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 bener.

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 mengunakan 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 kehadirat 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 membatu penulis yang tidak dapat diucapkan satu persatu namanya, penulis ucapkan terima kasih.

Jakarta, 22 Januari 2016

Penulis

Moh. Mulki Ridho

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN