

**MODIFIKASI HILL CIPHER DENGAN VIGENERE CIPHER  
TERMODIFIKASI UNTUK ENKRIPSI FILE DOKUMEN**

**SKRIPSI**

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana  
Program Studi Teknik Komputer



disusun oleh

**BERTHA ANJANI MAYLINIA**

**18.83.0174**

**FAKULTAS ILMU KOMPUTER  
UNIVERSITAS AMIKOM YOGYAKARTA  
YOGYAKARTA**

**2022**

**MODIFIKASI HILL CIPHER DENGAN VIGENERE CIPHER  
TERMODIFIKASI UNTUK ENKRIPSI FILE DOKUMEN**

**SKRIPSI**

untuk memenuhi salah satu syarat mencapai derajat Sarjana  
Program Studi Teknik Komputer



disusun oleh

**BERTHA ANJANI MAYLINIA**

**18.83.0174**

**FAKULTAS ILMU KOMPUTER  
UNIVERSITAS AMIKOM YOGYAKARTA  
YOGYAKARTA**

**2022**

**HALAMAN PERSETUJUAN**

**SKRIPSI**

**MODIFIKASI HILL CIPHER DENGAN VIGENERE CIPHER TERMODIFIKASI  
UNTUK ENKRIPSI FILE DOKUMEN**

yang disusun dan diajukan oleh

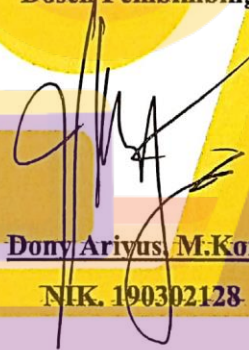
**Bertha Anjani Maylinia**

**18.83.0174**

telah disetujui oleh Dosen Pembimbing Skripsi

pada tanggal 27 Agustus 2022

**Dosen Pembimbing,**



**Dony Ariyus, M.Kom.**

**NIK. 190302128**

**HALAMAN PENGESAHAN**

**SKRIPSI**

**MODIFIKASI HILL CIPHER DEGAN VIGENERE CIPHER TERMODIFIKASI  
UNTUK ENKRIPSI FILE DOKUMEN**

yang disusun dan diajukan oleh

**Bertha Anjani Maylinia**

**18.83.0174**

Telah dipertahankan di depan Dewan Penguji  
pada tanggal 27 Agustus 2022

**Susunan Dewan Penguji**

**Nama Penguji**

**Tanda Tangan**

**Banu Santoso, S.T., M.Eng.**

**NIK. 190302327**

**Rini Indrayanti, S.T., M.Eng.**

**NIK. 190302417**

**Dony Ariyus, M. Kom.**

**NIK. 190302128**



Skripsi ini telah diterima sebagai salah satu persyaratan  
untuk memperoleh gelar Sarjana Komputer  
Tanggal 27 Agustus 2022

**DEKAN FAKULTAS ILMU KOMPUTER**



**Hanif Al Fatta, S.Kom., M.Kom.**

**NIK. 190302096**

## HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

**Nama mahasiswa : Bertha Anjani Maylinia**  
**NIM : 18.83.0174**

Menyatakan bahwa Skripsi dengan judul berikut:

### **Modifikasi Hill Cipher dengan Vigenere Cipher Termodifikasi untuk Enkripsi File Dokumen**

Dosen Pembimbing : Dony Ariyus, M.Kom.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 27 Agustus 2022

Yang Menyatakan,



Bertha Anjani Maylinia

## KATA PENGANTAR

Puji dan syukur kehadirat Tuhan Yang Maha Esa atas segala nikmat dan karunia-Nya. Penulis dapat menyelesaikan skripsi ini tentu dengan pertolongan dan kebaikan Tuhan untuk memenuhi persyaratan akademis guna memperoleh gelar Sarjana Strata Satu (S1) Teknik Komputer pada Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.

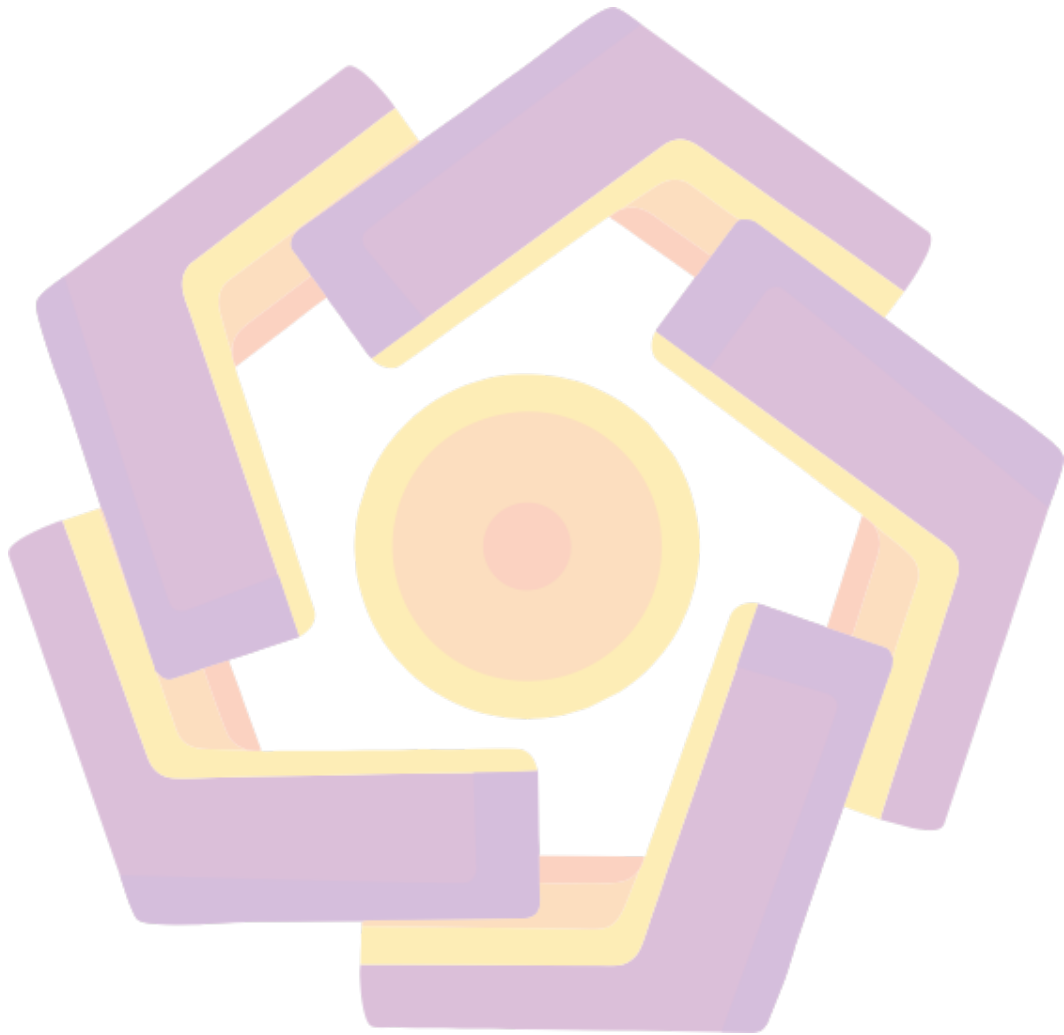
Penulis menyadari dalam proses penyusunan skripsi, bahwa pertolongan Tuhan telah tersalurkan melalui banyak pihak dan berbagai macam jalan agar terlaksana dengan tepat. Oleh karena itu, penulis sampaikan rasa terima kasih kepada :

1. Bapak Prof. Dr. Suyanto, MM., selaku Rektor Universitas Amikom Yogyakarta yang telah memberi kesempatan dapat menempuh pendidikan S1 Teknik Komputer.
2. Bapak Hanif Al Fatta, S.Kom, M.Kom., selaku Dekan Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.
3. Bapak Dony Ariyus, M.Kom., selaku Ketua Program Studi Teknik Komputer Universitas Amikom Yogyakarta dan sebagai dosen pembimbing yang telah memberi dukungan, arahan serta saran sehingga penulis dapat segera menyelesaikan dengan tuntas.
4. Para Dosen Fakultas Ilmu Komputer, yang telah mendidik, membekali penulis serta berbagi ilmu selama menempuh pendidikan di Universitas Amikom Yogyakarta.
5. Orang tua, yang tiada henti memberi dukungan dan cinta nya.
6. Leony Novita, Christine Constanta, Nabilla Fatmah, Yerri Bonyu Canno serta teman angkatan 18 Program Studi Teknik Komputer, untuk dukungan tenaga dan waktu nya.

Dalam penulisan skripsi tentu belum sempurna dan adanya kekurangan. Oleh karena itu, kritik dan saran yang membangun yang akan menyempurnakan skripsi dan kedepannya akan menghasilkan gagasan dari pembaca lain.

Yogyakarta, 8 Agustus 2022

Penulis

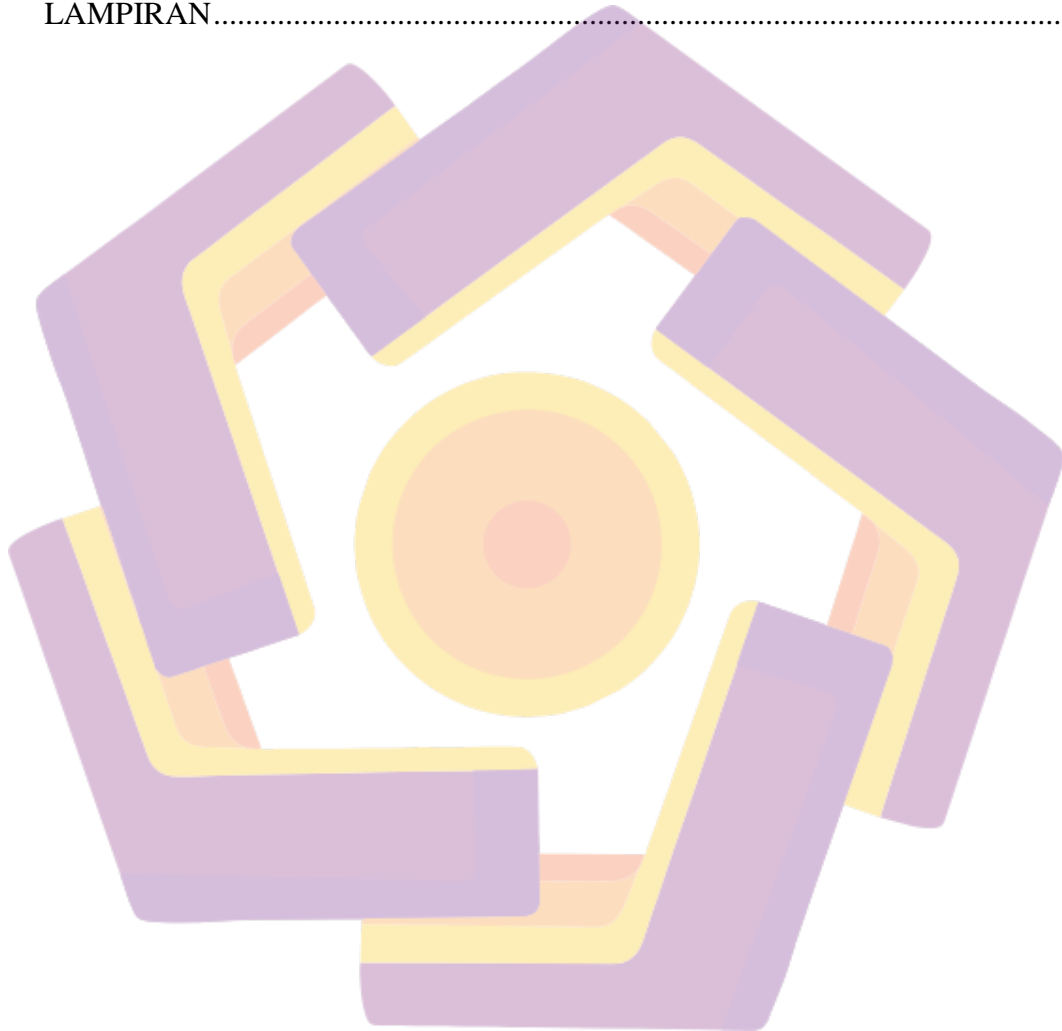


## DAFTAR ISI

HALAMAN JUDUL .....	i
HALAMAN PERSETUJUAN.....	ii
HALAMAN PENGESAHAN .....	iii
HALAMAN PERNYATAAN KEASLIAN SKRIPSI .....	iv
KATA PENGANTAR .....	v
DAFTAR ISI.....	vii
DAFTAR TABEL.....	ix
DAFTAR GAMBAR .....	x
DAFTAR LAMPIRAN.....	xi
INTISARI .....	xii
ABSTRACT.....	xiii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang .....	1
1.2 Rumusan Masalah.....	2
1.3 Batasan Masalah .....	2
1.4 Tujuan Penelitian .....	3
1.5 Manfaat Penelitian .....	3
1.6 Sistematika Penulisan .....	3
BAB II TINJAUAN PUSTAKA .....	5
2.1 Studi Literatur .....	5
2.2 Dasar Teori .....	9
2.2.1 Kriptografi .....	9
2.2.2 Pesan, Plainteks, dan Cipherteks .....	12
2.2.3 <i>Black Box Testing</i> .....	12
2.2.4 Python .....	13
2.2.5 Pengirim dan Penerima.....	13
2.2.6 Enkripsi dan Deskripsi.....	14
2.2.7 Algoritma Hill Cipher.....	14
2.2.8 Algoritma Vigenere Cipher .....	15
BAB III METODE PENELITIAN .....	19
3.1 Alat dan Bahan.....	19
3.2 Alur Penelitian .....	20
3.3 Rancangan Program.....	21
BAB IV HASIL DAN PEMBAHASAN .....	25

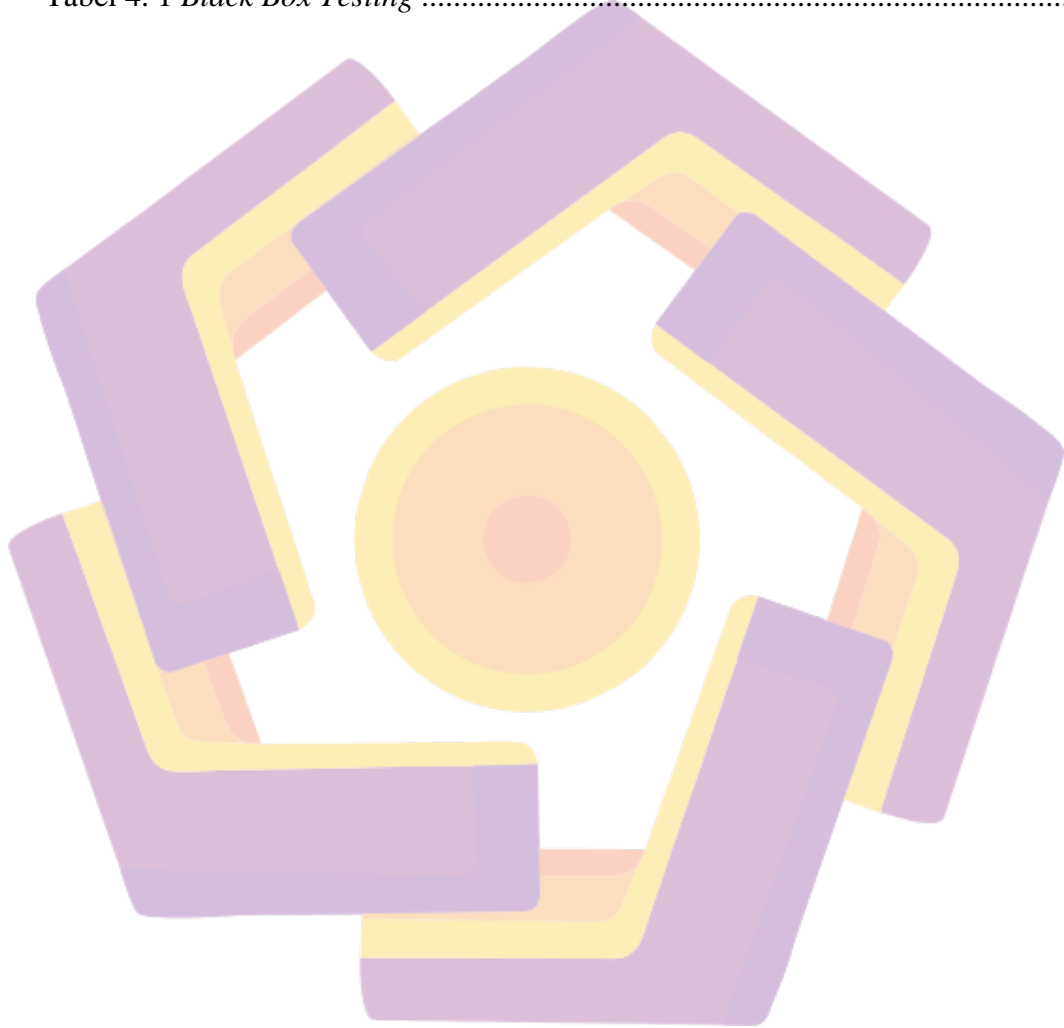


4.1 Implementasi.....	25
4.2 Pengujian .....	30
4.3 <i>Black Box Testing</i> .....	32
BAB V PENUTUP .....	34
5.1 Kesimpulan .....	34
5.2 Saran .....	34
REFERENSI .....	35
LAMPIRAN.....	37



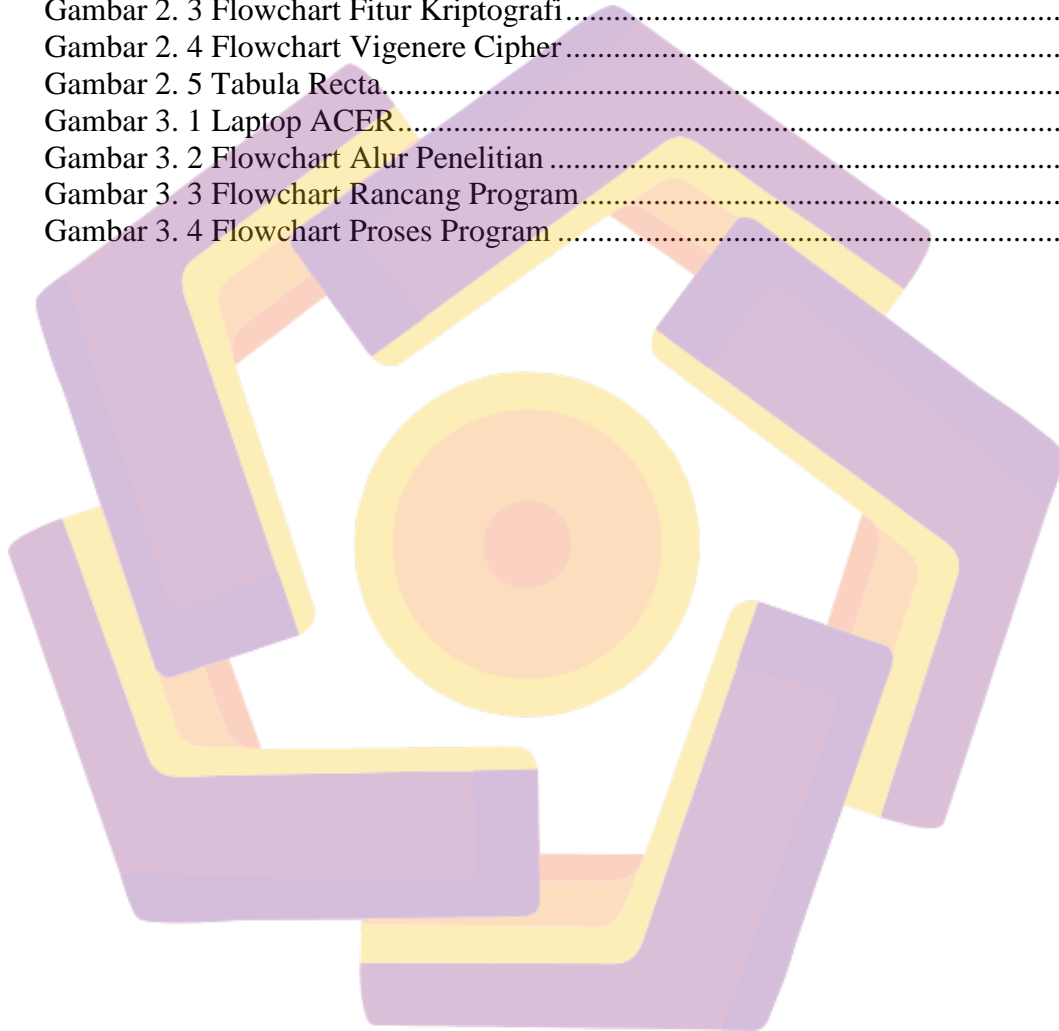
## DAFTAR TABEL

Tabel 2. 1 Referensi Penelitian Terdahulu.....	7
Tabel 2. 2 Hill Cipher .....	14
Tabel 4. 1 <i>Black Box Testing</i> .....	33



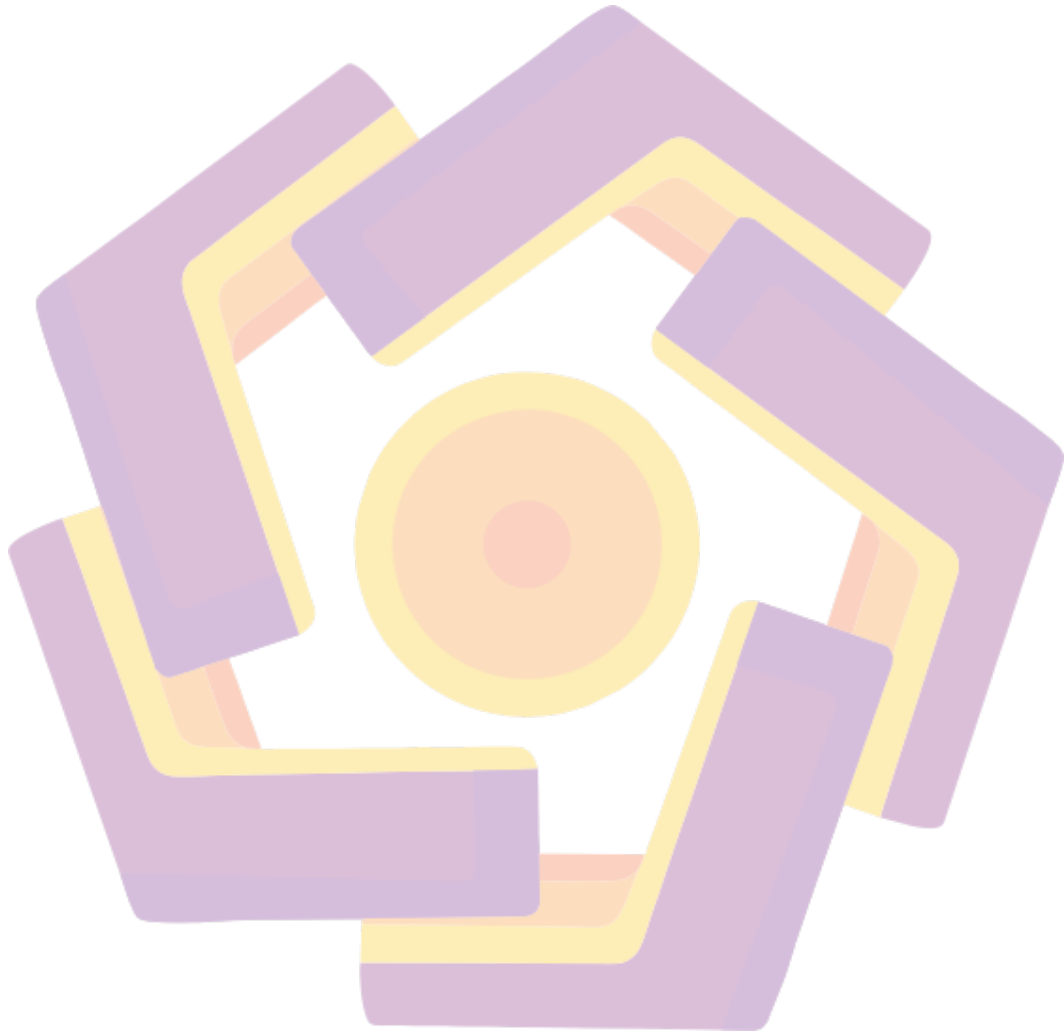
## DAFTAR GAMBAR

Gambar 2. 1 Flowchart Algoritma Simetris.....	9
Gambar 2. 2 Flowchart Asimetris.....	10
Gambar 2. 3 Flowchart Fitur Kriptografi.....	11
Gambar 2. 4 Flowchart Vigenere Cipher.....	16
Gambar 2. 5 Tabula Recta.....	16
Gambar 3. 1 Laptop ACER.....	19
Gambar 3. 2 Flowchart Alur Penelitian.....	20
Gambar 3. 3 Flowchart Rancang Program.....	21
Gambar 3. 4 Flowchart Proses Program.....	24



## DAFTAR LAMPIRAN

Lampiran 1. 1 Vigenere Cipher.....	38
Lampiran 2. 1 Hill Cipher dan Vigenere Cipher.....	38



## INTISARI

Dahulu penggunaan kriptografi hanya eksklusif di lingkungan militer saja, tetapi dengan perkembangan jaman dan hadirnya tim riset untuk kebutuhan akademis maka sekarang dikembangkan dan menjadi dasar sebuah sistem keamanan data pada komputasi dan terutama jaringan komputer termasuk internet. Sekarang berkembang dengan menghadirkan berbagai macam algoritma. Dengan begitu tentu mempunyai kelebihan serta kekurangan pada setiap algoritma tersebut. Salah satu permasalahannya ialah mudah dilacak atau tanpa adanya kunci dalam proses enkripsi dan deskripsi pesannya. Dalam dunia kriptografi terdapat dua jaman berupa algoritma klasik dan algoritma modern. Yang pada algoritma klasik hanya menggunakan metode substitusi dan mutasi, dan sekarang algoritma modern yang dapat dimengerti oleh sistem komputasi dengan angka 0 dan 1 disebut dengan biner.

Untuk menjunjung keamanan sistem lebih ketat pada pesan atau informasi, maka dibutuhkan kombinasi serta modifikasi. Dalam penelitian berikut menggunakan metode penggabungan dua algoritma simetris yaitu Hill Cipher dan Vigenere Cipher yang di dalamnya terdapat perhitungan matriks dan tentunya menggunakan kunci sebagai tambahan pengamanan dalam pengiriman pesan ke tujuan. Ketika menjalankan program, melalui tahap menambahkan pesan asli dengan format .txt (dokumen) beserta kunci yang hanya diketahui kedua belah pihak saja. Kemudian akan disetujui, dengan menampilkan hasil enkripsi (pesan rahasia) berupa format .txt juga.

Dalam prosesnya, program berikut menggunakan table ASCII untuk hasil enkripsi dan deskripsi. Hasil akhir dalam modifikasi ini berupa file teks dengan format txt. Dan di dukung untuk di uji kembali dengan metode *Black Box Testing* yang merupakan pengujian program dari segi fungsional. Dalam kasus ini, ditujukan untuk mengetahui apakah hasil dari program yang dibuat sesuai dengan tujuan penulis. Pada pembuktiannya melalui metode *Black Box Testing*, untuk input plainteks dan kunci enkripsi serta deskripsi berhasil 100%. Tetapi tidak dengan hasil enkripsi pada perhitungan manual dan pada program yang dirancang, mencapai 80% keberhasilan.

**Kata kunci:** Modifikasi, Hill Cipher, Vigenere Cipher, *Black Box Testing*

## ABSTRACT

*In the past, the use of cryptography was exclusively in the military environment, but with the times and the presence of research for academic needs, it is now developed and becomes a basic system of data security in computing and especially computer networks including the internet. Now growing by presenting various kinds of yahoo. Thus, of course, each algorithm has advantages and disadvantages. One of the problems is that it is easy to track or without a key in the description and description of the message. In the world of cryptography, there are two eras in the form of classical algorithms and modern algorithms. Which in the classical algorithm only uses substitution and mutation methods, and now modern algorithms that can be facilitated by computing systems with numbers 0 and 1 are called binary.*

*To uphold system security more stringently on messages or information, combinations and modifications are needed. In the following research using the method of combining two symmetrical algorithms namely Hill Cipher and Vigenere Cipher in which there is a matrix calculation and of course using a key as an additional security in sending messages to the destination. When running the program, it goes through the stages of adding the original message in .txt format (document) along with a key known only to both parties. Then it will be approved, by displaying the result of encryption (secret message) in .txt format as well.*

*In the process, the following program uses the ASCII table for encryption and description results. The final result in this modification is a text file with txt format. And it is supported to be tested again with the Black Box Testing method which is a program testing from a functional point of view. In this case, it is intended to find out whether the results of the program made are in accordance with the author's goals. In proving it through the Black Box Testing method, for input of plain text and encryption keys and descriptions it is 100% successful. But not with the results of encryption on manual calculations and on designed programs, achieving 80% success.*

**Keyword:** *Modification, Hill Cipher, Vigenere Cipher, Black Box Testing*