IMPLEMENTASI ALGORTIMA RIJNDAEL UNTUK KEAMANAN DATA TEKS

SKRIPSI

Untuk memenuhi sebagian persyaratan

mencapai gelar Sarjana Komputer

Disusun oleh :

SEPTYANDI KUSUMA RAHARJO

NIM. 0710963034

PROGRAM STUDI INFORMATIKA/ILMU KOMPUTER
PROGRAM TEKNOLOGI INFORMASI DAN ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA
MALANG
2013

LEMBAR PERSETUJUAN

IMPLEMENTASI ALGORITMA RIJNDAEL UNTUK KEAMANAN DATA TEKS

Disusun oleh :

SEPTYANDI KUSUMA RAHARJO

NIM. 0710963034

Telah diperiksa dan disetujui oleh :

Pembimbing I,	Pembimbing II,
Dian Eka Ratnawati, S.Si., M.Kom	**Lailil Muflikhah, S.Kom., M.Sc**
NIP. 19730619 200212 2 001	**NIP.19741113 200501 2 001**

PERNYATAAN ORISINALITAS SKRIPSI

Saya menyatakan dengan sebenar-benarnya bahwa sepanjang pengetahuan saya, di dalam naskah SKRIPSI ini tidak terdapat karya ilmiah yang pernah diajukan oleh orang lain untuk memperoleh gelar akademik di suatu perguruan tinggi, dan tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis dikutip dalam naskah ini dan disebutkan dalam sumber kutipan dan daftar pustaka.

Apabila ternyata didalam naskah SKRIPSI ini dapat dibuktikan terdapat unsur-unsur PLAGIASI, saya bersedia SKRIPSI ini digugurkan dan gelar akademik yang telah saya peroleh (SARJANA) dibatalkan, serta diproses sesuai dengan peraturan perundang-undangan yang berlaku. (UU No. 20 Tahun 2003, Pasal 25 ayat 2 dan Pasal 70).

Malang, Juli 2013

Mahasiswa,

Septyandi Kusuma Raharjo

NIM. 0710963034

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Allah SWT yang telah melimpahkan segala Rahmat, Karunia dan Hidayah-Nya sehingga Penulis dapat menyelesaikan skripsi dengan judul: "**Implementasi Algoritma Rijndael Untuk Keamanan Data Teks**"

Skripsi ini diajukan sebagai syarat ujian seminar skripsi dalam rangka untuk memperoleh gelar Sarjana Komputer di Program Studi Ilmu komputer dan informatika Universitas Brawijaya Malang. Atas terselesaikannya skripsi ini, Penulis mengucapkan terima kasih kepada:

1. Dian Eka Ratnawati, S.Si., M.Kom., selaku Dosen Pembimbing Skripsi I.
2. Lailil Muflikhah, S.Kom., M.Sc., selaku Dosen Pembimbing Skripsi II.
3. Drs. Marji, MT., selaku Ketua Program Studi Teknik InformatikaProgram Teknologi Informasi & Ilmu Komputer Universitas Brawijaya.
4. Yusi Tyroni Mursityo, S.Kom, MS., selaku Dosen Penasehat Akademik.
5. Ir. Sutrisno, MT., selaku Ketua Program Teknologi Informasi & Ilmu Komputer Universitas Brawijaya.
6. Segenap Bapak dan Ibu dosen yang telah mendidik dan mengajarkan ilmunya kepada Penulis selama menempuh pendidikan di Program Teknologi Informasi & Ilmu Komputer Universitas Brawijaya.
7. Segenap staff dan karyawan di Program Studi Teknologi Informasi & Ilmu Komputer Universitas Brawijaya yang telah banyak membantu Penulis dalam pelaksanaan penyusunan skripsi ini.

8. Orang tua Penulis dan saudara-saudaraku atas segala dukungan materi dan doa restunya kepada Penulis.
9. Rekan-rekan Program Studi Teknik Informatika yang telah memberikan dukungannya kepada penulis.
11. Steampowered.com / dota2game , yang selalu menemani saya saat inspirasi mulai berhenti , dan setiap malam saya
12. Teman-teman ilmu komputer 07 dan ilmu komputer 06 yang senantiasa memberikan motifasi untuk trus mengerjakan skripsi ini , khususnya sodara Welly , Aditya hari, Briant , Yosi , Johanes , Novieta putri ,
13. Semua pihak yang telah membantu terselesaikannya skripsi ini yang tidak dapat kami sebutkan satu per satu.

Penulis menyadari bahwa skripsi ini tentunya tidak terlepas dari berbagai kekurangan dan kesalahan. Oleh karena itu, segala kritik dan saran yang bersifat membangun sangat Penulis harapkan dari berbagai pihak demi penyempurnaan penulisan skripsi ini.

Akhirnya penulis berharap agar skripsi ini dapat memberikan sumbangan dan manfaat bagi semua pihak yang berkepentingan.

Malang, Juli 2013

Septyandi Kusuma Raharjo

Penulis

IMPLEMENTASI ALGORTIMA RIJNDAEL UNTUK KEAMANAN DATA TEKS

SKRIPSI

Untuk memenuhi sebagian persyaratan

mencapai gelar Sarjana Komputer

Disusun oleh :

SEPTYANDI KUSUMA RAHARJO

NIM. 0710963034

PROGRAM STUDI INFORMATIKA/ILMU KOMPUTER
PROGRAM TEKNOLOGI INFORMASI DAN ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA
MALANG
2013

ABSTRAK

Keamanan jaringan komputer merupakan hal yang sangat penting karena akses internet terbuka bebas bagi siapapun. Setiap data yang dikirim dan diterima di internet sangat mudah diketahui oleh siapapun. Sehingga diperlukan pengamanan lebih terhadap data-data penting yang akan dilewatkan pada jaringan internet. Aplikasi enkripsi dekripsi dapat digunakan untuk mengamankan data yang penting dan berharga. Suatu berkas dapat di enkripsi atau menjadi ciphertext menggunakan suatu kunci dan dapat secara aman dipertukarkan tanpa khawatir tentang kerahasiaan isi berkas tersebut. Dekripsi dengan kunci akan mengolah berkas terenkripsi menjadi plaintext atau berkas semula.

Algoritma Rijndael sebagai standar dalam pengamanan data dapat menambah efisiensi waktu dan keamanan, dengan algoritma ini dapat dibangun sebuah aplikasi enkripsi dan dekripsi yang ringan dan dapat diandalkan.

Untuk mengetahui ketahanan sebuah algoritma enkripsi maka di perlukan uji ketahanan dengan menggunakan *exhautistive attack dan avalanche effect* . *Exhaustive attack* menggunakan tipe penyerangan *trial and error* , jika lama waktu sebesar 10^6 percobaan perdetik adalah 5.4 x 10^{24} tahun dan sebesar 10^{12} percobaan perdetik maka lama yang dibutuhkan adalah 5.4 x 10^{18} perdetik . Pada avalanche effect dilakukan testing sebanyak tiga kali dengan perbandingan dua data untuk dua kondisi yakni untuk perubahan 1 bit key dan 1 bit plaintext. effect untuk kondisi menggunakan key yang berbeda diperoleh avalance effect rata-rata sebesar 54,16%, sedangkan pada tabel 4.6 hasil testing untuk avalanche effect untuk kondisi dengan menggunakan plaintext yang berbeda didapatkan hasil rata-rata avalanche effect sebesar 53,12%

Keyword : avalanche effect , Rijndael , exhautive attack

ABSTRACT

Computer network security is important because internet access is open for anybody. Any data that is sent and received on the internet is easily known by anyone. So more security is needed for the data that will be passed on the Internet. Encryption decryption application can be used to secure important and valuable data. A file can be encrypted or become ciphertext using a key and can be safely exchanged without worrying about the confidentiality of the file content. Decryption using the key will process the encrypted file to become plaintext or original file.

Rijndael algorithm as the standard in data security can increase time efficiency and security, using this algorithm, encryption and decryption application that lightweight and reliable can be constructed.

To find the resistance of an encryption algorithm then endurance test using exhautistive attack and avalanche effect is needed. Exhaustive attack using a trial and error type of attack, if the trial duration is 10^6 trials per second it takes 5.4×10^{24} years and if the trial time is 10^{12} trial per second it takes 5.4×10^{18} years. Testing on avalanche effect performed three times with two comparative data for two conditions that is 1 bit key and 1 bit plaintext changes. The effect for condition using a different key, 54.16% average avalance effect is obtained, while in Table 4.6 the results of testing for the avalanche effect for conditions using different plaintext, 53.12% average avalanche effect is obtained.

Keyword : avalanche effect , Rijndael , exhautive attack