



UNIVERSITAS
MERCU BUANA

**APLIKASI ENKRIPSI ARTIKEL MENGGUNAKAN METODE CAESAR
CIPHER BERDASARKAN PERGESERAN JAM DAN MENIT**



UNIVERSITAS
MERCU BUANA

IKA NUR CAHYA SARTIKA

41513120155

PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2016



UNIVERSITAS
MERCU BUANA

**APLIKASI ENKRIPSI ARTIKEL MENGGUNAKAN METODE CAESAR
CIPHER BERDASARKAN PERGESERAN JAM DAN MENIT**

Laporan Tugas Akhir

Diajukan Untuk Melengkapi Persyaratan
Memperoleh Gelar Sarjana Komputer

UNIVERSITAS
MERCU BUANA

IKA NUR CAHYA SARTIKA

41513120155

PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA

2016

LEMBAR PERNYATAAN

Yang bertanda tangan di bawah ini:

NIM : 41513120155
Nama : Ika Nur Cahya Sartika
Judul Skripsi : Aplikasi Enkripsi Artikel Menggunakan Metode
Caesar Cipher Berdasarkan Pergeseran Jam Dan
Menit

Menyatakan bahwa skripsi tersebut diatas adalah judul hasil karya saya sendiri dan bukan plagiat. Apabila ternyata ditemukan di dalam laporan skripsi saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Jakarta, 4 Januari 2017



Ika Nur Cahya Sartika

LEMBAR PENGESAHAN

Yang bertanda tangan di bawah ini menyatakan bahwa skripsi dari mahasiswa :

Nama Mahasiswa : Ika Nur Cahya Sartika
NIM : 41513120155
Fakultas : Ilmu Komputer
Program Studi : Teknik Informatika
Judul : Aplikasi Enkripsi Artikel Menggunakan Metode
Caesar Cipher Berdasarkan Pergeseran Jam Dan
Menit

Jakarta, 4 Januari 2017
Disetujui dan diterima oleh,



Dr. Ir. Eliyanti, M.Hum
Dosen Pembimbing

UNIVERSITAS
MERCU BUANA



Afiyati, S.Si., MT

Kaprodi Teknik Informatika



Diky Firdaus S.Kom., MM

Koordinator Tugas Akhir

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh.

Puji syukur penulis panjatkan kehadiran Allah SWT yang senantiasa memberikan ilmu, bimbingan, perlindungan dan karunia-Nya, sehingga penulis dapat menyelesaikan tugas akhir yang berjudul "Aplikasi Enkripsi Artikel Menggunakan Metode *Caesar Cipher* Berdasarkan Pergeseran Jam dan Menit". Laporan ini disusun dengan tujuan untuk memenuhi salah satu syarat kelulusan dan mendapatkan gelar kesarjanaan Strata Satu (S1) pada Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Mercubuana.

Pada kesempatan kali ini, penulis ingin mengucapkan terimakasih kepada pihak-pihak yang telah memberikan dukungan dan kesempatan dalam proses penyusunan laporan tugas akhir ini hingga selesai, yaitu kepada:

1. Keluarga penulis Bapak Buyung Ali Mutazar dan Ibu Ukar Sukarsih yang selalu mendoakan dan memberikan dukungan serta motivasi dalam setiap langkah yang dilakukan penulis.
2. Ibu Dr. Ir. Eliyani, M.Hum, selaku pembimbing tugas akhir penulis yang telah memberikan motivasi yang begitu besar, saran, dukungan serta bersedia meluangkan waktu, pikiran dan tenaga untuk membimbing penulis.
3. Yaya Sudaryana Triana, Ph.D, selaku ketua prodi Teknik Informatika dan pembimbing akademik yang telah memberikan motivasi, bimbingan dan arahan selama penulis menjalani perkuliahan.
4. Ibu Desi Ramayanti, S.Kom., M.T, selaku koordinator tugas akhir yang telah memberikan motivasi, bimbingan dan arahan selama penulis menjalani perkuliahan.
5. Bapak Muhammad Rifqi, S.Kom yang telah bersedia meluangkan waktu

untuk berdiskusi dengan penulis terkait dengan Kriptografi.

6. Dosen dan staff sekretariat prodi Teknik Informatika, yang telah membantu banyak hal dalam kegiatan perkuliahan penulis.
7. Pak Adi, Rizki Nur Ikhsan Taufik, Eka Agus Sutrisno, Agung Prasetyo, Fajar Arifin, Bruno Mukti dan Ahmad Fathoni yang telah membantu dan memberikan masukan kepada penulis dalam menyelesaikan tugas akhir.
8. Rekan satu bimbingan tugas akhir penulis Ammar, Aji, Ari, Arya, Bobby, Nida dan Qalam yang telah berjuang bersama, selalu memberikan motivasi dan mengingatkan penulis agar dapat menyelesaikan tugas akhir tepat waktu.
9. Rekan-rekan seperjuangan penulis Rahmat Soleh, Yayat Suyatna, Siti Maesaroh yang telah menyemangati, dan berjuang bersama penulis selama ini.
10. Para sahabat penulis Citra Fatmala, Rusnah Setiani, Lia Lantika, Melinda Eka Saraswati, Novida Dara Rezita, Nur Azizah, Fitri Nurul Afiah, Ragil Adithiawarman, dan Trimurti Mega Cahya Rankuti yang selalu memberikan semangat dan dorongan untuk penulis.
11. Rekan-rekan seperjuangan Informatika Mercubuana khususnya 2014 dan seluruh pihak yang telah membantu kelancaran tugas akhir yang tidak bisa penulis sebutkan satu persatu.

Semoga Allah SWT membalas semua kebaikan dan ilmu serta semangat yang telah diberikan kepada penulis. Penulis menyadari bahwa penulisan laporan ini masih terdapat kekurangan. Oleh karena itu, penulis sangat mengharapkan kritik maupun saran yang bersifat membangun dari berbagai pihak. Semoga laporan ini dapat bermanfaat bagi penulis dan pembaca.

Jakarta, 4 Januari 2017

Ika Nur Cahya Sartika

Daftar Isi

LEMBAR PERNYATAAN	I
LEMBAR PENGESAHAN	II
KATA PENGANTAR	III
ABSTRAKSI	V
ABSTRACT	VI
DAFTAR ISI	VII
DAFTAR GAMBAR	IX
DAFTAR TABEL	XI
DEFINISI	XII
BAB 1. PENDAHULUAN	1
1.1 LatarBelakang	1
1.2 RumusanPermasalahan	3
1.3 Tujuan & Manfaat Penelitian	4
1.3.1 Tujuan Penelitian	4
1.3.2 Manfaat Penelitian	4
1.4 Ruang Lingkup & Batasan Penelitian	4
1.5 Sistematika Penulisan Laporan	5
1.5.1 Pendahuluan	5
1.5.2 Landasan Teori	5
1.5.3 Analisa Sistem	5
1.5.4 Perancangan Sistem	6
1.5.5 Implementasi dan Testing	6
1.5.6 Penutup	6
BAB 2. LANDASAN TEORI	7
2.1 Pengertian Kriptografi	7
2.2 Algoritma Kriptografi	7
2.2.1 Algoritma Kunci Simetris (Symmetric Key)	8
2.2.2 Algoritma Kunci Asimetris (Asymmetric Key)	9
2.3 Istilah-istilah Kriptografi	9
2.3.1 Keamanan Data	12
2.4 Caesar cipher	16
2.5 Media Massa	20
2.6 Media Massa Online	21
2.6.1 Artikel	22
2.6.2 Kode Etik Jurnalis	24
BAB 3. ANALISA SISTEM	26
3.1 Analisa Sistem	26
3.2 Analisis Kebutuhan Sistem	28
3.3 Kebutuhan Sistem	29
3.4 Kebutuhan Perangkat Lunak Dan Perangkat Keras	29
BAB 4. PERANCANGAN	30
4.1 Perancangan Sistem	30
4.2 Langkah-langkah Penyelesaian	32
4.2.1 Proses Enkripsi	32

4.2.2 Proses Dekripsi	33
4.3 Perancangan Antarmuka	34
BAB 5. IMPLEMENTASI DAN PENGUJIAN	39
5.1 Implementasi	39
5.2 Tujuan Pengujian	40
5.2.1 Tahap Pengujian	40
5.2.2 Hasil Pengujian	41
BAB 6. PENUTUP	74
6.1 Kesimpulan	74
6.2 Saran	75
DAFTAR PUSTAKA	76
LAMPIRAN	78



UNIVERSITAS
MERCU BUANA

Daftar Gambar

Gambar 2-1 Proses Enkripsi dan Dekripsi pada Algoritma Simetris	8
Gambar 2-2 Proses Enkripsi dan Dekripsi pada Algoritma Asimetris	9
Gambar 2-3 Contoh bentuk Plaintext	10
Gambar 2-4 Contoh bentuk Ciphertext.....	10
Gambar 2-5 Proses Enkripsi dan Dekripsi.....	11
Gambar 2-6 Metode Cipher Substitusi $k=3$	16
Gambar 2-7 Algoritma ROT13	18
Gambar 2-8 Alur Pergeseran $k=13$ berdasarkan table ASCII.....	19
Gambar 2-9 Hasil Pergeseran $k=13$	19
Gambar 2-10 Urutan Karakter ASCII.....	19
Gambar 4-1 Perancangan Antarmuka Menu Utama Aplikasi Enkripsi Artikel	36
Gambar 4-2 Perancangan Antarmuka Menu Enkripsi Aplikasi Enkripsi Artikel..	37
Gambar 4-3 Perancangan Antarmuka Menu Dekripsi Aplikasi Enkripsi Artikel .	37
Gambar 4-4 Perancangan Antarmuka Menu Help Aplikasi Enkripsi Artikel	38
Gambar 5-1 Tampilan Menu Enkripsi	44
Gambar 5-2 Tampilan Menu Dekripsi	44
Gambar 5-3 Tampilan Menu Help	45
Gambar 5-4 Uji coba memasukan kata pada Menu Enkripsi.....	45
Gambar 5-5 Hasil file enkripsi dan durasi waktu untuk mengenkripsi kata.....	46
Gambar 5-6 Memasukkan nama file yang sudah terenkripsi.....	46
Gambar 5-7 Memilih direktori file yang akan disimpan	47
Gambar 5-8 Memasukkan file enkripsi ke dalam folder.....	47
Gambar 5-9 File enkripsi berhasil disimpan di direktori	48
Gambar 5-10 Merubah Files of Type di Aplikasi Enkripsi	61
Gambar 5-11 Isi file di dalam Folder	61
Gambar 5-12 Isi file dengan ekstensi .txt tampil pada Menu Enkripsi.....	62
Gambar 5-13 Menampilkan password untuk mengenkripsi file .txt.....	62
Gambar 5-14 Hasil enkripsi file .txt	63
Gambar 5-15 File .txt berhasil dienkripsi	63
Gambar 5-16 File ekstensi .docx tidak dapat dienkripsi.....	66
Gambar 5-17 File ekstensi .pdf tidak dapat dienkripsi	67
Gambar 5-18 Mengenkripsi file pada Menu Dekripsi	68
Gambar 5-19 Password pada Menu Enkripsi.....	69
Gambar 5-20 Password terenkripsi	69
Gambar 5-21 Hasil file dekripsi dan durasi waktu untuk mendekripsi kata.....	70
Gambar 5-22 Hasil file yang dienkripsi pada Menu Enkripsi	71
Gambar 5-23 Hasil file yang didekripsi pada Menu Dekripsi	71
Gambar 5-24 File enkripsi .txt berhasil didekripsi	74

Daftar Tabel

Tabel 3-1 Activity Diagram Analisa Sistem yang Sedang Berjalan Saat Ini.....	28
Tabel 4-1 Activity Diagram Pengembangan Sistem Dengan Menerapkan Aplikasi Enkripsi Artikel.....	31
Tabel 4-2 Activity Diagram Proses Enkripsi	33
Tabel 4-3 Activity Diagram Proses Dekripsi	34
Tabel 5-1 Tahap Pengujian Aplikasi Enkripsi Artikel.....	40
Tabel 5-2 Hasil Pengujian Metode Black Box	42
Tabel 5-3 Enkripsi plaintext ke dalam bentuk ciphertext	48
Tabel 5-4 Urutan Karakter Ganjil dan Genap.....	49
Tabel 5-5 Urutan Karakter ASCII.....	55
Tabel 5-6 Uji coba memasukkan file .txt.....	63
Tabel 5-7 Enkripsi Password Plaintext ke dalam bentuk Ciphertext pada Menu Dekripsi.....	69
Tabel 5-8 Dekripsi Ciphertext ke dalam bentuk Plaintext.....	71



Definisi

Istilah	Pengertian
Algoritma	Urutan atau langkah-langkah yang disusun secara logis untuk menyelesaikan masalah dengan sistematis
Algoritma Kriptografi	Langkah-langkah logis bagaimana menyembunyikan pesan dari orang yang tidak berhak mengetahui isi dari pesan yang dikirimkan
Algoritma Kunci Asimetris	Algoritma yang menggunakan kunci berbeda untuk mengenkripsi dan mendekripsi pesan
Algoritma Kunci Simetris	Algoritma yang menggunakan satu kunci untuk memproses pesan enkripsi dan dekripsi
Caesar Cipher	Metode <i>enkripsi</i> berjenis <i>cipher substitusi</i> , dimana setiap huruf pada plaintext-nya akan digantikan dengan huruf lainnya
Cipher	Fungsi matematika yang akan digunakan untuk <i>enkripsi</i> dan <i>dekripsi</i> pesan
Ciphertext	Pesan yang sudah disandikan
Confidentiality	Informasi yang dikirimkan bersifat rahasia, dan tidak semua orang memiliki wewenang untuk melihat informasi yang dikirim dan diterima.
Dekripsi	Proses pengembalian pesan yang telah disandikan agar bisa dibaca dan dimengerti oleh pihak penerima pesan
Eavesdropper	Orang yang mempunyai hasrat untuk mengetahui dan mendapatkan informasi dari pesan yang sengaja disembunyikan oleh pengirim pesan
Enkripsi	Suatu proses untuk menyamarkan makna pesan yang dikirimkan kepada pihak penerima pesan sehingga orang yang tidak berhak melihat isi pesan tersebut

	menganggap pesan tersebut tidak berarti
Integrity	Keaslian isi pesan yang disampaikan tidak mengalami perubahan hingga pesan tersebut sampai ditangan pihak penerima.
Keyspace	Kunci memiliki nilai bilangan yang sangat besar, dan besar kecilnya sebuah kunci
Kriptanalis	Orang yang menyerang metode kriptografi untuk mencari tau isi pesan yang disampaikan pihak pengirim
Kriptanalisis	Orang yang mempelajari kriptanalis
Kriptografer	Orang yang mempelajari dan menggunakan metode kriptografi sebagai salah satu cara untuk mengamankan pesan yang akan di sampaikan kepada penerima
Kriptografi	Ilmu dan seni untuk menjaga keamanan pesan ketika pesan akan dikirimkan ke suatu tempat
Kriptologi	Cabang ilmu yang mempelajari kriptografi dan kriptanalisis
Kriptologis	Orang yang mempelajari kriptologi
Message Autentication	Kepastian siapa saja entitas yang terlibat dan keaslian sumber data yang diterima
Nonrepudiation	Setiap orang yang terlibat dalam pengiriman atau penerimaan pesan tidak bisa menyangkal atas data yang sudah dikirimkan maupun data yang sudah diterima
Plaintext	Pesan asli atau pesan yang belum disandikan menjadi bentuk tulisan yang tidak bisa terbaca maknanya
Receiver	Orang yang menerima Pesan
Sender	Orang yang mengirimkan pesan