

**TUGAS AKHIR**  
**RANCANG BANGUN SISTEM E-ARSIP BERBASIS WEBSITE**  
**MENGGUNAKAN METODE ENKRIPSI AES STUDI KASUS**  
**KPU SIDOARJO**



Diajukan Oleh :

Ravi Octian Nafis  
1462000234

**PROGRAM STUDI INFORMATIKA**  
**FAKULTAS TEKNIK**  
**UNIVERSITAS 17 AGUSTUS 1945 SURABAYA**  
**2024**

TUGAS AKHIR

RANCANG BANGUN SISTEM E-ARSIP BERBASIS  
WEBSITE MENGGUNAKAN METODE ENKRIPSI AES  
STUDI KASUS KPU SIDOARJO

Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana  
Komputer di Program Studi Informatika



Oleh :

Ravi Octian Nafis  
1462000234

PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS TEKNIK  
UNIVERSITAS 17 AGUSTUS 1945 SURABAYA  
2024

# FINAL PROJECT

## DESIGN AND DEVELOPMENT OF A WEBSITE-BASED E- ARCHIVE SYSTEM USING THE AES ENCRYPTION METHOD. CASE STUDY OF THE SIDOARJO KPU

Prepared as partial fulfilment of the requirement for the degree of Sarjana  
Komputer at Informatics Department



By :

Ravi Octian Nafis  
1462000234

INFORMATICS DEPARMENT  
FACULTY OF ENGINEERING  
UNIVERSITAS 17 AGUSTUS 1945 SURABAYA  
2024

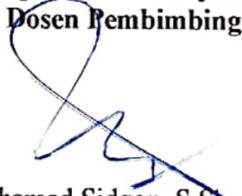
**PROGRAM STUDI TEKNIK INFORMATIKA**  
**FAKULTAS TEKNIK**  
**UNIVERSITAS 17 AGUSTUS 1945 SURABAYA**

---

**LEMBAR PENGESAHAN TUGAS AKHIR**

**Nama** : Ravi Octian Nafis  
**NBI** : 1462000234  
**Prodi** : S-1 Informatika  
**Fakultas** : Teknik  
**Judul** : RANCANG BANGUN SISTEM E-ARSIP BERBASIS  
WEBSITE MENGGUNAKAN METODE ENKRIPSI AES  
STUDI KASUS KPU SIDOARJO

**Mengetahui / Menyetujui**  
**Dosen Pembimbing**



Mochamad Sidqon, S.St., M.Si.  
NPP. 20410.96.0490

Dekan Fakultas Teknik  
Universitas 17 Agustus 1945  
Surabaya



Dr. Ir. Saipyo, S.T., M.Kes., IPU., ASEAN Eng.  
NPP. 20410.90.0197

Ketua Program Studi Informatika  
Universitas 17 Agustus 1945  
Surabaya



Aidil Primasetya Armin, S.ST., M.T.  
NPP. 20410.90.0197

## PERNYATAAN KEASLIAN DAN PERSETUJUAN PUBLIKASI TUGAS AKHIR

Saya yang bertanda tangan dibawah ini:

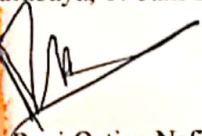
Nama : Ravi Octian Nafis  
NBI : 1462000234  
Fakultas/Program Studi : Teknik/Informatika  
Judul : RANCANG BANGUN SISTEM E-ARSIP  
BERBASIS WEBSITE MENGGUNAKAN  
METODE ENKRIPSI AES STUDI KASUS KPU  
SIDOARJO

Menyatakan dengan sesungguhnya bahwa :

1. Tugas Akhir dengan judul diatas bukan merupakan tiruan atau duplikasi dari Tugas Akhir yang sudah dipublikasikan dan atau pernah dipakai untuk mendapatkan gelar Sarjana Teknik di lingkungan Universitas 17 Agustus 1945 Surabaya maupun di Perguruan Tinggi atau Instansi manapun, kecuali bagian yang sumber informasinya dicantumkan sebagaimana mestinya.
2. Tugas Akhir dengan judul diatas bukan merupakan plagiarisme, pencurian hasil karya milik orang lain, hasil kerja orang lain untuk kepentingan saya karena hubungan material maupun non - material, ataupun segala kemungkinan lain yang pada hakekatnya bukan merupakan karya tulis tugas akhir saya secara orisinal dan otentik.
3. Demi pengembangan ilmu pengetahuan, saya memberikan hak atas Tugas Akhir ini kepada Universitas 17 Agustus 1945 Surabaya untuk menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan memublikasikan tugas akhir saya selamatap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.
4. Pernyataan ini saya buat dengan kesadaran sendiri dan tidak atas tekanan ataupun paksaan dari pihak maupun demi menegakan integritas akademik di institusi ini dan bila kemudian hari didugakut ada ketidaksesuaian antara fakta dengan kenyataan ini, saya bersedia diproses oleh tim Fakultas yang dibentuk untuk melakukan verifikasi, dengan sanksi terberat berupa pembatalan kelulusan/kesarjanaan.

Surabaya, 17 Juni 2024



  
Ravi Octian Nafis  
1462000234



UNIVERSITAS  
17 AGUSTUS 1945  
SURABAYA

BADAN PERPUSTAKAAN  
Jl. SEMOLOWARU 45 SURABAYA  
TELP. 031 593 1800 (Ext. 311)  
e-mail : perpustakaan@untag-sby.ac.id

**LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI KARYA  
ILMIAH UNTUK KEPENTINGAN AKADEMISI**

Sebagai Civitas Akademika Universitas 17 Agustus 1945 Surabaya, saya yang bertanda tangan di bawah ini:

Nama : Ravi Octian Nafis  
NBI/NPM : 1462000234  
Program Studi : Teknik Informatika  
Jenis Karya : Tugas Akhir

Demi perkembangan ilmu pengetahuan, saya menyetujui untuk memberikan kepada Badan Perpustakaan Universitas 17 Agustus 1945 Surabaya **Hak Bebas Royalti Noneksklusif (*Nonexclusive Royalty-Free Right*)**, atas karya saya yang berjudul:

**“RANCANG BANGUN SISTEM E-ARSIP BERBASIS WEBSITE  
MENGUNAKAN METODE ENKRIPSI AES STUDI KASUS KPU SIDOARJO”**

Dengan **Hak Bebas Royalti Noneksklusif (*Nonexclusive Royalty-Free Right*)**, Badan Perpustakaan Universitas 17 Agustus 1945 Surabaya berhak menyimpan, mengalihkan media atau memformatkan, mengolah dalam bentuk pangkalan data (*database*), merawat, mempublikasikan karya ilmiah selama tetap tercantum.

Dibuat di : Universitas 17 Agustus 1945 Surabaya  
Pada tanggal : 08 Agustus 2024

Yang Menyatakan,



Ravi Octian Nafis  
NBI. 1462000234

## KATA PENGANTAR

Puji syukur kehadiran kami panjatkan kehadirat Allah SWT yang telah melimpahkan rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan laporan tugas akhir ini dengan judul " Rancang Bangun Sistem E-Arsip Berbasis Website Menggunakan Metode Enkripsi Aes Studi Kasus Kpu Sidoarjo ". Laporan ini disusun sebagai syarat untuk menyelesaikan studi di Universitas 17 Agustus 1945 Surabaya (UNTAG Surabaya) dan meraih gelar Sarjana Komputer (S.Kom). penulisan laporan tugas akhir ini melibatkan serangkaian tahap penelitian yang membutuhkan waktu yang cukup lama agar menghasilkan sebuah karya yang dapat di pertanggung jawabkan.

Saya menyadari banyak pihak yang telah membantu dan membimbing saya sehingga laporan ini dapat terselesaikan tepat pada waktunya. Tidak lupa pada kesempatan ini, saya ingin menyampaikan terima kasih dan apresiasi kepada :

1. Bapak Mochamad Sidqon, S.Si., M.Si. Selaku Dosen Pembimbing yang sudah mencurahkan waktu, tenaga, pikiran, serta kesempatan untuk saya dapat mengambil bagian tugas akhir dapatterselesaikan dengan baik.
2. Bapak Dosen Wali yang telah membimbing dan mengarahkan saya selama studi di UntagSurabaya ini.
3. Bapak Ibu dosen serta para staf di Universitas 17 Agustus 1945 Surabaya (UNTAG SBY), yang telah memberikan pengetahuan, teladan, dan wejangan hikmah yang sangat berarti dan memotivasi saya untuk meraih pendidikan yang lebih tinggi lagi selama di UNTAG Surabaya.
4. KPU Kabupaten Sidoarjo, yang telah memberikan kesempatan untuk melakukan penelitian.
5. Keluarga tercinta, Bapak dan Ibu sebagai orang tua, yang selalu mendoakan, memotivasi, memperhatikan dan melengkapkan segala keperluan saya hingga terselesaikannya Tugas Akhir ini.
6. Jalu Dwi Bagaskara dan Amirah, yang telah mau sabar membimbing, mengajari, memberikan ilmunya dan yang selalu memberikan semangat kepada saya.
7. Teman-teman satu angkatan, satu perjuangan, dan satu bimbingan yang telah melewati proses Tugas Akhir bersama. Mulai dari briefing bersama, bimbingan bersama, suka dan duka bersama.

Sebagai manusia biasa saya menyadari bahwa penyusunan laporan tugas akhir masih banyak kekurangan karena keterbatasan ilmu dan pengetahuan yang saya miliki. Oleh karena itu saya ucapkan mohon maaf yang sebesar-besarnya dan bersedia menerima kritik yang membangun. Terakhir, saya harap laporan yang telah saya tulis dapat bermanfaat bagi yang membacanya.

Surabaya, 17 Juni 2024

A handwritten signature in black ink, consisting of several loops and a vertical stroke, positioned above the printed name.

Ravi Octian Nafis

1462000234

## ABSTRAK

Nama : Ravi Octian Nafis  
NBI : 1462000234  
Fakultas/Program Studi : Teknik/Informatika  
Judul : Rancang Bangun Sistem E-Arsip Berbasis Website  
Menggunakan Metode Enkripsi Aes Studi Kasus Kpu  
Sidoarjo

Studi ini bertujuan untuk merancang dan mengimplementasikan Sistem Informasi E-Arsip berbasis website di lingkungan Komisi Pemilihan Umum (KPU) Sidoarjo, dengan menerapkan metode pengembangan perangkat lunak Waterfall. Pusat perhatian utama penelitian adalah penerapan algoritma enkripsi AES dalam konteks manajemen arsip elektronik. Proses pengembangan melibatkan tahap analisis kebutuhan sistem, perancangan arsitektur, pembangunan website, dan penerapan algoritma secara berurutan, sesuai dengan prinsip-prinsip model Waterfall. Pada pengujian avalanche effect menunjukkan hasil yang memuaskan, dengan setiap perputaran bit mencapai rata-rata 50,15%, yang dianggap cukup baik. Evaluasi keberhasilan sistem akan dilakukan melalui pengukuran kehandalan, keamanan, dan efisiensi pencarian data, dengan metode validasi melalui evaluasi menyeluruh dan umpan balik pengguna untuk memastikan kecocokan sistem dengan kebutuhan khusus KPU Sidoarjo. Sebagai tambahan, penelitian ini juga akan memfokuskan perhatian pada pelatihan pengguna, dengan tujuan memastikan pemangku kepentingan, termasuk staf administratif dan petugas KPU, memahami secara mendalam penggunaan sistem, sehingga dapat meningkatkan penerapan optimal dan efektivitas sesuai dengan kebutuhan operasional KPU Sidoarjo.

**Kata Kunci** : Sistem Informasi E-Arsip, Metode Waterfall, Algoritma Enkripsi AES, avalanche effect

## ABSTRACT

Name : Ravi Octian Nafis  
NBI : 1462000234  
Department : Teknik/Informatika  
Title : Design and Development of a Website-Based E-archive System  
Using the AES Encryption Method. Case Study of the Sidoarjo KPU

This study aims to design and implement a website-based E-Archive Information System within the General Election Commission (KPU) of Sidoarjo, by applying the Waterfall software development method. The main focus of the research is the application of the AES encryption algorithm in the context of electronic records management. The development process involves analyzing system requirements, designing architecture, building websites, and implementing algorithms sequentially, according to the principles of the Waterfall model. The avalanche effect test showed satisfactory results, with each bit rotation reaching an average of 50.15%, which is considered good enough. Evaluation of the system's success will be done through measuring the reliability, security, and efficiency of data retrieval, with validation methods through thorough evaluation and user feedback to ensure the system's compatibility with the specific needs of KPU Sidoarjo. In addition, this research will also focus on user training, with the aim of ensuring that stakeholders, including administrative staff and KPU officers, have an in-depth understanding of the system's use, so as to improve optimal implementation and effectiveness in accordance with the operational needs of KPU Sidoarjo.

**Keywords:** E-Archive Information System, Waterfall Method, AES Encryption Algorithm, Avalanche effect

## DAFTAR ISI

LEMBAR PENGESAHAN TUGAS AKHIR .....	i
PERNYATAAN KEASLIAN & PERSETUJUAN PUBLIKASI TA.....	iii
KATA PENGANTAR.....	v
ABSTRAK.....	vii
ABSTRACT.....	ix
DAFTAR ISI .....	xi
DAFTAR GAMBAR.....	xv
DAFTAR TABEL.....	xix
DAFTAR PERSAMAAN .....	xxi
BAB 1 PENDAHULUAN .....	1
1.1        Latar Belakang .....	1
1.2        Rumusan Masalah .....	2
1.3        Batasan Masalah.....	2
1.4        Tujuan Penelitian.....	2
1.5        Manfaat Peneletian.....	3
BAB 2 TINJAUAN PUSTAKA DAN DASAR TEORI .....	5
2.1        Penelitian Terdahulu.....	5
2.2        Definisi E-arsip .....	13
2.3        Advanced Encryption Standard (AES).....	13
2.4        Metode Waterfall.....	14
2.5        Laravel.....	15
2.6        Mysql.....	16
2.7        BlacBox Testing .....	16

2.8	System Usability Scale .....	17
2.9	Avalanche Effect.....	18
BAB 3 METODOLOGI PENELITIAN .....		19
3.1	AES (Advanced Encryption Standard).....	19
3.2	Tahapan Penelitian.....	20
3.3	Subjek Penelitian .....	21
3.3.1	Kegiatan Penelitian .....	21
3.4	Bahan dan Alat.....	21
3.4.1	Perangkat Lunak .....	21
3.4.2	Perangkat Keras (Hardware).....	22
3.5	Metode Pengembangan Perangkat Lunak .....	22
3.5.1	Metode Waterfall.....	22
3.6	Analisis Kebutuhan.....	23
3.6.1	Kebutuhan Fungsional .....	23
3.6.2	Kebuthan Non Fungsional .....	25
3.7	Desain Sistem .....	27
3.7.1	Use Case Diagram.....	27
3.7.2	Activity Diagram.....	29
3.7.3	Perancangan Database.....	33
3.7.4	Tampilan sistem .....	37
3.8	Skenario Pengujian Perangkat Lunak.....	44
3.8.1	Metode BlackBox Testing.....	44
3.8.2	System Usability Scale.....	49
BAB 4 HASIL DAN PEMBAHASAN .....		53

4.1.	Perancangan Interface .....	53
4.2.	Halaman Admin TU .....	53
4.2.1	Halaman Staff Divisi .....	66
4.3.	Implementasi Metode AES.....	68
4.3.1	Enkripsi AES .....	69
4.3.2	Dekripsi AES .....	77
4.4.	Pengujian Sistem .....	86
4.4.1	Hasil Pengujian Blackbox.....	86
4.4.2	Hasil Pengujian System Usability Scale (SUS).....	92
4.4.3	Pengujian Avalanche Effect .....	96
BAB 5 KESIMPULAN DAN SARAN.....		99
5.1	Kesimpulan.....	99
5.2	Saran.....	99
DAFTAR PUSTAKA .....		101

## DAFTAR GAMBAR

Gambar 2. 1 Proses Metode AES .....	14
Gambar 2. 2 Tahapan Waterfall (Wahid Abdul, 2020) .....	15
Gambar 3. 1 Proses Enkripsi data metode AES .....	19
Gambar 3. 2 Tahapan Penelitian.....	20
Gambar 3. 3 Tahapan Metode Waterfall.....	22
Gambar 3. 4 Use Case Diagram .....	27
Gambar 3. 5 Activity diagram login.....	29
Gambar 3. 6 Activity diagram tambah data.....	30
Gambar 3. 7 Activity diagram edit data .....	31
Gambar 3. 8 Activity diagram hapus data halaman admin.....	31
Gambar 3. 9 Activity diagram hapus data halaman ketua KPU .....	32
Gambar 3. 10 Activity diagram konfirmasi data .....	32
Gambar 3. 11 Activity diagram kirim data .....	33
Gambar 3. 12 Class diagram .....	37
Gambar 3. 13 Halaman login .....	37
Gambar 3. 14 Halaman dashboard admin .....	38
Gambar 3. 15 Halaman dashboard ketua KPU.....	39
Gambar 3. 16 Halaman data masuk .....	39
Gambar 3. 17 Halaman tambah data .....	40
Gambar 3. 18 Halaman edit data .....	41
Gambar 3. 19 Halaman approve data .....	41
Gambar 3. 20 Approve data.....	42
Gambar 3. 21 halaman setelah approve data .....	42
Gambar 3. 22 Aksi data diterima.....	43
Gambar 3. 23 Halaman master data ketua KPU.....	43
Gambar 3. 24 Halaman master data admin .....	44

Gambar 3. 25 Halaman kirim data.....	44
Gambar 4. 1 Halaman Login .....	53
Gambar 4. 2 Halaman Dashboard.....	54
Gambar 4. 3 Halaman Master Surat Disposisi .....	54
Gambar 4. 4 Halaman Master Kategori Surat .....	55
Gambar 4. 5 Halaman Tambah Kategori .....	55
Gambar 4. 6 Halaman edit Kategori.....	56
Gambar 4. 7 Halaman rak.....	56
Gambar 4. 8 Halaman Tambah Rak.....	57
Gambar 4. 9 Halaman Edit Rak.....	57
Gambar 4. 10 Halaman.....	58
Gambar 4. 11 Halaman Data Masuk Teknis .....	58
Gambar 4. 12 Halaman Surat Masuk.....	59
Gambar 4. 13 Halaman Edit Data Teknis .....	59
Gambar 4. 14 Halaman detail data .....	60
Gambar 4. 15 Halaman edit surat masuk.....	60
Gambar 4. 16 Halaman Surat Keluar.....	61
Gambar 4. 17 Halaman Tambah Data Hukum.....	61
Gambar 4. 18 Halaman detail surat keluar .....	62
Gambar 4. 19 Halaman Master Data Hukum .....	62
Gambar 4. 20 Halaman Arsip Surat Masuk.....	63
Gambar 4. 21 Halaman Arsip Surat Keluar .....	63
Gambar 4. 22 Halaman User .....	64
Gambar 4. 23 Halaman Approve Data.....	64
Gambar 4. 24 Halaman Approve Data Ditolak.....	65
Gambar 4. 25 Approve Data sukses.....	65
Gambar 4. 26 Data Pindah ke Halaman Master Data .....	66
Gambar 4. 27 Halaman Master Data .....	66
Gambar 4. 28 Halaman Surat masuk staff.....	67

Gambar 4. 29 Halaman detail surat masuk staff.....	67
Gambar 4. 30 Halaman Surat masuk disposisi.....	68
Gambar 4. 31 Halaman Action Arsip .....	68
Gambar 4. 32 Gambar Table s-box .....	72
Gambar 4. 33 Proses shiftrows.....	72
Gambar 4. 34 Matriks mixcoloumn .....	73
Gambar 4. 35 Hasil enkripsi file .....	77
Gambar 4. 36 Proses invshiftrows.....	78
Gambar 4. 37 Tabel InvSubyte.....	79
Gambar 4. 38 Contoh Inversmixcoloumn .....	80
Gambar 4. 39 Input key dekripsi.....	85
Gambar 4. 40 Hasil dekripsi.....	86

## DAFTAR TABEL

Tabel 2. 1 Penelitian terdahulu.....	5
Tabel 3. 1 Perangkat lunak.....	21
Tabel 3. 2 Perangkat keras.....	22
Tabel 3. 3 Tabel data user.....	33
Tabel 3. 4 Tabel data arsip.....	33
Tabel 3. 5 Tabel data jenis_data .....	34
Tabel 3. 6 Tabel email .....	34
Tabel 3. 7 Tabel data.....	34
Tabel 3. 8 Table Rak.....	35
Tabel 3. 9 Tabel Password Enkripsi .....	35
Tabel 3. 10 Tabel Reset Password.....	36
Tabel 3. 11 Skenario pengujian blackbox.....	45
Tabel 3. 12 Skenario Pengujian SUS.....	50
Tabel 4. 1 Tabel Rcon.....	69
Tabel 4. 2 Tahap generate key .....	69
Tabel 4. 3 Genrate key baris 1 .....	70
Tabel 4. 4 XOR baris 1 dan tabel Rcon.....	70
Tabel 4. 5 XOR key dan baris 2 .....	70
Tabel 4. 6 XOR key dan baris 3 .....	70
Tabel 4. 7 XOR key dan baris 4 .....	71
Tabel 4. 8 Tahap preround key .....	71
Tabel 4. 9 Subtitusi bytes .....	72
Tabel 4. 10 Hasil shiftrows.....	73
Tabel 4. 11 Hasil mixcolumn.....	76
Tabel 4. 12 Hasil addroundkey dan mixcoloumn.....	76
Tabel 4. 13 Hasil prearound .....	77
Tabel 4. 14 Hasil invshitrows .....	78

Tabel 4. 15 Hasil invsubbyt .....	79
Tabel 4. 16 Hasil addroundkey .....	80
Tabel 4. 17 Hasil inversmixcoloumn .....	85
Tabel 4. 18 Hasil pengujian blackbox.....	86
Tabel 4. 19 Pengujian System Usability Scale .....	92
Tabel 4. 20 Hasil Pengujian System Usability Scale .....	94
Tabel 4. 21 Hasil Pengujian Avalanche Effect.....	96

## DAFTAR PERSAMAAN

Rumus skor rata-rata SUS (3. 1) .....	51
Rumus Avalanche Effect (4. 1).....	96