

UNIVERSITAS
MERCU BUANA

**PERANCANGAN APLIKASI PENGAMANAN DATA DENGAN
ALGORITMA AES RIJNDAEL**

Laporan Tugas Akhir

**Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer**

Oleh :
ANDRI EKO PRASETYO
4150401 - 113

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2009**

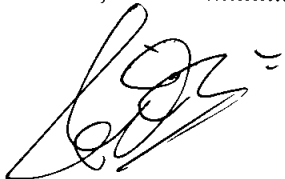
LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini:

NIM : 4150401 – 113
Nama : ANDRI EKO PRASETYO
Judul Skripsi : PERANCANGAN APLIKASI PENGAMANAN DATA
DENGAN ALGORITMA AES RIJNDAEL

Menyatakan bahwa skripsi tersebut diatas adalah hasil karya saya sendiri dan bukan plagiat. Apabila ternyata ditemukan didalam laporan skripsi saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Jakarta, 02. Sept - 2009



(Andri Eko Prasetyo)

LEMBAR PERSETUJUAN

NIM : 4150401 – 113
Nama : ANDRI EKO PRASETYO
Fakultas : ILMU KOMPUTER
Jurusan : TEKNIK INFORMATIKA
Judul Skripsi : PERANCANGAN APLIKASI PENGAMANAN DATA
DENGAN ALGORITMA AES RIJNDAEL

SKRIPSI INI TELAH DIPERIKSA DAN DISETUJUI

JAKARTA, 03-SEPTEMBER-2009.....

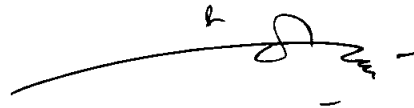


-Dharma-

M. Surya Dharma Siregar, S.Kom., MTI
Pembimbing



Devi Fitriyah, S.Kom., MTI
Koord. Tugas Akhir Teknik Informatika



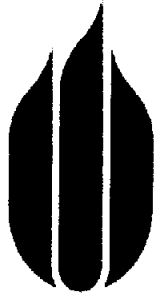
Abdusy Syarif, ST., MT
KaProdi Teknik Informatika

KATA PENGANTAR

Dengan mengucapkan segala puji dan syukur kehadirat Allah SWT yang telah melimpahkan taufik dan hidayah-Nya serta ridho-Nyalah, sehingga penulisan tugas akhir ini dapat terselesaikan dengan baik. Penulisan Tugas Akhir ini dimaksudkan untuk memenuhi salah satu syarat dalam menyelesaikan jenjang studi Strata Satu (S1) pada Program Studi Teknik Informatika di Universitas Mercu Buana.

Selesainya penulisan Tugas Akhir ini tidak lepas dari bantuan dan dukungan dari berbagai pihak, oleh karena itu dalam kesempatan ini penulis ingin menyampaikan rasa terima kasih yang sebesar-besarnya :

1. Ibu dan Bapak serta adikku tercinta, yang telah memberikan dukungan, doa, semangat, moril, materil dan kasih sayangnya sehingga penulisan tugas akhir ini dapat terwujud.
2. Bapak M. Surya Dharma Siregar, S.Kom, MTI. selaku pembimbing Tugas Akhir yang telah berkenan meluangkan waktunya serta memberi dukungan dan pengarahan hingga Tugas Akhir ini selesai. Makasih ya pak.
3. Ibu Devi Fitriana, S.Kom., MTI, selaku Koordinator Tugas Akhir Program Studi Teknik Informatika Universitas Mercu Buana.
4. Dosen – dosen Teknik Informatika Universitas Mercu Buana yg telah memberikan banyak ilmu bermanfaat, semoga jasa – jasa beliau mendapat banyak balasan dari Allah Swt.



UNIVERSITAS
MERCU BUANA

**PERANCANGAN APLIKASI PENGAMANAN DATA DENGAN
ALGORITMA AES RIJNDAEL**

Oleh :
ANDRI EKO PRASETYO
4150401 - 113

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2009**

Penulis menyadari sepenuhnya dalam penulisan Tugas Akhir ini masih banyak kekurangan dan ketidaksempurnaan. Oleh karena itu, penulis mengharapkan kritik dan saran yang sifatnya membangun sebagai bahan masukan demi sempurnanya Tugas Akhir ini.

Akhirnya penulis berharap, semoga penulisan Tugas Akhir ini dapat bermanfaat bagi semua pihak yang membacanya.

Jakarta, Agustus 2009

ANDRI EKO PRASETYO

DAFTAR ISI

| | |
|-------------------------------------|------------|
| Lembar Pernyataan | I |
| Lembar Persetujuan | II |
| Kata Pengantar | III |
| Abstrak | V |
| Daftar Isi | VI |
| Daftar Gambar | X |
| Daftar Tabel | XIV |
| | |
| BAB I PENDAHULUAN | 1 |
| 1.1 Latar Belakang | 1 |
| 1.2 Rumusan Masalah | 2 |
| 1.3 Batasan Masalah | 2 |
| 1.4 Manfaat | 3 |
| 1.5 Metodologi Yang Digunakan | 3 |
| 1.6 Sistematika Penulisan | 6 |
| | |
| BAB II LANDASAN TEORI | 8 |
| 2.1 Kriptografi | 8 |
| 2.1.1 Tujuan Kriptografi | 9 |
| 2.2 Algoritma Rijndael | 11 |
| 2.2.1 Transformasi SubByte | 18 |
| 2.2.2 Transformasi ShiftRow | 19 |
| 2.2.3 Transformasi MixColumn | 21 |

| | |
|---|-----------|
| 2.2.4 AddRound Key | 22 |
| 2.2.5 Ekspansi Kunci | 24 |
| 2.2.6 Inverse Chiper | 25 |
| 2.3 Visual Basic 6.0 | 28 |
| 2.3.1 IDE Visual Basic 6.0 | 28 |
| | |
| BAB III METODOLOGI PENELITIAN | 30 |
| 3.1 Kerangka Pemikiran | 30 |
| 3.2 Tahapan Pelaksanaan Penelitian | 30 |
| 3.2.1 Tahap Rekayasa Sistem | 31 |
| 3.2.2 Tahap Analisis | 31 |
| 3.2.3 Tahap Desain | 32 |
| 3.2.3.1 Perancangan Tampilan | 32 |
| 3.2.3.2 Perancangan Program | 32 |
| 3.2.4 Tahap Pengkodean | 34 |
| 3.2.5 Tahap Uji Coba | 34 |
| 3.2.6 Tahap Pengoperasian dan Pemeliharaan | 34 |
| 3.3 Alat dan Bahan Penelitian | 35 |
| | |
| BAB IV PERANCANGAN..... | 36 |
| 4.1 Analisis Masalah | 36 |
| 4.2 Perancangan Sistem | 37 |
| 4.2.1 Pengacakan File dengan Algoritma Rijndael | 37 |
| 4.2.2 Pengembalian File ke Bentuk Normal | 39 |

| | |
|--|-----------|
| 4.2.3 Perancangan Sistem Secara Umum | 42 |
| 4.2.4 Perancangan Sistem Secara Rinci | 44 |
| 4.3 Implementasi | 50 |
| 4.3.1 Implementasi Aplikasi | 50 |
| BAB V HASIL DAN PEMBAHASAN | 56 |
| 5.1 Tampilan Awal | 56 |
| 5.2 Proses Enkripsi Data | 57 |
| 5.2.1 Input dan Output Data | 58 |
| 5.3 Proses Dekripsi Data | 62 |
| 5.4 Pengujian | 65 |
| 5.5 Skenario Pengujian | 65 |
| 5.6 Hasil Pengujian Skenario | 68 |
| 5.7 Uji Coba File | 72 |
| 5.7.1 File Dokumen | 72 |
| 5.7.2 File Audio | 73 |
| 5.7.3 File Video | 75 |
| 5.7.4 File Gambar | 77 |
| 5.8 Uji Coba Waktu Proses Terhadap Jenis dan Ukuran Data | 79 |
| 5.8.1 Uji Coba File txt Dengan Beberapa Ukuran Berbeda | 80 |
| 5.8.2 Uji Coba File mp3 Dengan Beberapa Ukuran Berbeda | 83 |
| 5.8.3 Uji Coba File mpg Dengan Beberapa Ukuran Berbeda | 86 |
| 5.9 Exploitasi Sistem AES Terhadap Serangan | 88 |
| 5.9.1 Brute Force Attack | 88 |

| | |
|---|-----------|
| 5.9.2 Side Channel Attack Side | 88 |
| 5.10 Uji Coba Menu | 89 |
| 5.10.1 Validasi..... | 90 |
| 5.10.1.1 Uji Coba Proses <i>Input</i> Data (enkripsi) | 90 |
| 5.10.1.2 Uji Coba Proses <i>Input</i> Data (dekripsi) | 92 |
| 5.11 Analisis Hasil Pengujian | 93 |
| | |
| BAB VI KESIMPULAN DAN SARAN..... | 94 |
| 6.1 Kesimpulan..... | 94 |
| 6.2 Saran | 94 |
| | |
| DAFTAR PUSTAKA | 96 |
| LAMPIRAN..... | |

DAFTAR GAMBAR

| | |
|---|----|
| 1. Gambar 1.1. Skema Waterfall | 4 |
| 2. Gambar 2.1. Sistem Kriptografi | 9 |
| 3. Gambar 2.2. Diagram Proses Enkripsi | 15 |
| 4. Gambar 2.3. State | 16 |
| 5. Gambar 2.4. Masukan dan Keluaran Array State | 16 |
| 6. Gambar 2.5. Elemen state dan kunci dalam notasi HEX | 17 |
| 7. Gambar 2.6. Transformasi SubBytes | 18 |
| 8. Gambar 2.7. Ilustrasi Substitusi | 19 |
| 9. Gambar 2.8. Ilustrasi Transformasi <i>ShiftRows</i> | 20 |
| 10. Gambar 2.9. Ilustrasi <i>MixColumns</i> | 22 |
| 11. Gambar 2.10. Ilustrasi <i>AddRound Key</i> | 24 |
| 12. Gambar 2.11. Ekspansi cipher key menjadi round key | 24 |
| 13. Gambar 2.12. Diagram Alir Proses Dekripsi | 25 |
| 14. Gambar 2.13. Transformasi <i>InvShiftRows</i> | 26 |
| 15. Gambar 2.14. Matriks Invers Affine | 26 |
| 16. Gambar 2.15. Matriks <i>InvMixColumns</i> | 27 |
| 17. Gambar 3.1. Skema Waterfall | 31 |
| 18. Gambar 3.2. Diagram Alir Perancangan Program | 33 |
| 19. Gambar 4.1. Sistem Pengamanan Data | 36 |
| 20. Gambar 4.2. Proses Enkripsi Algoritma Rijndael | 37 |
| 21. Gambar 4.3. <i>Pseudo code</i> Enkripsi Rijndael..... | 39 |
| 22. Gambar 4.4. <i>Pseudo code</i> Transformasi <i>Invadd Round key</i> | 41 |

| | |
|---|----|
| 23. Gambar 4.5. Konteks Sistem Pengamanan Data Dengan Algoritma Rijndael | 42 |
| 24. Gambar 4.6. DFD Level 0 Sistem Pengamanan Data Dengan Algoritma Rijndael | 42 |
| 25. Gambar 4.7. <i>Flowchart</i> Sistem Pengamanan Data Dengan Algoritma Rijndael | 43 |
| 26. Gambar 4.8. Rancangan Menu Sistem Pengamanan Data Dengan Algoritma Rijndael | 44 |
| 27. Gambar 4.9. Perancangan <i>Frame</i> untuk <i>Properties</i> File..... | 45 |
| 28. Gambar 4.10. Perancangan <i>Frame</i> untuk <i>Help</i> | 46 |
| 29. Gambar 4.11. Perancangan <i>Frame</i> untuk <i>Operation</i> | 47 |
| 30. Gambar 4.12. Perancangan <i>Frame</i> untuk Halaman Awal..... | 48 |
| 31. Gambar 4.13. Perancangan <i>Form</i> Utama | 49 |
| 32. Gambar 4.14. <i>Form</i> utama | 51 |
| 33. Gambar 4.15. <i>Frame</i> untuk Halaman Awal | 52 |
| 34. Gambar 4.16. <i>Frame</i> untuk Halaman <i>Operation</i> | 53 |
| 35. Gambar 4.17. <i>Frame</i> untuk Halaman <i>Help</i> | 54 |
| 36. Gambar 4.18. <i>Frame</i> untuk Halaman <i>Properties</i> file..... | 55 |
| 37. Gambar 5.1. Tampilan Awal | 56 |
| 38. Gambar 5.2. Tampilan <i>Frame</i> untuk <i>Operation</i> | 58 |
| 39. Gambar 5.3. Pemilihan Data | 59 |
| 40. Gambar 5.4. Data telah dipilih untuk di enkripsi | 59 |
| 41. Gambar 5.5. Proses enkripsi selesai | 60 |
| 42. Gambar 5.6. Folder tempat file hasil eksekusi | 60 |

| | |
|--|----|
| 43. Gambar 5.7. Data telah dipilih untuk di dekripsi | 63 |
| 44. Gambar 5.8. Proses dekripsi selesai | 63 |
| 45. Gambar 5.9. Isi file txt sebelum dienkripsi (<i>plain text</i>)..... | 72 |
| 46. Gambar 5.10. Isi file txt setelah dienkripsi (<i>cipher text</i>)..... | 72 |
| 47. Gambar 5.11. Isi file txt setelah didekripsi kembali..... | 73 |
| 48. Gambar 5.12. Isi file txt setelah didekripsi dengan kunci salah..... | 73 |
| 49. Gambar 5.13. File Seandainya.mp3 dapat dimainkan dengan baik | 74 |
| 50. Gambar 5.14. File Seandainya.mp3 tidak dapat dimainkan..... | 74 |
| 51. Gambar 5.15. File Seandainya.mp3 dapat kembali dimainkan | 75 |
| 52. Gambar 5.16. File Seandainya.mp3 tidak dapat dimainkan..... | 75 |
| 53. Gambar 5.17. File Haji.mpg dapat dimainkan dengan baik | 76 |
| 54. Gambar 5.18. File Haji.mpg tidak dapat dimainkan | 76 |
| 55. Gambar 5.19. File Haji.mpg dapat kembali dimainkan | 76 |
| 56. Gambar 5.20. File Haji.mpg tidak dapat dimainkan | 77 |
| 57. Gambar 5.21. File geek.jpg dapat dilihat | 77 |
| 58. Gambar 5.22. File geek.jpg tidak dapat dilihat | 78 |
| 59. Gambar 5.23. File geek.jpg dapat kembali dilihat | 78 |
| 60. Gambar 5.24. File geek.jpg tidak dapat dilihat | 78 |
| 61. Gambar 5.25. file txt 1 mb proses <i>encrypt</i> | 80 |
| 62. Gambar 5.26. file txt 1 mb proses <i>decrypt</i> | 80 |
| 63. Gambar 5.27. file txt 2 mb proses <i>encrypt</i> | 81 |
| 64. Gambar 5.28. file txt 2 mb proses <i>decrypt</i> | 81 |
| 65. Gambar 5.29. file txt 3 mb proses <i>encrypt</i> | 82 |
| 66. Gambar 5.30. file txt 3 mb proses <i>decrypt</i> | 82 |

| | |
|---|----|
| 67. Gambar 5.31. file mp3 1 mb proses <i>encrypt</i> | 83 |
| 68. Gambar 5.32. file mp3 1 mb proses <i>decrypt</i> | 83 |
| 69. Gambar 5.33. file mp3 2 mb proses <i>encrypt</i> | 84 |
| 70. Gambar 5.34. file mp3 2 mb proses <i>decrypt</i> | 84 |
| 71. Gambar 5.35. file mp3 3 mb proses <i>encrypt</i> | 85 |
| 72. Gambar 5.36. file mp3 3 mb proses <i>decrypt</i> | 85 |
| 73. Gambar 5.37. file mpg 5 mb proses <i>encrypt</i> | 86 |
| 74. Gambar 5.38. file mpg 5 mb proses <i>decrypt</i> | 86 |
| 75. Gambar 5.39. file mpg 10 mb proses <i>encrypt</i> | 87 |
| 76. Gambar 5.40. file mpg 10 mb proses <i>decrypt</i> | 87 |
| 77. Gambar 5.41. Proses Input Kunci | 90 |
| 78. Gambar 5.42. Proses Input Data (Enkripsi) | 91 |
| 79. Gambar 5.43. Proses Input Kunci | 92 |
| 80. Gambar 5.44. Proses Input Data (Dekripsi) | 93 |

DAFTAR TABEL

| | |
|--|----|
| 1. Tabel 2.1. Perbandingan Algoritma | 12 |
| 2. Tabel 2.2. tiga buah versi <i>AES</i> | 13 |
| 3. Tabel 2.3. S-box | 18 |
| 4. Tabel 4.1. <i>Properties Frame</i> untuk <i>Properties file</i> | 45 |
| 5. Tabel 4.2. <i>Properties Frame</i> untuk <i>Help</i> | 46 |
| 6. Tabel 4.3. <i>Properties Frame</i> untuk <i>Operation</i> | 47 |
| 7. Tabel 4.4. <i>Properties Frame</i> untuk Halaman Awal..... | 48 |
| 8. Tabel 4.5. <i>Properties Form</i> Utama | 49 |
| 9. Tabel 5.1. Skenario Normal dan Tidak Normal Aplikasi Pengamanan Data Dengan Algoritma AES Rijndael | 65 |
| 10. Tabel 5.2. Menjelaskan hasil pengujian dari skenario normal dan tidak normal | 68 |
| 11. Tabel 5.3. Uji Coba Waktu Proses Terhadap Jenis dan Ukuran Data.. | 79 |
| 12. Tabel 5.4. Uji Coba Menu..... | 89 |
| 13. Tabel 5.5. Keterangan Proses <i>Input Kunci</i> | 91 |
| 14. Tabel 5.6. Keterangan Proses <i>Input plain text</i> | 91 |
| 15. Tabel 5.7. Keterangan Proses <i>Input Kunci</i> | 92 |
| 16. Tabel 5.8. Keterangan Proses <i>Input chipper text</i> | 93 |