



**IMPLEMENTASI ALGORITMA AES-128
PADA *MOBILE LEARNING* UNIVERSITAS JEMBER**

SKRIPSI

diajukan guna melengkapi tugas akhir dan memenuhi salah satu syarat untuk menyelesaikan pendidikan di Program Studi Sistem Informasi Universitas Jember dan mendapat gelar Sarjana Sistem Informasi

Oleh

Ragilliyandi Erick Putra Irawan

NIM 102410101099

**PROGRAM STUDI SISTEM INFORMASI
UNIVERSITAS JEMBER**

2014

PERSEMBAHAN

Skripsi ini saya persembahkan untuk :

1. Allah SWT;
2. Keluarga;
3. Dosen Pembimbing;
4. Almamater Program Studi Sistem Informasi Universitas Jember.

PERNYATAAN

Saya yang bertanda tangan di bawah ini:

Nama : Ragilliyandi Erick Putra Irawan

NIM : 102410101099

menyatakan sesungguhnya bahwa karya ilmiah yang berjudul “Implementasi Algoritma AES-128 pada *Mobile Learning* Universitas Jember” adalah benar-benar hasil karya sendiri, kecuali kutipan yang sudah saya sebutkan sumbernya, belum pernah diajukan pada institusi mana pun dan bukan karya jiplakan. Saya bertanggung jawab atas keabsahan dan kebenaran isisnya sesuai dengan sikap ilmiah yang harus dijunjung tinggi.

Demikian pernyataan ini saya buat dengan sebenarnya, tanpa ada tekanan dan paksaan dari pihak manapun serta bersedia mendapat sanksi akademik jika ternyata di kemudian hari pernyataan ini tidak benar.

Jember, September 2014

Yang menyatakan,

Ragilliyandi Erick Putra Irawan

NIM. 102410101099

PENGESAHAN PEMBIMBING

Skripsi berjudul “Implementasi Algoritma AES-128 pada Mobile Learning Universitas Jember”, telah diuji dan disahkan pada:

Hari tanggal : Kamis, 11 September 2014

Tempat : Program Studi Sistem Informasi Universitas Jember

Disetujui oleh:

Pembimbing I,

Pembimbing II,

Dwiretno Istiyadi Swasono ST.,M.Kom.

NIP. 197803302003121003

Yanuar Nurdiansyah ST.,M.Cs.

NIP. 19810123201021003

SKRIPSI

**IMPLEMENTASI ALGORITMA AES-128
PADA *MOBILE LEARNING* UNIVERSITAS JEMBER**

Oleh:

RAGILLIYANDI ERICK PUTRA IRAWAN

NIM. 102410101099

Pembimbing

Pembimbing Utama : Dwiretno Istiyadi Swasono ST.,M.Kom.

Pembimbing Anggota : Yanuar Nurdiansyah ST.,M.Cs.

PENGESAHAN

Skripsi berjudul “Implementasi Algoritma AES-128 pada *Mobile Learning* Universitas Jember”, telah diuji dan disahkan pada:

Hari tanggal : Kamis, 11 September 2014

Tempat : Program Studi Sistem Informasi Universitas Jember

Tim Penguji

Ketua,

Dr. Saiful Bukhori, ST., M.Kom

NIP. 196811131994121001

Anggota I,

Anggota II,

Anang Andrianto ST.,MT

NIP. 196906151997021002

Nelly Oktavia Adiwijaya, S.Si., MT.

NIP. 198410242009122008

Mengesahkan

Ketua Program Studi

Prof. Drs. Slamini, M.Comp.Sc.,Ph.D

NIP. 19670420 1992011001

DAFTAR ISI

	Halaman
HALAMAN JUDUL.....	i
PERSEMBAHAN.....	ii
PERNYATAAN	iii
PENGESAHAN PEMBIMBING.....	iv
PENGESAHAN	vi
DAFTAR GAMBAR	x
DAFTAR TABEL.....	xiii
BAB 1 . PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	2
1.3 Tujuan dan Manfaat	2
1.3.1 Tujuan	3
1.3.2 Manfaat	3
1.4 Batasan Masalah	4
1.5 Sistematika Penulisan	4
BAB 2 . TINJAUAN PUSTAKA.....	7
2.1 Pengertian Keamanan Data.....	7
2.2 Pengertian Kriptografi	7
2.3 Jenis Algoritma Kriptografi	9
2.4 Algoritma AES	10
2.5 Algoritma AES-128	11
2.6 <i>Mobile Learning</i>	19
2.7 <i>Mobile Android</i>	20
2.8 Model <i>Waterfall</i>	21
BAB 3 . METODOLOGI PENELITIAN	24

3.1 Jenis Penelitian	24
3.2 Alur Penelitian	24
3.3.1 Tahap Pengumpulan Data	25
3.3.2 Tahap Perancangan	26
3.3.3 Tahap Implementasi	27
3.3.4 Tahap Pengujian	27
3.3.5 Tahap Penyusunan Skripsi	28
BAB 4 . DESAIN DAN PERANCANGAN SISTEM	29
4.1 Analisis Kebutuhan Perangkat Lunak	29
4.2 Usecase Diagram	30
4.3 Skenario	32
4.4 <i>Activity Diagram</i>	41
4.5 <i>Sequence Diagram</i>	54
4.6 <i>Class Diagram</i>	68
4.7 <i>Entity Relation Diagram</i>	71
4.8 Implementasi Perancangan	73
4.9 Pengujian	73
BAB 5 . HASIL DAN PEMBAHASAN	79
5.1 <i>E-Learning</i> Universitas Jember	79
5.2 Hasil Implementasi <i>Mobile Learning</i>	80
5.2.1 Tampilan <i>Splash Screen</i>	80
5.2.2 Tampilan <i>Login</i>	81
5.2.3 Tampilan Halaman Utama	81
5.2.4 Tampilan Menu Utama	81
5.2.5 Tampilan Menu <i>Course</i>	82
5.2.6 Tampilan Aktivitas Perkuliahan	82
5.2.7 Tampilan Detail Aktivitas Perkuliahan	83
5.2.8 Tampilan Menu <i>Broadcast</i>	84
5.2.9 Tampilan <i>Pop-Up Notification</i>	85

5.2.10 Tampilan Detail Pemberitahuan	85
5.3 Hasil Implementasi AES-128 pada <i>mobile learning</i>	86
BAB 6 . PENUTUP	94
6.1 Kesimpulan	94
6.2 Saran	94
DAFTAR PUSTAKA	95
LAMPIRAN	97

DAFTAR GAMBAR

	Halaman
Gambar 2.1 Kriptografi simetri.....	10
Gambar 2.2 Kriptografi asimetri.....	10
Gambar 2.3 Enkripsi AES-128	12
Gambar 2.4 Matriks berita 4x4	13
Gambar 2.5 RotWord.....	13
Gambar 2.6 SubBytes	14
Gambar 2.7 XOR	14
Gambar 2.8 Round Key 1.....	15
Gambar 2.9 SubBytes State	15
Gambar 2.10 ShiftRows	16
Gambar 2.11 Perkalian Matriks a(x).....	16
Gambar 2.12 Implementasi MixColumns pada state	17
Gambar 2.13 Proses enkripsi AES-128 secara lengkap.....	18
Gambar 2.14 Dekripsi AES-128	18
Gambar 2.15. Arsitektur Mobile learning.....	20
Gambar 2.16 Arsitektur Android	21
Gambar 2.17 Model Waterfall	22
Gambar 3.1 Diagram alir penelitian.....	25
Gambar 4.1 Usecase mobile learning	30
Gambar 4.2 Usecase webservice.....	31
Gambar 4.3 Activity diagram login	42
Gambar 4.4 Activity diagram logout	43
Gambar 4.5 Activity diagram melihat daftar mata kuliah.....	44

Gambar 4.6 Activity diagram melihat daftar aktivitas perkuliahan	45
Gambar 4.7 Activity diagram melihat detail aktivitas perkuliahan	46
Gambar 4.8 Activity diagram melihat daftar pemberitahuan.....	47
Gambar 4.9 Activity diagram melihat detail pemberitahuan	48
Gambar 4.10 Activity diagram menyiarkan pesan.....	49
Gambar 4.11 Activity diagram keluar.....	50
Gambar 4.12 Activity diagram memvalidasi data login	50
Gambar 4.13 Activity diagram meminta daftar pemberitahuan.....	51
Gambar 4.14 Activity diagram meminta daftar mata kuliah.....	51
Gambar 4.15 Activity diagram meminta daftar aktivitas perkuliahan	52
Gambar 4.16 Activity diagram meminta detail aktivitas perkuliahan	52
Gambar 4.17 Activity diagram mengirimkan pesan siaran.....	53
Gambar 4.18 Activity diagram menghapus data login.....	53
Gambar 4.19 Activity diagram mengirimkan pemberitahuan aktivitas perkuliahan ..	54
Gambar 4.20 Sequence diagram login	55
Gambar 4.21 Sequence diagram logout	56
Gambar 4.22 Sequence diagram keluar	56
Gambar 4.23 Sequence diagram melihat daftar mata kuliah	57
Gambar 4.24 Sequence diagram melihat daftar aktivitas perkuliahan.....	58
Gambar 4.25 Sequence diagram melihat daftar pemberitahuan	59
Gambar 4.26 Sequence diagram melihat detail aktivitas perkuliahan	60
Gambar 4.27 Sequence diagram melihat detail pemberitahuan.....	61
Gambar 4.28 Sequence diagram menyiarkan pesan	62
Gambar 4.29 Sequence diagram memvalidasi data login	63
Gambar 4.30 Sequence diagram meminta daftar pemberitahuan	64
Gambar 4.31 Sequence diagram meminta daftar matakuliah	65
Gambar 4.32 Sequence diagram meminta daftar aktivitas perkuliahan.....	66
Gambar 4.33 Sequence diagram meminta detail aktivitas perkuliahan	67
Gambar 4.34 Sequence diagram mengirimkan pesan siaran	67

Gambar 4.35 Sequence diagram menghapus data login	68
Gambar 4.36 Sequence diagram mengirimkan pemberitahuan aktivitas perkuliahan	68
Gambar 4.37 Class diagram mobile learning	69
Gambar 4.38 Class diagram webservice	70
Gambar 5.1 Halaman Utama e-learning Universitas Jember	79
Gambar 5.2 Tampilan splash screen	80
Gambar 5.3 Tampilan menu login	80
Gambar 5.4 Tampilan saat berhasil login	81
Gambar 5.5 Tampilan menu mobile learning	81
Gambar 5.6 Tampilan menu course	82
Gambar 5.7 Tampilan aktivitas perkuliahan	82
Gambar 5.8 Tampilan detail aktivitas perkuliahan	83
Gambar 5.9 Tampilan menu broadcast	84
Gambar 5.10 Notifikasi aktivitas perkuliahan	84
Gambar 5.11 Tampilan menu notifikasi.....	85
Gambar 5.12 Tampilan detail pemberitahuan.....	85
Gambar 5.13 Komunikasi data tanpa AES-128	86
Gambar 5.14 Komunikasi data menggunakan AES-128	87
Gambar 5.15 Data daftar mata kuliah tanpa AES-128.....	87
Gambar 5.16 Data daftar mata kuliah dengan AES-128.....	88
Gambar 5.17 Data daftar aktivitas perkuliahan tanpa AES-128.....	89
Gambar 5.18 Data daftar aktivitas perkuliahan dengan AES-128	89
Gambar 5.19 Data detail aktivitas perkuliahan tanpa AES-128	90
Gambar 5.20 Data detail aktivitas perkuliahan dengan AES-128.....	91
Gambar 5.21 Data daftar pemberitahuan tanpa AES-128.....	92
Gambar 5.22 Data daftar pemberitahuan dengan AES-128.....	93

DAFTAR TABEL

	Halaman
Tabel 4.1 Definisi <i>usecase mobile learning</i>	30
Tabel 4.2 Definisi aktor <i>usecase mobile learning</i>	31
Tabel 4.3 Definisi <i>usecase webservice</i>	32
Tabel 4.4 Definisi aktor <i>usecase webservice</i>	32
Tabel 4.5 Skenario <i>login</i>	32
Tabel 4.6 Skenario <i>logout</i>	33
Tabel 4.7 Skenario melihat daftar mata kuliah	34
Tabel 4.8 Skenario melihat daftar aktivitas perkuliahan.....	34
Tabel 4.9 Skenario melihat detail aktivitas perkuliahan	35
Tabel 4.10 Skenario melihat daftar pemberitahuan	35
Tabel 4.11 Skenario melihat detail pemberitahuan.....	36
Tabel 4.12 Skenario menyiarkan pesan	36
Tabel 4.13 Skenario keluar	37
Tabel 4.14 Skenario memvalidasi <i>data login</i>	37
Tabel 4.15 Skenario meminta daftar pemberitahuan	38
Tabel 4.16 Skenario meminta daftar mata kuliah	38
Tabel 4.17 Skenario meminta daftar aktivitas perkuliahan.....	39
Tabel 4.18 Skenario meminta detail aktivitas perkuliahan	39
Tabel 4.19 Skenario menghapus <i>data login</i>	40
Tabel 4.20 Skenario mengirimkan pesan siaran	40
Tabel 4.21 Skenario mengirimkan pemberitahuan aktivitas perkuliahan	40
Tabel 4.22 <i>Test case</i> pengujian fungsi dekripsi jalur 1	74
Tabel 4.23 <i>Test case</i> pengujian fungsi dekripsi jalur 2.....	74

Tabel 4.24 <i>Test case</i> pengujian fungsi enkripsi jalur 1	75
Tabel 4.25 <i>Test case</i> pengujian fungsi enkripsi jalur 2	75
Tabel 4.26 Pengujian <i>blackbox</i> pada aplikasi <i>mobile learning</i>	76
Tabel 4.27 Pengujian <i>blackbox</i> pada aplikasi <i>webservice</i>	77