

**PENGAMANAN AGREGASI DATA PADA SISTEM E-VOTING
MENGUNAKAN ENKRIPSI HOMOMORFIK DENGAN
PAILLIER CRYPTOSYSTEM
TUGAS AKHIR**



Muhammad Fadhly Azuhri

NIM. 2001020022

**PROGRAM STUDI TEKNIK INFORMATIKA
JURUSAN TEKNIK ELEKTRO DAN INFORMATIKA
FAKULTAS TEKNIK DAN TEKNOLOGI KEMARITIMAN
UNIVERSITAS MARITIM RAJA ALI HAJI
TANJUNGPINANG**

2026

**PENGAMANAN AGREGASI DATA PADA SISTEM E-VOTING
MENGUNAKAN ENKRIPSI HOMOMORFIK DENGAN
PAILLIER CRYPTOSYSTEM**

Tugas Akhir

Skema Skripsi

*Tugas Akhir diajukan sebagai salah satu persyaratan memperoleh gelar Sarjana
Teknik pada Program Studi Teknik Informatika*



Muhammad Fadhly Azuhri

NIM. 2001020022

**PROGRAM STUDI TEKNIK INFORMATIKA
JURUSAN TEKNIK ELEKTRO DAN INFORMATIKA
FAKULTAS TEKNIK DAN TEKNOLOGI KEMARITIMAN
UNIVERSITAS MARITIM RAJA ALI HAJI
TANJUNGPINANG
2026**

PERNYATAAN MENGENAI TUGAS AKHIR DAN SUMBER INFORMASI SERTA PELIMPAAHAN HAK CIPTA

Dengan ini saya menyatakan bahwa tugas akhir berjudul "Pengamanan Agregasi Data Pada Sistem E-Voting Menggunakan Enkripsi Homomorfik dengan Paillier Cryptosystem" adalah benar karya saya dengan arahan dari komisi pembimbing dan belum diajukan dalam bentuk apa pun kepada perguruan tinggi mana pun. Sumber informasi yang berasal atau dikutip dari karya yang diterbitkan maupun tidak diterbitkan dari penulis lain telah disebutkan dalam teks dan dicantumkan dalam Daftar Pustaka di bagian akhir skripsi ini.

Apabila di kemudian hari terbukti pernyataan saya tidak benar dan melanggar peraturan yang berlaku dalam karya tulis dan hak intelektual, maka saya bersedia ijazah yang telah saya terima untuk ditarik kembali oleh Universitas Maritim Raja Ali Haji dan menerima sanksi lainnya sesuai dengan peraturan yang berlaku. Dengan ini saya melimpahkan hak cipta dari karya tulis saya kepada Universitas Maritim Raja Ali Haji.

Tanjungpinang, Januari 2026



Muhammad Fadhly Azuhri
NIM 2001020022

© Hak Cipta Milik Universitas Maritim Raja Ali Haji, Tahun 2021

Hak Cipta Dilindungi Undang- Undang

Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan atau menyebutkan sumbernya. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik, atau tinjauan suatu masalah; dan pengutipan tersebut tidak merugikan kepentingan Universitas Maritim Raja Ali Haji.

Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Universitas Maritim Raja Ali Haji.



HALAMAN PERSETUJUAN

Judul : Pengamanan Agregasi Data Pada Sistem E-Voting
Menggunakan Enkripsi Homomorphic Dengan
Paillier Cryptosystem
Nama : Muhammad Fadhly Azuhri
NIM : 2001020022
Program Studi : Teknik Informatika
Tanggal Persetujuan : Januari 2026

Disetujui oleh,
Komisi Pembimbing



Hendra Kurniawan, S.Kom, M.Sc.Eng., Ph.D.
(Ketua)



Nurul Hayaty, S.T., M.Cs.
(Anggota)

HALAMAN PENGESAHAN

Judul : Pengamanan Agregasi Data Pada Sistem E-Voting Menggunakan Enkripsi Homomorphic Dengan Paillier Cryptosystem
Nama : Muhammad Fadhly Azuhri
NIM : 2001020022

Telah berhasil dipertahankan di hadapan Komisi Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk melaksanakan tugas akhir dalam memperoleh gelar Sarjana Teknik pada Program Studi Teknik Informatika, Jurusan Teknik Elektro dan Informatika, Fakultas Teknik dan Teknologi Kemaritiman, Universitas Maritim Raja Ali Haji.

KOMISI PENGUJI

Ketua	: Nerfita Nikentari, S.T., M.Cs	(.....)
Anggota I	: Feri Irawan, S.Kom., M.Kom	(.....)
Anggota II	: Marisha Pertiwi, S.Tr.Kom, M.Kom	(.....)
Anggota III	: Hendra Kurniawan, S.Kom, M.Sc.Eng., Ph.D.	(.....)
Anggota IV	: Nurul Hayaty, S.T., M.Cs.	(.....)

Mengetahui,

Ketua Jurusan Teknik Elektro dan Informatika


Hollanda Arief Kusuma, S.IK., M.Si
NIP. 198904012019031016

Tanggal Ujian : 13 Januari 2026

Tanggal Lulus :

PRAKATA

Segala puji dan syukur penulis panjatkan kepada Tuhan Yang Maha Esa atas limpahan rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan skripsi dengan judul "Pengamanan Agregasi Data Pada Sistem E-Voting Menggunakan Enkripsi Homomorfik dengan Paillier Cryptosystem" dengan baik dan tepat waktu.

Skripsi ini disusun sebagai salah satu syarat untuk meraih gelar Sarjana Teknik pada Program Studi Teknik Informatika, Fakultas Teknik dan Teknologi Kemaritiman, Universitas Maritim Raja Ali Haji. Penulis berharap hasil penelitian ini dapat memberikan sumbangsih yang berarti bagi pengembangan ilmu pengetahuan, terutama dalam bidang pengamanan data pada aplikasi e-voting menggunakan enkripsi homomorfik dengan Paillier Cryptosystem.

Penulis menyadari bahwa skripsi ini masih memiliki kekurangan. Oleh karena itu, kritik dan saran yang membangun dari berbagai pihak sangat diharapkan untuk menyempurnakan penelitian di masa mendatang.

Akhir kata, penulis berharap skripsi ini dapat memberikan manfaat bagi siapa saja yang membutuhkan serta menjadi referensi yang berguna untuk penelitian selanjutnya.

Tanjungpinang, Januari 2026



Muhammad Fadhly Azuhri

DAFTAR ISI

HALAMAN PERSETUJUAN.....	iv
HALAMAN PENGESAHAN.....	v
ABSTRAK.....	vi
ABSTRACT.....	vii
PRAKATA.....	viii
DAFTAR ISI.....	ix
DAFTAR TABEL.....	xi
DAFTAR GAMBAR.....	xii
BAB I PENDAHULUAN.....	1
A. Latar Belakang.....	1
B. Perumusan Masalah.....	2
C. Batasan Penelitian.....	2
D. Tujuan Penelitian.....	3
E. Manfaat Penelitian.....	3
BAB II KAJIAN LITERATUR.....	5
A. Tinjauan Pustaka.....	5
B. Landasan Teori.....	7
a. Pengertian <i>E-voting</i>	7
b. Pengertian Homomorfik.....	8
c. Kriptografi.....	8
d. Enkripsi Homomorfik.....	9
e. Enkripsi Homomorfik Sebagian.....	11
f. Enkripsi Homomorfik Penuh.....	12
i. Replay Attack.....	15

BAB III METODE PENELITIAN.....	17
A. Waktu dan Tempat Penelitian.....	17
B. Alat atau Instrumen Penelitian.....	17
C. Alur Penelitian	18
D. Perancangan Algoritma Kriptografi.....	20
D. Analisis Data dan Validasi Algoritma	27
BAB IV HASIL DAN PEMBAHASAN	32
A. Implementasi Sistem.....	32
a. Lingkungan Implementasi	32
b. Implementasi Antarmuka Administrator (Admin Dashboard).....	32
c. Antarmuka Sistem (<i>User Interface</i>).....	38
d. Implementasi Algoritma Paillier (Kode Program).....	41
e. Validasi Perhitungan Matematis (Proof of Concept).....	44
f. Pengujian Keamanan Jaringan (Penetration Testing).....	46
g. Analisis Kinerja Waktu Komputasi (Time Complexity Analysis)	49
h. Analisis Komparatif Efisiensi Sistem	51
BAB V SIMPULAN DAN SARAN	52
A. Simpulan	52
B. Saran	52
DAFTAR PUSTAKA	53

DAFTAR TABEL

Table 3. 1 Perangkat keras yang digunakan.....	17
Table 3. 2 Perangkat lunak yang digunakan	17
Table 4. 1 Matriks Validasi Data Homomorfik (Data Riil Database).....	45
Table 4. 2 Perbandingan Efisiensi Waktu Enkripsi	51



DAFTAR GAMBAR

Gambar 2. 1 Alur Sederhana Proses Enkripsi dan Dekripsi	8
Gambar 2. 2 Struktur umum pendekatan Homomorfik E-Voting [12].....	10
Gambar 3. 1 Diagram Alir Penelitian	18
Gambar 3. 2 Flowchart Algoritma Pembangkitan Kunci dan Enkripsi	22
Gambar 3. 3 Flowchart Alur Logika Agregasi Homomorfik.....	24
Gambar 3. 4 Activity Diagram Pembangkitan Kunci (Key Generation) ..	25
Gambar 3. 5 Activity Diagram Proses Voting & Enkripsi.....	26
Gambar 3. 6 Activity Diagram Agregasi & Dekripsi Hasil	27
Gambar 4. 1 Tampilan Login Administrator.....	33
Gambar 4. 2 Halaman Manajemen Data Kandidat	34
Gambar 4. 3 Halaman Input Data Pemilih dan Status Voting	35
Gambar 4. 4 Status Pembangkitan Kunci Kriptografi	36
Gambar 4. 5 Monitoring Real-time (Status Suara Masih Terenkripsi).....	37
Gambar 4. 6 Tampilan Hasil Akhir Pasca-Dekripsi	38
Gambar 4. 7 Halaman Login dan Validasi Status Pemilih	39
Gambar 4. 8 Tampilan Bilik Suara Digital	40
Gambar 4. 9 Kode Program Pembangkitan Kunci.....	41
Gambar 4. 10 Kode Program Enkripsi Suara.....	42
Gambar 4. 11 Kode Program Agregasi Suara.....	43
Gambar 4. 12 Kode Program Dekripsi Hasil	44
Gambar 4. 13 Tampilan Database Tabel Suara.....	45
Gambar 4. 14 Hasil Audit Protokol Keamanan SSL/TLS via Python	47
Gambar 4. 15 Hasil Simulasi Replay Attack	48
Gambar 4. 16 Pengujian Kinerja Sistem	49