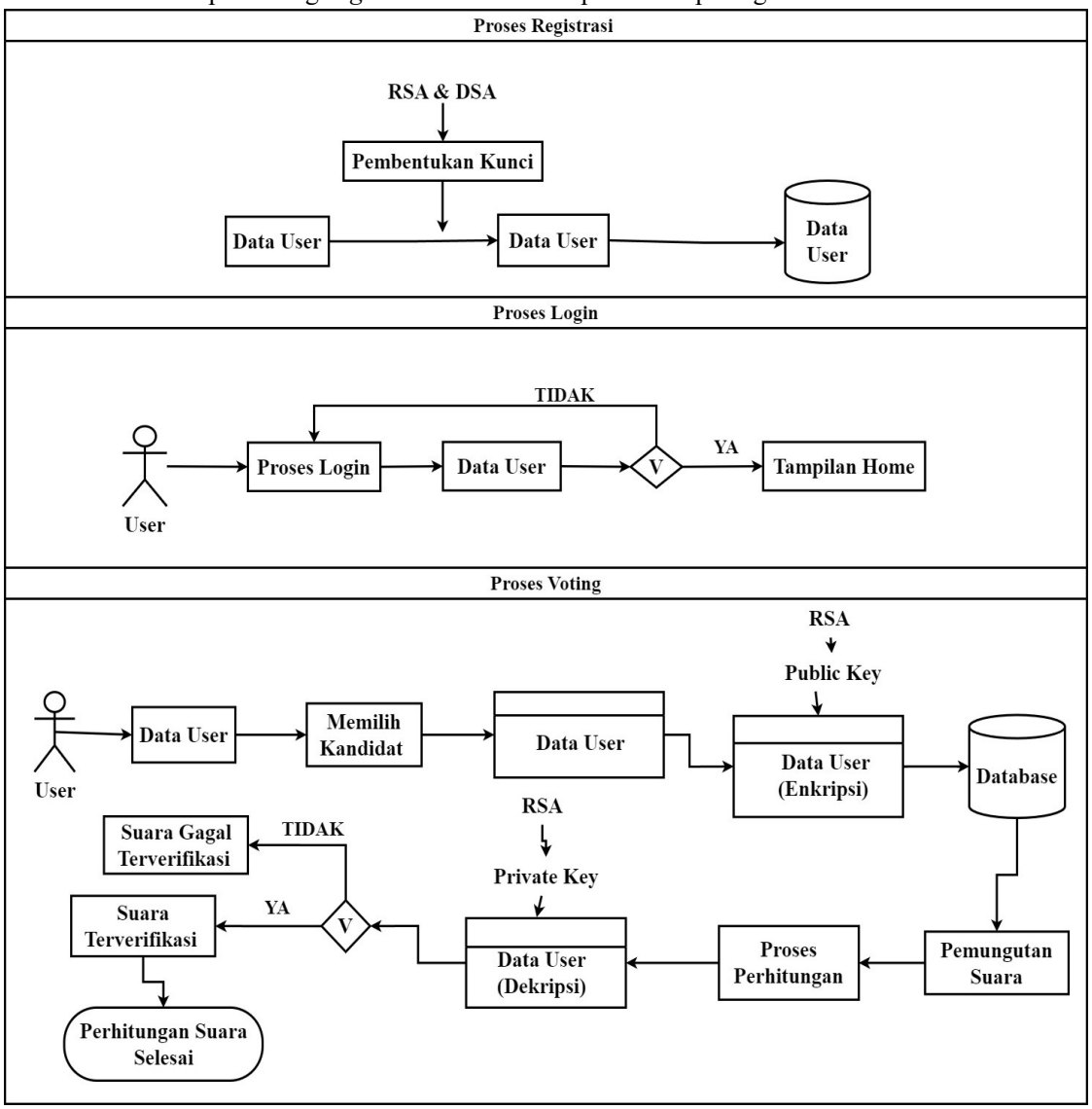
Berikut adalah perancangan *grand desain* secara keseluruhan dilihat pada gambar 2.2.



Gambar 2. 2 *Grand* Desain Keseluruhan

Diatas adalah *grand desain* alur e-voting secara keseluruhan yang didalamnya terdapat alur kerja RFID sebagai bentuk sistem login, terdapat algoritma RSA dan DSA untuk pengamanan data.

Berikut adalah perancangan *grand desain* RSA dapat dilihat pada gambar 2.3.



Gambar 2. 3 *Grand* Desain Algoritma RSA

Diatas adalah *grand desain* RSA, peran RSA didalam sistem tersebut adalah untuk mengamankan data suara sebelum tersimpan dalam database.

2.2.4. Implementasi Keamanan

Setelah melakukan desain perancangan tahap selanjutnya melakukan implementasi keamanan dengan alogoritma RSA. Peneliti akan mengimplementasikan hasil dari desain perancangan yang telah dibuat untuk mengamankan data suara dalam database sistem e-voting. Peneliti menggunakan spek perangkat prosesor AMD Ryzen™ 5 5625u 6 core 12 thread, RAM 8GB, penyimpanan 256GB SSD, dengan bahasa pemgrograman *Python* dan *Framework Django* untuk menuliskan kode-kode untuk diimplementasikan dalam bentuk codingan.

2.2.5. Pengujian

Saat implementasi selesai, sistem akan diuji untuk memastikan keamanannya sesuai dengan yang diharapkan. Pengujian dilakukan menggunakan skenario pengujian. Skenario yang dilakukan terdiri dari pengujian fungsionalitas dan pengujian sistem. Pengujian fungsionalitas dilakukan dengan memastikan

data yang terenkripsi dengan benar dan hasil deksripsinya sama dengan data aslinya didalam sebuah file *python* tersendiri. Dalam skenario pengujian sistem yang dilakukan adalah verifikasi suara, dengan mencoba mengubah nilai pada data suara didalam database secara langsung apakah data tersebut masih bisa terverifikasi oleh sistem atau tidak.

2.3. Objek Penelitian

Penelitian dilakukan pada sebuah lembaga pendidikan perguruan tinggi yang berada di samarinda, yaitu Universitas Muhammadiyah Kalimantan Timur (UMKT). UMKT merupakan kampus perguruan tinggi yang aktif dalam perkembangan teknologi informasi, termasuk dalam menerapkan sistem e-voting untuk pemilihan ketua dan wakil organisasi internal kampus yang sebelumnya sudah pernah dilakukan untuk pemilihan BEM (Badan Eksekutif Mahasiswa) pada saat wawancara bersama kemahasiswaan. Oleh karena itu, peneliti memiliki tujuan menerapkan algoritma RSA untuk melindungi keamanan dan kerahasian data pada sistem aplikasi e-voting tersebut.

BAB III
HASIL DAN PEMBAHASAN

3.1. Identifikasi Masalah

Berdasarkan studi literatur yang telah dilakukan, Identifikasi masalah diperoleh dari beberapa jurnal-jurnal ilmiah yang sudah pernah dilakukan, seperti pada penelitian Suarnatha (2022) permasalahan pada e-voting ini adalah pemilihan secara kesepakatan saat ini rentan akan kecurangan hasil suara dikarenakan banyak masyarakat yang memiliki hak pilih tetapi tidak ikut memilih dikarenakan proses administrasi yang menyulitkan. Pada penelitian Alam (2023) permaslahan pada e-votng berbasis sidik jari terdapat beberapa kekurangan dalam sistem, seperti adanya bug pada aplikasi dan aplikasi yang belum berbasis web. Masalah ini dapat mempengaruhi kinerja dan aksesibilitas sistem. Adapun penelitian dari Wibowo (2019) permasalahan pada e-voting yang diteliti adalah masih banyak kekurangan dari persiapan logistik, tidak transparannya data bahkan siswa tidak bisa memberikan suara karena keterbatasan waktu.

3.2. Analisis Kebutuhan

Analisis kebutuhan diperoleh pemahaman yang lebih jelas dari hasil wawancara bersama mahasiswa Universitas Muhammadiyah kalimantan Timur, yang merupakan narasumber sekaligus pengguna atau pemilih sistem aplikasi e-voting tersebut, mengenai kebutuhan spesifik terkait keamanan data dalam database aplikasi e-voting. Wawancara ini mengungkap kekhawatiran, harapan dan saran dari narasumber dalam mengimplementasikan sistem aplikasi e-voting.

Berikut hasil wawancara yang dilakukan bersama narasumber atau pengguna, yang merupakan ketua salah satu organisasi mahasiswa Universitas Muhammadiyah kalimantan Timur.

"Pemilihan saat ini masih dilakukan dengan cara voting manual menggunakan kertas dan menghitung suara langsung dipapan tulis. Selama proses pemilihan ada kendala yang dihadapi, terjadinya perkubuan antar pemilih, perhitungan yang cukup lama dan masih secara terbuka sehingga kurangnya privasi. Kelebihannya dari segi perhitungannya yang akurat meskipun cukup lama. Fitur seperti layaknya aplikasi e-voting pada umumnya yang mudah digunakan. Fitur real time, melakukan voting sampai selesai terlebih dahulu kemudian setelah itu menampilkan hasil suaranya. Keamanan data harus terjaga dengan baik secara aman untuk menghindari perentasan dari pihak yang tidak bertanggung jawab yang bisa memanipulasi data dan lakukan enkripsi yang sebaik baiknya untuk melindungi data. Data yang dienkripsi cukup data suara, karena didata suara nama pemilih, nama kandidat dan judul pemilihan sudah terenkripsi. Aplikasi digunakan untuk memberikan hak suaranya hanya mahasiswa aktif dalam keorganisasian dan kandidat yang mencalonkan diri menyesuaikan dengan aturan AD/ART (Anggaran Dasar / Anggaran Rumah Tangga) dari organisasi (24 Mei 2024).

Berdasarkan dari hasil wawancara tersebut bahwa *voting* tradisional memliki kekurangan dalam hal waktu, privasi dan terbentuknya kubu satu sama lain, akan tetapi kelebihannya akurat dalam akurasi perhitungannya. Narasumber menginginkan aplikasi e-voting yang mudah digunakan dengan fitur yang baik dan aman. Kemanan data harus aman dengan penggunaan enkripsi yang kuat. Aplikasi ini hanya digunakan oleh mahasiswa yang aktif dalam organisasi untuk memberikan hak suaranya dan kandidat yang mencalonkan menyesuaikan dengan aturan organisasi, dengan proses verifikasi yang dipastikan hanya anggota aktif yang dapat memberikan suara.

Berikut hasil wawancara yang dilakukan dengan narasumber atau pengguna yang merupakan mahasiswa perwakilan dari salah satu UKM (Unit Kegiatan Mahasiswa) Universitas Muhammadiyah Kalimantan Timur.

"Pemilihan saat ini masih menggunakan voting manual menggunakan kertas. Ada kendala pada saat proses pemilihan, banyak waktu yang terbuang cukup lama. Kelebihan selama proses pemilihan dari akurasi perhitungannya tepat meskipun cukup lama. Fitur aplikasi dari keamanannya, ketepatkan waktunya dan mudah digunakan. Fitur real time lebih baik voting diselesaikan terlebih dahulu kemudian menampilkan hasilnya, hasil pemilihan tidak dapat diubah setelah pemilihan selesai, pemilih tidak bisa memilih lebih dari satu kali. Keamanan data diamankan dengan sebaik baiknya sehingga tidak ada yang bisa membobol atau memanipulasi data. Data yang dienkripsi cukup data suara, karena didata suara nama pemilih, nama kandidat dan judul pemilihan sudah terenkripsi. Penggunaan aplikasi merupakan mahasiswa aktif dari ukm dan mempunyai hak suara memilih menyesuaikan dengan peraturan ukm sendiri, kandidat yang mencalonkan diri minimal semester tiga dengan menyesuaikan dengan peraturan ukm sendiri (13 Juni 2024).

Berdasarkan dari hasil wawancara tersebut bahwa *voting* tradisional memiliki kendala dari segi perhitungan suara, akan tetapi *voting* tersebut mempunyai kelebihan dari perhitungan yang akurat. Narasumber menginginkan aplikasi e-voting tersebut bisa digunakan dengan mudah dan aman dari segi keamanannya. Aplikasi tersebut hanya digunakan untuk mahasiswa aktif dalam ukm memberikan hak suara, dan kandidat yang mencalonkan menyesuaikan dengan aturan dari ukm tersebut.

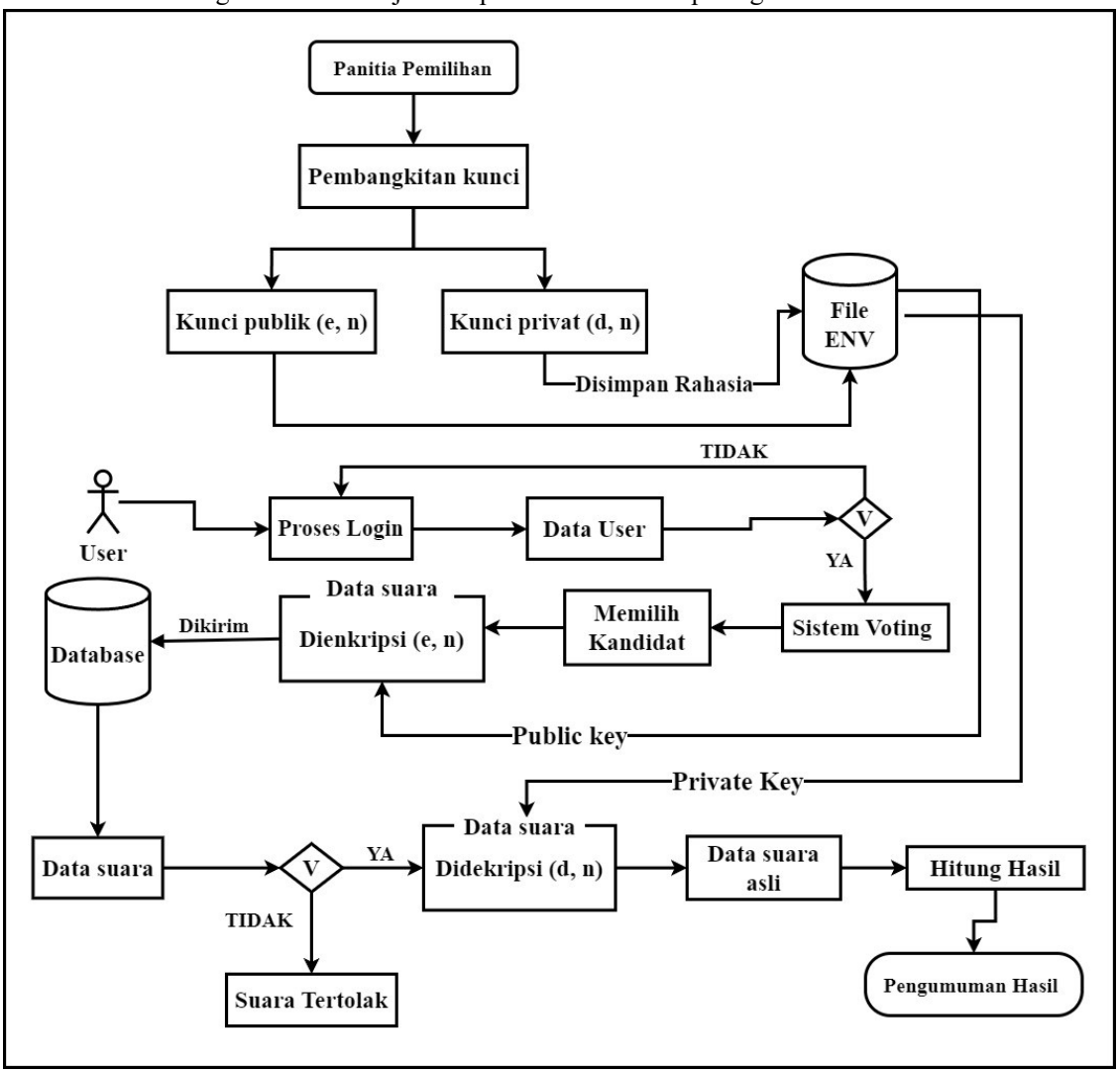
3.3. Desain Perancangan

Desain perancangan merupakan gambaran sistem yang akan diimplementasikan setelahnya. Desain perancangan ini menggunakan metode kriptografi algoritma RSA, yang bertujuan untuk kerahasiaan dan keamanan data suara dalam database. Desain perancangan ini mengcakup beberapa langkah, yaitu pembangkitan kunci, mekanisme enkripsi dan dekripsi serta verifikasi. Sebelum masuk kedalam desain tersebut berikut adalah alur kerja algoritma RSA pada sistem e-voting.

3.3.1. Alur Kerja Algoritma RSA pada Sistem

Proses dimulai dengan panitia pemilihan yang menghasilkan kunci publik (e, n) dan kunci privat (d, n). Kunci publik digunakan untuk mengenkripsi data, sedangkan kunci privat digunakan untuk mendekripsi data. Kunci-kunci ini disimpan secara rahasia dalam file ENV. User memulai dengan login ke sistem pemilihan. Setelah login berhasil, data pengguna diverifikasi. Jika verifikasi gagal, proses dihentikan dan user kembali ke halaman login. User yang berhasil login dapat melanjutkan untuk memilih kandidat di sistem voting. Data suara yang dipilih dienkripsi dengan kunci publik dan dikirim ke database. Keaslian data suara yang diterima diperiksa jika data tidak valid, maka ditolak. Data suara yang valid didekripsi menggunakan kunci privat untuk mendapatkan data suara asli. Data suara asli kemudian dihitung untuk menghasilkan hasil akhir pemilihan, yang diumumkan setelah proses penghitungan selesai.

Berikut adalah gambar akur kerja RSA pada sistem dilihat pada gambar 3.1

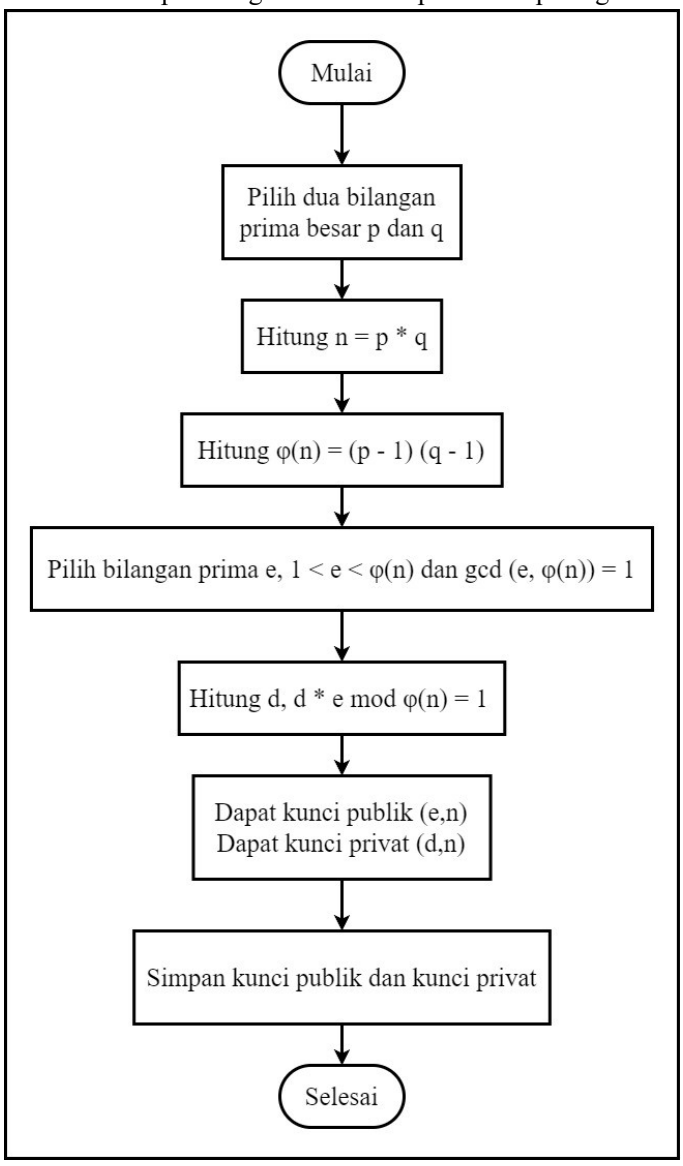


Gambar 3. 1 Alur Kerja RSA pada Sistem

3.3.2. Pembangkitan Kunci

Pembangkitan kunci merupakan proses awalan dalam algoritma RSA. Proses pembangkitan kunci tahap pertama yang dilakukan dengan cara memasukan angka prima besar nilai p dan q. Dimana nilai dari p dan q menjadi nilai dari n dan $\varphi(n)$. Hitung nilai e (enkripsi), maka nilai e berfungsi sebagai kunci publik terhadap (n). Lalu hitung nilai d (dekripsi) untuk mencari kunci privat terhdap (n). Sehingga mendapatkan kunci publik (e, n) dan kunci privat (d, n).

Berikut adalah *flowchart* Proses pembangkitan kunci dapat dilihat pada gambar 3.2.

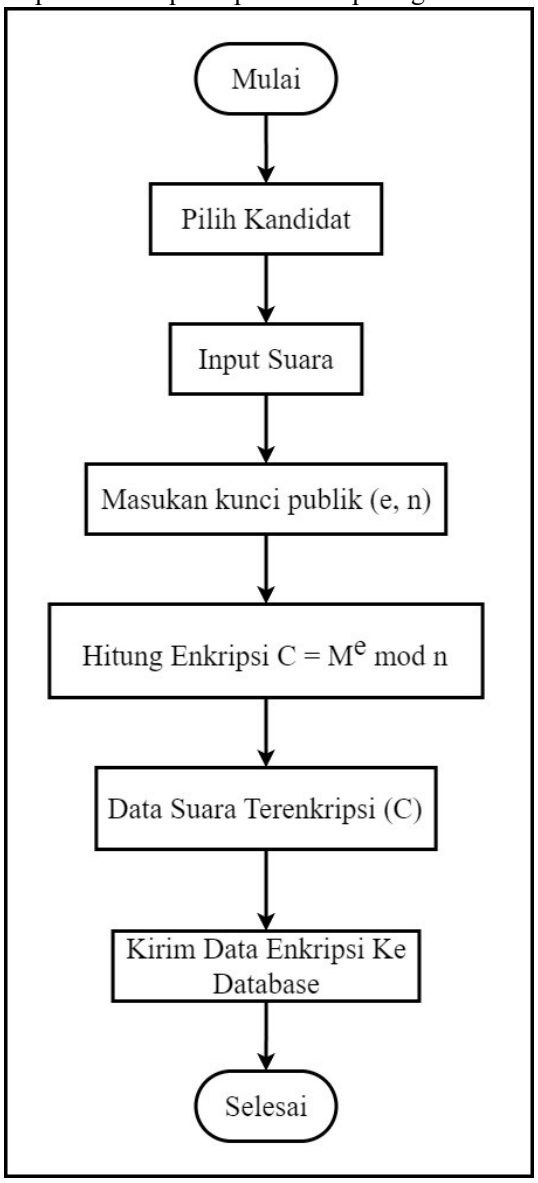


Gambar 3. 2 Pembangkitan kunci

3.3.3. Enkripsi

Enkripsi merupakan proses suatu data yang diubah nilainya agar tidak bisa terbaca dengan cara mengacak nilai data tersebut. Enkripsi dilakukan setelah dilakukannya pembangkitan kunci yang akan mendapatkan kunci publik (e, n) dan kunci privat (d, n). Enkripsi dimulai dari memilih kandidat, menginput suara, suara berupa data yang dikonversi dalam bentuk $UTF-8$, kunci publik yang telah didapatkan diambil untuk proses perhitungan enkripsi, proses enkripsi dimana suara atau data asli (m) dienkripsi menjadi cipherteks (c). Data suara yang terenkripsi disimpan atau dikirim kedalam database.

Berikut adalah *flowchart* proses enkripsi dapat dilihat pada gambar 3.3.

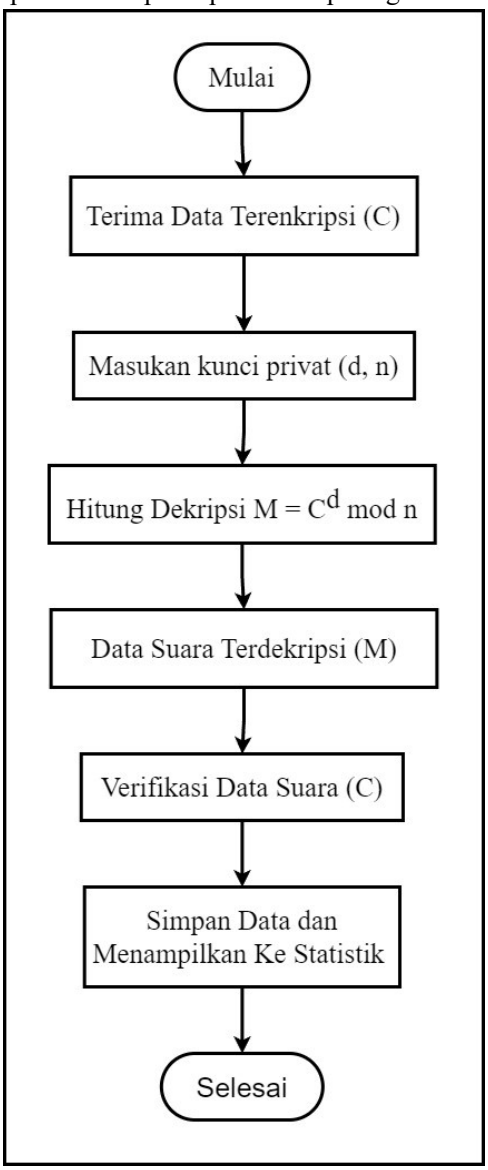


Gambar 3. 3 Proses Enkripsi

3.3.4. Dekripsi

Dekripsi merupakan proses suatu data yang terenkripsi (pesan acak) diubah atau dikembalikan pesan aslinya dengan menggunakan kunci privat (d, n). Sebelum melakukan dekripsi, penerima pesan harus ingat atau mengetahui kunci yang telah ditentukan antara pengirim dan penerima pesan. Dekripsi dimulai dari menerima cipherteks atau pesan enkripsi yang dikirim, kunci privat yang telah didapatkan diambil untuk proses perhitungan dekripsi, proses dekripsi dimana cipherteks (c) atau pesan didekripsi dalam bentuk $UTF-8$ dikembalikan menjadi pesan asli (m). Sistem melakukan verifikasi data suara yang didekripsi untuk memastikan data suara tersebut valid. Data suara yang telah diverifikasi disimpan dan ditampilkan ke statistik.

Berikut adalah *flowchart* proses dekripsi dapat dilihat pada gambar 3.4.



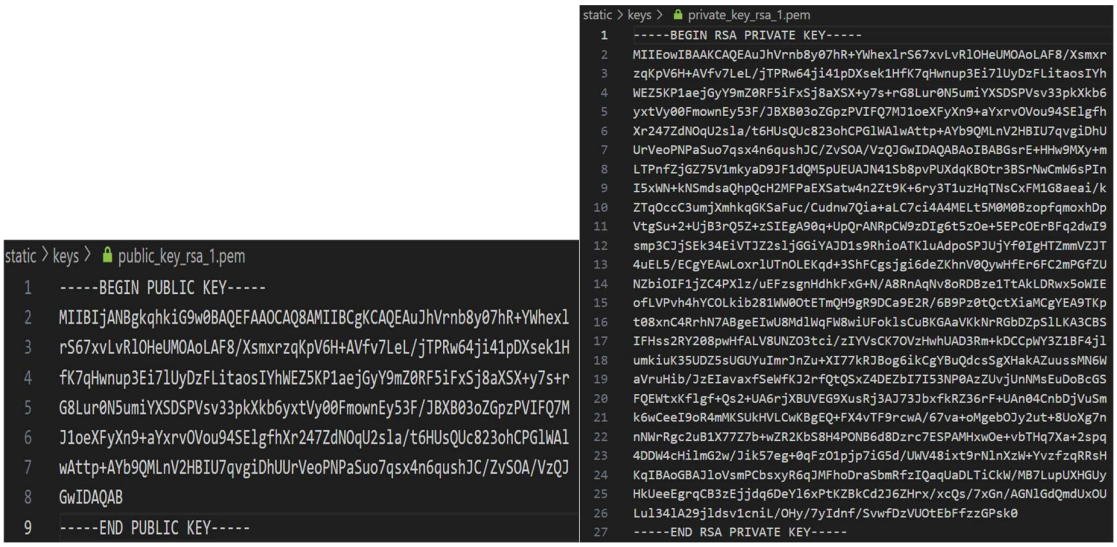
Gambar 3. 4 Proses Dekripsi

3.4. Implementasi Keamanan

Implementasi keamanan merupakan kelanjutan dari desain perancangan. Implementasi dilakukan berdasarkan hasil dari desain perancangan yang telah dilakukan. Implementasi yang dimaksud adalah proses pembuatan sistem keamanan data suara pada aplikasi e-voting dari tahap perancangan ke tahap codingan yang akan menghasilkan sistem keamanan aplikasi untuk mengamankan data suara dalam database yang telah dirancang sebelumnya.

3.4.1. Pembangkitan Kunci

Langkah pertama dalam menggunakan algoritma RSA adalah menghasilkan sepasang kunci publik dan kunci privat. Untuk menghasilkan kunci-kunci tersebut, peneliti membuat file bernama (utilsRSA.py) dalam bahasa *Python*. File ini berisi kode-kode *Python* yang digunakan untuk menghasilkan kunci publik *(e,n)* dan kunci privat *(d,n)*, yang kemudian disimpan dalam folder keys. Seperti pada gambar 3.5 berikut.



Gambar 3. 5 Hasil Pembangkitan kunci

Pada Gambar 3.5, kunci publik digunakan untuk mengenkripsi data. Kunci ini terdiri dari dua komponen eksponen publik (e) dan modulus (n). Karena kunci publik tidak dapat digunakan untuk mendekripsi data, kunci ini dapat dibagikan secara luas untuk keperluan enkripsi. Kunci privat digunakan untuk mendekripsi pesan yang telah terenkripsi. Kunci ini terdiri dari eksponen privat (d) dan modulus (n). Kunci privat harus dijaga kerahasiaannya, karena siapa pun yang memiliki kunci ini dapat mendekripsi data yang telah dienkripsi.

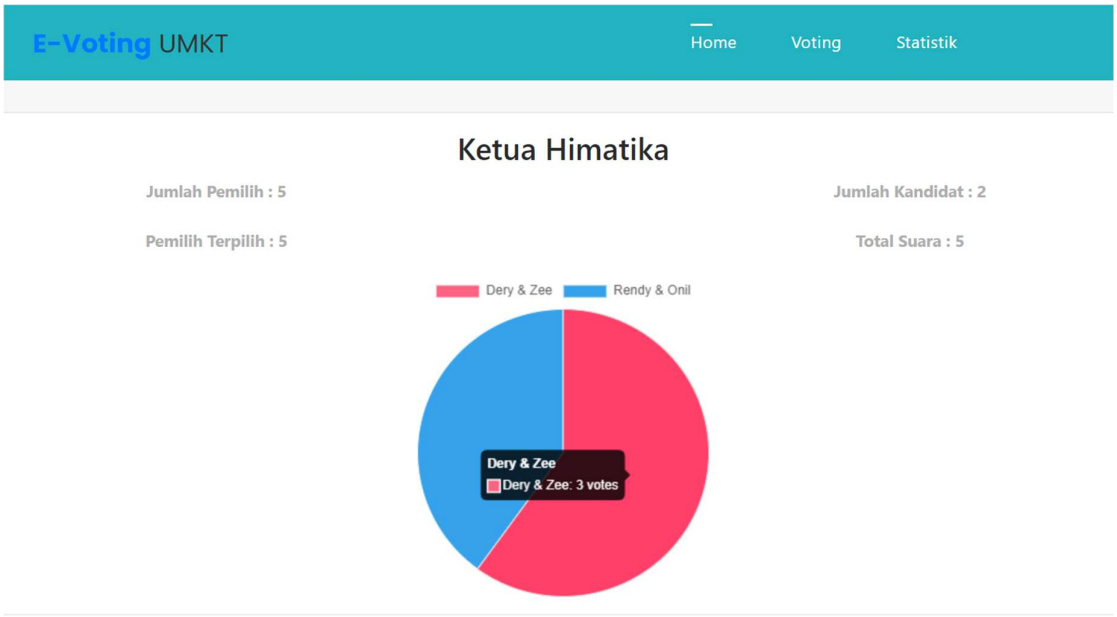
3.4.2 Mekanisme Enkripsi dan Dekripsi

Dalam mekanisme enkripsi dan dekripsi ditempatkan dalam file yang sama dengan file pembangkitan kunci sebelumnya (utilsRSA.py), namun berada pada baris kode yang berbeda. Meskipun terletak dalam file yang sama, setiap mekanisme memiliki kode dan fungsi yang berbeda, sehingga masing-masing mekanisme dapat menghasilkan *output* yang sesuai dengan perannya. Mekanisme enkripsi untuk mengamankan data dengan kunci publik, sedangkan mekanisme dekripsi berfungsi untuk mengembalikan data yang terenkripsi ke bentuk aslinya menggunakan kunci privat. Seperti pada gambar 3.6, 3.7, dan 3.8 berikut.

id	waktu_voting	judul_pemilihan	nama_kandidat	nama_pemilih
1	2024-07-06 09:30:46.705900	cYTeY/fyoB3LRZ1QPA5868+kjB1u	HbISE+B2i6r0Yy5+TXkYpH4uugW	SQjpA/ix1c7UFOAr+SN2406hiQ
2	2024-07-06 09:31:21.302984	awurVN/VnRgnlUJPC4AL0Hn6uva	agMdMr7jhWKx/Zyb6LCtAC8qBtu(	b37rNsRbuNIpId2LeRXas6c5/IsV
3	2024-07-06 09:31:37.028727	RUJqCuCmjYJgtXbwk4OL74ZH+H	d5rNi6rwa+OY3i7oSqW1ADXaPD7	CS8meGqrjIksamPGhiCQx8UDA
4	2024-07-06 09:31:53.422128	E9EjYTdbroEy1fFlGz1pNvwX1+Lx	YiOCBxu+ElZt4jfDsDRq0Jm/4xu5fl	KFO6W92X7r4nSReBBd7w5eRF
5	2024-07-06 09:32:07.827921	LvdZ9KMmLBlDZC1yjDevKgNlkv0	l3SP9k7anLg7zmqPM+hMPoeieoC	oE2Glw9vWarMtNbYzpqJmGpM(

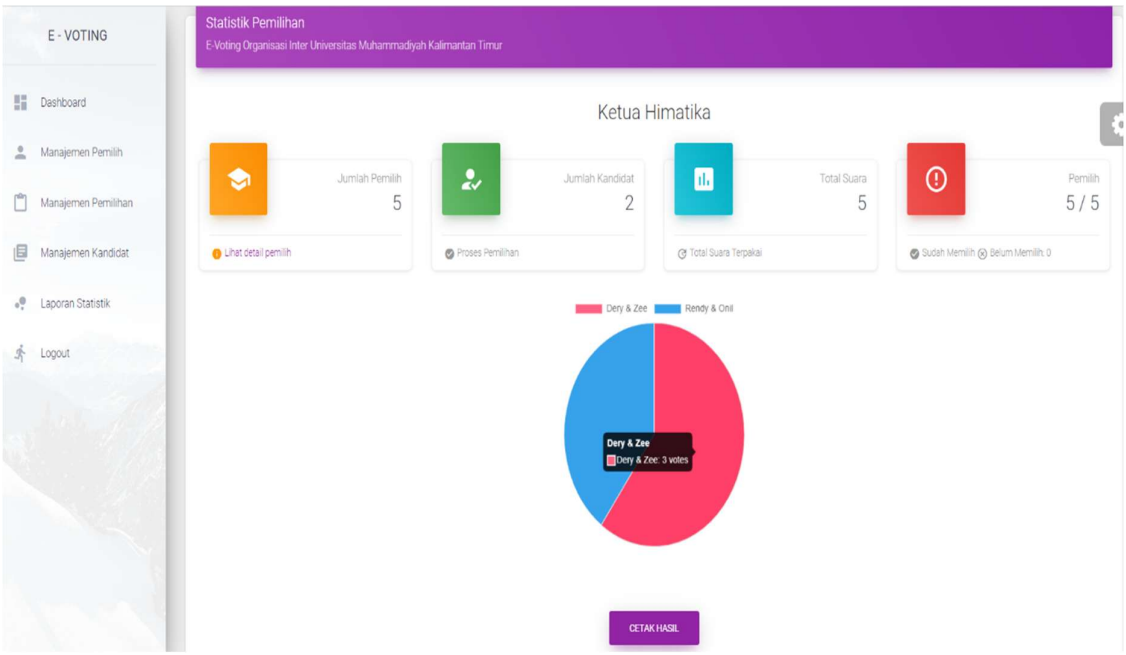
Gambar 3. 6 Hasil yang Enrkipsi di Database

Pada gambar 3.6 berikut merupakan data *voting* hasil dari enkripsi dengan kunci publik (e, n) disimpan dalam database yang hanya mengenkripsi "judul_pemilihan", "nama_kandidat" dan "nama_pemilih".



Gambar 3. 7 Tampilan *Front* Statistik

Pada gambar 3.7 merupakan tampilan website statistik bagian *front* dari hasil dekrispi data *voting* yang telah dienkripsi dan data otomatis akan menampilkan distatistik *home.*



Gambar 3. 8 Tampilan *Back* Statistik

Pada gambar 3.8 merupakan tampilan website statistik bagian *back* dari hasil dekrispi data *voting* yang telah dienkripsi dan data otomatis akan menampilkan distatistik *back.*

3.5. Pengujian

Pengujian merupakan proses penting dalam sistem untuk memastikan bahawa sistem tersebut berfungsi sesuai dengan yang diharapkan dan mampu memenuhi persyaratan yang telah didapatkan. Pengujian ini menggunakan dua skenario pengujian. Pengujian fungsional dan pengujian sistem.

3.5.1 Pengujian Fungsionalitas

Tabel 3. 1 Pengujian Fungsionalitas

NO	Deskripsi Pengujian	Langkah-Langkah Pengujian	Hasil Ynag Diharapkan	Keterangan
1	Enkripsi Data	Input data yang akan dienkripsi. simpan data yang terenkripsi.	Data berhasil terenkripsi dengan benar.	Berhasil
2	Dekripsi Data	Ambil data yang terenkripsi yang disimpan sebelumnya. lakukan proses dekripsi dengan kunci yang sesuai. verifikasi hasil dekripsi dengan daya yang asli	Data yang dekripsi kembali sesuai dengan data asli yang terenkripsi.	Berhasil
3	Kesesuaian Pesan Data	Enkripsi data dengan berbagai pesan (teks, angka, symbol, dll). Dekripsi data tersebut. Periksa apakah hasil dekripsi sesuai dengan format data asli atau tidak.	Data yang didekripsi kembali sesuai denga data asli yang terenkripsi.	Berhasil

Pengujian fungsional yang telah dilakukan sistem berhasil mengenkripsi dan mendekripsi data atau pesan dengan benar. Pengujian dilakukan dengan menghasilkan kunci publik, kemudian menggunakan kunci tersebut untuk mengenkripsi data asli dan mendekripsi data yang terenkripsi dengan kunci privat. Hasil pegujian bahwa data yang terenkripsi berhasil dikembalikan ke bentuk aslinya.

3.5.2 Pengujian Sistem

Tabel 3. 2 Pengujian Sistem

NO	Deskripsi Pengujian	Langkah – langkah pengujian	Hasil yang diharapkan	Keterangan
1	Menggunakan kunci privat yang sesuai	Pilih data yang sudah dienkripsi menggunakan kunci publik. Gunakan kunci privat yang sesuai untuk mendekripsi data yang telah dienkripsi.	Data asli berhasil didekripsi dengan kunci privat yang sesuai.	Berhasil
2	Menggunakan kunci privat yang tidak sesuai	Pilih data yang sudah dienkripsi menggunakan kunci publik. Gunakan kunci privat yang tidak sesuai untuk mendekripsi data yang telah dienkripsi.	Data gagal didekripsi dengan kunci privat yang tidak sesuai dengan data asli.	Berhasil

3	Jika cipherteks dihapus 5 karakter	Pilih data yang telah dienkripsi dengan kunci piblik. Hapus 5 karakter dari cipherteks yang telah dienkripsi. Gunakan kunci privat yang sesuai untuk mendekripsi data yang telah diubah.	Data gagal didekripsi dengan kunci privat yang sesuai, hasil dekripsi berupa data yang rusak dan tidak dapat dimengerti.	Berhasil
4	Jika cipherteks tidak dihapus 5 karakter	Pilih data yang telah dienkripsi dengan kunci publik. Gunakan kunci privat yang sesuai untuk mendekripsi cipherteks tanpa menghapus 5 karakter pada cipherteks yang telah dienkripsi.	Data asli berhasil didekripsi dengan kunci privat yang sesuai tanpa menghapus 5 karakter cipherteks.	Berhasil

Pengujian sistem yang telah dilakukan menunjukkan bahwa enkripsi dan dekripsi berjalan dengan baik. Kunci privat yang sesuai berhasil mendekripsi data yang dienkripsi dengan kunci publik yang benar, sementara kunci privat yang tidak sesuai gagal melakukan dekripsi. Penghapusan 5 karakter dari cipherteks menyebabkan kegagalan dalam dekripsi, menunjukkan bahwa perubahan kecil pada cipherteks dapat merusak integritas data. Cipherteks yang utuh, tanpa penghapusan 5 karakter, dapat didekripsi dengan benar, menunjukkan keandalan proses enkripsi dan dekripsi.

BAB IV
PENUTUP

4.1 Kesimpulan

Penerapan metode kriptografi RSA dalam sistem aplikasi e-voting memberikan perlindungan yang signifikan terhadap data suara yang tersimpan dalam database. Dengan pengujian yang telah dilakukan, dapat disimpulkan bahwa penerapan algoritma RSA berhasil meningkatkan keamanan data suara dalam database e-voting. Algoritma RSA, yang menggunakan kunci publik dan kunci privat, terbukti efektif dalam melindungi data dari akses dan manipulasi yang tidak sah. Hasil pengujian menunjukkan bahwa data suara yang terenkripsi tidak dapat diakses atau diubah oleh pihak yang tidak berwenang, sehingga integritas dan kerahasiaan data suara dalam sistem e-voting tetap terjaga. Dengan demikian, penggunaan algoritma RSA dalam sistem e-voting ini dapat diandalkan untuk memberikan perlindungan yang kuat terhadap data suara pada aplikasi e-voting.

4.2 Saran

Penelitian ini memiliki kekurangan untuk perbaikan penelitian selanjutnya. Keterbatasan data dan sampel yang digunakan dalam penelitian ini dengan menggunakan sampel yang lebih banyak, sehingga hasil penelitian dapat lebih lengkap. Meskipun penelitian ini memilih algoritma RSA sebagai keamanan data, masih ada kemungkinan algoritma yang lain lebih efektif untuk digunakan. Uji keamanan yang lebih lengkap sangat diperlukan, penelitian ini perlu mancangkup berbagai jenis ancaman dari serangan *cyber.* Pengujian lapangan, pengujian ini dapat memberikan wawasan mengenai operasional sistem dilapangan dan juga sekaligus mengidentifikasi masalah pada lapangan.

DAFTAR PUSTAKA

Alam, S., Zainal, M., Mahendra, J., 2023. KLIK: Kajian Ilmiah Informatika dan Komputer Perancangan Aplikasi E-Voting Berbasis Sidik Jari. Media Online 3, 516–522.

Anggoro, N.D., Suhery, C., Ruslianto, I., 2019. Penerapan Algoritma Knapsack dan Fungsi Hash pada Sistem E-Voting (Studi Kasus: Pemilihan Raya Mahasiswa Universitas Tanjungpura Pontianak). J. Coding 07, 85–96.

Angriani, H., Saharaeni, Y., 2019. Implementasi Algoritma Caesar Cipher pada Keamanan Data Sistem e-voting Pemilihan Ketua Organisasi Kemahasiswaan. Inspir. J. Teknol. Inf. dan Komun. 9, 123.

Arif, Z., Nurokhman, A., 2023. Analisis Perbandingan Algoritma Kriptografi Simetris Dan Asimetris Dalam Meningkatkan Keamanan Sistem Informasi. J. Teknol. Sist. Inf. 4, 394–405.

Dairi, M.S., Setiani Asih, M., author, corespondent, 2022. Implementasi Algoritma Kriptografi RSA Dalam Aplikasi Sistem Informasi Perpustakaaan Implementation Of RSA Cryptographic Algorithms in Library Information System Applications. Januari 2023, 214–223.

Diny Hermawati, F., Tahir, M., 2023. Keamanan E-Voting Di Indonesia Melalui Pemanfaatan Kriptografi Pada Sistem AES (Advance Encryption Standard). Jaya Abadi Amroin 2, 45–56.

Fatonah, Dadang Iskandar Mulyana, 2022. Implementasi Metode Rivest Shamir Adleman untuk Enkripsi dan Dekripsi Text. J. Inform. dan Teknol. Komput. (J-ICOM) 3, 32–39.

Fitrianto Wibowo, B., Iwan Wahyuddin, M., Tri Esthi Handayani, E., Teknologi Komunikasi dan Informasi, F., Nasional, U., Sawo Manila Kec Pasar Minggu, J., Selatan, J., 2019. E-Voting Application Using RSA Algorithm Method Based Prototype Android. J. Tek. Inform. C.I.T 11, 8–14.

Hasbulloh, H., Fitri, I., Ningsih, S., 2022. Algoritma RSA (Rivest–Shamir–Adleman) pada Sistem Informasi Pemilihan Ketua Organisasi Ikatan Pondok Pesantren Smart-SIPKOTREN. J. JTIK (Jurnal Teknol. Inf. dan Komunikasi) 6, 424–428.

Kasus, S., Presiden, P., Stmik, M., 2021. Implementasi Kriptografi Dalam Pengamanan Database E-Voting Menggunakan Algoritma Rsa Dan Base64 Berbasis Progresive Web Apps. e-Jurnal JUSITI (Jurnal Sist. Inf. dan Teknol. Informasi) 10, 30–40.

Liana, L., Zarlis, M., Tulus, T., 2023. Hybrid Cryptosystem Analysis RSA Algorithm And Triple DES Algorithm. Sinkron 8, 1461–1473.

Munir, R., 2023. Algoritma RSA 1, 1–6.

Pramadipta, M.B., 2024. Rancang Bangun Frontend Website Untuk Pemungutan Suara Dengan Menggunakan React.Js. J. Inform. dan Tek. Elektro Terap. 12.

Rizki, M., Farida Ariyani, P., 2021. Penerapan Kriptografi Dengan Menggunakan Algoritma Rsa Untuk Pengamanan Data Berbasis Desktop Pada Pt Trias Mitra Jaya Manunggal. Skanika 4, 1–6.

Setiawan, D., Andrianingsih, A., Soepriyono, G., 2023. Rancang Bangun Website Pengamanan Database E-Voting dengan Menerapkan Algoritma Rivest Shamir Adleman (RSA). J. Teknol. Inform. dan Komput. 9, 1341–1355.

Silalahi, L., Sindar, A., 2020. Penerapan Kriptografi Keamanan Data Administrasi Kependudukan

Desa Pagar Jati Menggunakan SHA-1. J. Nas. Komputasi dan Teknol. Inf. 3, 182–186.

Suarnatha, I.P.D., Agus, I.M., Gunawan, O., 2022. Jurnal Computer Science and Information Technology (CoSciTech) manusia. CoSciTech 3, 73–80.

Susanto, A.E., 2022. Aplikasi Keamanan Pesan Teks Secara Enkripsi Dan DekripsiMenggunakan Algoritma Rivest Shamir Adleman. Teknologipintar.org 2, 1–11.

Ungkawa, U., Rosmala, D., Fauzi, H., 2021. Penerapan Advance Encryption Standart dalam Pengamanan Elektronik Voting. J. Inf. Technol. 3, 17–23.

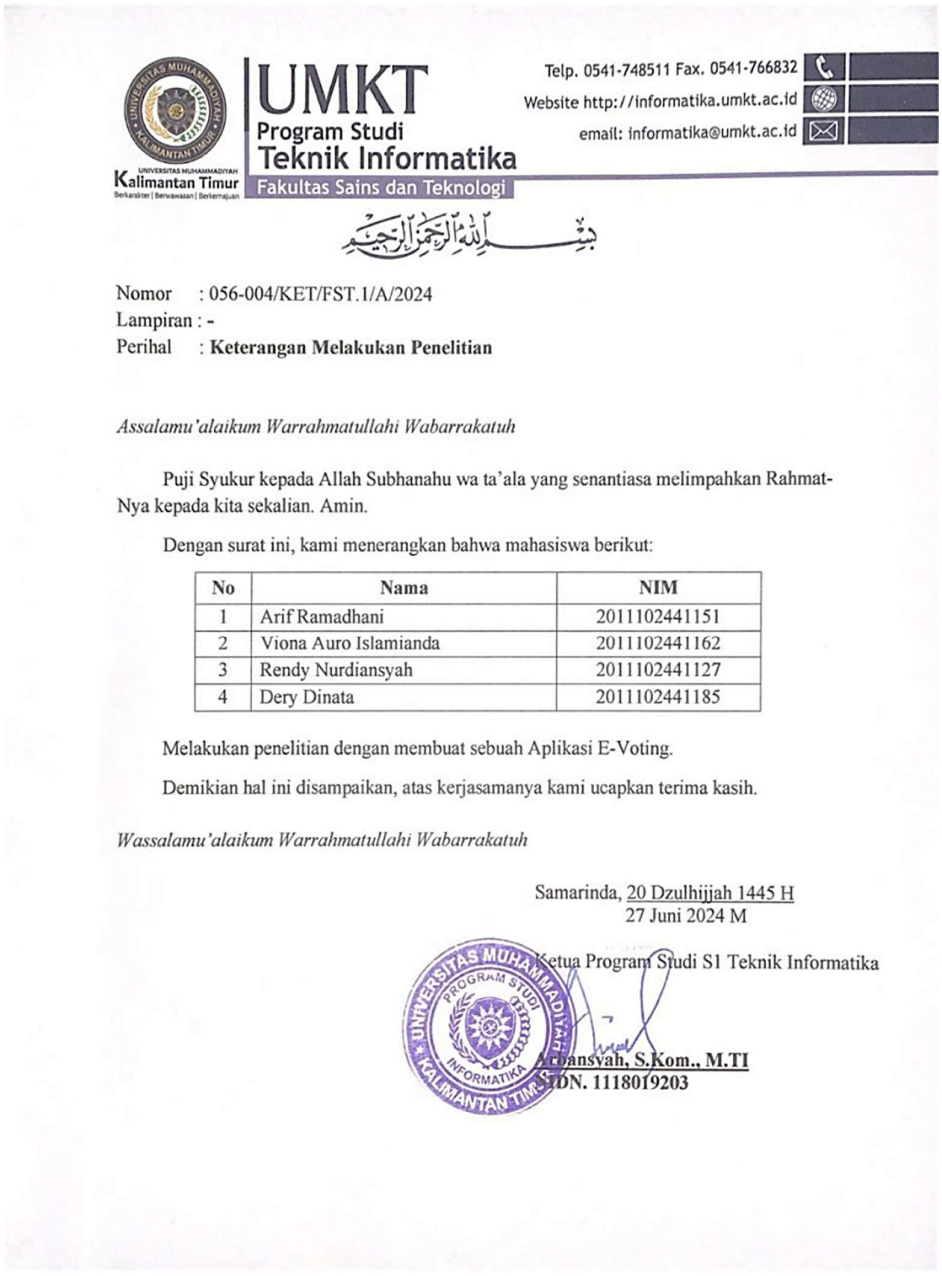
Yafi, A., Arhandi, P.P., Firdaus, V.A.H., Ismail, A., ..., 2023. Sistem Keamanan E-Voting Menggunakan Arsitektur Publik Blockchain Ethereum. KLIK Kaji. Ilm. … 4, 1313–1322.

LAMPIRAN

Lampiran 1. Jadwal Penelitian

NO	Jenis Penelitian	Bulan/2024					
		Feb	Maret	April	Mei	Juni	Juli
Tahap Pra Penelitian							
1	Menentukan Judul Penelitian						
2	Mengidentifikasi Permasalahan						
3	Menyusun Metode Penelitian						
4	Menentukan Studi Kasus						
5	Menyusun Proposal Penelitian						
6	Review Desk Simpel						
Tahap Penelitian							
1	Analisis Kebutuhan						
2	Desain Perancangan						
3	Implementasi Keamanan						
4	Pengujian						
5	Kesimpulan						
Tahap Akhir Penelitian							
1	Penyusunan laporan						
2	Seminar Hasil						

Lampiran 2. SK Melakukan Penelitian



UMKT
Program Studi
Teknik Informatika
Fakultas Sains dan Teknologi
Universitas Muhammadiyah Kalimantan Timur
Berkarakter | Berwawasan | Berkemajuan

Telp. 0541-748511 Fax. 0541-766832
Website http://informatika.umkt.ac.id
email: informatika@umkt.ac.id

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

Nomor : 056-004/KET/FST.1/A/2024
Lampiran : -
Perihal : **Keterangan Melakukan Penelitian**

Assalamu'alaikum Warrahmatullahi Wabarrakatuh

Puji Syukur kepada Allah Subhanahu wa ta'ala yang senantiasa melimpahkan Rahmat-Nya kepada kita sekalian. Amin.

Dengan surat ini, kami menerangkan bahwa mahasiswa berikut:

No	Nama	NIM
1	Arif Ramadhani	2011102441151
2	Viona Auro Islamianda	2011102441162
3	Rendy Nurdiansyah	2011102441127
4	Dery Dinata	2011102441185

Melakukan penelitian dengan membuat sebuah Aplikasi E-Voting.

Demikian hal ini disampaikan, atas kerjasamanya kami ucapkan terima kasih.

Wassalamu'alaikum Warrahmatullahi Wabarrakatuh

Samarinda, 20 Dzulhijjah 1445 H
27 Juni 2024 M

Ketua Program Studi S1 Teknik Informatika

Rendy Nurdiansyah, S.Kom., M.TI
NIDN. 1118019203

Lampiran 3. Kartu Bimbingan

KARTU KENDALI BIMBINGAN LAPORAN KARYA ILMIAH

Nama Mahasiswa : Dery Dinata
NIM : 2011102441185
Nama Dosen Pembimbing : Sayekti Harits Suryawan, S.Kom, M.Kom
Judul Penelitian : KEAMANAN SISTEM DATABASE APLIKASI E-VOTING MENGGUNAKAN METODE RSA *(Rivest Shamir Adleman)*

No	Tanggal	Uraian Pembimbingan	Paraf Dosen
1	22-02-2024	Konsultasi RTA	
2	26-02-2024	Menentukan Topik RTA dan Pembagian Fokus Penelitian Masing-masing	
3	29-02-2024	Diskusi Menentukan Judul Penelitin serta Metode dan Algoritma yang akan digunakan	
4	04-03-2024	Konsultasi Penulisan Canvas dan Tanda Tangan	
5	08-03-2024	Bimbingan Bab 1	
6	19-03-2024	Revisi Bab 1 dan tata cara penulisan	
7	20-03-2024	Konsultasi penentuan studi kasus tempat penelitian	
8	21-03-2024	Konsultasi Bab 2	
9	02-04-2024	Revisi Bab 2 mengenai cara melakukan alur bagan penelitian	
10	25-04-2024	Persetuajuan Upload Simpel	
11	07-06-2024	Bimbingan tentang mekanisme algoritma RSA	
12	20-06-2024	Bimbingan bab 3 hasil dan pembahasan	
13	27-06-2024	Revisi bab 3, kententuan jurnal atau naskah dan keseluruhan	

Mengetahui

Dosen Pembimbing

Sayekti Harits Suryawan, S.Kom, M.Kom
NIDN. 1119048901

Ketua Program Studi

Arbansyah., S.Kom, M.TI
NIDN. 1118019203

Lampiran 4. Wawancara Narasumber Organisasi HIMATIKA

Lampiran 5. Wawancara Narasumber Organisasi UKM Pencak Silat

Lampiran 6. Hasil Wawancara

No	Pertanyaan	Narasumber 1	Narasumber 2	Narasumber 3	Narasumber 4
1	Apa peran Anda dalam organisasi interkampus?	Ketua Himatika	Anggota Himatika	Anggota UKM Silat	Wakil UKM Silat dan Kordinator Pelatih
2	Bagaimana biasanya proses pemilihan dilakukan di organisasi Anda?	Menggunakan pemungutan suara manual dan penghitungan langsung	Menggunakan pemungutan suara manual dan penghitungan langsung	Menggunakan pemungutan suara manual dan penghitungan langsung	Menggunakan pemungutan suara manual dan penghitungan langsung
3	Apa tantangan terbesar yang Anda hadapi dengan proses pemilihan saat ini?	Proses penghitungan suara yang memakan waktu dan dan kurang efisien	Proses penghitungan suara yang memakan waktu dan dan kurang efisien	Proses penghitungan suara yang memakan waktu dan dan kurang efisien	Proses penghitungan suara yang memakan waktu dan dan kurang efisien
4	Apa saja kelebihan dari proses pemilihan saat ini yang ingin Anda pertahankan dalam sistem E-voting?	Kelebihannya dalam akurasinya yang tepat	Kelebihannya dalam akurasinya yang tepat	Kelebihannya dalam akurasinya yang tepat	Kelebihannya dalam akurasinya yang tepat
5	Fitur apa yang menurut Anda paling penting dalam aplikasi E-voting?	Antarmuka yang mudah digunakan	Keamanan dan validitas suara	Antarmuka yang mudah digunaka dan aman digunakan	Antarmuka yang mudah digunaka dan aman digunakan
6	Bagaimana Anda ingin proses pendaftaran pemilih dilakukan?	Yang mendaftar adalah anggota aktif sesuai peraturan organisasi	Yang mendaftar adalah anggota aktif sesuai peraturan organisasi	Yang mendaftar adalah anggota aktif sesuai peraturan organisasi	Yang mendaftar adalah anggota aktif sesuai peraturan organisasi
7	Bagaimana menurut Anda sistem verifikasi identitas pemilih harus dilakukan?	Yang berhak memilih adalah anggota aktif dari organisasi dan ukm	Yang berhak memilih adalah anggota aktif dari organisasi dan ukm	Yang berhak memilih adalah anggota aktif dari organisasi dan ukm	Yang berhak memilih adalah anggota aktif dari organisasi dan ukm

No	Pertanyaan	Narasumber 1	Narasumber 2	Narasumber 3	Narasumber 4
8	Apakah Anda membutuhkan fitur pemantauan real-time untuk hasil pemilihan?	Sepertinya Tidak perlu hasilnya keluar saat pemilihan selesai saja	Sepertinya Tidak perlu hasilnya keluar saat pemilihan selesai saja	Sepertinya Tidak perlu hasilnya keluar saat pemilihan selesai saja	Sepertinya Tidak perlu hasilnya keluar saat pemilihan selesai saja
9	Apa saja kekhawatiran Anda terkait keamanan dalam E-voting?	Risiko peretasan dan manipulasi hasil	Keamanan data pemilih dan hasil pemilihan	Privasi dan anonimitas pemilih	Keamanan data pemilih dan hasil pemilihan
10	Seberapa penting bagi Anda bahwa hasil pemilihan tidak dapat diubah setelah pemungutan suara selesai?	Sangat penting, untuk menjaga integritas proses voting	Penting karena seharusnya pemilih wajib Cuma menggunakan 1 suara	Penting karena seharusnya pemilih wajib Cuma menggunakan 1 suara	Penting karena seharusnya pemilih wajib Cuma menggunakan 1 suara
11	Bagaimana Anda ingin sistem menangani pemilih yang mencoba memberikan suara lebih dari sekali?	Pemilih hanya boleh menggunakan satu ID untuk satu suara	Pemilih hanya boleh menggunakan satu ID untuk satu suara	Pemilih hanya boleh menggunakan satu ID untuk satu suara	Pemilih hanya boleh menggunakan satu ID untuk satu suara
12	Seberapa mudah Anda ingin proses pemilihan dalam aplikasi ini?	Sangat mudah	Mudah dan proses yang sederhana	Mudah dimengerti oleh semua pemilih	Mudah digunakan

Lampiran 7 Surce Code Pembangkiat Kunci

```python
from Crypto.PublicKey import RSA
from Crypto.Cipher import PKCS1_OAEP
import base64
import logging

logger = logging.getLogger(__name__)

def generate_rsa_keys(pemilih_id):
    key = RSA.generate(2048)
    private_key = key.export_key()
    public_key = key.publickey().export_key()

    # Save private key to file
    private_key_path = f'static/keys/private_key_rsa_{pemilih_id}.pem'
    with open(private_key_path, 'wb') as f:
        f.write(private_key)

    # Save public key to file
    public_key_path = f'static/keys/public_key_rsa_{pemilih_id}.pem'
    with open(public_key_path, 'wb') as f:
        f.write(public_key)

def load_rsa_private_key(pemilih_id):
    private_key_path = f'static/keys/private_key_rsa_{pemilih_id}.pem'
    with open(private_key_path, 'rb') as f:
        private_key = RSA.import_key(f.read())
    return private_key

def load_rsa_public_key(pemilih_id):
    public_key_path = f'static/keys/public_key_rsa_{pemilih_id}.pem'
    with open(public_key_path, 'rb') as f:
        public_key = RSA.import_key(f.read())
    return public_key
```

Lampiran 8 Source Code Enkripsi

```python
            # untuk mengenkripsi RSA
            public_key_rsa = load_rsa_public_key(pemilih_id)
            encrypted_nama_pemilih = encrypt_with_public_key(public_key_rsa.export_key(), pemilih.nama)
            encrypted_nama_kandidat = encrypt_with_public_key(public_key_rsa.export_key(), kandidat.nama)
            encrypted_judul_pemilihan = encrypt_with_public_key(public_key_rsa.export_key(), pemilihan.judul)
            waktu_voting = datetime.now()

            # simpan suara
            voting = Voting(
                nama_pemilih=encrypted_nama_pemilih,
                nama_kandidat=encrypted_nama_kandidat,
                judul_pemilihan=encrypted_judul_pemilihan,
                waktu_voting=waktu_voting
            )
            voting.save()
```

Lampiran 9 Source Code Dekripsi

```python
    for vote in voting_results:
        decrypted = False
        for pemilih_id in pemilih_ids:
            private_key_rsa = load_rsa_private_key(pemilih_id)
            try:
                decrypted_nama_kandidat = decrypt_with_private_key(private_key_rsa, vote.nama_kandidat).strip()
                decrypted_nama_pemilih = decrypt_with_private_key(private_key_rsa, vote.nama_pemilih).strip()
                decrypted_judul_pemilihan = decrypt_with_private_key(private_key_rsa, vote.judul_pemilihan).strip()

                logger.debug(f"Decrypted kandidat: {decrypted_nama_kandidat}")
                logger.debug(f"Decrypted pemilih: {decrypted_nama_pemilih}")
                logger.debug(f"Decrypted pemilihan: {decrypted_judul_pemilihan}")

                # Only count votes that match the current pemilihan
                if decrypted_judul_pemilihan == pemilihan.judul:
                    if decrypted_nama_kandidat in vote_counts:
                        vote_counts[decrypted_nama_kandidat] += 1
                    else:
                        vote_counts[decrypted_nama_kandidat] = 1

                    decrypted = True
                    break
            except Exception as e:
                logger.error(f"Error decrypting vote for vote ID {vote.id} with pemilih ID {pemilih_id}: {str(e)}")
                continue
        if not decrypted:
            logger.error(f"Error decrypting vote for vote ID {vote.id}: Unable to decrypt with any pemilih private key")
```

Lampiran 10. *Source Code* Pengujian Fungsional

```
from cryptography.hazmat.primitives.asymmetric import rsa

from cryptography.hazmat.primitives.asymmetric import padding

from cryptography.hazmat.primitives import hashes

from cryptography.hazmat.primitives import serialization


# Fungsi untuk membuat kunci RSA

def buat_kunci():

    kunci_privat = rsa.generate_private_key(

        public_exponent=65537,

        key_size=2048,

    )

    kunci_publik = kunci_privat.public_key()

    return kunci_privat, kunci_publik


# Fungsi untuk mengenkripsi data dengan kunci publik

def enkripsi_data(kunci_publik, data):

    ciphertext = kunci_publik.encrypt(

        data,

        padding.OAEP(

            mgf=padding.MGF1(algorithm=hashes.SHA256()),

            algorithm=hashes.SHA256(),

            label=None

        )

    )

    return ciphertext
```

```
# Fungsi untuk mendekripsi data dengan kunci privat
def dekripsi_data(kunci_privat, ciphertext):
    plaintext = kunci_privat.decrypt(
        ciphertext,
        padding.OAEP(
            mgf=padding.MGF1(algorithm=hashes.SHA256()),
            algorithm=hashes.SHA256(),
            label=None
        )
    )
    return plaintext

# Fungsi untuk menampilkan kunci dalam format PEM
def tampilkan_kunci(kunci_privat, kunci_publik):
    kunci_privat_pem = kunci_privat.private_bytes(
        encoding=serialization.Encoding.PEM,
        format=serialization.PrivateFormat.PKCS8,
        encryption_algorithm=serialization.NoEncryption()
    ).decode('utf-8')

    kunci_publik_pem = kunci_publik.public_bytes(
        encoding=serialization.Encoding.PEM,
        format=serialization.PublicFormat.SubjectPublicKeyInfo
    ).decode('utf-8')

    print("Kunci Privat:")
```

```
    print(kunci_privat_pem)
    print("Kunci Publik:")
    print(kunci_publik_pem)

# Fungsi utama untuk pengujian
def utama():
    # Membuat kunci
    kunci_privat, kunci_publik = buat_kunci()

    # Menampilkan kunci
    tampilkan_kunci(kunci_privat, kunci_publik)

    # Data asli yang akan dienkripsi
    data_asli = b"dery dinata"

    # Mengenkripsi data
    data_enkripsi = enkripsi_data(kunci_publik, data_asli)
    print(f"Data terenkripsi: {data_enkripsi}")

    # Mendekripsi data
    data_dekripsi = dekripsi_data(kunci_privat, data_enkripsi)

    # Simulasikan ketidaksesuaian data dengan mengubah data asli untuk verifikasi
    # data_asli_baru = b"Data ini sudah diubah."

    # Cetak data yang didekripsi
```

```
    print(f"Data terdekripsi: {data_dekripsi}")


    # Memastikan data terdekripsi sama dengan data asli (dengan ketidaksesuaian)
    # try:
    #     assert data_dekripsi == data_asli_baru, "Dekripsi gagal, data tidak cocok!"
    print("Dekripsi berhasil, data cocok!")
    # except AssertionError as e:
    #     print(e)


if __name__ == "__main__":
    utama()
```

Lampiran 11. Output Hasil Pengujian Fungsionalitas

```
PS C:\Users\MSI USER\OneDrive\Documents\kriptoRSA\evoting> & "C:/Users/MSI
USER/AppData/Local/Programs/Python/Python312/python.exe" "c:/Users/MSI
USER/OneDrive/Documents/kriptoRSA/evoting/dashboard/coba.py"
Kunci Privat:
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQDG+KOjKf+nBTiF
teXWpmT7gwSZ91p+EVuuSJ8AO0DGhmPslHqkSWJmVu69w5sa9Rt2qIkU8gy8+7lZ
98ZUehPnOH4z9GSJYdVQbQL/9hiEM3qIuZplunLFxkFxxEGXT6udMet1sBWj46JQ
h7ILzm61F9OcU/OzIJkZI5ifPSs11b/du2vNj+C7ocbbZUyv3qYYEBV49DkFg0t+
Ehww6mOJZY56k9kyiq/wuN24YLpYV/ZrhQ1HKptxjEywbv6IBoeEpmN/97U7w6is
v5Og7/eBW2Xp7PrCnwusftbD08SPVPqGgfcR+npmvTAH1APqZ/Pq1D89/dFLaEKE
heqqFOGTAgMBAAECggEAJMVLfHplAClTVkaU6LPMgrymS4vuYdD0aAOMut64bFfm
vJB+D8FuGWqkaVZuYi98+VNRLhlDaGN+0BUdxnvfFMKYdCKMt+ToJppWzRXeVwQq
d30Rfw5TaqBmdM9nrb5wATd6A8BcZ3LIiuhg65SlWftCxKexKF/0WzR8XqVPyH1a
IMwsXdq4xXLplQOFnBnMYJr9NAuUWbb+wEHUNrARJlK/g+s0glLEg3FbPU8ct76A
```

+JU8FvrKrAcJkRuG0fpYUVYMeikkF93mUt/hkZ5mjEzqVMWOBYmoRZZMnDOxaDHT

CVWwU6LiVmf7Przc5mc8bMnjSorpQQ6v7AUf4Hm1lQKBgQDrAbWZpbmrk8oSar4W

a+VSpQfZN37LO7IeuRk75EFGiUfReolPUKSx6FaSngYvcSktd9oz4MS4D3SfWPma

M3gBeJSRH5sslJX/iBTGBkmNKZ05ycZ7pRNpxjYWyCKVoPzwhlRmXZJvpgFILtH1

2oj3oMCUJdq3GVpAQ3szjiK3NwKBgQDYvtju5ARbg/w1KmGYSRSX1FFXbS9faLTq

X3tCjdyzj6jFF5KOamqA0tt/0KGVUOevs7EtE5tsxDoTUwSQgaNpRqSUWHxGrztP

p3q3wlMh4Y5z9JxW3mUisTqdoAPLc9Gab8QDuZy582cvhLYuVRzeFYuApGh6YTvN

avy0IybehQKBgEIRy/Vzczy6oxAEdIanNOTEQu2dvYbztIMQtPhylqt3AvrwwVPM

L1FZKaW0ybZi0RnYXT9CjOvWZIo8IIhque1n8hTO1vh0masqnfSCZgFK1sodYTD3

2vpc4G4NPDPm+9W/XlEdM4MyH6AkkaDWHLXJuvqrnc7mUMpKboOzDS2HAoGBAKon

QPRhis4xUjiGmfFMRd9fra+9pnf3IjfwVzqLVdydBfgcJlCpWAzj+69eoMswpYH4

xjnF77k2XwU2ohmzvA50h9VxlbaD8EL7DsrdwheSFBwRxv4nPyw6B/MgYHpC5SSh

Yzctas1MORBD1iWPaccrEMYfy2lvldwQhmwAQI5lAoGAbGXtUCJbExqjJ4DrIyt4

jXBaUYppv1VhyHnl3TcGSORRusM/u/jMen5OIIhgPF24lGh0AyBu+r3KHuZt9HNt

UpzXHsu3QXW2wRFdTbTbzceVFY+mu4+tpRuU4yWMCBwE7ghNZ2JbagRHV4n3Aon5

I2UU+VGmgYiVLyTNDR8acfY=

-----END PRIVATE KEY-----

Kunci Publik:

-----BEGIN PUBLIC KEY-----

MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxvijoyn/pwU4hbXl1qZk

+4MEmfdafhFbrkifADtAxoZj7JR6pEliZlbuvcObGvUbdqiJFPIMvPu5WffGVHoT

5zh+M/RkiWHVUG0C//YYhDN6iLmaZbpyxcZBccRBl0+rnTHrdbAVo+OiUIeyC85u

tRfTnFPzsyCZGSOYnz0rNdW/3btrzY/gu6HG22VMr96mGBAVePQ5BYNLfhIcMOpj

iWWOepPZMoqv8LjduGC6WFf2a4UNRyqbcYxMsG7+iAaHhKZjf/e1O8OorL+ToO/3

gVtl6ez6wp8LrH7Ww9PEj1T6hoH3Efp6Zr0wB9QD6mfz6tQ/Pf3RS2hChIXqqhTh

kwIDAQAB

-----END PUBLIC KEY-----

Data terenkripsi:
b'n\xd5\x9f\x80\xca\xe3F\xb4\xef\xac\xa6@+\x13|\xf7;!\x1e?\xb5\x10\x9bP"S\xbd\x9d\xbd\xe9\xb0\
xe6\x04\x95L&\x08\xfa\x92\x1e\x02\xe3\xdfm\xa0\xda\n
\xa5\xa2\xd8V\x1a\xbe$\xd2\xfcw\x12\xe3f\xfb/A\x94G\x9c\xae\xd8Ab.\xfb\x139\xc4t\xf40\xde\n\x
0f}\xcfo\x11{?\xf9\xdf\xe7y\xf4\xe9\xd9\x8d\xc8A9B\xef~\xc1\x97\xac\xd0\x9e\xces\xe2\xac\xcb\xf
6\xdcOG-
\xd2\xf2\xb4\xd1\xaa\xd7\xc9\x13P\xad\xf0\x8er\x1a2Zf\xc6\xe00&\xd8\x9e\xfc\xe1\xe6g\xe5\x12\x
16\r\xe3)\x94\xeb\x81e\xff\x12\xee\xe1f\x99\xb7U\xf0\xc0MM\xd7z\x9e\x88\xe7oVx\x1e0\xbd\x9a=
\xb0g\xff\xe6En\xe0*+t\xc4\xfa\xe3\xc7\xc0\xb5\xd1\x9ag\xea03\xea\xc0\x95o\x83X\xb5Ro\xc8P\n\
xe7%\xa0\xbbKz\xdfG\x940\x9fX\x0bVG\xd6<\x04z\xb64\xbaZ\x07=\x93~\xe4\xcdY\xdd}\xae\x87\
xdb\xd3j\xb4\xad\xd1\x8a\xe5\xee'

Data terdekripsi: b 'dery dinata'

Dekripsi berhasil, data cocok!

SKRIPSI DERY DINATA

by Teknik Informatika Universitas Muhammadiyah Kalimantan Timur

Submission date: 25-Jul-2024 01:41PM (UTC+0800)
Submission ID: 2422154094
File name: SKRIPSI_DERY_DINATA.docx (3.43M)
Word count: 4836
Character count: 31976

SKRIPSI DERY DINATA

ORIGINALITY REPORT

14%	11%	6%	5%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Delaware Military Academy Student Paper	1%
2	docplayer.info Internet Source	1%
3	text-id.123dok.com Internet Source	1%
4	dspace.umkt.ac.id Internet Source	1%
5	informatika.stei.itb.ac.id Internet Source	1%
6	Submitted to Universitas Brawijaya Student Paper	1%
7	sinta.unud.ac.id Internet Source	1%
8	Nircho Dwi Anggoro , Cucu Suhery , Ikhwan Ruslianto. "PENERAPAN ALGORITMA KNAPSACK DAN FUNGSI HASH PADA SISTEM E-VOTING (Studi Kasus: Pemilihan Raya Mahasiswa Universitas Tanjungpura	<1%

RIWAYAT HIDUP

Dery Dinata lahir pada tanggal 13 Oktober 2001 di Separi. Putra pasangan dari bapak Asrul Sani, S.Pd dan ibu Normaningsih merupakan anak ke dua dari tiga bersaudara. Bertempat tinggal di Desa Separi Kec. Tenggarong Seberang Kutai Kartanegara. Pendidikan yang pernah ditempuh. SD 004 Separi Kec.Tenggarong Seberang pada tahun 2013, SMP 04 Embalut kec. Tenggarong Seberang 2016, SMA Negeri 2 Tenggarong Seberang 2020 dan saat ini melanjutkan pendidikan di perguruan tinggi Universitas Muhammadiyah Kalimantan Timur pada Fakultas Sains & Teknologi jurusan Teknik Informatika yang berada di Provinsi Kalimantan Timur, Samarinda. Pada saat menjadi mahasiswa, penulis pernah menjadi anggota keorganisasian HIMATIKA (Himpunan Mahasiswa Teknik Informatika) pada semester 5 dan melaksanakan program magang di stasiun televisi TVRI Kaltim pada semester 7.