

**PENERAPAN KOMBINASI ALGORITMA CAESAR
DAN VIGENERE UNTUK PENGAMANAN DATA
PESAN**

SKRIPSI



Oleh :

FAUZAN ARIVANDI

NPM. 1134010070

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN"
JAWA TIMUR
2018**

**LEMBAR PENGESAHAN
SKRIPSI**

**Judul : PENERAPAN KOMBINASI ALGORITMA CAESAR DAN
VIGENERE UNTUK PENGAMANAN DATA PESAN**
Oleh : FAUZAN ARIVANDI
NPM : 1134010070

**Telah Diseminarkan Dalam Ujian Skripsi Pada :
Hari, Senin Tanggal 21 Mei 2018**

Mengetahui

Dosen Pembimbing

Dosen Penguji

1.

1.

Intan Yuniar Purbasari, S.Kom, M.Sc
NPT : 3 8006 04 0198 1

Intan Yuniar Purbasari, S.Kom, M.Sc
NPT : 3 8006 04 0198 1

2.

2.

Eva Yulia .S.Kom, M.Kom
NPT : 3 8907 13 0346 1

Yisti Vita Via, S.ST, M.Kom
NPT : 3 8604 13 0347 1

3.

Ronggo Alit, S.Kom, MM, MT
NPT : 3 8412 10 0321 1

Menyetujui

**Dekan
Fakultas Ilmu Komputer**

**Koordinator Program Studi
Teknik Informatika**

Dr. Ir. Ni Ketut Sari, MT
NPT : 19650731 1199203 2 001

Budi Nugroho, S.Kom, M.Kom
NPT : 3 8009 05 0205 1

SURAT PERNYATAAN ANTI PLAGIAT

Saya, mahasiswa Teknik Informatika UPN “Veteran” Jawa Timur, yang bertandatangan di bawah ini:

Nama : Fauzan Arivandi

NPM : 1134010070

Menyatakan bahwa Judul Skripsi/ Tugas Akhir Saya, yang berjudul:

PENERAPAN KOMBINASI ALGORITMA CAESAR DAN VIGENERE
UNTUK PENGAMANAN DATA PESAN.

Bukan merupakan plagiat dari Skripsi/ Tugas Akhir/ Penelitian orang lain dan juga bukan merupakan produk dan atau *software* yang saya beli dari pihak lain. Saya juga menyatakan bahwa Skripsi/ Tugas Akhir ini adalah pekerjaan Saya sendiri, kecuali yang dinyatakan dalam Daftar Pustaka dan tidak pernah diajukan untuk syarat memperoleh gelar di UPN “Veteran” Jawa Timur maupun di institusi pendidikan lain.

Jika ternyata di kemudian hari pernyataan ini terbukti tidak benar, maka Saya siap menerima segala konsekuensinya.

Surabaya, 25 Mei 2018
Hormat Saya,

Fauzan Arivandi
NPM : 1134010070

PENERAPAN KOMBINASI ALGORITMA CAESAR DAN VIGENERE UNTUK PENGAMANAN DATA PESAN PADA SURAT ELEKTRONIK

Nama Mahasiswa : Fauzan Arivandi
NPM : 1134010070
Program Studi : Teknik Informatika
Dosen Pembimbing : Intan Yuniar Purbasari, S.Kom, M.sc
Eva Yulia , S.Kom, M.Kom

Abstrak

Pengamanan data pesan sangat penting. Oleh karena itu penanganan terhadap pengamanan data pesan ini harus ditanggapi dengan serius. Pengiriman pesan dalam kehidupan sehari-hari sangat rawan dengan aksi-aksi penyadapan data pesan, yang mana itu merupakan kejahatan yang melanggar hak asasi manusia. Oleh karena itu harus dilakukan pengamanan data pesan dengan mengkombinasi algoritma *Caesar* dan *Vigenere*.

Aplikasi yang dibuat dalam bentuk pesan pribadi yang berbasis web. Pada saat melakukan pengiriman pesan disaat itu juga proses enkripsi dilakukan yang pertama dienkripsi dengan algoritma *Caesar* yang hasilnya nantinya akan dienkripsi dengan algoritma *Vigenere*. Untuk proses deskripsi dilakukan oleh penerima pesan di dalam *inbox*.

Dengan mengkombinasikan kedua metode ini pada pesan pribadi, data yang kita terima dalam bentuk kode atau huruf yang berbeda dengan isi pesan yang dikirim. Sehingga jika ada penyadapan maka akan sulit untuk membaca pesan tersebut, karena proses deskripsi hanya ada pada menu *inbox* serta pesan yang disimpan pada *database* sudah dalam bentuk *chiperteks* (kode).

Kata kunci: *Caesar Chiper*, Enkripsi, Deskripsi, *Vigenere Chiper*,

KATA PENGANTAR

Syukur Alhamdulillah terucap kehadirat Allah SWT atas segala limpahan Rahmat-Nya sehingga dengan segala keterbatasan waktu, tenaga, dan pikiran yang dimiliki, akhirnya penulis dapat menyelesaikan Tugas Akhir yang berjudul “Penerapan Kombinasi Algoritma Caesar dan Vigenere Untuk Pengamanan Data Pesan”.

Tugas Akhir ini disusun guna diajukan sebagai salah satu syarat untuk menyelesaikan program Strata Satu (S1) pada jurusan Teknik Informatika, Fakultas Ilmu Komputer, UPN “Veteran” Jawa Timur.

Dalam penyusunan Tugas akhir ini, Penulis berusaha untuk menerapkan ilmu yang telah didapat selama menjalani perkuliahan dengan tidak terlepas dari petunjuk, bimbingan, bantuan, dan dukungan berbagai pihak.

Penulis menyadari sepenuhnya bahwa dalam penyusunan tugas akhir ini masih banyak kekurangan. Oleh karena itu penulis sangat mengharapkan saran dan kritik dari para pembaca untuk pengembangan aplikasi lebih lanjut.

Surabaya, 25 Mei 2018

Penulis

UCAPAN TERIMA KASIH

Puji syukur ke hadirat Allah SWT yang telah memberikan rahmat dan karunia-Nya, sehingga dapat terselesaikannya Tugas Akhir ini. Dengan selesainya tugas akhir ini penulis ingin mengucapkan terima kasih kepada pihak-pihak yang telah membantu, karena tanpa bantuan, saran, kritik, serta dukungan mereka mungkin penulis tidak akan dapat menyelesaikan laporan ini. Pada kesempatan ini, penulis ingin mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Allah SWT, karena berkat Rahmat dan berkahNya penulis dapat menyusun dan menyelesaikan Laporan Skripsi ini hingga selesai.
2. Ibu Dr. Ir. Ni Ketut Sari, MT selaku Dekan Fakultas Ilmu Komputer.
3. Bapak Budi Nugroho, S.Kom, M.Kom selaku Ketua Jurusan Teknik Informatika.
4. Ibu Intan Yuniar Purbasari., S.Kom, M.sc selaku Dosen Pembimbing I Tugas Akhir yang telah meluangkan begitu banyak waktu, tenaga dan pikiran serta dengan sabar membimbing penulis dari awal hingga tugas akhir ini dapat terselesaikan.
5. Ibu Eva Yulia P, S.Kom, M.Kom selaku Dosen Pembimbing II yang telah banyak memberikan petunjuk, masukan serta kritik yang bermanfaat hingga terselesainya tugas akhir ini.
6. Bapak Hendra Maulana, S.Kom selaku koordinator PKL & Skripsi

7. Keluarga tercinta, terutama Bapak, Ibu dan Istriku tersayang, terima kasih atas semua doa, dukungan serta harapan-harapannya pada saat penulis menyelesaikan tugas akhir ini.
8. Rekan – rekan jurusan Teknik Informatika khususnya Hanindyo Rizkie, Alfian Akbar Pratama, Angga Kurniawan, Indra Septian, M. Rizal, M. Amin, Kukuh dan yang tak bisa penulis sebutkan satu persatu yang telah membantu dalam penyelesaian tugas akhir ini beserta laporannya. Terima Kasih yang tak terhingga untuk kalian semua.

Akhir kata, semoga dengan laporan ini dapat berguna bagi pembaca dan memberikan manfaat bagi pihak yang membutuhkannya.

Surabaya, 25 Mei 2018

Penulis

DAFTAR ISI

HALAMAN JUDUL	
LEMBAR PENGESAHAN	
ABSTRAK	i
KATA PENGANTAR	ii
UCAPAN TERIMA KASIH	iii
DAFTAR ISI	v
DAFTAR GAMBAR	vii
BAB I PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Permasalahan	2
1.3 Batasan Masalah	2
1.4 Tujuan	3
1.5 Manfaat	3
1.6 Sistematika Penulisan	3
BAB II TINJAUAN PUSTAKA	5
2.1 Penelitian Terdahulu	5
2.2 Dasar Teori	6
2.2.1 Keamanan Data	6
2.2.2 Pengenalan Kriptografi	9
2.2.3 Enkripsi dan Dekripsi	11
2.2.4 Algoritma Kriptografi	13
2.2.5 Serangan pada Kriptografi	18

2.2.6 Algoritma Caesar	20
2.2.7 Algoritma Vigenere	22
BAB III METODOLOGI PENELITIAN	30
3.1 Metode Penelitian	30
3.2 Analisis Sistem	32
3.3 Perancangan Proses.....	32
3.3.1 Diagram Alir (Flowchart)	32
3.3.2 Use Case Diagram	40
3.3.3 Activity Diagram	41
1 Activity Diagram Login	41
2 Activity Diagram Kirim Pesan	42
3 Activity Diagram Inbox	43
3.3.4 Class Diagram	43
3.4 Perancangan Antar Muka	44
3.4.1 Tampilan Login Aplikasi	45
3.4.2 Tampilan Halaman Utama	45
3.4.3 Tampilan Halaman Inbox	46
3.4.4 Tampilan Halaman Outbox	46
3.4.5 Tampilan Halaman Select User	47
3.4.6 Tampilan Halaman Kirim Pesan	47
3.4 Perhitungan Algoritma Caesar dan Vigenere	48
BAB IV HASIL DAN PEMBAHASAN	51
4.1 Kebutuhan Sistem	51
4.2 Implementasi Sistem	52

4.2.1 Implementasi Login	52
4.2.2 Implementasi Halaman Utama	53
4.2.3 Implementasi Halaman Inbox	53
4.2.4 Implementasi Halaman Outbox.....	55
4.2.5 Implementasi Halaman Send New Messege	56
BAB V KESIMPULAN DAN SARAN.....	58
5.1 Kesimpulan.....	58
5.2 Saran.....	58
DAFTAR PUSTAKA	59

DAFTAR GAMBAR

Gambar 2.1 Proses Enkripsi dan Deskripsi (Rinaldi,2006).....	12
Gambar 2.2 Proses Algoritma Simetri	13
Gambar 2.3 Proses Algoritma Asimetri	16
Gambar 2.4 Sandi Caesar	20
Gambar 2.5 Bujursangkar Vigenere	26
Gambar 3.1 Flowchat Sistem	33
Gambar 3.2 Flowchat Proses Enkripsi	34
Gambar 3.3 Flowchat Proses Deskripsi	35
Gambar 3.4 Flowchat Proses Enkripsi Caesar	36
Gambar 3.5 Flowchat Proses Deskripsi Caesar.....	37
Gambar 3.6 Flowchat Proses Enkripsi Vigenere.....	38
Gambar 3.7 Flowchat Proses Deskripsi Vigenere	39
Gambar 3.8 Use Case Diagram	40
Gambar 3.9 Activity Diagram Login.....	41
Gambar 3.10 Activity Diagram Kirim Pesan	42
Gambar 3.11 Activity Diagram Inbox	43
Gambar 3.12 Class Diagram	44
Gambar 3.13 Perancangan Antar Muka Tampilan Login Petugas	45
Gambar 3.14 Perancangan Antar Muka Menu Utama	45
Gambar 3.15 Perancangan Antar Muka Halaman Inbox	46
Gambar 3.16 Perancangan Antar Muka Halaman Outbox.....	46
Gambar 3.17 Perancangan Antar Muka Halaman Select User	47

Gambar 3.18 Perancangan Antar Muka Halaman Kirim Pesan	47
Gambar 4.1 <i>Login</i> Aplikasi Pesan pribadi	52
Gambar 4.2 Tampilan Notifikasi Ketika Gagal Login.....	52
Gambar 4.3 Halaman Utama	53
Gambar 4.4 Halaman Inbox	53
Gambar 4.5 Halaman Inbox Yang Menerima Pesan	54
Gambar 4.6 Pesan Yang telah di Deskripsi.....	54
Gambar 4.7 Halaman Outbox.....	55
Gambar 4.8 Halaman Outbox Sudah kirim pesan	55
Gambar 4.9 Halaman Pilih User.....	56
Gambar 4.10 Proses Kirim Pesan	56