

**IMPLEMENTASI TEKNOLOGI HOMOMORPHIC  
ENCRYPTION UNTUK MENINGKATKAN KEAMANAN  
DATA PADA APLIKASI E-VOTING MENGGUNAKAN  
ALGORITMA BFV ( Brakerski/Fan -Vercauteren )**

**TUGAS AKHIR**



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

**IMPLEMENTASI TEKNOLOGI HOMOMORPHIC  
ENCRYPTION UNTUK MENINGKATKAN KEAMANAN  
DATA PADA APLIKASI E-VOTING MENGGUNAKAN  
ALGORITMA BFV ( Brakerski/Fan -Vercauteren )**

Tugas Akhir

Skema Skripsi

*Tugas Akhir diajukan sebagai salah satu persyaratan memperoleh gelar Sarjana*

*Teknik pada Program Studi Teknik Informatika*



Iqbal Firmansyah

NIM. 180155201032

**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 PELIMPAHAN HAK CIPTA

Dengan ini saya menyatakan bahwa tugas akhir berjudul “Implementasi Teknologi Homomorphic Encryption Untuk Meningkatkan Keamanan Data Pada Aplikasi *E-voting* Menggunakan Algoritma BFV (Brakersi/Fan Vercauteren)” 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, Desember 2025



*Iqbal Firmansyah*  
NIM 180155201032



© 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 : Implementasi Teknologi *Homomorphic Encryption*  
Untuk Meningkatkan Keamanan Data Pada Aplikasi  
*E-voting* Menggunakan Algoritma BFV  
(Brakerski/Fan Vercauteren)

Nama : Iqbal Firmansyah

NIM : 180155201032

Program Studi : Teknik Informatika

Tanggal Persetujuan : 4 Desember 2025

Disetujui oleh,  
Komisi Pembimbing



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



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

## HALAMAN PENGESAHAN

Judul : Implementasi Teknologi *Homomorphic Encryption* Untuk Meningkatkan Keamanan Data Pada Aplikasi *E-voting* Menggunakan Algoritma BFV (Brakersi/Fan Vercauteren)

Nama : Iqbal Firmansyah

NIM : 180155201032

Telah berhasil dipertahankan di hadapan Komisi Penguji sebagai bagian persyaratan yang diperlukan 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 : Tekad Matulatan, S.Sos., S.Kom., M.Inf. Tec (.....)

Anggota I : Feri Irawan, S.Kom., M.Kom (.....)

Anggota II : Nolan Efranda, 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: 18 Desember 2025

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 **"Implementasi Teknologi *Homomorphic Encryption* Untuk Meningkatkan Keamanan Data Pada Aplikasi *E-voting* Menggunakan Algoritma BFV (Brakersi/Fan Vercauteren)"** 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 analisis data pada aplikasi *e-voting* menggunakan algoritma BFV.

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, Desember 2025



Iqbal Firmansyah

## DAFTAR ISI

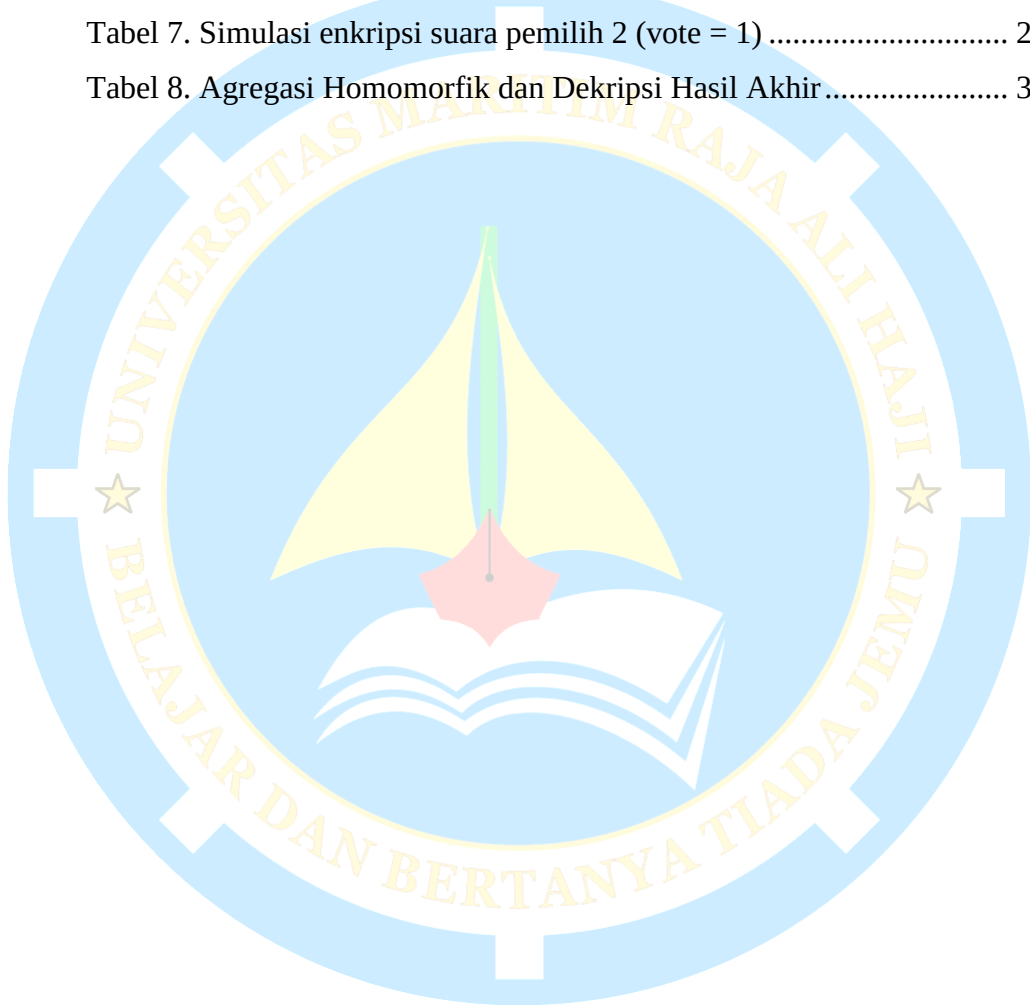
|                                   |      |
|-----------------------------------|------|
| COVER .....                       | i    |
| HALAMAN PERSETUJUAN.....          | iv   |
| HALAMAN PENGESAHAN.....           | v    |
| ABSTRAK .....                     | vi   |
| ABSTRACT .....                    | 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 .....        | 2    |
| E. Manfaat Penelitian .....       | 2    |
| BAB II KAJIAN LITERATUR .....     | 4    |
| A. Tinjauan Pustaka .....         | 4    |
| B. Landasan Teori.....            | 5    |
| Pengertian <i>E-voting</i> .....  | 6    |
| Pengertian Homomorfik.....        | 7    |
| Kriptografi.....                  | 7    |
| Enkripsi Homomorfik .....         | 7    |
| Enkripsi Homomorfik Sebagian..... | 8    |
| Enkripsi Homomorfik Penuh .....   | 9    |



|                                                   |    |
|---------------------------------------------------|----|
| Algoritma BFV (Brakerski/Fan - Vercauteren) ..... | 9  |
| BAB III METODE PENELITIAN.....                    | 11 |
| A. Waktu dan Tempat Penelitian .....              | 11 |
| B. Alat atau Instrumen Penelitian .....           | 11 |
| C. Prosedur Pelaksanaan Penelitian.....           | 12 |
| 1. Pengumpulan Data .....                         | 12 |
| 2. Analisis dan Perancangan .....                 | 12 |
| D. Perancangan Sistem .....                       | 13 |
| E. Analisis Data .....                            | 15 |
| BAB IV HASIL DAN PEMBAHASAN .....                 | 16 |
| A. Implementasi Sistem .....                      | 16 |
| B. Pengujian Kinerja Sistem .....                 | 18 |
| C. Analisis Keamanan.....                         | 19 |
| 1. ★ Analisis Kerahasiaan Data .....              | 19 |
| 2. Analisis Integritas Proses.....                | 20 |
| 3. Ketahanan Terhadap Serangan .....              | 20 |
| D. Perhitungan Manual Algoritma BFV .....         | 27 |
| E. Pembahasan.....                                | 31 |
| F. Keterbatasan Penelitian.....                   | 32 |
| BAB V SIMPULAN DAN SARAN.....                     | 33 |
| A. Simpulan .....                                 | 33 |
| B. Saran.....                                     | 34 |
| DAFTAR PUSTAKA .....                              | 35 |

## DAFTAR TABEL

|                                                             |    |
|-------------------------------------------------------------|----|
| Tabel 1. Perangkat keras yang digunakan.....                | 11 |
| Tabel 2. Perangkat lunak yang digunakan .....               | 11 |
| Tabel 3. Data waktu pemrosesan suara .....                  | 18 |
| Tabel 4. Pengujian <i>brute force</i> .....                 | 22 |
| Tabel 5. Pengaturan Parameter & Kunci.....                  | 27 |
| Tabel 6. Simulasi enkripsi suara pemilih 1 (vote = 1) ..... | 28 |
| Tabel 7. Simulasi enkripsi suara pemilih 2 (vote = 1) ..... | 29 |
| Tabel 8. Agregasi Homomorfik dan Dekripsi Hasil Akhir.....  | 30 |



## DAFTAR GAMBAR

|                                                 |    |
|-------------------------------------------------|----|
| Gambar 1. Alur Enkripsi .....                   | 7  |
| Gambar 2. <i>Homomorphic e-voting</i> .....     | 8  |
| Gambar 3. <i>Flowchart e-voting</i> .....       | 14 |
| Gambar 4. Antarmuka login.....                  | 16 |
| Gambar 5. Antarmuka pemilihan suara .....       | 17 |
| Gambar 6. Hasil pilih suara.....                | 17 |
| Gambar 7. Hasil total suara.....                | 18 |
| Gambar 8. Serangan A tanpa pertahanan.....      | 23 |
| Gambar 9. Skenario B pertahanan longgar .....   | 23 |
| Gambar 10. Skenario C pertahanan kuat.....      | 24 |
| Gambar 11. Serangan known plaintext attack..... | 26 |

