ENKRIPSI DATA MENGGUNAKAN MODIFIKASI ALGORITMA AES RIJNDAEL DAN MD5

SKRIPSI

Oleh:
SHANDY PRIMADIAN MULYANA PUTRA
0910962010-96

PROGRAM STUDI ILMU KOMPUTER
JURUSAN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUANALAM
UNIVERSITAS BRAWIJAYA
MALANG

2012

ENKRIPSI DATA MENGGUNAKAN MODIFIKASI ALGORITMA AES RIJNDAEL DAN MD5

SKRIPSI

Sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer
dalam bidang Ilmu Komputer

Oleh:
SHANDY PRIMADIAN MULYANA PUTRA
0910962010-96

PROGRAM STUDI ILMU KOMPUTER
JURUSAN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUANALAM
UNIVERSITAS BRAWIJAYA
MALANG

2012

UNIVERSITAS BRAWIJAYA

LEMBAR PENGESAHAN SKRIPSI

ENKRIPSI DATA MENGGUNAKAN MODIFIKASI ALGORITMA AES RIJNDAEL DAN MD5

Oleh :

SHANDY PRIMADIAN MULYANA PUTRA
0910962010-96

Setelah dipertahankan di depan Majelis Penguji
pada tanggal 16 Juli 2012

dan dinyatakan memenuhi syarat untuk memperoleh gelar
Sarjana Komputer dalam bidang Ilmu Komputer

Pembimbing I,	Pembimbing II,
Drs. Achmad Ridok, M.Kom	Drs. Marji, MT
NIP. 196808251994031002	NIP. 196708011992031001

Mengetahui,
Ketua Jurusan Matematika
Fakultas MIPA Universitas Brawijaya

Dr. Abdul Rouf Alghofari, M.Sc
NIP.196709071992031001

UNIVERSITAS BRAWIJAYA

LEMBAR PERNYATAAN

Saya yang bertanda tangan di bawah ini :

Nama : Shandy Primadian Mulyana Putra
NIM : 0910962010-96
Jurusan : Matematika
Program Studi : Ilmu Komputer
Penulis skripsi berjudul : Enkripsi Data Menggunakan Modifikasi Algoritma Aes Rijndael Dan Md5

Dengan ini menyatakan bahwa :

1. Isi dari Skripsi yang saya buat adalah benar-benar karya sendiri dan tidak menjiplak karya orang lain, selain nama-nama yang termaktub di isi dan tertulis di daftar pustaka dalam Skripsi ini.
2. Apabila dikemudian hari ternyata Skripsi yang saya tulis terbukti hasil jiplakan, maka saya akan bersedia menanggung segala resiko yang akan saya terima.

Demikian pernyataan ini dibuat dengan segala kesadaran.

Malang, 16 Mei 2012
Yang menyatakan,

Shandy Primadian Mulyana Putra
NIM. 0910962010-96

UNIVERSITAS BRAWIJAYA

ENKRIPSI DATA MENGGUNAKAN MODIFIKASI ALGORITMA AES RIJNDAEL DAN MD5

ABSTRAK

Cara untuk menjaga keamanan informasi adalah dengan enkripsi. Enkripsi merupakan salah satu teknik yang dapat digunakan untuk mengamankan data digital dalam jaringan terbuka. Salah satu algoritma yang dapat digunakan untuk mengamankan data digital adalah algoritma AES RIJNDAEL.

AES RIJNDAEL adalah sebuah block cipher yang dijadikan standar enkripsi oleh pemerintah Amerika Serikat. Enkripsi ini diharapkan juga digunakan secara luas di seluruh dunia dan dianalisa secara luas, untuk menggantikan algoritma *Data Encryption Standard* (DES), Algoritma AES RIJNDAEL memiliki beberapa panjang kunci, 128, 192, dan 256 bit, atau maksimal 32 bytes kunci. Proses enkripsi Rijndael memiliki parameter masukan in = 16 byte, parameter keluaran out = 16 byte, serta array 1-dimensi w sebesar 44 byte untuk kunci 128 bit. Modifikasi AES RIJNDAEL dan MD5 adalah mengubah kunci standart AES RIJNDAEL menggunakan algoritma MD5 untuk membuat kunci menjadi 128 bit dan membuat proses enkripsi maupun dekripsi tidak mengalami banyak perubahan.

Kata kunci : enkripsi, dekripsi, AES, RIJNDAEL, MD5

UNIVERSITAS BRAWIJAYA

DATA ENCRYPTION USING AES RIJNDAEL ALGORITHM AND MD5 MODIFICATION

ABSTRACT

To keep information secure is encryption. Encryption is one technique that can be used to secure digital data in open network. algorithm that can be used to secure digital data is AES Rijndael algorithm.

AES Rijndael is a standard block cipher encryption used the United States. Encryption is also expected to be widely used worldwide and analyzed extensively, to replace Data Encryption Standard (DES) algorithm, AES Rijndael algorithm has some key length, 128, 192, and 256 bits, or a maximum of 32 bytes key. AES Rijndael encryption process has input parameter state = 16 bytes, the output parameter = 16 bytes, and have 1-dimensional array w 44 bytes for 128 bit key. AES Rijndael algorithm and MD5 modification is to change the standard key AES Rijndael uses the MD5 algorithm to create a 128 bit key and make equal process encryption and decryption.

Keywords: encryption, decryption, AES, Rijndael, MD5

UNIVERSITAS BRAWIJAYA

KATA PENGANTAR

Puji dan syukur kehadirat Allah SWT atas segala limpahan rahmat, taufik dan hidayah-Nya serta shalawat dan salam kepada junjungan kita Nabi Muhammad SWT, sehingga penulis dapat menyelesaikan skripsi yang berjudul "Enkripsi Data Menggunakan Modifikasi Algoritma AES Rijndael Dan MD5".

Penyusunan skripsi ini juga tak lepas dari bantuan banyak pihak, baik itu berupa bimbingan, kritik, saran, dukungan, motivasi maupun doa. Oleh karena itu, ucapan terima kasih penulis disampaikan kepada :

1. Drs. A. Ridok, M.Kom selaku dosen pembimbing, atas ketersediaan meluangkan waktu untuk memberikan bimbingan, pengarahan, saran, dan dukungan selama penyusunan skripsi ini.
2. Dr. Abdul Rouf Alghofari,M.Sc selaku Ketua Jurusan Matematika Fakultas MIPA Universitas Brawijaya Malang.
3. Drs. Marji, MT selaku Ketua Program Studi Ilmu Komputer Jurusan Matematika Fakultas MIPA Universitas Brawijaya Malang.
4. Dian Eka Ratnawati,SSi.,M.Kom selaku dosen pembimbing akademik, atas nasehat, bimbingan, saran, dukungan dan kenangan yang tidak terlupakan yang diberikan selama penulis menuntut ilmu di bangku perkuliahan.
5. Segenap bapak dan ibu dosen yang telah mendidik dan mengajarkan ilmunya kepada penulis selama menempuh pendidikan di Program Studi Ilmu Komputer Jurusan Matematika Fakultas MIPA Universitas Brawijaya.
6. Segenap staf dan karyawan di Jurusan Matematika Fakultas MIPA Universitas Brawijaya yang telah banyak membantu penulis dalam pelaksanaan penyusunan skripsi ini.
7. Secara khusus penulis ingin mengucapkan terima kasih kepada Ayahanda yang penulis banggakan dan Ibundaku tercinta dan adik penulis yang telah banyak memberikan dukungan dan pengorbanan baik secara moril maupun materil sehingga penulis dapat menyelesaikan studi dengan baik.
8. Nur Fadilahtul yang terus mensuport penulis untuk menyelesaikan skripsi ini.

9. Teman-teman di Program Studi Ilmu Komputer Fakultas MIPA Universitas Brawijaya yang telah banyak memberikan bantuannya demi kelancaran pelaksanaan penyusunan skripsi ini
10. Dan semua pihak yang terlibat baik secara langsung maupun tidak langsung yang tidak dapat disebutkan satu per satu. Terima kasih atas semua bantuan yang telah diberikan.

Penulis sadari bahwa dalam laporan ini kemungkinan masih ada kekurangan, oleh karena itu penulis sangat menghargai saran dan kritik yang sifatnya membangun dari pembaca. Semoga skripsi ini dapat bermanfaat.

Malang, 16 Mei 2012

Penulis

DAFTAR ISI

Halaman
HALAMAN JUDUL i
LEMBAR PENGESAHAN iii
LEMBAR PERNYATAAN v
ABSTRAK vii
ABSTRACT ix
KATA PENGANTAR xi
DAFTAR ISI xiii
DAFTAR GAMBAR xvii
DAFTAR SOURCE CODE xix
DAFTAR TABEL xxi

BAB I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 2
1.3 Tujuan Penelitian 3
1.4 Batasan Masalah 3
1.5 Manfaat Penelitian 3
1.6 Metode Penelitian 4
1.7 Sitematika Penulisan 4

BAB II TINJAUAN PUSTAKA 5
2.1 Konsep Dasar Kriptografi 5
2.2 Algoritma Kriptografi 6
2.3 Dasar Metode Chiper Blok 8
2.3.1 Rangkaian Bit 8
2.3.2 Operator XOR 9
2.4 Algoritma *Advanced Encryption Standart* (AES) 10
2.4.1 Operasi Enkripsi Algoritma AES 13
2.4.1.1 Transformasi *SubBytes* 13
2.4.1.2 Transformasi *ShiftRows* 15
2.4.1.3 Transformasi *MixColumn* 15
2.4.1.4 Transformasi AddRoundKey 16
2.4.2 Algoritma Dekripsi Algoritma AES 17

2.5 Algoritma MD5 19

BAB III METODE PENELITIAN 23
3.1 Analisa Sistem 24
3.1.1 Deskripsi Sistem 24
3.1.2 Batasan Sistem 27
3.2 Perancangan Sistem 27
3.2.1 Proses Modifikasi Kunci Dengan Algoritma MD5 31
3.2.2 Proses Inisialisasi *RoundKey* 31
3.2.3 Proses Inisialisasi *AddRoundKey* 34
3.3 Perancangan Antarmuka 39
3.4 Perhitungan Manual 40
3.4.1 Perhitungan Manual Enkripsi AES 40
3.4.2 Perhitungan Manual Dekripsi AES 42
3.5 Perancangan Uji Coba 43
3.5.1 Bahan Pengujian 43
3.5.2 Pengujian Keamanan File Dekripsi 44
3.5.3 Penghitungan Waktu Komputasi 44
3.5.4 Pengujian Ketahan File Dekripsi 45

BAB IV HASIL DAN PEMBAHASAN 47
4.1 Lingkungan Implementasi 47
4.1.1 Lingkungan Perangkat Keras 47
4.1.2 Lingkungan Perangkat Lunak 47
4.2 Implementasi Program 47
4.2.1 Implementasi Enkripsi 48
4.2.1.1 Implementasi Load File Enkripsi 48
4.2.1.2 Implementasi Mengubah File Ke Bentuk String 48
4.2.1.3 Implementasi Pembentukan Kunsi AES MD5 Modifikasi 49
4.2.1.4 Implementasi Enkripsi AES 49
4.2.2 Implemtasi Dekripsi AES 51
4.2.2.1 Implementasi Load File Dekripsi 51
4.2.2.2 Implementasi Mengembalikan Nilai String Ke Bentuk File 51
4.2.2.3 Implementasi Dekripsi AES 52
4.3 Implementasi Antarmuka 54
4.4 Implementasi Uji Coba 56

4.4.1 Waktu Komputasi 56
4.4.1.1 Perbandingan Waktu Enkripsi Dan Dekripsi 3 Type AES 56
4.4.1.2 Perbandingan Waktu Enkripsi Dan Dekripsi AES Dengan AES MD5+ 58
4.4.2 Pengujian Keamanan File Dekripsi 59
4.4.2.1 Pengujian Dengan Password Salah 59
4.4.2.2 Pengujian Dengan Type AES Berbeda 60
4.4.3 Pengujian Ketahanan File Dekripsi 60
4.5 Pembahasan 63
4.5.1 Analisa Hasil Pengujian Waktu Komputasi 63
4.5.2 Analisa Hasil Pengujian Keamanan File Dekripsi 66
4.5.2.1 Analisa Hasil Pengujian Dengan Password Salah 66
4.5.2.2 Analisa Hasil Pengujian Dekripsi DenganType AES Yang Berbeda 66
4.5.3 Analisa Hasil Pengujian Ketahanan File Dekripsi 66

BAB V PENUTUP 67
5.1 Kesimpulan 67
5.2 Saran 67
DAFTAR PUSTAKA 69

UNIVERSITAS BRAWIJAYA

DAFTAR GAMBAR

Gambar 2.1 Proses Enkripsi dan Deskripsi 6
Gambar 2.2 Algoritma Kriptografi Simetris 6
Gambar 2.3 Algoritma Kriptografi Asimetris 7
Gambar 2.4 Varian AES Dengan Parameternya..... 11
Gambar 2.5 Masukan Dan Keluaran *Array State* 11
Gambar 2.6 Data Masukan Ke State..... 12
Gambar 2.7 Proses Enkripsi AES Rijndael 13
Gambar 2.8 Operasi *SubBytes* Menggunakan Kotak-S..... 14
Gambar 2.9 Operasi *ShiftRows* Memutar 3 Baris Terakhir..... 15
Gambar 2.10 Operasi *MixColumn* Pada State Perkolom 16
Gambar 2.11 Algoritma MD5 21
Gambar 3. 1 Tahapan Penelitian..... 23
Gambar 3.2 *Flowchart* Enkripsi Data..... 25
Gambar 3.3 *Flowchart* Dekripsi Data..... 26
Gambar 3.4 *Flowchart* Initial Round..... 27
Gambar 3.5 *Flowchart* Standart Round 28
Gambar 3.6 *Flowchart* Final Round 29
Gambar 3.7 *Flowchart* Addround Key..... 30
Gambar 3.8 *Flowchart* MD5 Modifikasi..... 31
Gambar 3.9 *Flowchart* Round Key..... 32
Gambar 3.10 Skema Proses RotCol AES..... 33
Gambar 3.11 Contoh Array Kunci Eksternal 34
Gambar 3.12 Contoh Transformasi RotCol..... 35
Gambar 3.13 Contoh Transformasi *SubBytes*..... 35
Gambar 3.14 Contoh Memperoleh Kolom Pertama RoundKey1 36
Gambar 3.15 Contoh Memperoleh Kolom Kedua RoundKey1..... 37
Gambar 3.16 Contoh Memperoleh Kolom Ketiga Round Key1 37
Gambar 3.17 Contoh Memperoleh Kolom Keempat Round Key1.. 38
Gambar 3.18 Kunci Eksternal Dan Round Key..... 39
Gambar 3.18 User Interface Sistem 39
Gambar 4.1 Antarmuka Utama..... 54
Gambar 4.2 Antarmuka Proses Enkripsi 55
Gambar 4.3 Antarmuka Proses Dekripsi..... 55
Gambar 4.4 Grafik Perbandingan Waktu Komputasi Enkripsi..... 63
Gambar 4.5 Grafik Perbandingan Waktu Komputasi Dekripsi 64

Gambar 4.6 Grafik Perbandingan Waktu Komputasi Enkripsi AES Dengan AESMD5 Modifikasi. 65
Gambar 4.7 Grafik Perbandingan Waktu Komputasi Dekripsi AES Dengan AESMD5 Modifikasi 65

DAFTAR SOURCE CODE

Sourcecode 4.1 Prosedure Load File Enkripsi 48
Sourcecode 4.2 Prosedure Pengubahan File Ke String 48
Sourcecode 4.3 Prosedure Pembentukan Kunci AES MD5 Modifikasi 49
Sourcecode 4.4 Prosedure Enkripsi AES..... 51
Sourcecode 4.5 Prosedure Load File Dekripsi..... 51
Sourcecode 4.6 Prosedure Mengembalikan Nilai String Kebentuk File 51
Sourcecode 4.7 Prosedure Dekripsi AES 53

UNIVERSITAS BRAWIJAYA

DAFTAR TABEL

Tabel 2.1 Tabel Subtitusi AES Rijndael 14
Tabel 2.2 Tabel Inverse S-Box 20
Tabel 3.1 Tabel Rcon Untuk 10 Round Key 34
Tabel 3.2 Pengujian Fungsionalitas Sistem Dengan Password Berbeda 44
Tabel 3.3 Tabel Pengujian Fungsionalitas Sistem Dengan Type AES Berbeda 44
Tabel 3.4 Tabel Waktu Proses Enkripsi Dengan AES 44
Tabel 3.5 Tabel Waktu Proses Dekripsi Dengan AES 45
Tabel 3.6 Tabel Waktu Proses Enkripsi Dengan AES MD5 45
Tabel 3.7 Tabel Waktu Proses Dekripsi Dengan AES MD5 45
Tabel 3.8 Tabel Pengujian Ketahanan..... 46
Tabel 4.1 Tabel Daftar File 56
Tabel 4.2 Tabel Waktu Proses Enkripsi Dengan Algoritma AES . 56
Tabel 4.3 Tabel Waktu Proses Dekripsi Dengan Algoritma AES . 57
Tabel 4.4 Tabel Perbandingan Waktu Proses Enkripsi AES 256 Dengan AES MD5 Modifikasi 58
Tabel 4.5 Tabel Perbandingan Waktu Proses Dekripsi AES 256 Dengan AES MD5 Modifikasi 59
Tabel 4.6 Tabel Uji Coba Dengan Password Salah 59
Tabel 4.7 Tabel Uji Coba Dengan Type AES Berbeda..... 60
Tabel 4.8 Tabel Pengujian Ketahanan..... 61