

**PERANCANGAN APLIKASI KRIPTOGRAFI MENGGUNAKAN
ALGORITMA MODIFIKASI VIGENERE CIPHER
DENGAN KEY GENERATOR**

SKRIPSI



disusun oleh

Hernu Rifwiyatmo

14.11.8370

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

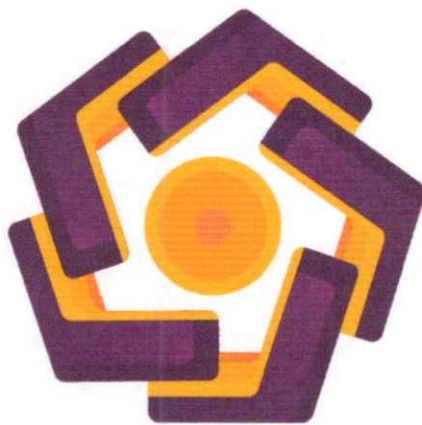
2018



**PERANCANGAN APLIKASI KRIPTOGRAFI MENGGUNAKAN
ALGORITMA MODIFIKASI VIGENERE CIPHER
DENGAN KEY GENERATOR**

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai gelar Sarjana
pada Program Studi Informatika



disusun oleh

Hernu Rifwiyatmo

14.11.8370

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2018

PERSETUJUAN

SKRIPSI

PERANCANGAN APLIKASI KRIPTOGRAFI MENGGUNAKAN ALGORITMA MODIFIKASI VIGENERE CIPHER DENGAN KEY GENERATOR

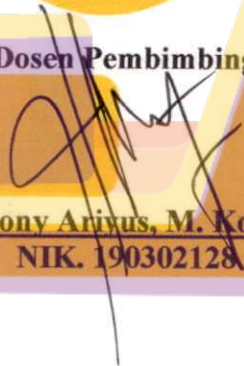
yang dipersiapkan dan disusun oleh

Hernu Rifwiyatmo

14.11.8370

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 01 Agustus 2018

Dosen Pembimbing,


Dony Ariyus, M. Kom
NIK. 190302128

PENGESAHAN

SKRIPSI

**PERANCANGAN APLIKASI KRIPTOGRAFI MENGGUNAKAN
ALGORITMA MODIFIKASI VIGENERE CIPHER
DENGAN KEY GENERATOR**

yang dipersiapkan dan disusun oleh

Hernu Rifwiyatmo

14.11.8370

telah dipertahankan di depan Dewan Penguji
pada tanggal 20 September 2018

Susunan Dewan Penguji

Nama Penguji

Dony Ariyus, M.Kom
NIK. 190302128

Bayu Setiaji, M.Kom
NIK. 190302216

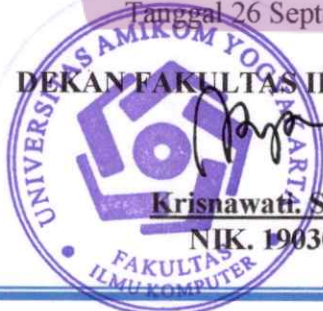
Ali Mustopa, M.Kom
NIK. 190302192

Tanda Tangan



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 26 September 2018

DEKAN FAKULTAS ILMU KOMPUTER



Krisnawati, S.Si, M.T.
NIK. 190302038

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

Yogyakarta, 26 September 2018



Hernu Rifwiyatmo
NIM. 14.11.8370

MOTTO

“Hidup adalah seni menggambar tanpa penghapus” -**John W. Gardne**

“Jangan percaya orang yang sering tersenyum. Mereka mungkin sedang menjual
sesuatu” -**Laurell K. Hamilton**

“Kesuksesan tak pernah dimiliki. Ia disewakan dan itu dibayar tiap hari” -**Rory
Vaden**

“Jika kau tak suka sesuatu, ubahlah. Jika tak bisa, maka ubahlah cara pandangmu
tentangnya” -**Maya Angelou**

PERSEMBAHAN

Syukur alhamdulillah atas kehadiran Allah SWT yang telah memberikan rahmat dan karunia-Nya sehingga karya ini dapat terselesaikan dengan baik dan lancar. Skripsi ini saya persembahkan kepada :

1. Kedua orang tua tercinta, motivator terbesar dalam hidup yang tak pernah jemu mendo'akan dan menyayangi, atas semua pengorbanan dan kesabaran hingga saat ini.
2. Bapak Suyanto sebagai rektor UNIVERSITAS AMIKOM YOGYAKARTA.
3. Bapak Dony Ariyus selaku dosen pembimbing yang tidak pernah berhenti dalam membimbing dan memotivasi saya untuk menyelesaikan skripsi ini dengan baik .
4. Teman kelas seperjuangan 14-SITI-13 yang selalu menyertai dalam menimba ilmu.
5. Semua yang telah membantu serta mendoakan untuk kelancaran dan kemudahan menyelesaikan skripsi ini.

KATA PENGANTAR

Puji syukur Alhamdulillah penyusun panjatkan kehadiran Allah SWT karena berkat rahmat dan karunia-Nya penulis dapat menyelesaikan penyusunan skripsi ini. Shalawat dan salam semoga senantiasa tercurahkan kepada nabi Muhammad SAW, kepada keluarga, para sahabat, dan kita selaku umatnya hingga akhir zaman, amiin..

Penulisan ini diajukan untuk memenuhi salah satu syarat untuk memperoleh gelar sarjana pada Program Studi Informatika, Universitas AMIKOM Yogyakarta yang penulis ajukan dengan judul “Perancangan Aplikasi Kriptografi Menggunakan Algoritma Modifikasi Vigenere Cipher Dengan Key Generator”.

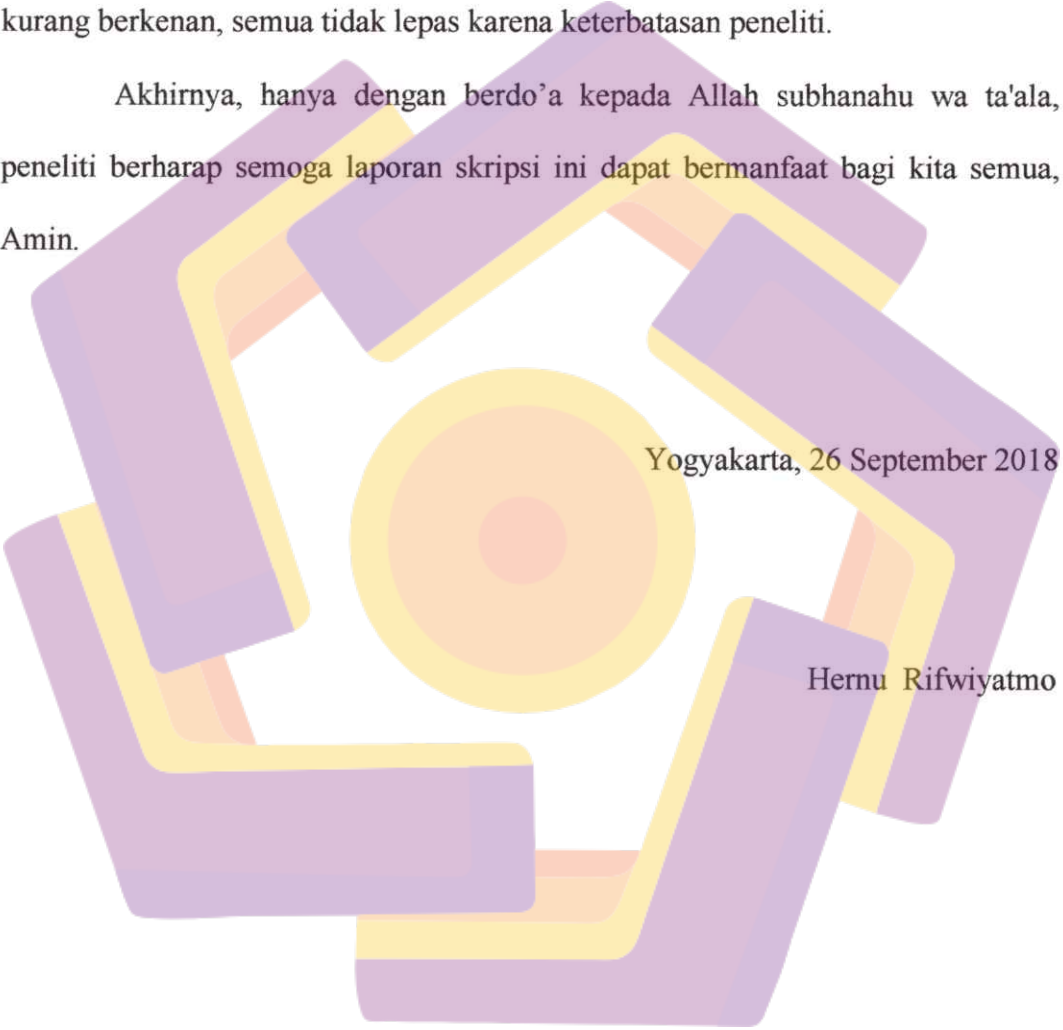
Penulis menyadari masih banyak kekurangan dalam penyusunan skripsi ini dan masih jauh dari sempurna. Dengan selesainya skripsi ini penulis ingin mengucapkan banyak terimakasih kepada :

1. Bapak Prof. Dr. M. Suyanto, MM. selaku Rektor Universitas AMIKOM Yogyakarta.
2. Ibu Krisnawati, S.Si, M.T. Selaku Dekan Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta.
3. Bapak Dony Ariyus, M.Kom selaku Dosen Pembimbing yang telah memberikan banyak bantuan, masukan dan bimbingan dalam menyelesaikan skripsi.
4. Bapak Bayu Setiaji, M.Kom. dan Bapak Ali Mustopa, M.Kom. selaku dosen penguji.

5. Keluarga dan rekan-rekan yang telah memberi dukungan dan bantuan untuk kelancaran skripsi.

Peneliti juga memohon maaf kepada semua pihak jika dalam pelaksanaan penelitian dan penulisan laporan skripsi ini terdapat kesalahan atau hal yang kurang berkenan, semua tidak lepas karena keterbatasan peneliti.

Akhirnya, hanya dengan berdo'a kepada Allah subhanahu wa ta'ala, peneliti berharap semoga laporan skripsi ini dapat bermanfaat bagi kita semua, Amin.



Yogyakarta, 26 September 2018

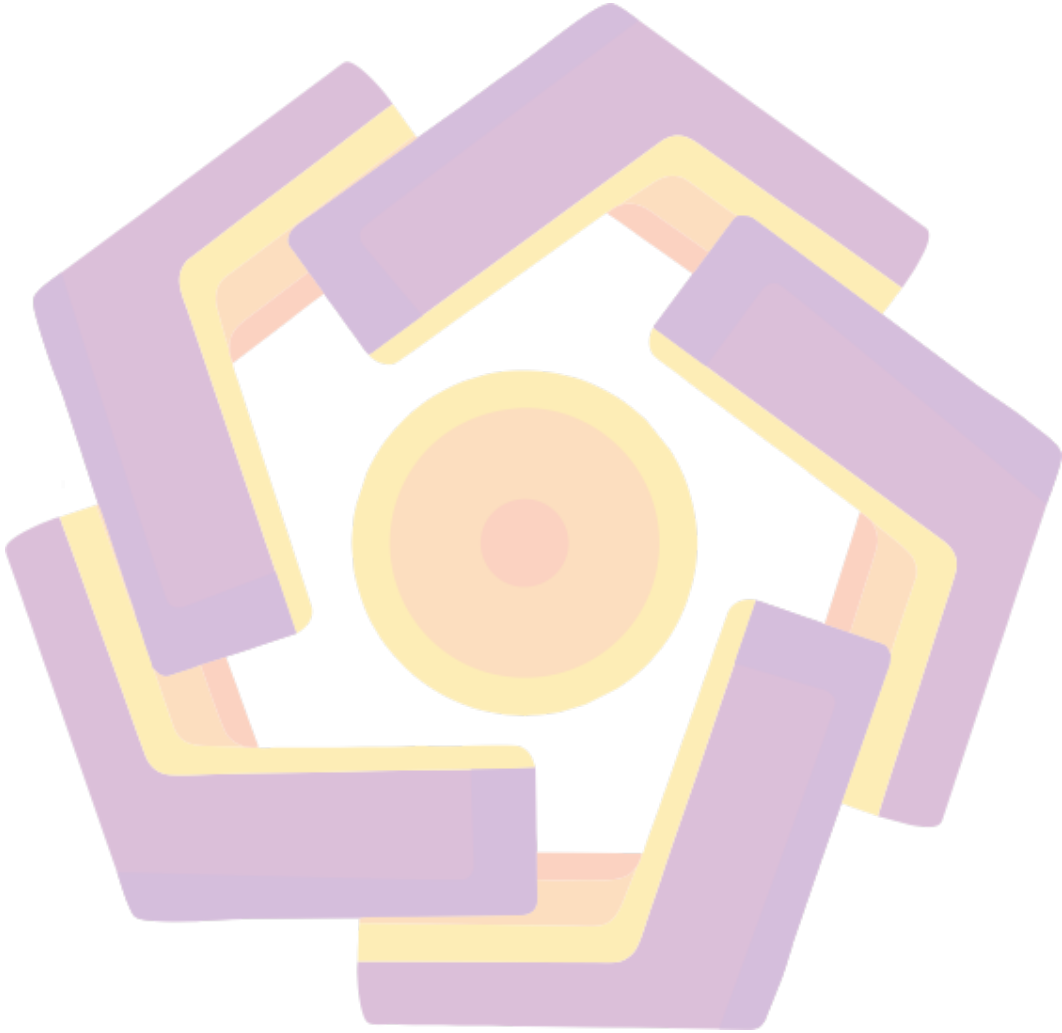
Hernu Rifwiyatmo

DAFTAR ISI

| | |
|---|------|
| JUDUL | i |
| PERSETUJUAN | ii |
| PENGESAHAN | iii |
| PERNYATAAN | iv |
| MOTTO | v |
| PERSEMBAHAN | vi |
| KATA PENGANTAR | vii |
| DAFTAR ISI | ix |
| DAFTAR TABEL | xii |
| DAFTAR GAMBAR | xiii |
| BAB I PENDAHULUAN | 1 |
| 1.1 Latar Belakang | 1 |
| 1.2 Rumusan Masalah | 2 |
| 1.3 Batasan Masalah | 2 |
| 1.4 Maksud dan Tujuan Penelitian | 3 |
| 1.5 Manfaat Penelitian | 3 |
| 1.6 Metode Penelitian | 3 |
| 1.7 Sistematika Penulisan | 4 |
| BAB II LANDASAN TEORI | 6 |
| 2.1 Tinjauan Pustaka | 6 |
| 2.2 Konsep Dasar Kriptografi | 6 |
| 2.3 Algoritma Kriptografi | 9 |
| 2.4 Vigenere Cipher | 10 |
| 2.5 Metode Kasiski | 11 |
| 2.6 Perangkat Lunak Yang Digunakan | 11 |
| 2.7 Bahasa C# | 12 |
| 2.8 Bagan Alur (Flowchart) | 12 |
| 2.9 UML (Unified Modeling Language) | 14 |

| | |
|--|----|
| BAB III ANALISIS DAN PERANCANGAN | 21 |
| 3.1 Tinjauan Umum Aplikasi..... | 21 |
| 3.2 Analisis Sistem..... | 22 |
| 3.2.1 Identifikasi Masalah..... | 22 |
| 3.2.2 Analisis SWOT | 23 |
| 3.2.3 Analisis Kebutuhan..... | 24 |
| 3.3 Perancangan Algoritma..... | 26 |
| 3.3.1 Urutan Indeks Huruf dan Angka..... | 26 |
| 3.3.2 Proses Pembentukan Kunci..... | 26 |
| 3.3.3 Proses Enkripsi..... | 28 |
| 3.3.4 Proses Dekripsi | 29 |
| 3.4 Perancangan Sistem..... | 30 |
| 3.4.1 Flowchart | 30 |
| 3.4.2 UML (Unified Modeling Language) | 31 |
| 3.4.2.1 Use Case Diagram..... | 31 |
| 3.4.2.2 Activity Diagram | 32 |
| 3.4.2.3 Sequence Diagram | 33 |
| 3.4.3 User Interface..... | 35 |
| BAB IV IMPLEMENTASI DAN PEMBAHASAN | 37 |
| 4.1 Implementasi dan Pembahasan..... | 37 |
| 4.1.1 Halaman Enkripsi..... | 37 |
| 4.1.2 Halaman Dekripsi | 38 |
| 4.1.3 Halaman Bantuan..... | 39 |
| 4.1.4 Halaman Tentang | 40 |
| 4.2 Pengujian Aplikasi | 41 |
| 4.2.1 Blackbox Testing | 41 |
| 4.2.2 Whitebox Testing..... | 46 |
| 4.2.3 Pengujian Menggunakan Metode Kasiski | 47 |
| BAB V PENUTUP | 52 |
| 5.1 Kesimpulan | 52 |
| 5.2 Saran | 52 |

DAFTAR PUSTAKA 54
LAMPIRAN..... 56



DAFTAR TABEL

| | |
|---|----|
| Tabel 2.1 Simbol Diagram Use Case..... | 15 |
| Tabel 2.2 Simbol Diagram Aktifitas..... | 17 |
| Tabel 2.3 Simbol Diagram Sekuen..... | 18 |
| Tabel 3.1 Analisis SWOT..... | 23 |
| Tabel 3.2 Indeks Huruf dan Angka..... | 26 |
| Tabel 3.3 Pembentukan Kunci..... | 27 |
| Tabel 3.4 Contoh Plainteks..... | 28 |
| Tabel 3.5 Hasil Key Generator untuk Enkripsi..... | 28 |
| Tabel 3.6 Hasil Enkripsi..... | 29 |
| Tabel 3.7 Contoh Cipherteks..... | 29 |
| Tabel 3.8 Hasil Key Generator untuk Dekripsi..... | 29 |
| Tabel 3.9 Hasil Dekripsi..... | 30 |
| Tabel 4.1 Testing Halaman Enkripsi..... | 42 |
| Tabel 4.2 Testing Halaman Dekripsi..... | 42 |
| Tabel 4.3 Testing Halaman Bantuan..... | 43 |
| Tabel 4.4 Testing Halaman tentang..... | 43 |

DAFTAR GAMBAR

| | |
|--|----|
| Gambar 2.1 Contoh Enkripsi Menggunakan Vigenere Cipher | 10 |
| Gambar 3.1 Flowchart Proses Enkripsi | 30 |
| Gambar 3.2 Flowchart Proses Dekripsi | 31 |
| Gambar 3.3 Use Case Diagram..... | 32 |
| Gambar 3.4 Activity Diagram Enkripsi..... | 32 |
| Gambar 3.5 Activity Diagram Dekripsi..... | 33 |
| Gambar 3.6 Sequence Diagram Enkripsi..... | 34 |
| Gambar 3.7 Sequence Diagram Dekripsi..... | 34 |
| Gambar 3.8 Rancangan Halaman Enkripsi..... | 35 |
| Gambar 3.9 Rancangan Halaman Dekripsi..... | 35 |
| Gambar 3.10 Rancangan Halaman Bantuan | 36 |
| Gambar 3.11 Rancangan Halaman Tentang | 36 |
| Gambar 4.1 Implementasi Halaman Enkripsi..... | 38 |
| Gambar 4.2 Implementasi Halaman Dekripsi..... | 39 |
| Gambar 4.3 Implementasi Halaman Bantuan | 40 |
| Gambar 4.4 Implementasi Halaman Tentang | 41 |
| Gambar 4.5 Testing Karakter..... | 45 |
| Gambar 4.6 Whitebox Testing..... | 46 |

INTISARI

Sangat pentingnya sebuah nilai informasi menyebabkan seringkali informasi hanya boleh diakses oleh orang-orang tertentu saja. Jatuhnya informasi ke tangan pihak lain dapat menimbulkan kerugian bagi pemilik informasi. Untuk mengatasi permasalahan tersebut diperlukan suatu pengamanan, salah satunya menggunakan kriptografi.

Pada skripsi ini berisi perancangan aplikasi kriptografi pada komputer yang bisa digunakan untuk enkripsi dan dekripsi pesan teks. Algoritma kriptografi yang digunakan adalah modifikasi vigenere cipher dengan key generator. Apabila panjang kunci yang dimasukkan oleh user kurang dari panjang plain teks maka kunci baru akan dibangkitkan secara acak. Hal tersebut bertujuan untuk mengatasi kelemahan dari algoritma vigenere cipher yang mana kata kunci nya selalu diulang – ulang.

Aplikasi yang dihasilkan berbasis desktop dengan bahasa C#. Cara kerja aplikasi ini adalah dengan meminta user untuk memasukkan sebuah pesan yang akan dienkripsi atau didekripsi beserta kata kunci yang digunakan untuk pengamanan pada tempat yang tersedia, kemudian hasilnya akan langsung ditampilkan.

Kata Kunci: enkripsi, dekripsi, vigenere cipher, kunci

ABSTRACT

The very importance of an information value often causes information to be accessed only by certain people. The fall of information into the hands of others can cause harm to the owner of the information. To overcome these problems, a security is needed, one of which uses cryptography.

This thesis contains the design of cryptographic applications on a computer that can be used for encryption and decryption of text messages. The cryptographic algorithm used is a modified vigenere cipher with a key generator. If the length of the key entered by the user is less than the plain length of the text, the new key will be generated randomly. It aims to overcome the weaknesses of the vigenere cipher algorithm where the keywords are always repeated.

The application created is a desktop-based application with the C # language. The way this application works is by asking the user to enter a message that will be encrypted or decrypted along with the keywords that are used for security in the available places, then the results will be immediately displayed.

Keywords: encryption, decryption, vigenere cipher, key

