

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 dengan 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 )

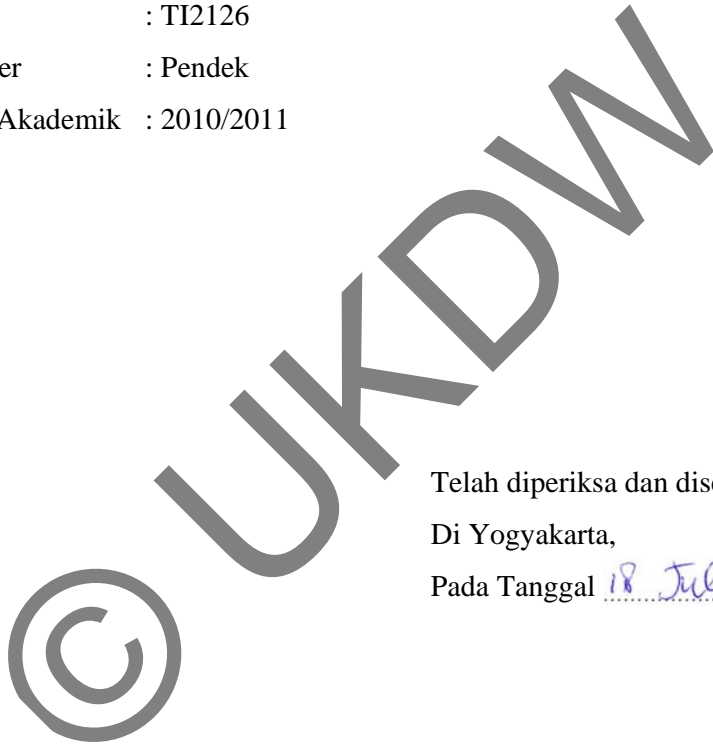
Pesatnya perkembangan algoritma kriptografi yang baru membuat bertambahnya orang-orang ahli yang mampu memecahkan kode rahasia pada pesan yang telah dienkripsi ( *ciphertext* ) menjadi pesan asli ( *plaintext* ). Ketika sebuah algoritma kriptografi telah dipecahkan maka diperlukan algoritma baru yang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

Restyandito, S.Kom., MSIS

Dosen Pembimbing II

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.

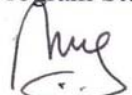


Dekan



( 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 Kriptanalisis 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

HALAMAN JUDUL .....	
PERNYATAAN KEASLIAN SKRIPSI .....	i
HALAMAN PERSETUJUAN .....	ii
HALAMAN PENGESAHAN .....	iii
UCAPAN TERIMA KASIH .....	iv
INTISARI .....	v
DAFTAR ISI .....	vi
DAFTAR TABEL .....	viii
DAFTAR GAMBAR .....	ix
DAFTAR GRAFIK .....	xii
BAB 1 PENDAHULUAN .....	1
1.1 Latar Belakang .....	1
1.2 Rumusan Masalah .....	1
1.3 Batasan Masalah .....	1
1.4 Tujuan Penulisan .....	2
1.5 Metode / Pendekatan .....	2
1.6 Sistematika Penulisan .....	2
BAB 2 TINJAUAN PUSTAKA .....	3
2.1 Tinjauan Pustaka .....	3
2.2 Landasan Teori .....	4
2.2.1 Kriptografi .....	4
2.2.2 Kriptanalisis .....	4
2.2.3 <i>Brute Force Attack</i> .....	6
2.2.4 Analisis Frekuensi .....	6
2.2.5 Algoritma <i>Caesar Code</i> .....	7
2.2.6 Algoritma Pengembangan <i>Caesar Code</i> .....	8
2.2.7 Algoritma <i>Vigenere</i> Cara Angka .....	9
BAB 3 PERANCANGAN SISTEM .....	10



3.1 Rancangan Kerja Sistem .....	10
3.2 Rancangan <i>User Interface</i> .....	13
3.3 Rancangan <i>Database</i> .....	14
3.4 Cara Kerja Sistem .....	14
<b>BAB 4 IMPLEMENTASI DAN ANALISIS SISTEM .....</b>	<b>15</b>
4.1 Implementasi Sistem .....	15
4.1.1 Halaman Login .....	15
4.1.2 Halaman Utama .....	15
4.1.3 Halaman Data kamus .....	15
4.1.4 Halaman Frekuensi Huruf .....	16
4.1.5 Halaman Enkripsi .....	17
4.1.6 Halaman Pembobolan .....	17
4.1.7 Implementasi Enkripsi .....	19
4.1.7.1 Enkripsi Dengan Algoritma <i>Caesar Code</i> .....	19
4.1.7.2 Enkripsi Dengan Algoritma Pengembangan <i>Caesar Code</i> .....	20
4.1.7.3 Enkripsi Dengan Algoritma <i>Vigenere</i> .....	22
4.1.8 Implementasi Pembobolan Hasil Enkripsi .....	24
4.2 Analisis Sistem .....	26
4.2.1 Contoh Kasus Pertama .....	26
4.2.2 Contoh Kasus Kedua .....	29
4.2.3 Contoh Kasus Ketiga... .....	33
4.2.4 Contoh Kasus Keempat .....	38
4.2.5 Contoh Kasus Kelima .....	40
4.2.6 Contoh Kasus Keenam .....	46
<b>BAB 5 KESIMPULAN DAN SARAN .....</b>	<b>52</b>
5.1 Kesimpulan .....	52
5.2 Saran .....	52
<b>DAFTAR PUSTAKA .....</b>	<b>53</b>

## DAFTAR TABEL

Tabel 2.1	Tipe Serangan .....	4
Tabel 2.2	Huruf Yang Sering Muncul Dalam Bahasa Indonesia .....	6
Tabel 2.3	Tabel Pergeseran Karakter .....	7
Tabel 3.1	Tabel Rancangan <i>Database</i> .....	14
Tabel 4.1	Tabel Data Contoh Kasus <i>Caesar</i> .....	19
Tabel 4.2	Tabel Data Contoh Kasus Pengembangan <i>Caesar</i> .....	20
Tabel 4.3	Tabel Data Contoh Kasus <i>Vigenere</i> .....	23
Tabel 4.4	Masukan Pada Contoh Kasus Kedua .....	29
Tabel 4.5	Tabel Hasil Pembobolan Pertama Toleransi Rendah .....	34
Tabel 4.6	Tabel Hasil Pembobolan Pertama Toleransi Sedang .....	35
Tabel 4.7	Tabel Percobaan Pada Contoh Kasus Ketiga .....	36
Tabel 4.8	Tabel Hasil Pembobolan Pertama Dan Kedua Pada Contoh Kasus Kelima .....	43
Tabel 4.9	Tabel Hasil Pembobolan Ketiga Pada Contoh Kasus Kelima .....	44
Tabel 4.10	Tabel Hasil Enkripsi Dengan <i>Caesar Code</i> Pada Contoh Kasus Keenam .....	47
Tabel 4.11	Tabel Hasil Enkripsi Dengan Pengembangan <i>Caesar Code</i> Pada Contoh Kasus Keenam .....	49
Tabel 4.12	Tabel Hasil Enkripsi Dengan <i>Vigenere</i> Pada Contoh Kasus Keenam .....	50

## DAFTAR GAMBAR

Gambar 3.1	<i>Flow Chart</i> Sistem .....	10
Gambar 3.2	<i>Flow Chart</i> Pemecahan Masukan Dengan Asumsi Algoritma <i>Caesar Code</i> .....	11
Gambar 3.3	<i>Flow Chart</i> Pemecahan Masukan Dengan Asumsi Algoritma Pengembangan <i>Caesar Code</i> .....	11
Gambar 3.4	<i>Flow Chart</i> Pemecahan Masukan Dengan Asumsi Algoritma <i>Vigenere</i> .....	12
Gambar 3.5	Tampilan Sistem .....	13
Gambar 4.1	Tampilan Halaman <i>Login</i> .....	15
Gambar 4.2	Tampilan Halaman Utama .....	16
Gambar 4.3	Tampilan Halaman Data kamus .....	16
Gambar 4.4	Tampilan Halaman Frekuensi Huruf .....	17
Gambar 4.5	Tampilan Halaman Enkripsi .....	18
Gambar 4.6	Tampilan Halaman Pembobolan .....	18
Gambar 4.7	Tampilan Penerapan Contoh Kasus <i>Caesar</i> .....	19
Gambar 4.8	Tampilan Hasil Penerapan Contoh Kasus <i>Caesar</i> .....	20
Gambar 4.9	Tampilan Penerapan Contoh Kasus Pengembangan <i>Caesar</i> .....	21
Gambar 4.10	Tampilan Peringatan Bila Jumlah Kunci Melebihi Batas .....	21
Gambar 4.11	Tampilan Peringatan Bila Kunci Belum Dimasukkan .....	22
Gambar 4.12	Tampilan Hasil Penerapan Contoh Kasus Pengembangan <i>Caesar</i> .....	22
Gambar 4.13	Tampilan Penerapan Contoh Kasus <i>Vigenere</i> .....	23
Gambar 4.14	Tampilan Hasil Penerapan Contoh Kasus <i>Vigenere</i> .....	24
Gambar 4.15	Tampilan Penerapan Contoh Kasus Pembobolan .....	24
Gambar 4.16	Tampilan Hasil Penerapan Kemungkinan 1 Pada Contoh Kasus Pembobolan .....	25

Gambar 4.17	Tampilan Hasil Penerapan Kemungkinan 2 Pada Contoh Kasus Pembobolan .....	25
Gambar 4.18	Tampilan Hasil Penerapan Kemungkinan 3 Pada Contoh Kasus Pembobolan .....	26
Gambar 4.19	Tampilan Hasil Pembobolan Pertama Pada Contoh Kasus Pertama .....	28
Gambar 4.20	Tampilan Hasil Pembobolan Kedua Pada Contoh Kasus Pertama .....	28
Gambar 4.21	Tampilan Hasil Pembobolan Ketiga Pada Contoh Kasus Pertama .....	29
Gambar 4.22	Tampilan Hasil Pembobolan Keempat Pada Contoh Kasus Pertama .....	29
Gambar 4.23	Tampilan Hasil Pembobolan Masukan Dengan 22 Karakter .....	32
Gambar 4.24	Tampilan Hasil Pembobolan Masukan Dengan 52 Karakter .....	32
Gambar 4.25	Tampilan Hasil Pembobolan Masukan Dengan 72 Karakter .....	32
Gambar 4.26	Tampilan Hasil Pembobolan Dengan Satu Hasil .....	33
Gambar 4.27	Tampilan Hasil Pembobolan Pertama Toleransi Rendah .....	33
Gambar 4.28	Tampilan Hasil Pembobolan Pertama Toleransi Sedang .....	35
Gambar 4.29	Tampilan Hasil Pembobolan Pertama Toleransi Tinggi .....	35
Gambar 4.30	Tampilan Hasil Pembobolan Pertama Toleransi Maksimum	36
Gambar 4.31	Tampilan Hasil Pembobolan Pertama Pada Contoh Kasus Keempat .....	38
Gambar 4.32	Tampilan Hasil Pembobolan Kedua Pada Contoh Kasus Keempat .....	38
Gambar 4.33	Tampilan Hasil Pembobolan Ketiga Pada Contoh Kasus Keempat .....	39
Gambar 4.34	Tampilan Hasil Pembobolan Keempat Dengan Kemungkinan 1 Pada Contoh Kasus Keempat .....	39

Gambar 4.35	Tampilan Hasil Pembobolan Keempat Dengan Kemungkinan 2 Pada Contoh Kasus Keempat .....	40
Gambar 4.36	Tampilan Hasil Pembobolan Keempat Dengan Kemungkinan 3 Pada Contoh Kasus Keempat .....	40
Gambar 4.37	Tampilan Kamus Kata Dengan 19 Kata .....	41
Gambar 4.38	Tampilan Kamus Kata Dengan 27 Kata .....	41
Gambar 4.39	Tampilan Kamus Kata Dengan 59 Kata .....	41
Gambar 4.40	Tampilan Hasil Pembobolan Pertama Pada Contoh Kasus Kelima .....	42
Gambar 4.41	Tampilan Hasil Pembobolan Kedua Pada Contoh Kasus Kelima .....	42
Gambar 4.42	Tampilan Hasil Pembobolan Ketiga Pada Contoh Kasus Kelima .....	43
Gambar 4.43	Tampilan Hasil Pembobolan Ke-8 Dengan Kemungkinan 1 Pada Contoh Kasus Keenam .....	48
Gambar 4.44	Tampilan Hasil Pembobolan Ke-8 Dengan Kemungkinan 2 Pada Contoh Kasus Keenam .....	48
Gambar 4.45	Tampilan Hasil Pembobolan Ke-8 Dengan Kemungkinan 3 Pada Contoh Kasus Keenam .....	49



## DAFTAR GRAFIK

Grafik 4.1 Grafik Perbandingan Waktu Pembobolan ( Menggunakan Toleransi Maksimum ) Dan Banyaknya Kunci Yang Digunakan Pada Masukan .....	28
Grafik 4.2 Grafik Perbandingan Waktu Pembobolan ( Menggunakan Toleransi Maksimum ) Dan Banyaknya Karakter Pada Masukan.....	31
Grafik 4.3 Grafik Perbandingan Banyaknya Hasil Pembobolan Dan Tingkat Toleransi Yang Digunakan Saat Membobol.....	37
Grafik 4.4 Grafik Perbandingan Banyaknya Hasil Pembobolan Dan Banyaknya Kata Pada Kamus Kata .....	46
Grafik 4.5 Grafik Perbandingan Waktu Pembobolan ( Menggunakan Toleransi Maksimum ) Dan Banyaknya Kata Pada Kamus Kata.....	46
Grafik 4.6 Grafik Waktu Pembobolan ( Menggunakan Toleransi Maksimum ) Dari Sepuluh Percobaan Pada Tiga Kriptografi Klasik Yang Digunakan .....	51



# 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.

Opllinger, 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.

© UKDW