# IMPLEMENTASI *MULTITHREADING* PECAHAN *PASSWORD*

**TUGAS AKHIR**


**Diajukan kepada Fakultas Teknik Informatika**
**Universitas Kristen Duta Wacana**
**Sebagai salah satu syarat dalam memperoleh gelar**
**Sarjana Komputer**

**Disusun Oleh**
**Deni Eko Guntoro**
**22064124**

**Program Studi Teknik Informatika Fakultas Teknologi Informasi**
**Universitas Kristen Duta Wacana**
**2011**

**PERNYATAAN KEASLIAN TUGAS AKHIR**

Saya menyatakan dengan sesunggunya bahwa tugas akhir dengan judul:

**Implementasi *Multithreading* Pemecahan *Password***

yang saya kerjakan untuk melengkapi sebagian persyaratan menjadi Sarjana Komputer pada pendidikan sarjana Program Studi Teknik Informatika, Fakultas Teknik Informasi Universitas Kristen Duta Wacana, bukan merupakan tiruan atau duplikasi dari skripsi kesarjanaan di lingkungan Universitas Kristen Duta Wacana maupun Perguruan Tinggi atau instansi manapun, kecuali bagian yang sumber infomasinya dicantumkan sebagaimana mestinya.

Jika di kemudian hari didapati bahwa skripsi ini adalah hasil plagiasi atau tiruan dari skripsi lain, saya bersedia menerima sanksi berupa pencabutan gelar kesarjanaan saya.

Yogyakarta, 31 Mei 2011

(Deni Eko Guntoro)

22064124

## HALAMAN PESETUJUAN

| | | | |
|---|---|---|---|
| Judul | : **Impementasi *Multithreading* Pemecahan *Password*** | | |
| Nama | : Deni Eko Guntoro | | |
| NIM | : 22 06 4124 | | |
| Matakuliah | : Tugas Akhir | Kode | : TI2126 |
| Semester | : Genap | Tahun Akademik | : 2010/2011 |

Telah diperiksa dan disetujui

Di Yogyakarta,

Pada Tanggal 31 Mei 2011

| Dosen Pembimbing I, | Dosen Pembimbing II, |
|---|---|
| (Junius Karel T, S.Si.,M.T) | (Budi Susanto, S.Kom.,M.T) |

**HALAMAN PENGESAHAN**

**SKRIPSI**

**IMPLEMENTASI MULTITHREADING PEMECAHAN PASSWORD**

Oleh: Deni Eko Guntoro / 22064124

Dipertahankan di depan dewan Penguji Tugas Akhir/Skripsi
Program Studi Teknik Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana – Yogyakarta
Dan dinyatakan diterima untuk memenuhi salah satu syarat memperoleh gelar
Sarjana Komputer
Pada tanggal
9 Juni 2011

Yogyakarta, 6171 2011

Mengesahkan,

Dewan Penguji :

1. Junius Karel T, S.Si.,M.T
2. Budi Susanto, S.Kom.,M.T
3. Willy Sudiarto Raharjo, S.Kom.,M.Cs
4. Yuan Lukito, S.Kom

Dekan Fakultas Teknologi Informasi

(Drs. Wimmie Handiwidjojo, MIT)

Ketua Program Studi

(Nugroho Agus H, S.Si. M.Si)

## KATA PENGANTAR

Puji Syukur penulis panjatkan ke hadapan Tuhan Yang Maha Esa karena atas karunia-Nya penulis dapat menyelesaikan tugas akhir ini.

Tugas akhir ini disusun untuk memenuhi persyaratan mencapai derajat Strata-1 (S-1) di jurusan Teknik Informatika Fakultas Teknologi Informasi Universitas Kristen Duta Wacana Yogyakarta.

Setelah menyelesaikan tugas akhir ini, penulis berharap semoga hasil akhir dari apa yang telah ditempuh selama ini dapat memberikan manfaat yang sebesar-besarnya bagi pengguna.

Selama penyusunan tugas akhir ini penulis menyadari sepenuhnya telah mendapatkan banyak bantuan dari berbagai pihak, sehingga tidak lupa penulis mengucapkan terima kasih yang sebesar-besarnya kepada :

1. Bapak Nugroho Agus Haryono, S.Si.,M.Si, selaku Ketua jurusan Teknik Informatika - Fakultas Teknologi Informasi Universitas Kristen Duta Wacana Yogyakarta.
2. Bapak Ir. Sri Suwarno, M.Eng, selaku Koordinator Skripsi Teknik Informatika Fakultas Teknologi Informasi Universitas Kristen Duta Wacana Yogyakarta.
3. Bapak Junius Karel, S.Si.,M.T, selaku pembimbing I dan Bapak Budi Susanto,S.Kom.,M.T, selaku pembimbing II, yang telah memberikan arahan, bimbingan serta dorongan semangat selama dalam penyelesaian tugas akhir ini.
4. Papa dan Mama atas segala bentuk dukungan dan doa yang telah diberikan.
5. Suriyati, yang dahulu selalu mendampingi saya, membantu banyak hal dalam perkuliahan saya dan memberikan doa serta dukungan dalam segala hal kepada saya untuk menyelesaikan tugas akhir ini, terima kasih semoga tuhan membalas jasamu.
6. Ade Gatra Galang yang selalu memberikan semangat, dukungan dan memberi nasehat berharga.
7. Dwi Putra atas segala dorongan semangat yang diberikan untuk segera menyelesaikan tugas akhir ini.

8. Riris, Imel, dan Elha buat dukungan semangat untuk mengerjakan tugas akhir ini.
9. Teman – teman Happy Hour khususnya Angga Ferdianto, Randi, Ndarjo(natanael sandi), Andre, Irfan terima kasih sudah memberikan kenangan indah yang tak terlupakan selama masa kuliah.
10. Keluarga Sukoharjo, pakde bude terima kasih atas doanya.
11. Seluruh Dosen Teknik Informatika, yang telah mengamalkan ilmu pengetahuannya.
12. Seluruh Staf dari Universitas Kristen Duta Wacana Yogyakarta yang telah membantu kelancaran administrasi penulis.
13. Teman-teman seperjuangan Teknik Informatika angkatan 2006 yang saling mendukung dalam penyelesaian perkuliahan.

Seiring dengan selesainya tugas akhir ini, penulis masih mengharapkan kritik dan saran yang berguna untuk menyempurnakan karya ini hingga dapat lebih bermanfaat.

Yogyakarta, 31 mei 2011

Penulis

## ABSTRAK

Dalam penelitian ini ingin dibuat sebuah sistem pemecahan password yang digunakan untuk memecahkan password yang terenkripsi. Input dari penelitian ini adalah password yang telah dienkripsi. Output dari aplikasi ini adalah teks sebagai password yang didapatkan dari proses perbandingan hasil md5 dari password asli dengan dugaan password yang didapat dari *generate looping*.

Dugaan password diperoleh dari 35 *thread* yang melakukan looping. Setiap *thread* mempunyai pekerjaan yang berbeda – beda antara *thread* yang satu dengan yang lainnya. Didalam thread terjadi looping untuk menghasilkan dugaan password berdasarkan pekerjaan thread tersebut. Pengujian dilakukan dengan membandingkan input password yang terenkripsi dengan enkripsi dari dugaan password, apabila dari perbandingan dinyatakan sama. Maka thread berhenti, dugaan password dinyatakan sebagai password original dan ditampilkan sebagai output. Apabila dari perbandingan dinyatakan berbeda maka thread akan berjalan terus sampai password ditemukan. Enkripsi yang digunakan adalah md5.

Hasil pengujian menunjukkan output cepat ditemukan apabila input password yang terenkripsi berasal dari password pendek yang mempunyai kombinasi sedikit atau sama. Waktu proses semakin lama untuk input password terenkripsi yang berasal dari password panjang yang terdiri dari berbagai macam kombinasi rumit. Multithreading berhasil mempercepat waktu yang diperlukan untuk memecahkan password dibandingkan dengan sistem yang tidak menerapkan multithreading.

**DAFTAR ISI**

## DAFTAR TABEL

## DAFTAR GAMBAR

# BAB 1

# PENDAHULUAN

## 1.1 Latar Belakang

Pada sistem pemecahan *password* yang umumnya menjadi permasalahan adalah banyaknya proses iterasi yang harus dikerjakan untuk memecahkan sebuah *password*. Banyaknya proses iterasi mengakibatkan sistem pemecahan *password* berjalan lambat untuk menemukan sebuah *password*. Untuk mengatasi hal ini maka diperlukan metode yang bisa digunakan untuk mempercepat proses iterasi dalam pemecahan *password*, salah satunya dengan *multithreading*.

*Multithreading* adalah metode yang menjalankan beberapa *thread* dalam sebuah proses dan dapat berjalan secara independen. Fungsi *multithreading* yaitu menjalankan beberapa *thread* dalam waktu yang bersamaan sehingga proses komputasi menjadi lebih cepat. Pada arsitektur *multiprocessor*, *thread* berjalan parallel diatas prosesor yang berbeda – beda.

Pada penelitian ini akan dibuat aplikasi yang menggunakan mekanisme *multithreading* untuk diterapkan dalam proses pemecahan *password*. *Multithreading* diharapkan dapat mempercepat proses iterasi didalam sistem pemecahan *password*.



## 1.2 Perumusan Masalah

Masalah yang akan dibahas dalam penelitian ini antara lain : Bagaimana menerapkan *multithreading* untuk software pemecahan password?

## 1.3 Batasan Masalah

Pada permasalahan ini, pembuatan program akan dibatasi oleh parameter-parameter sebagai berikut :

1. *Password* merupakan karakter huruf kecil (lower case), huruf besar (upper case) dan angka.
2. Panjang *password* maksimal 8 minimal 4.
3. Proses *enkripsi* menggunakan algoritma MD5.
4. Input *password* tidak ada spasi.
5. Jumlah *thread* ada 35 *thread*.
6. Proses pemecahan *password* menggunakan *brute force attack*.

## 1.4 Tujuan Penelitian

Tujuan penulisan tugas akhir ini adalah

1. Mengimplementasikan *multithreading* pada software pemecahan password yg menggunakan *brute force attack* untuk proses pemecahan *password*.
2. Sistem menghasilkan output *password* yang sama dengan *password* originalnya.

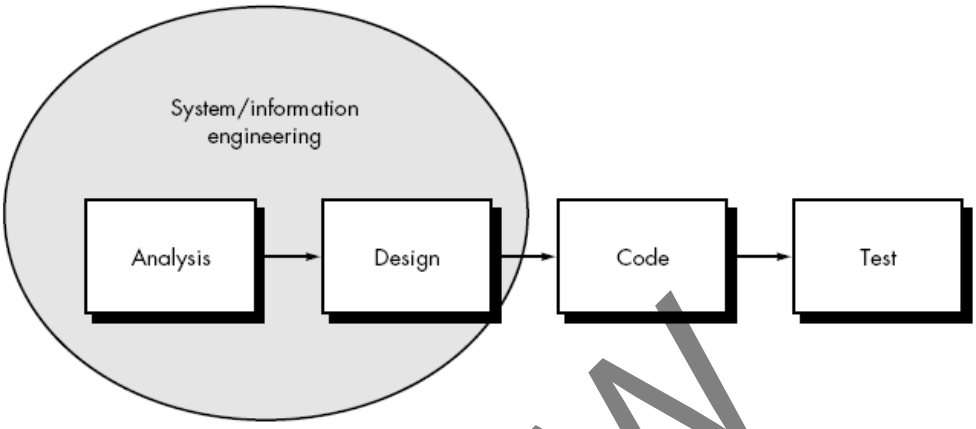


## 1.5 Metode / Pendekatan

Metodologi yang digunakan dalam menyelesaikan tugas akhir adalah *linear sequential model* yang terdiri dari tahapan sebagai berikut:

1. Menganalisa kebutuhan dan mengumpulkan data.
2. Desain : mengubah kebutuhan menjadi representasi perangkat lunak (desain interface dan cara kerja).
3. Pembuatan program: desain diubah menjadi bahasa mesin.
4. Program diimplementasikan dan diuji supaya bebas dari error.

Tahapan *linear sequential model* dapat dilihat pada Gambar 1.1




Gambar 1.1 : *Linear Sequential Model*

(Pressman, S. P., 2001, hal 29)



1.6 Sistematika Penulisan

Bab 1: Pendahuluan

Pendahuluan disusun dengan sistematika seperti ini : latar belakang masalah, perumusan masalah, batasan masalah, hipotesis, tujuan penelitian, metode/pendekatan yang dipakai dalam penelitian, serta sistematika penulisan.

Bab 2: Tinjuan Pustaka

Tinjuan pustaka terdiri dari 2 subbagian yakni Tinjauan Pustaka dan Landasan Teori

Bab 3: Perancangan Sistem

Bab ini memuat requirement, spesifikasi hardware untuk pengembangan, spesifikasi software untuk pengembangan, flowchart, cara perancangan sistem.

Bab 4: Implementasi dan Analisis Sistem

Bab ini memuat hasil riset, implementasi serta analisisnya secara mendetail.

Bab 5: Kesimpulan dan Saran

Bab ini memuat kesimpulan dari hasil penelitian dan saran untuk penelitian.

# BAB 5

# KESIMPULAN DAN SARAN

## 5.1 Kesimpulan

Dari hasil percobaan pada bab sebelumnya dapat diperoleh kesimpulan antara lain :

1. Sistem efektif untuk menemukan input password dengan variasi yang sedikit. Sistem memakan waktu lama untuk menemukan input yang terdiri dari variasi karakter yang banyak.
2. Penggunaan variasi yang berasal dari karakter dalam array yang banyak mengakibatkan proses looping yang lama sehingga program tidak responsive, dalam kasusnya bisa terjadi hang. Sebaliknya input yang terdiri dari variasi karakter yang berasal dari array kecil lebih cepat untuk ditemukan. Hal ini tergantung juga dari thread mana yang berjalan terlebih dahulu. Waktu proses ditentukan dari banyaknya variasi karakter, karakter yang tersimpan dalam array, thread yang lebih dahulu dieksekusi. Variasi yang terlalu banyak dan pemilihan karakter untuk variasi yang berasal dari penyimpanan array besar mengakibatkan lamanya proses pencarian dan hasil yang kurang tepat.

## 5.2 Saran

Dari hasil percobaan pada bab sebelumnya dapat diberikan saran antara lain :

1. Program dapat ditambahkan atribut yang lain supaya hasil lebih baik dan lebih kompleks. Sebagai contoh ditambahkan algoritma enkripsi yang lain seperti sha1 dan manajemen thread yang lebih terkontrol.
2. Program dapat memecahkan password pada file .rar , .zip dsb nya.
3. Program dapat dikembangkan menjadi distributed shared memory sehingga proses komputasi bisa berjalan pada banyak computer yang diharapkan bisa lebih mempercepat proses komputasi.

4. Proses cracking sebaiknya menggunakan algoritma yang memiliki proses cepat dan akurat untuk memecahkan password.

# DAFTAR PUSTAKA


Byrnes, Silverman dan Barret.(2005). *SSH The Secure Shell : The Definitive Guide*, O'Reilly Media, Inc.

Gray.(2003). *Interprocess Communications in Linux : The Nooks & Crannies*, Prentice Hall PTR.

Low, M.R dan Stamp, M.(2007). *Applied Cryptanalysis: Breaking Chippers in The Real World*, Wiley-IEEE.

Samik, M.R.(2008). Pengantar Sistem Operasi: Jilid Pertama, diakses 29 April 2011 dari http://bebas.vlsm.org/ v06/ Kuliah/ SistemOperasi/ BUKU/.

Shrivastava, M. dan Saxena, V.(2009). *UML Modeling and Performance Evaluation of Multithreaded Programs on Dual Core Processor*, diakses 29 april 2011 dari http://www.sersc.org/journals/IJHIT/vol2_no3_2009/.