



**IMPLEMENTASI ALGORITMA KRIPTOGRAFI *ADVANCED ENCRYPTION STANDARD* (AES) DAN RSA PADA APLIKASI PENOMORAN DAN PENYIMPANAN SURAT BERBASIS WEB**

**LAPORAN SKRIPSI**

**TOPAZ MALIK AZIZ**

**41516120104**

**UNIVERSITAS  
MERCU BUANA**

**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS MERCU BUANA JAKARTA  
2023**



**IMPLEMENTASI ALGORITMA KRIPTOGRAFI *ADVANCED ENCRYPTION STANDARD* (AES) DAN RSA PADA APLIKASI PENOMORAN DAN PENYIMPANAN SURAT BERBASIS WEB**

**LAPORAN SKRIPSI**

**TOPAZ MALIK AZIZ**

**41516120104**

**UNIVERSITAS  
MERCU BUANA**

**Diajukan sebagai salah satu syarat untuk memperoleh gelar sarjana**

**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS MERCU BUANA JAKARTA  
2023**

## HALAMAN PENGESAHAN

Laporan Skripsi ini diajukan oleh:

Nama : Topaz Malik Aziz  
NIM : 41516120104  
Program Studi : Teknik Informatika  
Judul Laporan Skripsi : IMPLEMENTASI ALGORITMA KRIPTOGRAFI  
ADVANCED ENCRYPTION STANDARD (AES) DAN  
RSA PADA APLIKASI PENOMORAN DAN  
PENYIMPANAN SURAT BERBASIS WEB

Telah berhasil dipertahankan pada sidang di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Strata 1 pada Program Studi Informatika Fakultas Teknologi Informasi Universitas Mercu Buana.

Disahkan oleh:

Pembimbing : Saruni Dwiasnati, ST, MM, M.Kom  
NIDN : 0325128802  
Ketua Penguji : Sabar Rudiarto, M.Kom  
NIDN : 0309036902  
Penguji 1 : Eugenius Kau Suni, ST, MT  
NIDN : 0342018204  
Penguji 2 : Yaya Sudarya Triana, Ph.D.  
NIDN : 0016016404

  
(Runi)





Jakarta, 12 Januari 2023

Mengetahui,

Koordinator Tugas Akhir

Ketua Program Studi

  
Wawan Gunawan, S.Kom, M.T

  
Ir. Emil R. Kaburuan, Ph.D., IPM

## HALAMAN PERNYATAAN KARYA SENDIRI

Saya yang bertanda tangan di bawah ini:

Nama : Topaz Malik Aziz

NIM : 41516120104

Program Studi : Informatika

Judul Laporan Skripsi : IMPLEMENTASI ALGORITMA KRIPTOGRAFI  
*ADVANCED ENCRYPTION STANDARD (AES) DAN  
RSA PADA APLIKASI PENOMORAN DAN  
PENYIMPANAN SURAT BERBASIS WEB*

Menyatakan bahwa Laporan Skripsi ini adalah hasil karya saya sendiri dan bukan plagiat, serta semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar. Apabila ternyata ditemukan di dalam Laporan Skripsi saya terdapat unsur plagiat, maka saya siap mendapatkan sanksi akademis yang berlaku di Universitas Mercu Buana.

Jakarta, 12 Januari 2023

UNIVERSITAS  
MERCU BUANA



Topaz Malik Aziz

## KATA PENGANTAR

Puji syukur kita panjatkan kehadirat Allah Subhanahu Wa Ta'ala yang telah melimpahkan Rahmat dan Hidayah-nya sehingga penulis dapat menyelesaikan penulisan Laporan Tugas Akhir yang berjudul **“implementasi algortima kriptografi *advanced encryption standard* (aes) dan rsa pada aplikasi penomoran dan penyimpanan surat berbasis web”**.

Penulisan Laporan Tugas Akhir ini disusun sebagai salah satu syarat untuk memperoleh gelar sarjana pada Program Studi Teknik Informatika Fakultas Ilmu Komputer di Universitas Mercubuana. Keberhasilan dalam penyusunan Laporan Tugas Akhir ini tidak dapat lepas dari dukungan dan bimbingan berbagai pihak khususnya Ibu Saruni Dwiasnati, ST.MM., M.Kom selaku dosen Pembimbing Tugas Akhir, Bapak Wawan Gunawan, S.Kom., M.T. selaku Koordinator Tugas Akhir dan Bapak Ir. Emil R. Kaburuan, Ph.D., IPM selaku Ketua Program Studi Teknik Informatika Universitas Mercubuana yang telah memberikan saran, waktu, bimbingan, semangat, pengetahuan dan nasehat-nasehat yang bermanfaat yang telah diberikan kepada penulis. Dan pada kesempatan ini penulis tidak lupa juga mengucapkan ribuan terima kasih kepada :

- a. Bapak Prof.Dr.Ir. Andi Adriansyah,M.Eng. selaku Rektor Universitas Mercubuana.
- b. Bapak Dr. Mujiono, ST., MT. selaku Dekan Fakultas Ilmu Komputer Universitas Mercubuana.
- c. Bapak Ir. Emil R. Kaburuan, Ph.D., IPM selaku Ketua Program Studi Teknik Informatika Universitas Mercubuana
- d. Ibu Saruni Dwiasnati, ST.MM., M.Kom, selaku Dosen Pembimbing Akademik.
- e. Bapak dan Ibu Dosen Pengajar Fakultas Ilmu Komputer Universitas Mercubuana.
- f. Orang tua tercinta Yaitu Ibunda Nenden Hazrianthi dan Ayahanda Indra Purnama. Yang selalu memberikan support dan motivasi dukungan kepada penulis.
- g. PT. Arranet Indonesia Sejahtera serta seluruh Manajemen serta rekan kerja atas doa dan dukungannya yang senantiasa diberikan kepada penulis.
- h. Para sahabat penulis atas kebersamaanya dan bantuannya, serta semangat yang diberikan kepada penulis dalam menyelesaikan laporan ini.
- i. Pihak-pihak lain yang tidak bisa penulis sebutkan satu persatu. Terima kasih atas bantuan, motivasi serta doanya.

Penulis menyadari sepenuhnya bahwa laporan ini masih jauh dari sempurna dikarenakan terbatasnya pengalaman dan pengetahuan yang dimiliki penulis. Oleh karena itu, penulis mengharapkan segala bentuk saran serta masukan bahkan kritik yang membangun dari berbagai pihak. Semoga laporan ini bermanfaat dan dapat menambah pengetahuan khususnya bagi penulis dan pembaca pada umumnya. Akhir kata dengan segala ketulusan dan kerendahan diri, penulis mohon maaf apabila ada kesalahan dan kelemahan dalam laporan ini.

Jakarta, 12 Januari 2023



Topaz Malik Aziz



## HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Mercu Buana, saya yang bertanda tangan dibawah ini :

Nama : Topaz Malik Aziz  
NIM : 41516120104  
Program Studi : Informatika  
Judul Laporan Skripsi : IMPLEMENTASI ALGORITMA KRIPTOGRAFI  
*ADVANCED ENCRYPTION STANDARD (AES) DAN  
RSA PADA APLIKASI PENOMORAN DAN  
PENYIMPANAN SURAT BERBASIS WEB*

Demi pengembangan ilmu pengetahuan, dengan ini memberikan izin dan menyetujui untuk memberikan kepada Universitas Mercu Buana **Hak Bebas Royalti Non-Eksklusif (Non-exclusive Royalty-Free Right)** atas karya ilmiah saya yang berjudul di atas beserta perangkat yang ada (jika diperlukan).

Dengan Hak Bebas Royalti Non-Eksklusif ini Universitas Mercu Buana berhak menyimpan, mengalihmedia/format-kan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan Laporan Magang/Skripsi/Tesis/Disertasi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 12 Januari 2023

Yang menyatakan,



Topaz Malik Aziz

## DAFTAR ISI

|  |      |
|--|------|
| <b>HALAMAN JUDUL</b>   | i    |
| <b>HALAMAN PERNYATAAN KARYA SENDIRI</b>  | ii   |
| <b>KATA PENGANTAR</b>  | iv   |
| <b>HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS<br/>AKHIR UNTUK KEPENTINGAN AKADEMIS</b> | vi   |
| <b>ABSTRAK</b>   | vii  |
| <b>ABSTRACT</b>  | viii |
| <b>DAFTAR ISI</b>  | ix   |
| <b>DAFTAR TABEL</b>  | xi   |
| <b>DAFTAR GAMBAR</b>   | xii  |
| <b>DAFTAR LAMPIRAN</b>   | xiii |
| <b>BAB I PENDAHULUAN</b>   | 1    |
| 1.1 Latar Belakang   | 1    |
| 1.2 Perumusan Masalah  | 3    |
| 1.3 Tujuan Penelitian  | 3    |
| 1.4 Manfaat Penelitian   | 4    |
| 1.5 Batasan Penelitian   | 4    |
| <b>BAB II TINJAUAN PUSTAKA</b>   | 5    |
| 2.1 Penelitian Terdahulu   | 5    |
| 2.2 Teori Pendukung  | 8    |
| <b>BAB III METODE PENELITIAN</b>   | 10   |
| 3.1 Metode Penelitian  | 10   |
| 3.2 Tahapan Penelitian   | 11   |
| <b>BAB IV PEMBAHASAN</b>   | 14   |
| 4.1 <i>Use Case Diagram</i>  | 14   |
| 4.2 <i>Activity Diagram</i>  | 15   |
| 4.3 <i>Sequence Diagram</i>  | 20   |
| 4.4 <i>User Interface</i>  | 22   |
| 4.5 Implementasi Algoritma   | 25   |
| 4.6 Analisis Hasil   | 26   |



|  |    |
|--|----|
| 4.6.1 Pengujian Aplikasi                               | 26 |
| 4.6.2 Pengujian Algoritma                              | 32 |
| <b>BAB V KESIMPULAN DAN SARAN</b>                      | 34 |
| 5.1 Kesimpulan   | 34 |
| 5.2 Saran  | 34 |
| <b>DAFTAR PUSTAKA</b>                                  | 35 |
| <b>LAMPIRAN</b>  | 37 |
| Lampiran Bimbingan                                     | 37 |
| Lampiran Luaran Tugas Akhir                            | 38 |
| Lampiran Bukti Submit / Published Artikel Ilmiah / HKI | 40 |
| Lampiran Naskah Artikel Jurnal                         | 41 |
| Curriculum Vitae                                       | 46 |
| Lembar ACC Pembimbing                                  | 47 |
| Lampiran Surat Pernyataan HKI                          | 48 |



## DAFTAR TABEL

|  |    |
|--|----|
| Tabel 2.1 Penelitian Terdahulu.....    | 5  |
| Tabel 3.1 Perbandingan Fitur.....      | 12 |
| Tabel 4.1 Hasil Pengujian Peforma..... | 33 |



## DAFTAR GAMBAR

|   |    |
|---|----|
| Gambar 3.1 Tahapan Penelitian.....                                      | 11 |
| Gambar 4.1 Use Case Diagram Aplikasi Penomoran Dan Penyimpanan Surat    | 14 |
| Gambar 4.2 Activity Diagram Login.....                                  | 15 |
| Gambar 4.3 Activity Diagram Penomoran Surat.....                        | 16 |
| Gambar 4.4 Activity Diagram Penyimpanan Surat.....                      | 17 |
| Gambar 4.5 Activity Diagram Management Pengguna.....                    | 18 |
| Gambar 4.6 Activity Diagram Management Role.....                        | 19 |
| Gambar 4.7 Sequence Diagram Login.....                                  | 20 |
| Gambar 4.8 Sequence Diagram Penomoran Surat.....                        | 21 |
| Gambar 4.9 Sequence Diagram Penyimpanan Surat.....                      | 22 |
| Gambar 4.10 Sequence Diagram Management Pengguna.....                   | 22 |
| Gambar 4.11 Sequence Diagram Management Role.....                       | 23 |
| Gambar 4.12 Tampilan Halaman Login.....                                 | 23 |
| Gambar 4.13 Tampilan Halaman Utama.....                                 | 24 |
| Gambar 4.14 Tampilan Halaman Daftar Nomor Surat - Surat Keluar.....     | 24 |
| Gambar 4.15 Tampilan Halaman Daftar Nomor Surat - Surat Keluar.....     | 25 |
| Gambar 4.16 Tampilan Halaman Daftar Surat.....                          | 25 |
| Gambar 4.17 Tampilan Halaman Penyimpanan Surat.....                     | 26 |
| Gambar 4.18 Alur Implementasi Enkripsi Dokumen.....                     | 26 |
| Gambar 4.19 Alur Implementasi Dekripsi Dokumen.....                     | 27 |
| Gambar 4.20 Halaman Management Pengguna.....                            | 27 |
| Gambar 4.21 Halaman Management Pengguna Membuat Pengguna Baru.....      | 28 |
| Gambar 4.22 Halaman Management Pengguna - Pengguna Berhasil Dibuat..    | 28 |
| Gambar 4.23 Halaman Management Role.....                                | 29 |
| Gambar 4.24 Halaman Management Role Membuat Role Admin.....             | 29 |
| Gambar 4.25 Halaman Management Role - Role Berhasil Dibuat.....         | 29 |
| Gambar 4.26 Halaman Daftar Nomor Surat.....                             | 29 |
| Gambar 4.27 Halaman Daftar Nomor Surat Membuat Nomor Surat.....         | 30 |
| Gambar 4.28 Halaman Daftar Nomor Surat - Nomor Surat Berhasil Dibuat... | 30 |
| Gambar 4.29 Halaman Daftar Surat.....                                   | 31 |
| Gambar 4.30 Halaman Daftar Surat Upload Dokumen Surat.....              | 31 |
| Gambar 4.31 Halaman Daftar Surat - Surat Berhasil Di Upload.....        | 32 |
| Gambar 4.32 Hasil Enkripsi Dokumen .pdf.....                            | 32 |
| Gambar 4.33 Hasil Enkripsi Dokumen .docs.....                           | 33 |

## DAFTAR LAMPIRAN

|  |    |
|--|----|
| Lampiran 1 Lampiran Bimbingan.....                                     | 37 |
| Lampiran 2 Lampiran Luaran Tugas Akhir.....                            | 38 |
| Lampiran 3 Lampiran Bukti Submit / Published Artikel Ilmiah / HKI..... | 39 |
| Lampiran 4 Lampiran Naskah Artikel Jurnal.....                         | 40 |
| Lampiran 5 Curriculum Vitae.....                                       | 45 |
| Lampiran 6 Lembar ACC Pembimbing.....                                  | 46 |
| Lampiran 7 Lampiran Surat Pernyataan HKI.....                          | 47 |

