KRIPTOANALISIS BRUTE FORCE ATTACK
PADA KRIPTOGRAFI KLASIK
(Caesar Code, Pengembangan Caesar Code, Vigenere)

Tugas Akhir

Oleh

Lutfi Rahadian
22043441

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

KRIPTOANALISIS BRUTE FORCE ATTACK
PADA KRIPTOGRAFI KLASIK
(Caesar Code, Pengembangan Caesar Code, Vigenere)

Tugas Akhir

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

Disusun oleh :

Lutfi Rahadian
22043441

Program Studi Teknik Informatika
Universitas Kristen Duta Wacana
Tahun 2011

PERNYATAAN KEASLIAN TUGAS AKHIR

Saya menyatakan dengun sesungguhnya bahwa tugas akhir dengan judul :

KRIPTOANALISIS BRUTE FORCE ATTACK
PADA KRIPTOGRAFI KLASIK
(Caesar Code, Pengembangan Caesar Code, Vigenere)

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

Jika dikemudian hari didapati bahwa hasil skripsi ini adalah hasil plagiasi atau tiruan dari skripsi lain, saya bersedia dikenai sanksi yakni pencabutan gelar kesarjanaan saya.

Yogyakarta, 29 April 2011

(Lutfi Rahadian)
22043441

INTISARI

KRIPTOANALISIS BRUTE FORCE ATTACK
PADA KRIPTOGRAFI KLASIK
(Caesar Code, Pengembangan Caesar Code, Vigenere)

Pesatnya perkembangan algoritma kriptografi yang baru membuat bertambahnya orang–orang ahli yang mampu memecahkan kode rahasia pada pesan yang telah dienkripsi (*ciphertext*) menjadi pesan asli (*plaintext*). Ketika sebuah algoritma kriptografi telah dipecahkan maka diperlukan algoritma baru yang lebih handal. Kriptografi dan pemecahannya tidak pernah berhenti berkembang. Oleh karena itu, penulis akan membangun sistem yang mengimplementasikan sebuah serangan (*Brute Force Attack*) terhadap beberapa algoritma kriptografi klasik yang ada. Melalui penulisan ini, maka diharapkan dapat diketahui tingkat kehandalan *Brute Force Attack*.

Pada penulisan ini, penulis melakukan berbagai uji coba pada sistem. Uji coba tersebut antara lain, uji coba dari segi kunci, panjang karakter masukan, tingkat toleransi, banyaknya isi kamus kata, tingkat keamanan, dan uji coba dimana masukan diluar batasan masalah.

Dari uji coba tersebut, *Brute Force Attack* berhasil diimplementasikan untuk memecahkan kriptografi klasik tetapi tingkat kesuksesannya dipengaruhi oleh panjang kunci dan karakter masukan, tingkat toleransi, serta banyaknya kata pada kamus kata. Dari ketiga kriptografi klasik yang digunakan, Algoritma Pengembangan *Caesar Code* memiliki tingkat keamanan tertinggi.

HALAMAN PERSETUJUAN

Judul	: Kriptoanalisis Brute Force Attack Pada Kriptografi Klasik (Caesar Code, Pengembangan Caesar Code, Vigenere)
Nama	: Lutfi Rahadian
NIM	: 22043441
Mata Kuliah	: Tugas Akhir
Kode	: TI2126
Semester	: Pendek
Tahun Akademik	: 2010/2011

Telah diperiksa dan disetujui
Di Yogyakarta,
Pada Tanggal 18 Juli 2011

Dosen Pembimbing I	Dosen Pembimbing II
Restyandito, S.Kom., MSIS	Ir. Sri Suwarno, M.Eng.

HALAMAN PENGESAHAN

SKRIPSI

KRIPTOANALISIS BRUTE FORCE ATTACK

PADA KRIPTOGRAFI KLASIK

(Caesar Code, Pengembangan Caesar Code, Vigenere)

Oleh : Lutfi Rahadian / 22043441

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

26 Juli 2011

Yogyakarta, 31/8/2011

Mengesahkan,

Dewan Penguji :

1. Restyandito, S.Kom., MSIS. _____
2. Ir. Sri Suwarno, M.Eng. _____
3. Junius Karel T., S.Si., M.T. _____
4. Budi Susanto, S.Kom., M.T. _____

Dekan

(Drs. Wimmie Handiwidjojo, MIT.)

Ketua Program Studi

(Nugroho Agus Haryono S.Si.,MSi.)

UCAPAN TERIMA KASIH

Puji dan syukur kepada Tuhan sehingga penulis dapat menyelesaikan Tugas Akhir dengan judul Kriptoanalisis Brute Force Attack Pada Kriptografi Klasik (Caesar Code, Pengembangan Caesar Code, Vigenere) dengan baik. Penulisan ini disusun sebagai kelengkapan dan pemenuhan dari salah satu syarat dalam memperoleh gelar Sarjana Komputer. Dalam penulisan ini, penulis banyak menerima bimbingan dan masukan dari berbagai pihak. Pada kesempatan ini, penulis ingin menyampaikan ucapan terima kasih kepada :

1. Bapak Restyandito, S.Kom., MSIS. selaku Dosen Pembimbing I yang telah meluangkan waktu dengan sabar dalam memberikan bimbingan dan petunjuk kepada penulis.
2. Bapak Ir. Sri Suwarno, M.Eng. selaku Dosen Pembimbing II yang telah memberikan waktunya untuk bimbingan dan mengarahkan penulis.
3. Keluarga dan seseorang yang tercinta yang mendukung dan menyemangati tanpa kenal lelah.
4. Teman-teman yang telah memberikan saran dan semangat.
5. Pihak lain yang tidak dapat disebutkan satu persatu, sehingga Tugas Akhir ini dapat terselesaikan dengan baik.

Penulisan ini masih jauh dari sempurna. Oleh karena itu, dalam kesempatan ini penulis mengharapkan saran dan kritik yang membangun sehingga suatu saat dapat menghasilkan karya yang lebih baik. Akhir kata, penulis ingin meminta maaf bila ada kesalahan dalam penyusunan laporan maupun program Tugas Akhir. Semoga Tugas Akhir ini dapat berguna bagi kita semua.

Yogyakarta, 29 April 2011

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR GRAFIK

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Pesatnya perkembangan algoritma kriptografi yang baru membuat bertambahnya orang–orang ahli yang mampu memecahkan kode rahasia pada pesan yang telah dienkripsi (*ciphertext*) menjadi pesan asli (*plaintext*). Ketika sebuah algoritma kriptografi telah dipecahkan maka diperlukan algoritma baru yang lebih handal.

Kriptografi dan pemecahannya tidak pernah berhenti berkembang. Oleh karena itu, penulis akan membangun sistem yang mengimplementasikan sebuah serangan (*Brute Force Attack*) terhadap beberapa algoritma kriptografi klasik yang ada.

Melalui penulisan ini, maka diharapkan dapat diketahui tingkat kehandalan *Brute Force Attack*.

1.2 Rumusan Masalah

Berdasarkan uraian pada Subbab 1.1 akan dibuat, bagaimana implementasi *Brute Force Attack* pada sistem kriptografi klasik?

1.3 Batasan Masalah

Batasan masalah dari sistem yang akan dibangun untuk keperluan analisis adalah sistem akan memecahkan *ciphertext* dengan metode *Brute Force Attack.* Algoritma kriptografi yang digunakan adalah *Caesar Code*, Pengembangan *Caesar Code*, dan *Vigenere* cara angka. Bahasa yang digunakan pada *database* (kamus kata) adalah Bahasa Indonesia sesuai EYD (Ejaan Yang Disempurnakan). Semua karakter yang akan dibobol, hanya karakter yang terdapat pada Tabel 2.3

dan ada dalam kamus kata. Pembobolan hanya ditujukan untuk file teks saja. Pada proses, huruf kecil akan dijadikan huruf besar. Kunci berupa angka dan maksimum menggunakan 4 kombinasi kunci. Penggunaan kunci hanya satu tingkat.

1.4 Tujuan Penulisan

Penulisan ini bertujuan untuk membuktikan tingkat kesuksesan sebuah serangan (*Brute Force Attack*) terhadap beberapa algoritma kriptografi klasik (*Caesar Code*, pengembangan dari *Caesar Code*, dan *Vigenere* cara angka).

1.5 Metode / Pendekatan

Pada penulisan ini akan diadakan penelitian dua tahap. Tahap pertama, meneliti algoritma kriptografi klasik dan serangannya yang telah diuraikan pada Subbab 1.3. Algoritma kriptografi klasik dan serangan yang diteliti akan diambil dari berbagai sumber media cetak maupun elektronik. Tahap kedua, membangun sistem yang mengimplementasikan sebuah serangan terhadap beberapa algoritma klasik.

1.6 Sistematika Penulisan

Penulisan ini memiliki sistematika sebagai berikut : Bab 1 PENDAHULUAN mencakup latar belakang masalah dan rencana penulisan yang akan dilakukan. Bab 2 TINJAUAN PUSTAKA mencakup uraian teori-teori yang akan digunakan. Bab 3 ANALISIS DAN PERANCANGAN SISTEM mencakup analisis teori-teori yang digunakan dan menerapkannya ke dalam sistem yang akan dirancang. Bab 4 IMPLEMENTASI DAN ANALISIS SISTEM mencakup hasil implementasi dan analisis terhadap sistem yang telah dibangun. Bab 5 KESIMPULAN mencakup pernyataan singkat dari hasil implementasi dan analisis sistem.

BAB 5

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan sistem yang telah dibuat dan percobaan yang telah dilakukan, *Brute Force Attack* berhasil diimplementasikan untuk memecahkan kriptografi klasik tetapi tingkat kesuksesannya dipengaruhi oleh :

- panjang kunci,
- panjang karakter pada masukan,
- tingkat toleransi, dan
- banyaknya kata pada kamus kata.

Di antara ketiga algoritma yang digunakan (Algoritma *Caesar Code*, Pengembangan *Caesar Code*, dan *Vigenere*), yang memiliki tingkat keamanan paling tinggi adalah Algoritma Pengembangan *Caesar Code*.

5.2 Saran

Jika ada mahasiswa yang tertarik ingin mengambil penulisan ini sebagai topik skripsi, maka dapat dikembangkan dengan menggunakan bahasa *assembly*. Pada umumnya kode *assembly* jauh lebih cepat dari kode Delphi, sehingga dapat mempercepat proses pembobolan. Selain itu, dapat juga dikembangkan dengan penggunaan banyak CPU dalam waktu yang bersamaan untuk mempercepat pembobolan. Jika ingin dikembangkan dari segi *database*, sistem tidak hanya dapat membobol pesan Bahasa Indonesia tetapi juga dapat untuk membobol bahasa lain, seperti Bahasa Inggris, Bahasa Sunda, dan lain – lain. Jika ingin mengembangkan tabel pergeseran, tabel dapat ditambahkan karakter bebas seperti tanda baca dan angka. Tentunya sistem juga perlu ditambahkan sistem pakar untuk menentukan kemungkinan posisi dari karakter bebas tersebut.

DAFTAR PUSTAKA

Ariyus, D. (2008). *Pengantar Ilmu Kriptografi : Teori, Analisis, dan Implementasi*. Yogyakarta : Andi Offset.

Chandrawijaya, F. (1998). *Program Cryptoanalyzer Untuk Monosubstitution Cipher*. Yogyakarta : Universitas Kristen Duta Wacana.

Dermawan, H. (2001). *Membandingkan Kecepatan Algoritma Brute Force (BF), Algoritma Knuth-Morris-Pratt (KMP), Dan Algoritma Boyer-Moore (BM) Dalam Mencocokkan String Pada Sebuah Dokumen*. Yogyakarta : Universitas Kristen Duta Wacana.

Henry (2001). *Aplikasi Cryptanalysis Dalam Usaha Mendekripsi Ciphertext Dari Secure Talk Dengan Pendekatan Metode Dictionary Search*. Yogyakarta : Universitas Kristen Duta Wacana.

Kadir, A. (2001). *Dasar Pemrograman Delphi 5.0 (Jilid 1)*. Yogyakarta : Andi Offset.

Mogollon, M. (2007). *Cryptography and Security Services : Mechanisms and Applications*. New York : Cybertech Publishing.

Mollin, R.A. (2007). *An Introduction to Cryptography, Second Edition*. Boca Raton : Taylor & Francis Group, LCC.

Narayanan, A., & Shmatikov, V. (2005). *Fast Dictionary Attacks on Passwords Using Time-Space Tradeoff*. USA : The University of Texas at Austin.

Olivia (2001). *Enkripsi, Dekripsi, dan Kriptoanalisis Pada Vigenere Cipher*. Yogyakarta : Universitas Kristen Duta Wacana.

Oplliger, R. (2005). *Contemporary Cryptography*. Norwood : ARTECH House Inc.

Stallings, W. (2005). *Cryptography and Network Security Principles an Practices, Fourth Edition*. New Jersey : Prentice Hall.

Tim Penyusun Kamus Pusat Bahasa (2008). *Kamus Bahasa Indonesia*. Jakarta : Pusat Bahasa.