

**PENGAMANAN ARSIP DENGAN ALGORITMA ENKRIPSI
AES-256 UNTUK WEB APP E-ARSIP YAYASAN
UNIVERSITAS ISLAM SUMATERA UTARA**

SKRIPSI

Oleh

IBNU HAJAR

71170915004



**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS ISLAM SUMATERA UTARA
MEDAN
2022**

KATA PENGANTAR

Puji syukur bagi Allah SWT yang telah berikan rahmat dan hidayah-nya sehingga penulis dapat menyelesaikan skripsi dengan judul **“Pengamanan Arsip Dengan Algoritma Enskripsi AES-256 Untuk Web App E-Arsip Yayasan Universitas Islam Sumatera Utara”**.

Adapun penulisan Skripsi adalah sebagai salah satu syarat untuk memperoleh gelar Strata 1 Teknik Informatika pada Universitas Islam Sumatera Utara. Penulis menyadari sepenuhnya bahwa hasil skripsi masih jauh dari kata sempurna, namun demikian penulis telah berupaya semaksimal mungkin untuk menyusun skripsi ini dengan sebaik-baiknya.

Dalam penyelesaian skripsi, penulis tidak terlepas berdoa kepada Allah SWT yang telah memberikan imajinasi dan inspirasi dalam menyelesaikan skripsi ini dan untuk kedua orang tua saya yang tercinta, saya ucapkan terimakasih atas doa dan dukungan baik secara moril maupun materi dan motivasinya.

Selanjutnya penulis mengucapkan terima kasih kepada:

1. Bapak Ir. H. Abdul Haris Nasution, MT. Selaku Dekan Fakultas Teknik Universitas Islam Sumatera Utara
2. Bapak Mhd.Zulfansyuri S, S.T, M.Kom selaku Ketua Program Studi Teknik Informatika Universitas Islam Sumatera Utara
3. Bapak Oris Krianto Sulaiman ST,M.Kom Selaku pembimbing akademik Teknik Informatika Universitas Islam Sumatera Utara.
4. Bapak Mhd.Zulfansyuri S, S.T, M.Kom selaku Dosen Pembimbing I yang telah banyak mengarahkan dan membantu dalam penyusunan skripsi ini.

5. Bapak Oris Krianto Sulaiman ST,M.Kom selaku Dosen Pembimbing II yang telah membantu dalam penyusunan skripsi.
6. Seluruh staf pengajar Jurusan Teknik Informatika Universitas Islam Sumatera Utara yang telah banyak memberikan ilmu kepada saya selama masa perkuliahan.
7. Kepada teman seangkatan dan seperjuangan stambuk 2017 yang saling menyemangati dan berbagai informasi.
8. Semua pihak yang tidak dapat disebutkan satu persatu.

Semoga Allah memberikan balasan yang baik dan berlipat ganda kepada semuanya. Penulis menyadari bahwa dalam penulisan skripsi ini masih memiliki banyak kekurangan dalam penyusunannya. Oleh sebab itu, kritik dan saran yang membangun akan sangat penulis terima dengan senang hati demi penyempurnaan dan kemajuan laporan kerja praktik ini.

Akhirnya, hanya kepada Allah penulis serahkan segalanya, mudah-mudahan dapat bermanfaat khususnya bagi penulis, umumnya bagi kita semua.

Medan, Maret 2022

Penulis

IBNU HAJAR

71170915004

DAFTAR ISI

KATA PENGANTAR	ii
ABSTRAK	iv
DAFTAR ISI	v
DAFTAR GAMBAR	vii
DAFTAR TABEL	ix
BAB I PENDAHULUAN	
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah	3
1.4 Tujuan	3
1.5 Manfaat	3
1.6 Sistematika Penulisan	4
BAB II TINJAUAN PUSTAKA	
2.1 Arsip	5
2.2 Algoritma <i>AES-256</i>	6
2.3 Proses Enkripsi <i>AES 256</i>	7
2.3.1 <i>AddRoundKey</i>	8
2.3.2 <i>SubBytes</i>	9
2.3.3 <i>ShiftRows</i>	10
2.3.4 <i>MixColumns</i>	10
2.4 Proses Dekripsi <i>AES 256</i>	12
2.4.1 <i>InvShiftRows</i>	13
2.4.2 <i>InvSubBytes</i>	13
2.4.3 <i>InvMixColumns</i>	14
2.4.4 <i>AddRoundKey</i>	14
2.5 Tools Perancangan	15
2.6 Langkah-langkah Pembuatan UML	15
2.7 Teknologi Yang Digunakan	22
2.7.1 <i>HTML</i>	22
2.7.2 <i>CSS</i>	24

2.7.3	<i>XAMPP</i>	26
2.7.4	<i>Codeigniter (CI)</i>	27
2.7.5	<i>Bootstrap</i>	29
BAB III METODE PENELITIAN		
3.1	Metode Pengumpulan Data	31
3.2	Analisa Kebutuhan Sistem	31
3.2.1	<i>Software</i>	32
3.2.2	<i>Hardware</i>	32
3.3	Desain Sistem	32
3.3.1	<i>Desain logic</i>	32
3.3.2	Algoritma <i>AES-256</i> Pada Sistem	40
3.3.3	<i>Desain User Interface</i>	45
BAB IV HASIL DAN PEMBAHASAN		
4.1	Implementasi Algoritma Aes 256	57
4.2	Hasil Tampilan Aplikasi	58
BAB V KESIMPULAN DAN SARAN		
5.1	Kesimpulan	66
5.2	Saran	66
DAFTAR PUSTAKA		67
LAMPIRAN		

DAFTAR GAMBAR

Gambar 2.1 Proses Enkripsi <i>AES</i>	8
Gambar 2.2 <i>S-Box</i>	9
Gambar 2.3 Ilustrasi <i>ShiftRows</i>	10
Gambar 2.4 Perkalian <i>Matrix</i>	11
Gambar 2.5 Proses Dekripsi <i>AES</i>	12
Gambar 2.6 Ilustrasi <i>InvShiftRows</i>	13
Gambar 2.7 <i>Inverse S-Box</i>	13
Gambar 2.8 Perkalian <i>Matrix Invercolumn</i>	14
Gambar 2.9 Contoh Dari <i>Sequence Diagram</i>	20
Gambar 2.10 Contoh <i>Class Diagram</i>	21
Gambar 2.11 Alur Kerja Codeigniter	28
Gambar 3.1 <i>Use Case Diagram</i> Administrator	33
Gambar 3.2 <i>Use Case Diagram</i> Petugas	34
Gambar 3.3 <i>Use Case Diagram</i> KSB	34
Gambar 3.4 Desain Database Aplikasi Web App E-Arsip	35
Gambar 3.5 Diagram <i>Activity</i> dari Administrator	37
Gambar 3.6 Diagram <i>Activity</i> dari Petugas	38
Gambar 3.7 Diagram <i>Activity</i> dari KSB	39
Gambar 3.8 <i>Flowchart</i> Enkripsi Data Surat	40
Gambar 3.9 <i>Flowchart</i> Enkripsi Data <i>User</i>	41
Gambar 3.10 <i>Flowchart</i> Dekripsi <i>Password User</i>	42
Gambar 3.11 <i>Flowchart</i> Dekripsi Data Surat	43
Gambar 3.12 <i>Mockup</i> Tampilan <i>Login</i>	46
Gambar 3.13 <i>Mockup</i> Tampilan <i>Dashboard Admin</i>	47
Gambar 3.14 <i>Mockup</i> Tampilan Data <i>User</i> dan Data Pegawai	48
Gambar 3.15 <i>Mockup</i> Tampilan Tambah Data <i>User</i> dan Data Pegawai	49
Gambar 3.16 <i>Mockup Profile</i> Yayasan	50
Gambar 3.17 <i>Mockup</i> Tampilan <i>Profile User</i>	51
Gambar 3.18 <i>Mockup</i> Tampilan Pengaturan <i>Profile User</i>	52

Gambar 3.19 <i>Mockup</i> Tampilan Surat Masuk dan Surat Keluar	53
Gambar 3.20 <i>Mockup</i> Tampilan Tambah Surat Masuk dan Surat Keluar	54
Gambar 3.21 <i>Mockup</i> Tampilan Laporan Surat Masuk dan Surat Keluar	55
Gambar 3.22 <i>Mockup</i> Tampilan Hasil <i>Ekport</i> Laporan	56
Gambar 4.1 Nama <i>File</i> Surat Terenkripsi	57
Gambar 4.2 Password <i>User</i> Terenkripsi	58
Gambar 4.3 Tampilan <i>Login</i>	58
Gambar 4.4 Tampilan <i>Dashboard</i>	59
Gambar 4.5 Tampilan Data <i>User</i>	59
Gambar 4.6 Tambah Data <i>User</i>	60
Gambar 4.7 Tampilan Data Pegawai	60
Gambar 4.8 Tampilan Tambah Data Pegawai	61
Gambar 4.9 Tampilan <i>Profile User</i>	61
Gambar 4.10 Tampilan Pengaturan <i>Profile User</i>	62
Gambar 4.11 Tampilan Data Surat Masuk	62
Gambar 4.12 Tampilan Tambah Data Surat Masuk	63
Gambar 4.13 Tampilan Data Surat Keluar	63
Gambar 4.14 Tampilan Tambah Data Surat Keluar	64
Gambar 4.15 Tambilan Laporan Surat Masuk	64
Gambar 4.16 Hasil Eksport Laporan Surat Masuk	65

DAFTAR TABEL

Table 2.1 Simbol <i>Flowchart</i> Diagram	16
Table 2.2 Simbol <i>Use Case</i> Diagram	19
Table 2.3 Simbol <i>Activity</i> Diagram	21

DAFTAR PUSTAKA

- Amalia A, Suwarjono S. 2018. "Sistem Penjadwalan Perkuliahan Pada Universitas Musamus Menggunakan Algoritma Genetika Berbasis Web". *Musamus Journal Of Research Information And Communications Technology Vol 1 No 1*.
- Booch G, Rumbaugh J, Jacobson I . 1999. "Uml Basics: An Introduction To The Unified Modeling Language".
- Dwi Mawarni P, Yoga Prasetyawan Y. "Pengelolaan Arsip Dinamis Aktif Di Kantor Perpustakaan Dan Arsip Daerah Kabupaten Kendal".
- Destiningrum M, Adrian Q. 2017. "Sistem Informasi Penjadwalan Dokter Berbasis Web Dengan Menggunakan Framework Codeigniter (Studi Kasus: Rumah Sakit Yukum Medical Centre)". *Jurnal Teknoinfo, Vol. 11, No. 2*.
- Fathurrahman M. 2018. "Pentingnya Arsip Sebagai Sumber Informasi". *Jipi (Jurnal Ilmu Perpustakaan Dan Informasi Vol. 3 No. 2*.
- Irsyad S, Sitio A. 2019. "Penerapan Konsep Mvc Pada Sistem Penjualan Online Dengan Sistem Keamanan Menggunakan Algoritma Rijndael". *Jurnal Informatika, Manajemen Dan Komputer Vol 11 No 2*.
- Muharram F. "Analisis Algoritma Pada Proses Enkripsi Dan Dekripsi File Menggunakan Advanced Encryption Standard". *Prosiding Seminar Nasional Ilmu Komputer Dan Teknologi Informatika Vol 3 No 2*.
- Nahado M, Mei Hellyana C, Faqih H. 2016. "Perancangan Sistem Pakar Pendeteksi Error Bahasa Pemrograman Php Berbasis Web". *Konferensi Nasional Ilmu Sosial & Teknologi (Knist)*.

Rasuliano Laberto Kelen Y. 2018. "Implementasi Model-View-Controller (Mvc) Pada Ujian Online Melalui Penerapan Framework Codeigniter". *Jurnal Pendidikan Teknologi Informasi (Jukanti) Volume (1) No (1)*.

Wisnu Bhaudhayana G, Made Widiartha I..2015. "Implementasi Algoritma Kriptografi Aes 256 Dan Metode Steganografi Lsb Pada Gambar Bitmap". *Jurnal Ilmiah Ilmu Komputer Universitas Udayana. Vol 8 No 2*.

Yuniati V, Gani I, Rahmat A. 2009. "Enkripsi Dan Dekripsi Dengan Algoritma Aes 256 Untuk Semua Jenis File". *Jurnal Informatika, Volume 5 Nomor 1*.