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.

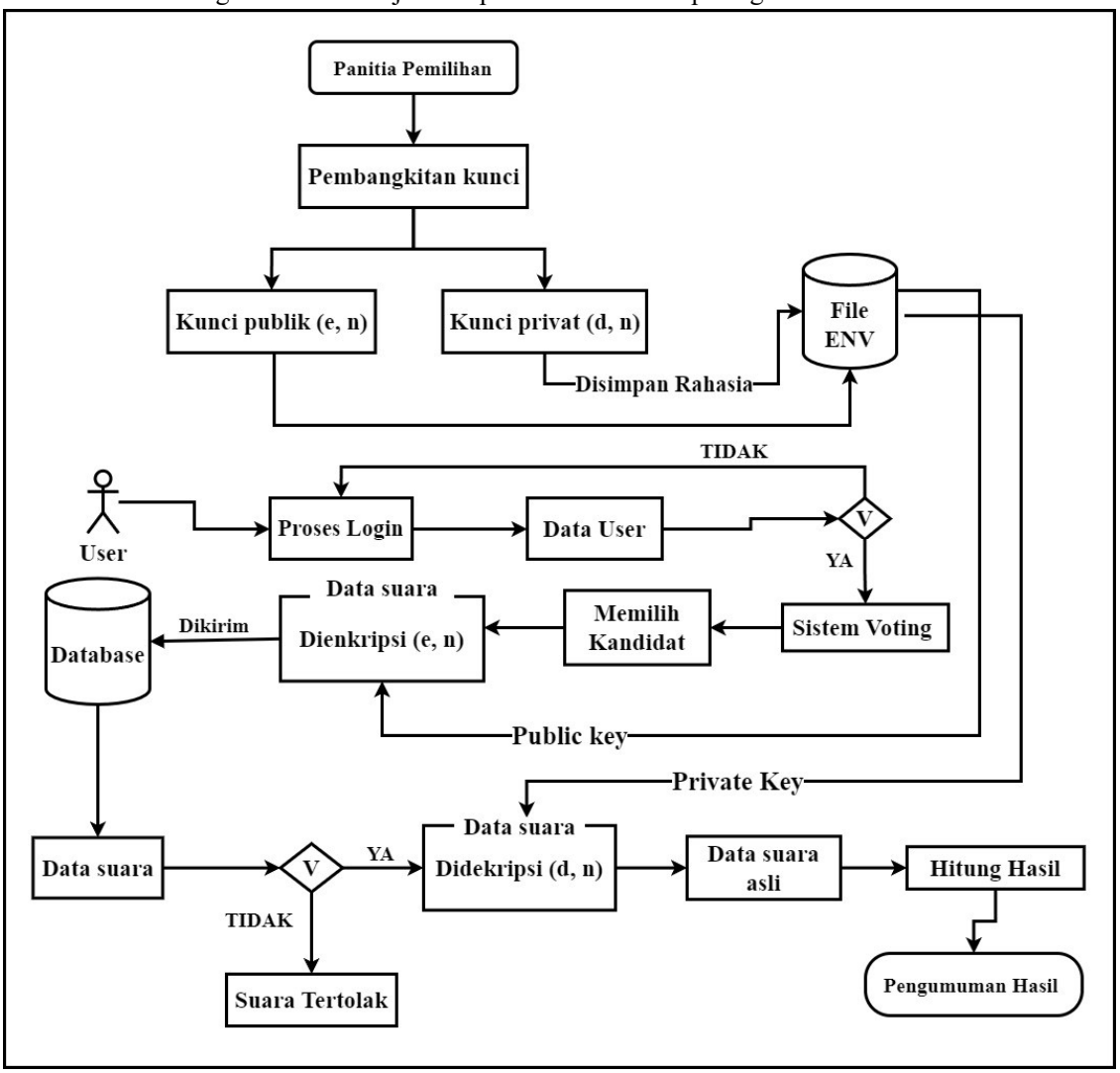
3.3. Desain Perancangan

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

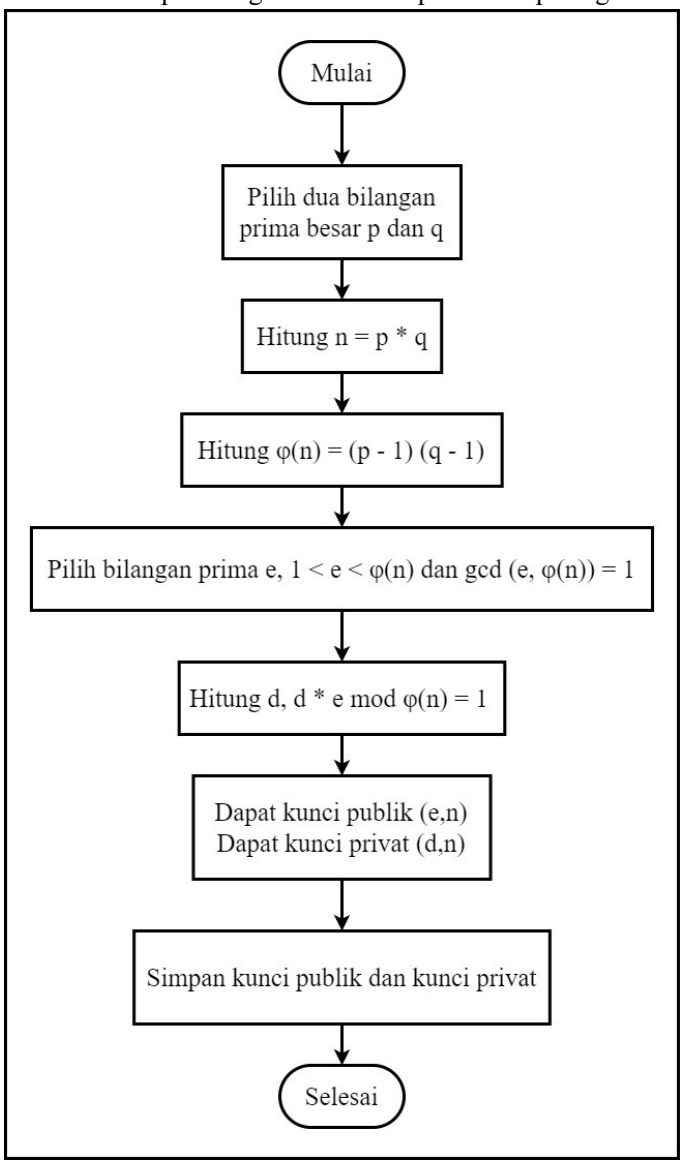


Gambar 3. 1 Alur Kerja RSA pada Sistem

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.

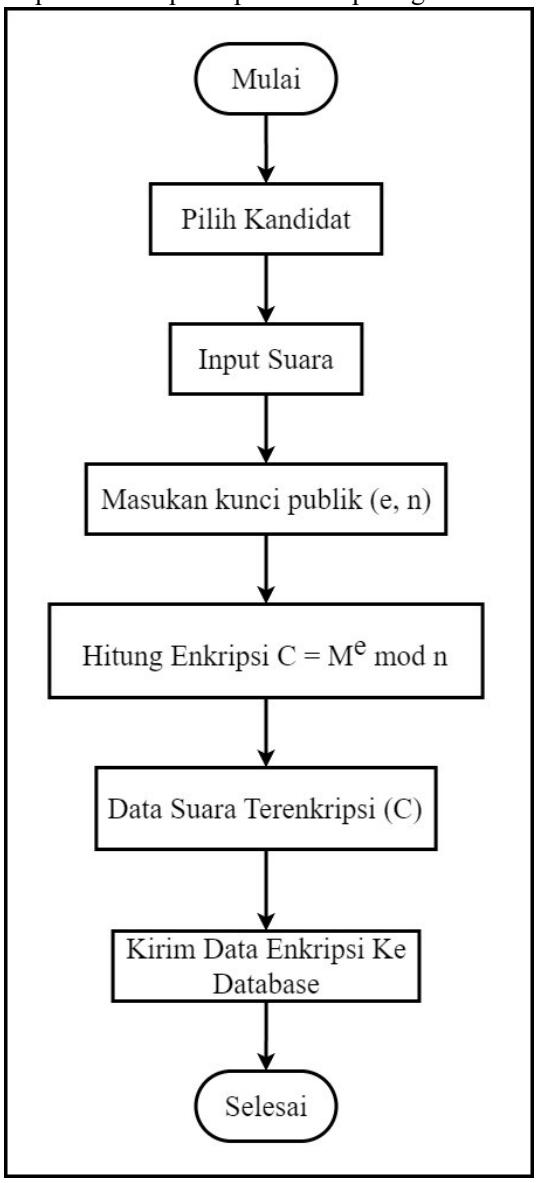


Gambar 3. 2 Pembangkitan kunci

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.

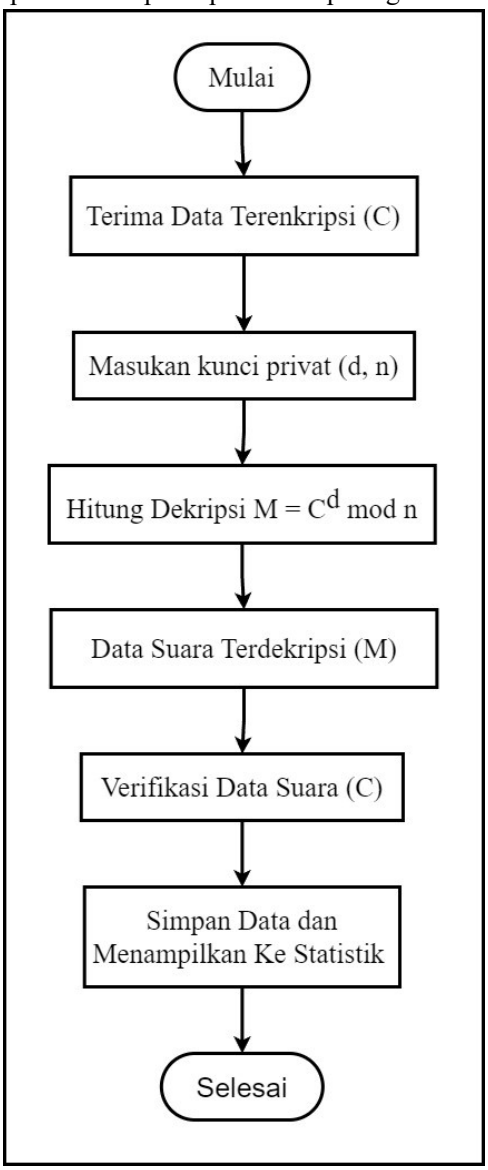


Gambar 3. 3 Proses Enkripsi

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.



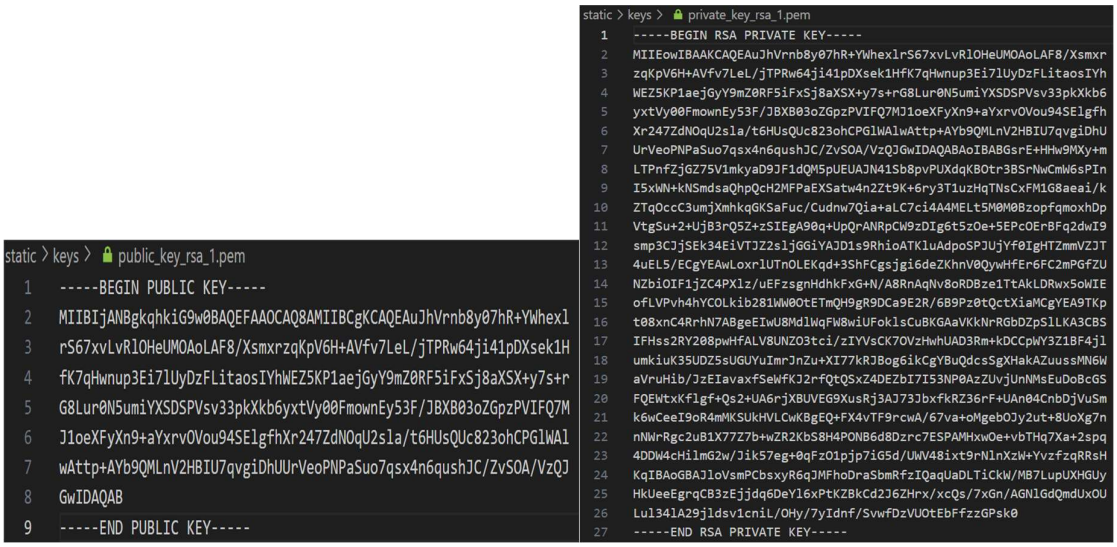
Gambar 3. 4 Proses Dekripsi

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.

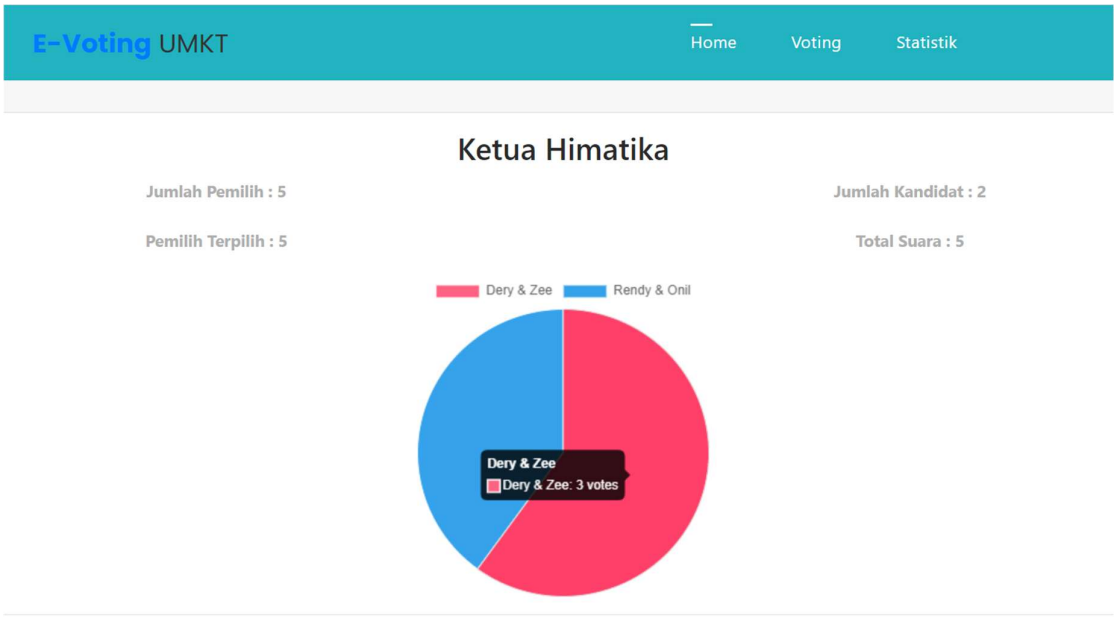
3.4.2 Mekanisme Enkripsi dan Dekripsi

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+SN2406hiQh
2	2024-07-06 09:31:21.302984	awurVN/VnRgnlUJPC4AL0Hn6uva	agMdMr7jhWKx/Zyb6LCtAC8qBtuC	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

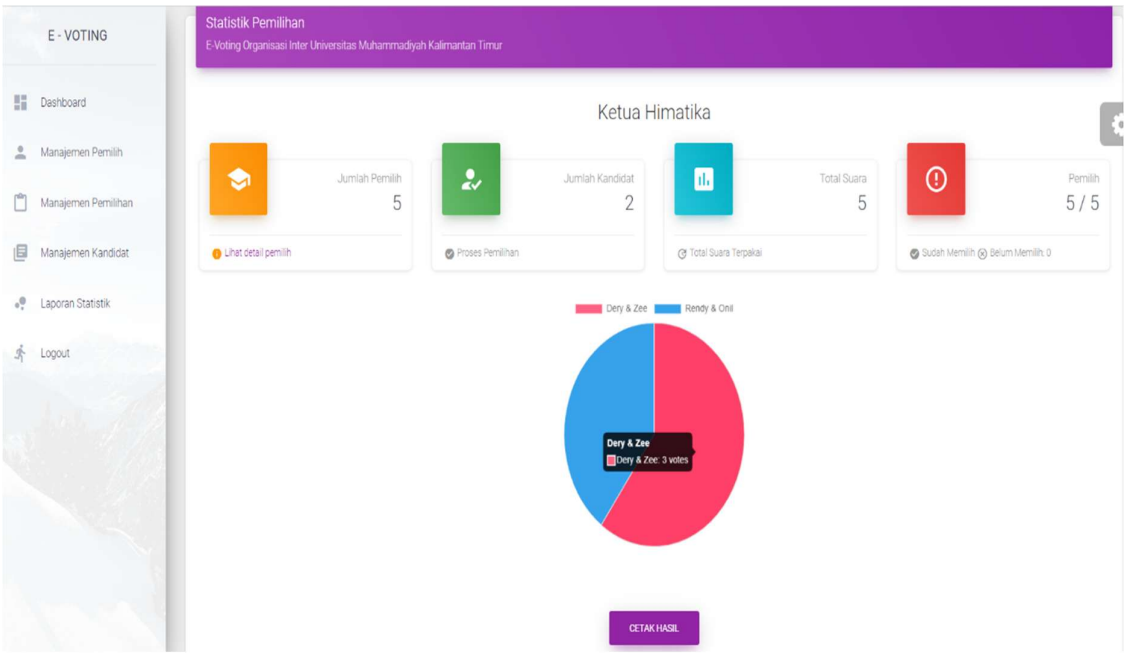
Gambar 3. 6 Hasil yang Enrkipsi di Database

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.