**USULAN TUGAS AKHIR**

# **IDENTITAS PENGUSUL**

**Nama : Gracius Cagar Gunawan**

**NRP : 5109100168**

**Dosen Wali : Arya Yudhi Wijaya, S. Kom., M. Kom.**

1. **JUDUL TUGAS AKHIR**

Implementasi Algoritma Rijndael dengan menggunakan kunci enkripsi yang berukuran melebihi 256 bit.

Implementation of Rijndael Algorithm using more than 256 bit cipher key.

1. **URAIAN SINGKAT**

Algoritma Rijndael adalah sebuah algoritma enkripsi yang setiap bit keluarannya dipengaruhi oleh setiap bit yang terdapat pada masukan dan setiap bit yang terdapat pada kunci enkripsi [[1](#Dae02)].

Algoritma Rijndael menerima sebuah *string* yang akan di enkripsi, yang disebut dengan *state*, dan sebuah *cipher* *key*. Panjang *cipher* *key* yang digunakan dalam algoritma ini adalah 128 bit, 192 bit, atau 256 bit. Panjang *state* dan *cipher* *key* selalu berupa kelipatan 32 bit. Alur pemrosesan pada enkripsi Rijndael terdiri dari empat bagian, yaitu:

1. *key* *expansion*

*Key* *expansion* adalah proses transformasi dari *cipher* *key* menjadi *expanded* *key*. Pada bagian ini, panjang cipher key diubah dari 4\*Nk menjadi Nb\*(Nr+1). Nk adalah panjang *cipher* *key* dalam satuan *word* (1 *word* = 32 bit). Nb adalah panjang *state* dalam satuan *word* dan Nr = Nk + 6.

1. *add* *round* *key*

Proses ini merupakan proses XOR antara *state* dengan sebuah round key. *Round* *key* merupakan bagian dari *expanded* *key*. Pada sebuah *expanded* *key*, terdapat Nr+1 *round* *key* dengan panjang setiap *round* *key* sama. *Round* yang digunakan pada *add* *round* *key* pertama adalah *round* ke-0.

1. *round*

*Round* diulang sebanyak Nr kali. Pada setiap *round*, terjadi proses *byte* *sub*, *shift* *row*, *mix* *column*, dan *add* *round* *key*. *Round* *key* yang digunakan pada *round* ke-i adalah *round* ke-i.

1. *final* *round*

Sama seperti *round*, hanya pada tahap ini *add* *round* *key* tidak dilakukan. Setelah *final* *round* selesai, maka enkripsi Rjindael selesai.

Pada tugas akhir kali ini, enkripsi Rjindael akan diimplementasikan menggunakan *cipher* *key* yang panjangnya melebihi 256 bit atau 8 *word*.

1. **PENDAHULUAN**
2. **LATAR BELAKANG**

Komputer tercanggih zaman sekarang jika digunakan untuk mencari kunci enkripsi yang tepat dapat mencoba 2^55 *cipher* *key* berbeda setiap detik. Solusi yang sudah pernah dilakukan adalah AES (Advanced Encryption Standard) [[2](#Nat01)]. AES adalah sebuah kontes yang diadakan oleh NIST untuk mencari sebuah algoritma enkripsi yang hanya dapat dipecahkan dengan menggunakan *brute* *force*. Algoritma Rijndael terpilih sebagai AES. Algoritma tersebut dapat menggunakan 256 bit kunci enkripsi. Untuk memecahkan algoritma tersebut menggunakan *brute* *force*, sebuah komputer wajib mencoba 2^128 kunci enkripsi berbeda sehingga sebuah komputer membutuhkan waktu 2^73 detik.

Namun, pemecahan kunci enkripsi tidak harus menggunakan sebuah komputer dan tingkat pertumbuhan kecepatan komputer sangat tinggi. Berdasarkan hukum Moore, kecepatan komputer bertambah sebanyak dua kali lipat setiap 18 bulan [[3](#Bow04)]. Jadi, kira-kira dalam 20 tahun lagi, kunci enkripsi 256 bit dapat dipecahkan menggunakan teknik *brute* *force*.

Untuk mencegah hal tersebut, maka ukuran kunci enkripsi perlu ditingkatkan. Oleh karena itu, dalam tugas akhir ini, ditawarkan sebuah solusi yaitu implementasi Algoritma Rijndael yang dapat menerima kunci enkripsi yang berukuran melebihi 256 bit.

1. **RUMUSAN MASALAH**

Permasalahan yang dibahas dalam tugas akhir ini dapat diuraikan sebagai berikut:

1. Dapatkah Algoritma Rijndael diimplementasikan agar dapat menerima ukuran kunci enkripsi yang melebihi 256 bit?
2. **RUANG LINGKUP MASALAH**

Permasalahan yang diselesaikan pada tugas akhir ini dibatasi ruang lingkupnya :

1. ukuran *cipher* *key* yang digunakan adalah 32 bit sampai 64 kbit
2. ukuran masukan yang akan dienkripsi mencapai 32 kbit.
3. **TUJUAN PENELITIAN**

Tujuan dari tugas akhir ini adalah membuat sebuah perangkar keras perangkat lunak yang dapat melakukan enkripsi Rijndael menggunakan kunci enkripsi yang berukuran 32 bit sampai dengan 64 kbit.

1. **MANFAAT PENELITIAN**

Manfaat yang diberikan dari tugas akhir ini adalah keamanan suatu informasi dapat terjaga dari serangan *brute* *force*.

1. **TINJAUAN PUSTAKA**
2. C

C merupakan bahasa pemrograman yang dibuat oleh Dennis Ritchie pada tahun 1969. Bahasa C merupakan bahasa pemrograman yang bersifat terstruktur. Oleh karena itu, urutan eksekusi hasil kompilasi bahasa C sama dengan urutan baris-baris perintah yang tertulis pada berkasnya.

1. Dev-C

Dev-C adalah sebuah perangkat lunak yang berfungsi sebagai lingkungan kerja untuk pemrograman bahasa C yang menggunakan sistem operasi Windows. Dev-C menggunakan MinGW pada saat melakukan kompilasi.

1. Algoritma Rijndael

Algoritma Rijndael adalah algoritma yang terpilih sebagai AES. Sifat khusus dari algoritma ini adalah setiap bit keluaran dipengaruhi oleh setiap bit masukan dan kunci enkripsinya. Alur kerja Algoritma Rijndael meliputi *key* *expansion*, *add* *round* *key*, *round*, dan *final* *round*.

1. **METODOLOGI**

Pembuatan tugas akhir ini dilakukan dengan mengikuti metodologi sebagai berikut :

1. Studi literatur

Tahap ini adalah tahap pengumpulan informasi yang diperlukan untuk perancangan algoritma enkripsi ini. Informasi-informasi tersebut dapat diperoleh melalui *paper*.

1. Implementasi

Implementasi dari algoritma Rijndael dilakukan pada tahap ini. Implementasi dilakukan dalam bahasa pemrograman C dengan menggunakan perangkat lunak Dev-C.

1. Uji coba dan evaluasi

Pada tahap ini, dilakukan uji coba terhadap hasil implementasi yang dilakukan pada tahap sebelumnya. Uji coba enkripsi menggunakan tes data yang terdapat pada situs spoj.com. Uji coba dikatakan berhasil apabila situs tersebut menerima solusi enkripsi yang dikirimkan.

1. Penyusunan buku tugas akhir

Tahap ini merupakan tahap penyusunan laporan yang menjelaskan dasar teori dan metode yang digunakan dalam tugas akhir ini dan juga hasil implementasinya.

1. **JADWAL PEMBUATAN TUGAS AKHIR**

Tugas akhir ini diharapkan dapat dikerjakan sesuai jadwal berikut.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| No. | Tahapan | 2013 | | | |
| Maret | April | Mei | Juni |
| 1 | Studi Literatur |  |  |  |  |
| 2 | Implementasi |  |  |  |  |
| 3 | Uji coba dan evaluasi |  |  |  |  |
| 4 | Penyusunan Buku Tugas Akhir |  |  |  |  |

1. **DAFTAR PUSTAKA**

x

|  |  |
| --- | --- |
| [1] | Joan Daemen and Vincent Rijmen, *The Design of Rijndael : AES - The Advanced Encryption Standard*. Verlag, Germany: Springer, 2002. |
| [2] | National Institute of Standards and Technology (NIST), Federal Information Processing Standards Publication 197, 2001. |
| [3] | Murrae Bowden, Moore’s Law and the Technology S-Curve, 2004. |

x

**LEMBAR PENGESAHAN**

###### Surabaya, 11 Maret 2013

Menyetujui,

Pembimbing I

Ahmad Saikhu, S.Si, M. T

NIP: 197107182006041001

Pembimbing II

Rully Soelaiman S.Kom, M. Kom

NIP: 197002131994021001