# IMPLEMENTASI MAC DAN RC6 UNTUK MENDETEKSI PERUBAHAN FILE PADA PROSES DUPLIKASI FILE

**SKRIPSI**

**Disusun Sebagai Salah Satu Syarat**
**Untuk Memperoleh Gelar Sarjana Komputer**
**Pada Jurusan Ilmu Komputer / Informatika**

**Disusun Oleh:**
**RACHMAN MULIAWAN DERMAWAN**
**J2F007042**

**JURUSAN ILMU KOMPUTER / INFORMATIKA**
**FAKULTAS SAINS DAN MATEMATIKA**
**UNIVERSITAS DIPONEGORO**
**2014**

# HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Saya yang bertanda tangan di bawah ini :

Nama : Rachman Muliawan Dermawan

NIM : J2F007042

Judul : Implementasi MAC dan RC6 Untuk Mendeteksi Perubahan File Pada Proses Duplikasi File

Dengan ini saya menyatakan bahwa dalam tugas akhir/ skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan di dalam daftar pustaka.

Semarang, 29 Agustus 2014


Rachman Muliawan Dermawan

NIM. J2F007042

# HALAMAN PENGESAHAN

Judul : Implementasi MAC dan RC6 Untuk Mendeteksi Perubahan File Pada Proses Duplikasi File

Nama : Rachman Muliawan Dermawan

NIM : J2F007042

Telah diujikan pada sidang tugas akhir pada tanggal 29 Agustus 2014 dan dinyatakan lulus pada tanggal 29 Agustus 2014

Mengetahui,
Ketua Jurusan Ilmu Komputer / Informatika
FSM UNDIP

Nurdin Bahtiar, S.Si, M.T.
NIP. 1979 0720 2003 12 1 002

Semarang, 29 Agustus 2014
Panitia Penguji Tugas Akhir
Ketua

Sukmawati Nur Endah, S.Si, M.Kom
NIP. 1978 0502 2005 01 2 002

# HALAMAN PENGESAHAN

Judul : Implementasi MAC dan RC6 Untuk Mendeteksi Perubahan File Pada Proses Duplikasi File

Nama : Rachman Muliawan Dermawan

NIM : J2F007042

Telah diujikan pada sidang tugas akhir pada tanggal 29 Agustus 2014.

Semarang, 29 Agustus 2014

| Pembimbing Utama | Pembimbing Anggota |
| --- | --- |
| Drs. Suhartono, M.Kom | Ragil Saputra, S.Si, M.Cs |
| NIP. 19550407 198303 1 003 | NIP. 19801021 200501 1 003 |

# ABSTRAK

Seiring dengan ilmu pengetahuan dan teknologi yang semakin berkembang, keamanan data juga semakin rentan terhadap tindak kejahatan. Kejahatan yang ada memiliki banyak tipe yang beragam, dimulai dari pemalsuan data, duplikasi data tanpa seijin pemilik, serta pemalsuan hak milik. Perlu adanya teknik yang mampu memeriksa terjadinya perubahan dalam proses duplikasi. Dalam ilmu kriptografi terdapat suatu mekanisme untuk memeriksa integritas terhadap sebuah file, yaitu dengan teknik MAC (*Message Authentication Code*). MAC menghasilkan sebuah nilai unik yang dapat diperoleh dari file yang selanjutnya disisipkan ke dalam file tersebut sebelum diduplikasi. Pendeteksian perubahan dilakukan dengan membandingkan MAC yang telah disisipkan dengan MAC hasil generasi dari potongan file tanpa MAC. MAC dapat diimplementasikan dengan menggunakan fungsi kriptografi hash SHA-1 dan algoritma kriptografi RC6. SHA-1 digunakan untuk mengenerate kunci sebelum menghasilkan nilai MAC. RC6 digunakan untuk mengacak nilai MAC sebelum disisipkan dengan tujuan untuk meningkatkan keamanan. Hasil penerapan dapat berupa file yang telah disisipi MAC yang terenkripsi algoritma kriptografi RC6 dan dapat pula informasi jika file tetap atau mengalami perubahan.

**Kata kunci:** Kriptografi, MAC, SHA-1, RC6

# ABSTRACT

Along with science and technology growth, data security is also increasingly vulnerable to crime. The evil that is in possession of many types of variety, starting from the forgery of data, data duplication without owners permissions, and forgery of ownership. There should be a technique that capable of examining the occurrence of changes in the duplication process. In the cryptography, there is a mechanism for checking the integrity of a file, which is using MAC (Message Authentication Code). MAC produces an unique value that can be obtained from the file further embedded into the file before duplicated. Authenticity checking is done by comparing the MAC has been embedded into file with MAC revenue generation from the part of file without MAC. MAC can be implemented by using a cryptographic hash function SHA-1 and cryptographic algorithms RC6. SHA-1 is used to generate key before getting MAC value. RC6 is used to randomize the MAC before embedded in order to improve security. The results of the application can be a file that have been inserted MAC encrypted with RC6 algorithms and also if file has been modified or not.

**Keywords:** Cryptography, MAC, SHA-1, RC6

# KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah SWT yang telah melimpahkan rahmat dan hidayah-Nya sehingga penulis dapat menyusun tugas akhir yang berjudul "**Implementasi MAC dan RC6 Untuk Mendeteksi Perubahan File Pada Proses Duplikasi File**"

Tugas akhir ini disusun sebagai salah satu syarat untuk memperoleh gelar sarjana strata satu pada Jurusan Ilmu Komputer / Informatika Fakultas Sains Dan Matematika Universitas Diponegoro Semarang.

Dalam penyusunan tugas akhir ini, penulis mendapat bantuan dan dukungan dari banyak pihak. Atas peran sertanya dalam membantu dalam penyelesaian tugas akhir ini, penulis ingin mengucapkan terima kasih kepada:

1. Bapak Dr. Muhammad Nur, DEA selaku Dekan Fakultas Sains dan Matematika Universitas Diponegoro.
2. Bapak Nurdin Bahtiar, S.Si, M.T Ketua Jurusan Ilmu Komputer / Informatika Fakultas Sains dan Matematika Universitas Diponegoro.
3. Bapak Drs. Suhartono, M.Kom selaku pembimbing I beserta bapak Ragil Saputra, S.Si, M.Cs selaku pembimbing II yang telah meluangkan waktu untuk membimbing dan mengarahkan Penulis dalam menyelesaikan tugas akhir ini.
4. Semua pihak yang telah membantu hingga selesainya tugas akhir ini, yang tidak dapat penulis sebutkan satu persatu. Semoga Allah membalas segala kebaikan yang telah Anda berikan kepada penulis.

Penulis menyadari bahwa masih terdapat kekurangan dalam penyusunan laporan tugas akhir ini, untuk itu penulis mohon maaf dan mengharapkan saran serta kritik yang membangun dari pembaca. Semoga laporan tugas akhir ini dapat bermanfaat bagi pengembangan ilmu dan pengetahuan, khususnya pada bidang Informatika.

Semarang, 29 Agustus 2014

Penulis

# DAFTAR ISI

# DAFTAR GAMBAR

# DAFTAR TABEL

Hal

# BAB I
# PENDAHULUAN

Bab ini membahas latar belakang, rumusan masalah, tujuan dan manfaat, ruang lingkup, serta sistematika penulisan laporan tugas akhir mengenai Implementasi MAC dan RC6 Untuk Mendeteksi Perubahan File Pada Proses Duplikasi File.

## 1.1. Latar Belakang

Seiring dengan ilmu pengetahuan dan teknologi yang semakin berkembang, keamanan data juga semakin rentan terhadap tindak kejahatan. Kejahatan yang ada memiliki banyak tipe yang beragam, dimulai dari pemalsuan data, duplikasi data tanpa seijin pemilik, serta pemalsuan hak milik (Pradana, 2011). Perlu adanya teknik yang mampu memeriksa terjadinya perubahan dalam proses duplikasi. Kriptografi dapat menjadi salah satu solusi dalam mengatasi masalah jika terjadi perubahan pada file saat proses duplikasi.

Kriptografi adalah ilmu menggunakan matematika untuk mengenkripsi dan mendekripsi data. Kriptografi memungkinkan untuk menyimpan informasi sensitif atau mengirimkannya melalui jaringan yang tidak aman (seperti internet) sehingga tidak dapat dibaca oleh siapa pun kecuali penerima yang dimaksud. Jika kriptografi adalah ilmu mengamankan data, kriptanalis adalah ilmu menganalisis dan memecahkan komunikasi yang aman. Kriptanalisis klasik melibatkan kombinasi menarik dari penalaran analitis, penerapan alat-alat matematika, pola temuan, kesabaran, tekad, dan keberuntungan. Kriptanalis juga disebut penyerang. Kriptologi mencakup baik kriptografi dan kriptanalis. (Zimmermann, 1998)

Dalam banyak pandangan, privasi seringkali identik dengan kriptografi. Akan tetapi otentikasi pesan dapat pula dikatakan lebih penting. Terkadang seseorang tidak peduli mengenai kerahasiaan sebuah pesan namun seringkali perlu adanya kepastian mengenai asal ataupun keaslian dari pesan tersebut. Otentikasi pesan mampu memberikan jaminan akan hal itu. (Bellare & Rogaway, 2005).

MAC (*Message Authentication Code*) adalah potongan pendek dari informasi yang digunakan untuk otentikasi pesan dan untuk menyediakan integritas dan jaminan keaslian pada pesan tersebut. MAC juga dikenal sebagai kriptografi *checksum* atau fungsi hash berkunci, sering digunakan dalam berbagai kegiatan. Dalam hal

keamanan, MAC mempunyai beberapa kesamaan sifat dengan tanda tangan digital (*digital signature*) mengingat keduanya menyediakan integritas pesan dan otentikasi pesan. Namun tidak seperti tanda tangan digital, MAC merupakan skema kunci simetris dan tidak mendukung *nonrepudation*. Salah satu kelebihan dari MAC adalah proses berjalan lebih cepat dibandingkan dengan tanda tangan digital mengingat MAC dapat berbasis chiper blok ataupun fungsi hash (Paar & Pelz, 2010). Salah satu cara untuk membangkitkan MAC yaitu dengan menggunakan fungsi hash SHA-1

Untuk memperkuat keamanannya, dapat pula dilakukan enkripsi lebih lanjut, salah satunya dengan algoritma RC6. RC6 merupakan pilihan ideal untuk kebanyakan aplikasi dengan keamanan dan kinerja tingkat tinggi. RC6 berfokus pada antisipasi serangan dari penggunaan kriptanalisis lanjar dan kriptanalisis diferensial, serta serangan dalam bentuk lain. Algoritma ini berproses lebih cepat dibandingkan dengan algoritma Rinjdael yang merupakan standar AES.

Pada penelitian ini akan diteliti bagaimana implementasi MAC dan RC6 sehingga dapat digunakan untuk mendeteksi jika terjadi perubahan pada file pada saat proses duplikasi.

## 1.2. Rumusan Masalah

Berdasarkan latar belakang di atas dapat dirumuskan permasalahan yang akan diselesaikan yaitu bagaimana mengimplementasikan MAC dan RC6 untuk mendeteksi jika terjadi perubahan pada file pada saat proses duplikasi.

## 1.3. Tujuan dan Manfaat

Tujuan yang ingin dicapai dalam penelitian ini adalah menghasilkan sebuah aplikasi yang dapat mendeteksi jika terjadi perubahan pada file pada saat proses duplikasi melalui hasil implementasi MAC dan RC6.

Adapun manfaat yang diharapkan dari penelitian ini adalah memahami kinerja MAC dan RC6, serta pengguna sebagai penerima data dapat mewaspadai tindakan kejahatan yang mungkin saat proses duplikasi berlangsung hingga file sampai ke penerima.

## 1.4. Ruang Lingkup

Dalam penyusunan penelitian ini, diberikan ruang lingkup yang jelas agar pembahasan lebih terarah dan tidak menyimpang dari tujuan penulisan. Ruang lingkup

implementasi MAC dan RC6 untuk mendeteksi perubahan file pada proses duplikasi file adalah sebagai berikut :

1. Input berupa kunci beserta file yang akan ditanamkan MAC atau file yang akan dicek jika terjadi perubahan ataupun tidak. Panjang kunci tidak lebih dari 16 karakter
2. Membangkitkan nilai MAC menggunakan SHA-1 digunakan untuk membangkitkan nilai hash dari file
3. Mengenkripsi nilai MAC menggunakan algoritma RC6 saat proses penanaman atau mendekripsi nilai MAC terenkripsi yang tertanam dalam file saat proses pencocokan.
4. Mengimplementasi penelitian ini menggunakan bahasa pemrograman C++.
5. Output berupa file yang telah tertanam MAC atau notifikasi jika terjadi perubahan pada file
6. Proses pertukaran kunci tidak diatur dalam sistem

## 1.5. Sistematika Penulisan

Sistematika penulisan yang digunakan dalam laporan tugas akhir ini terbagi menjadi beberapa pokok bahasan, yaitu:

BAB I PENDAHULUAN

Dalam bab ini dituliskan pembahasan mengenai latar belakang masalah, perumusan masalah, tujuan dan manfaat, ruang lingkup, serta sistematika penulisan laporan tugas akhir

BAB II LANDASAN TEORI

Dalam bab ini dijelaskan dasar teori, landasan, cara pandang, dan metode-metode yang telah ada dan digunakan yang berhubungan dengan laporan tugas akhir yang telah diuji kebenarannya.

BAB III ANALISIS DAN PERANCANGAN

Dalam bab ini dibahas proses pengembangan sistem pada tahap definisi kebutuhan, analisis dan perancangan, dengan hasilnya berupa desain dan rancangan sistem yang akan dikembangkan.

BAB IV IMPLEMENTASI DAN PENGUJIAN

Dalam bab ini dibahas hasil pengembangan sistem pada tahap implementasi dan menerangkan rincian pengujian sistem.

BAB V PENUTUP

Dalam bab ini berisi kesimpulan yang diambil berkaitan dengan sistem yang dibangun dan saran untuk pengembangan lebih lanjut.