



**IMPLEMENTASI ALGORITMA *ADVANCED ENCRYPTION*
STANDARD (AES) DAN *HASH* UNTUK IDENTIFIKASI KEASLIAN
IJAZAH**

SKRIPSI

MOH. MULKI RIDHO

1110511099

**UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN” JAKARTA
FAKULTAS ILMU KOMPUTER
PROGRAM STUDI TEKNIK INFORMATIKA
2016**



**IMPLEMENTASI ALGORITMA *ADVANCED ENCRYPTION*
STANDARD (AES) DAN *HASH* UNTUK IDENTIFIKASI KEASLIAN
IJAZAH**

SKRIPSI

**Diajukan Sebagai Salah Satu Syarat untuk Memperoleh Gelar
Sarjana Komputer**

MOH. MULKI RIDHO

1110511099

**UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN” JAKARTA
FAKULTAS ILMU KOMPUTER
PROGRAM STUDI TEKNIK INFORMATIKA
2016**

PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya sendiri, dan semua sumber yang dikutip maupun yang dirujuk telah saya nyatakan dengan benar.

Nama : Moh. Mulki Ridho

NRP : 111.0511.099

Tanggal : 22 Januari 2016

Bilamana dikemudian hari ditemukan ketidak sesuaian dengan pernyataan saya ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 22 Januari 2016

Yang Menyatakan,



Moh. Mulki Ridho

PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai civitas akademik Universitas Pembangunan Nasional “Veteran” Jakarta, saya yang bertanda tangan di bawah ini :

Nama : Moh. Mulki Ridho
NRP : 111.0511.099
Fakultas : **Fakultas Ilmu Komputer**
Program Studi : **Teknik Informatika**

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberika kepada Universitas Pembangunan Nasional “Veteran” Jakarta Hak Bebas Royalti Non eksklusif (*Non-exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul : *Implementasi Algoritma Advanced Encryption Standard (AES) dan Hash Untuk Identifikasi Keaslian Ijazah.*

Berserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional “Veteran” Jakarta berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan Tugas Akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta

Pada tanggal : 22 Januari 2016

Yang menyatakan,



Moh. Mulki Ridho

PENGESAHAN

Skripsi diajukan oleh :

Nama : Moh. Mulki Ridho
NRP : 111.0511.099
Program Studi : Teknik Informatika
Judul Tugas Akhir : Implementasi Algoritma *Advanced Encryption Standard*
(AES) dan *Hash* Untuk Identifikasi Keaslian Ijazah.

Telah berhasil dipertahankan dihadapan Tim Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional “Veteran” Jakarta.



Titin Pramiyati, S.Kom., M.Si
Ketua Penguji



Anita Muliawati, S.Kom., MTI
Penguji I



Henki Bayu Seta, S.Kom., MTI
Penguji II (Pembimbing)



Dr. Nidjo Sandjojo, M.Sc
Dekan



Yuni Widiastiwi, S.Kom., M.Si
Ka. Prodi

Ditetapkan di : Jakarta

Tanggal Ujian : 22 Januari 2016

IMPLEMENTASI ALGORITMA *ADVANCED ENCRYPTION* *STANDARD* (AES) DAN HASH UNTUK IDENTIFIKASI KEASLIAN IJAZAH

Moh. Mulki Ridho

Abstrak

Penelitian ini dilakukan untuk mengetahui keaslian suatu ijazah dengan cepat. Masalah pemalsuan ijazah merupakan salah satu aspek penting dari suatu studi yang telah dilakukan. Dalam hal ini, sangat terkait dengan betapa pentingnya keaslian ijazah tersebut sebagai salah satu bukti kelulusan seseorang dalam studi atau pendidikannya. Pada umumnya ijazah yang ada hanya memerlukan legalisasi untuk menyatakan keasliannya atau dengan cara menghubungi pihak atau lembaga yang mengeluarkan ijazah tersebut. Proses ini sangat membutuhkan waktu yang lama dan kurang efisien. Oleh karena itu, penelitian ini akan menggunakan fungsi *hash* dengan menggunakan algoritma MD5 sebagai nilai integritas dari ijazah tersebut dan memanfaatkan algoritma AES sebagai keamanan dalam basis data. Dalam penelitian ini, MD5 dapat menghasilkan sidik jari digital dari informasi ijazah yang ada sehingga mempunyai nilai integritas digital untuk membuktikan keaslian suatu ijazah tersebut. Akan tetapi nilai integritas ini belum cukup untuk mengamankan data ijazah. Maka dari itu penelitian ini menerapkan algoritma AES sebagai keamanan untuk menjaga keamanan nilai integritas ini.

Kata kunci : Ijazah, *Message Digest 5* (MD5), *Advance Encryotion Standard* (AES).

IMPLEMENTASI ALGORITMA *ADVANCED ENCRYPTION* *STANDARD* (AES) DAN *HASH* UNTUK IDENTIFIKASI KEASLIAN IJAZAH

Moh. Mulki Ridho

Abstract

This study was conducted to determine the authenticity of a certificate quickly. Certificate forgery problem is one of the important aspects of a study that has been done. In this case, it is related to the importance of the authenticity of the certificate as proof of someone that has already passed in the study or education. In general, certificate requires legalization process for stating its authenticity or by contacting the person or institution that published the certificate. This process takes a long time and inefficient. Therefore, this study will use the hash function by using the MD5 algorithm as the value of the integrity of the certificate and utilizing AES algorithm as security in the database. In this study, MD5 can produce a digital fingerprint of the existing certificate information that has value digital integrity to prove the authenticity of a certificate. But the integrity is not enough to secure the data certificate. Therefore, this study will implement the AES algorithm to maintain the security of this integrity value.

Keyword : Certificate, Message Digest 5 (MD5), Advance Encryotion Standard (AES).

KATA PENGANTAR

Puji dan syukur penulis panjatkan kehadiran Allah SWT atas segala karunia-Nya sehingga skripsi ini berhasil diselesaikan. Judul yang dipilih dalam penelitian ini yang dilaksanakan sejak Desember 2015 ini adalah Implementasi Algoritma *Advanced Encryption Standard* (AES) dan *Hash* Untuk Identifikasi Keaslian Ijazah.

Pada kesempatan ini penulis menyampaikan penghargaan dan ucapan terima kasih kepada :

1. Bapak **Dr. Nidjo Sandjojo, M.Sc.** selaku Dekan Fakultas Ilmu Komputer Universitas Pembangunan Nasional “Veteran” Jakarta.
2. Ibu **Yuni Widiastiwi, S.Kom., M.Si** selaku ketua Program Studi Jurusan Teknik Informatika, Fakultas Ilmu Komputer Universitas Pembangunan Nasional “Veteran” Jakarta.
3. Bapak **Henki Bayu Seta, S.Kom., MTI** selaku Dosen Pembimbing yang telah membantu penulis dalam menyelesaikan skripsi ini dengan menyumbangkan ilmu pengetahuan serta arahan.
4. Orang tua, kakak dan adik penulis, yaitu Bapak **Moh. Ocin Marjuki, S.Sos**, Ibu **Ani Nariah**, kakak **Untari Uni Comara, S.Si**, **Meylla Cintia, Cintari Fauziah Bijanah** dan **Moh. Rajib Jahid** yang telah memberikan semangat dan membantu penulis dari segi materi dan moril sehingga penulis dapat menyelesaikan skripsi ini dengan sebaik - baiknya.
5. **Aditiya Nugraha, S.Kom**, sahabat seperjuangan yang selama proses perkuliahan banyak membantu penulis dalam memberikan ilmu dan pengetahuan yang bermanfaat.
6. **Andini Prima Putri Octaviani** yang memberikan semangat, motivasi kepada penulis, terima kasih atas pengertian dan kesabarannya selama ini.

7. Teman seperjuangan skripsi, yaitu **Windu Nugroho C. Pamungkas, Reza Pahlevi** serta teman - teman **TI 2011** yang telah memberikan semangat dan juga sumbangan pikiran terhadap penulis.
8. Tidak lupa juga penulis ucapkan terima kasih kepada seluruh staff kelurahan **Bakti Jaya** Kecamatan **Setu** yang menghibur penulis saat menyusun skripsi ini.

Dalam kesempatan ini, penulis mengharapkan saran-saran ataupun kritik yang bersifat membangun agar di kemudian hari penulis akan menjadi lebih baik lagi. Semoga skripsi ini bermanfaat bagi para pembaca. Penulis sadar dalam penyusunan skripsi ini masih banyak kekurangan dikarenakan pengalaman penulis yang amat terbatas.

Kepada semua pihak yang telah membantu penulis yang tidak dapat diucapkan satu persatu namanya, penulis ucapkan terima kasih.

Jakarta, 22 Januari 2016

Penulis

Moh. Mulki Ridho

DAFTAR ISI

HALAMAN JUDUL	i
PERNYATAAN ORISINALITAS	ii
PERNYATAAN PERSETUJUAN PUBLIKASI	iii
PENGESAHAN	iv
ABSTRAK	v
ABSTRACT	vi
KATA PENGANTAR	vii
DAFTAR ISI	ix
DAFTAR TABEL	xi
DAFTAR GAMBAR	xii
DAFTAR LAMPIRAN	xiii
BAB I PENDAHULUAN	1
I.1 Latar Belakang	1
I.2 Perumusan Masalah	2
I.3 Ruang Lingkup Penelitian	2
I.4 Tujuan dan Manfaat Penelitian	3
I.5 Luaran yang diharapkan	3
I.6 Sistematika Penulisan	4
BAB II TINJAUAN PUSTAKA	5
II.1 Keamanan Data dan Informasi	5
II.2 Kriptografi	7
II.3 <i>Advance Encrytion Standard</i> (AES)	9
II.4 <i>Message Digets</i> 5 (MD5)	16
II.5 Manajemen Sistem Basis Data	21
II.6 <i>Unified Modeling Language</i>	22
II.7 Review Penelitian Relevan	23
BAB III METODOLOGI PENELITIAN.....	26
III.1 Kerangka Penelitian	26
III.2 Identifikasi Masalah	27
III.3 Studi Kepustakaan	27
III.4 Analisis	28
III.5 Perancangan	28
III.6 Pengujian	29
III.7 Implementasi	30
III.8 Simpulan dan Dokumentasi	30
III.9 Jadwal Penelitian	30
III.10 Bahan dan Alat Penelitian	31
BAB IV ANALISIS, PERANCANGAN DAN IMPLEMENTASI	32
IV.1 Analisis Kebutuhan Sistem	33
IV.2 Perancangan Aplikasi	40
IV.3 Perancangan Implementasi MD5 dan AES	60

IV.4 Pengujian	78
IV.5 Implementasi	85
 BAB V PENUTUP	 89
V.1 Kesimpulan	89
V.2 Saran	89
 DAFTAR PUSTAKA	 90
RIWAYAT HIDUP	
LAMPIRAN	

DAFTAR TABEL

Tabel 1	Hubungan antara jumlah ronde dan panjang kunci AES	10
Tabel 2	Rincian Operasi Pada Fungsi $F(b,c,d)$	20
Tabel 3	Rincian Operasi Pada Fungsi $G(b,c,d)$	21
Tabel 4	Rincian Operasi Pada Fungsi $H(b,c,d)$	21
Tabel 5	Rincian Operasi Pada Fungsi $I(b,c,d)$	22
Tabel 6	Jadwal Penelitian	29
Tabel 7	Daftar Use Case Admin	43
Tabel 8	Daftar Use Case Pengguna	44
Tabel 9	Narasi Use Case Diagram Aplikasi Identifikasi Ijazah	44
Tabel 10	Narasi Use Case <i>Login</i> Admin	45
Tabel 11	Narasi Use Case <i>Entry</i> Data Ijazah	47
Tabel 12	Narasi Use Case Identifikasi Ijazah	49
Tabel 13	Tabel Basis Data Ijazah	56
Tabel 14	Tabel Basis Data Admin	57
Tabel 15	Contoh Perhitungan $4B \oplus 05 \oplus 01$ pada Ekspansi Kunci AES	68
Tabel 16	Contoh Perhitungan $75 \oplus 9A \oplus 00$ pada Ekspansi Kunci AES	68
Tabel 17	Contoh Perhitungan $6E \oplus 07 \oplus 00$ pada Ekspansi Kunci AES	69
Tabel 18	Contoh Perhitungan $63 \oplus 96 \oplus 00$ pada Ekspansi Kunci AES	69
Tabel 19	Contoh Perhitungan AddRoundKey	73
Tabel 20	Basis Data Ijazah	78
Tabel 21	Pengujian Waktu	80
Tabel 22	Pengujian Akurasi	80
Tabel 23	Pengujian Black-Box Pada Validasi Login	81
Tabel 24	Pengujian Black-Box Pada Entry Data Ijazah	82
Tabel 25	Pengujian Black-Box Pada Form Identifikasi Ijazah	84

DAFTAR GAMBAR

Gambar 1	Unit Data AES	10
Gambar 2	Substitusi untuk transformasi SubBytes	12
Gambar 3	Substitusi untuk transformasi InvSubBytes	13
Gambar 4	Ekspansi Kunci AES	15
Gambar 5	Fungsi Hash Satu Arah	17
Gambar 6	Struktur Algoritma MD5	18
Gambar 7	Tabel $T[i]$	19
Gambar 8	Kemungkinan Fungsi Pada Tiap Putaran	20
Gambar 9	Kerangka Penelitian	25
Gambar 10	Perkalian Matriks	37
Gambar 11	Transformasi ShiftRow	38
Gambar 12	Transformasi MixColumns	38
Gambar 13	Transformasi AddRoundKey	39
Gambar 14	Transformasi InvShiftRow	40
Gambar 15	Transformasi InvMixColumns	40
Gambar 16	Tampilan <i>Login</i> Admin.....	41
Gambar 17	Tampilan <i>Input</i> Data	42
Gambar 18	Tampilan Identifikasi Ijazah	42
Gambar 19	Tampilan <i>Alert</i> Hasil Identifikasi	43
Gambar 20	Use Case Diagram Aplikasi Identifikasi Ijazah	44
Gambar 21	Use Case <i>Login</i> Admin	45
Gambar 22	Use Case <i>Entry</i> Data Ijazah	47
Gambar 23	Use Case Identifikasi Ijazah	48
Gambar 24	Activity Diagram <i>Login</i> Admin	50
Gambar 25	Activity Diagram Menu <i>Entry</i> Admin	51
Gambar 26	Activity Diagram Identifikasi Ijazah	52
Gambar 27	Sequence Diagram <i>Login</i> Admin	53
Gambar 28	Sequence Diagram Menu <i>Entry</i> Admin	54
Gambar 29	Sequence Diagram Identifikasi Ijazah	55
Gambar 30	Class Diagram Identifikasi Ijazah	56
Gambar 31	Flowchart Program <i>Entry</i> Data Ijazah Admin	57
Gambar 32	Flowchart Program Hapus Admin	58
Gambar 33	Flowchart Program Identifikasi Ijazah	59
Gambar 34	Halaman <i>Login</i> Admin Aplikasi Identifikasi Ijazah	85
Gambar 35	Form <i>Login</i> Admin Aplikasi Identifikasi Ijazah	86
Gambar 36	Form <i>Entry</i> Data dan Data Ijazah	87
Gambar 37	Form Identifikasi Ijazah	88

DAFTAR LAMPIRAN

- Lampiran 1 Kode ASCII
- Lampiran 2 Struktur Enkripsi pada AES
- Lampiran 3 Struktur Dekripsi pada AES