

**KEAMANAN SISTEM DATABASE APLIKASI E-VOTING
MENGUNAKAN 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
MENGUNAKAN 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
MENGUNAKAN 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**

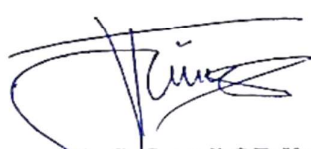
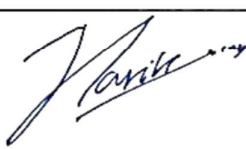
LEMBAR PENGESAHAN

KEAMANAN SISTEM DATABASE APLIKASI E-VOTING MENGUNAKAN 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 NIDN. 1111089501	 Savekti Harits Suryawan, S.Kom, M.Kom 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
MENGUNAKAN 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.

ABSTRACT

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 Peneliti 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 Universitas 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 Informatika 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.

Walaikumsalam Wr. Wb

Samarinda, Juli 2024

Peyusun



Dery Dinata

2011102441185

DAFTAR ISI

LEMBAR PERSETUJUAN.....	i
LEMBAR PENGESAHAN.....	ii
PERNYATAAN KEASLIAN PENELITIAN.....	iii
ABSTRAK	iv
ABSTARACT	v
PRAKATA.....	vi
DAFTAR ISI	vii
DAFTAR TABEL.....	ix
DAFTAR GAMBAR.....	x
DAFTAR LAMPIRAN	xi
BAB I PENDAHULUAN	1
1.1. Latar Belakang	1
1.1.1. Tahapan Pembangkitan kunci.....	2
1.1.2. Tahapan Enkripsi	2
1.1.3. Tahapan Dekripsi.....	2
1.2 Rumusan Masalah	3
1.3 Tujuan Penelitian.....	3
1.4 Manfaat Penelitian.....	3
BAB II METODOLOGI	4
2.1 Jenis Penelitian.....	4
2.2. Diagram Alur Penelitian.....	4
2.2.1. Identifikasi Masalah	4
2.2.3. Desain Perancangan	5
2.2.4. Implementasi Keamanan	6
2.2.5. Pengujian.....	6
2.3. Objek Penelitian	7
BAB III HASIL DAN PEMBAHASAN	8
3.1. Identifikasi Masalah	8
3.2. Analisis Kebutuhan.....	8
3.3. Desain Perancangan	9
3.3.1. Alur Kerja Algoritma RSA pada Sistem.....	9
3.3.2. Pembangkitan Kunci	10
3.3.3. Enkripsi	11
3.3.4. Dekripsi	12
3.4. Implementasi Keamanan	13

3.4.1. Pembangkitan Kunci	14
3.4.2 Mekanisme Enkripsi dan Dekripsi	14
3.5. Pengujian.....	15
3.5.1 Pengujian Fungsionalitas.....	16
3.5.2 Pengujian Sistem	16
BAB IV PENUTUP.....	18
4.1 Kesimpulan.....	18
4.2 Saran.....	18
DAFTAR PUSTAKA	19
LAMPIRAN.....	21
RIWAYAT HIDUP.....	36

DAFTAR TABEL

Tabel	Halaman
3.1 Pengujian Fungsionalitas.....	16
3.2 Pengujian Sistem	16

DAFTAR GAMBAR

Gambar	Halaman
1. 1 Proses Algoritma Asimetris	1
2. 1 Diagram Alur.....	4
2. 2 Grand Desain Keseluruhan.....	5
2. 3 Grand Desain Algoritma RSA	6
3. 1 Alur Kerja RSA pada Sistem.....	10
3. 2 Pembangkitan kunci	11
3. 3 Proses Enkripsi	12
3. 4 Proses Dekripsi.....	13
3. 5 Hasil Pembangkitan kunci.....	14
3. 6 Hasil yang Enrkripsi di Database	14
3. 7 Tampilan Front Statistik	15
3. 8 Tampilan Back Statistik.....	15

DAFTAR LAMPIRAN

Lampiran	Halaman
1. Jadwal Penelitian.....	21
2. SK Melakukan Penelitian.....	22
3. Kartu Bimbingan.....	23
4. Wawancara Narasumber Organisasi HIMATIKA.....	24
5. Wawancara Narasumber Organisasi UKM Pencak Silat.....	24
6. Hasil Wawancara.....	25
7. Surce Code Pembangkit Kunci.....	27
8. Source Code Enkripsi.....	27
9. Source Code Dekripsi.....	27
10. Source Code Pengujian Fungsional.....	28
11. Output Hasil Pengujian Fungsionalitas.....	31