

**IMPLEMENTASI KRIPTOGRAFI PADA FILE PHOTO DAN VIDEO  
DENGAN MENGGUNAKAN ALGORITMA AES DAN  
MODIFIKASI CAESAR CIPHER PADA  
PRIVATE KOMPUTER**

**SKRIPSI**



disusun oleh

**Febrianto Ramadhan**

**14.11.8199**

**PROGRAM SARJANA  
PROGRAM STUDI INFORMATIKA  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS AMIKOM YOGYAKARTA  
YOGYAKARTA  
2018**

**IMPLEMENTASI KRIPTOGRAFI PADA FILE PHOTO DAN VIDEO  
DENGAN MENGGUNAKAN ALGORITMA AES DAN  
MODIFIKASI CAESAR CIPHER PADA  
PRIVATE KOMPUTER**

**SKRIPSI**

untuk memenuhi sebagian persyaratan  
mencapai gelar Sarjana  
pada Program Studi Informatika



disusun oleh

**Febrianto Ramadhan**

**14.11.8199**

**PROGRAM SARJANA  
PROGRAM STUDI INFORMATIKA  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS AMIKOM YOGYAKARTA  
YOGYAKARTA  
2018**

**PERSETUJUAN**

**SKRIPSI**

**IMPLEMENTASI KRIPTOGRAFI PADA FILE PHOTO DAN VIDEO  
DENGAN MENGGUNAKAN ALGORITMA AES DAN  
MODIFIKASI CAESAR CIPHER PADA  
PRIVATE KOMPUTER**

yang dipersiapkan dan disusun oleh

**Febrianto Ramadhan**

**14.11.8199**

telah disetujui oleh Dosen Pembimbing Skripsi  
pada tanggal 09 April 2018

**Dosen Pembimbing,**



**Dony Arivus, M. Kom**  
**NIK. 190302128**

**PENGESAHAN**

**SKRIPSI**

**IMPLEMENTASI KRIPTOGRAFI PADA FILE PHOTO DAN VIDEO  
DENGAN MENGGUNAKAN ALGORITMA AES DAN  
MODIFIKASI CAESAR CIPHER PADA  
PRIVATE KOMPUTER**

yang dipersiapkan dan disusun oleh

**Febrianto Ramadhan**

**14.11.8199**

telah dipertahankan di depan Dewan Penguji  
pada tanggal 24 April 2018

**Susunan Dewan Penguji**

**Nama Penguji**

Erni Seniwati, M.Cs  
NIK. 190302231

Bety Wulan Sari, M.Kom  
NIK. 190302254

Dony Ariyus, M.Kom  
NIK. 190302128

**Tanda Tangan**



Skripsi ini telah diterima sebagai salah satu persyaratan  
untuk memperoleh gelar Sarjana Komputer  
Tanggal 24 April 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 tanggung jawab saya pribadi.

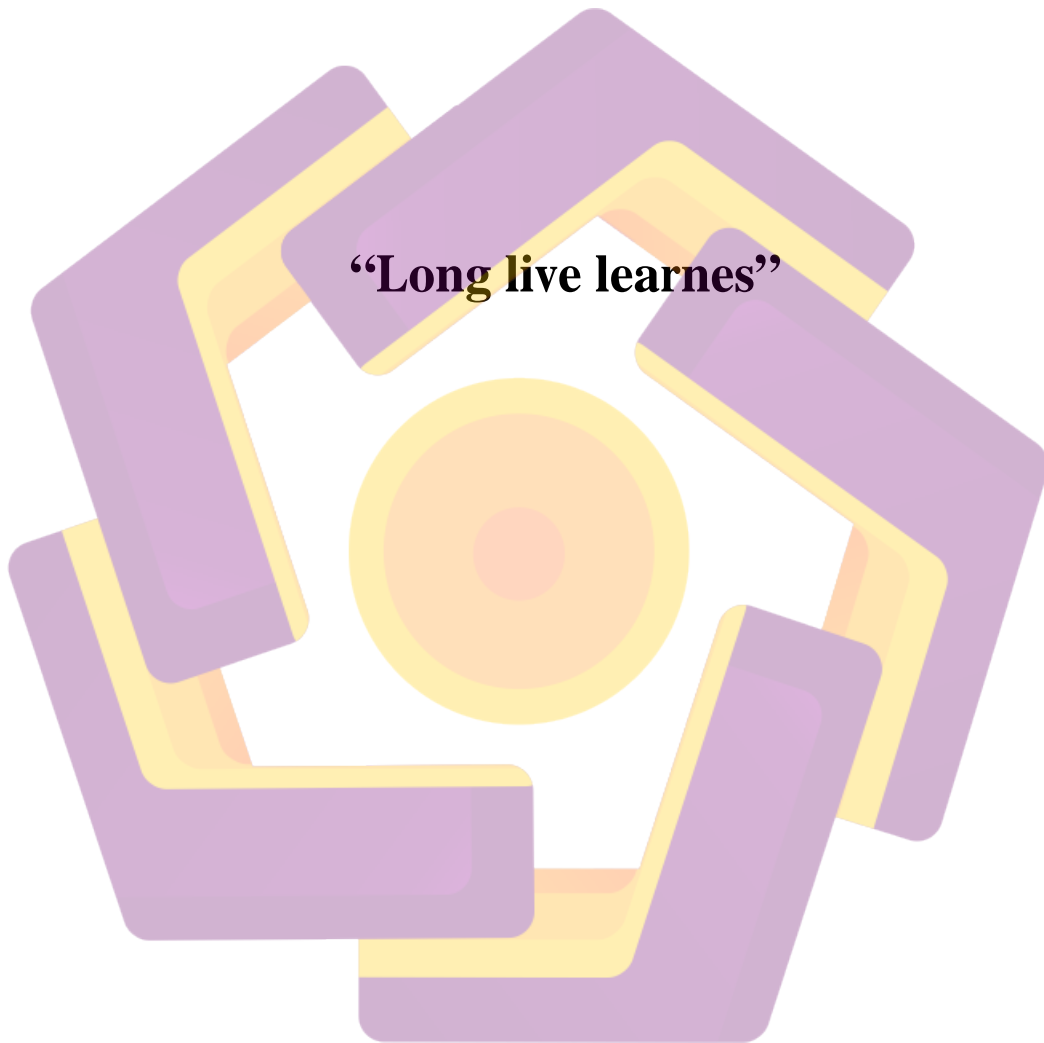
Yogyakarta, 7 Mei 2018



Febrianto Ramadhan

Nim 14.11.8199

**MOTTO**



## PERSEMBAHAN

Skripsi ini penulis persembahkan kepada:

1. Allah SWT yang telah memberikan rahmat dan hidayahnya kepada penulis, sehingga penulis selalu diberikan kesehatan, kelancaran, dan kemudahan dalam setiap usaha yang penulis lakukan.
2. Kepada bapak dan ibu penulis yang tercinta, terima kasih atau kasih sayang dan kesabaran untuk selalu menjaga dan membimbing penulis untuk menjadi lebih baik. Semoga Allah selalu memberikan yang terbaik kepada bapak dan ibu. Sehat selalu bapak dan ibu.
3. Terima kasih untuk kakakku tercinta, semoga Allah selalu memudahkan jalanmu meraih cita – cita, sehat selalu, dan tetap semangat.
4. Bapak Dony Ariyus, M.Kom selaku dosen pembimbing yang selalu memberikan masukan – masukan baik kepada penulis serta terima kasih untuk beliau yang selalu menyempatkan waktu untuk penulis.
5. Seluruh dosen Universitas AMIKOM yang sudah mendidik penulis hingga saat ini.
6. Keluarga besar kelas 14-S1 TI-10 yang telah berbagi banyak pengalaman, membuat penulis mendapat banyak pelajaran, pengalaman, dan teman yang berharga.
7. Serta seluruh pihak yang tidak bisa disebutkan satu persatu yang telah memberikan dukungan secara langsung ataupun tidak langsung.

## KATA PENGANTAR

Puji syukur penulis panjatkan atas kehadiran Allah SWT yang telah memberikan rahmat-Nya, sehingga penulis dapat menyelesaikan skripsi ini dengan judul “Implementasi Kriptografi Pada File Photo Dan Video Dengan Menggunakan Algoritma AES Dan Modifikasi Caesar Cipher Pada Private Komputer”.

Penulisan skripsi ini dimaksudkan untuk memenuhi syarat kelulusan program S1 Informatika di Universitas Amikom Yogyakarta.

Selesainya tugas akhir ini tidak lepas dari dukungan berbagai pihak yang telah memberikan dorongan moril maupun materil dan juga bimbingan ilmu pengetahuan. Oleh karena itu penulis mengucapkan terima kasih kepada :

1. Bapak Prof. Dr. M. Suyanto, MM selaku rektor Universitas Amikom Yogyakarta.
2. Bapak Dony Ariyus, M.Kom selaku dosen pembimbing saya yang telah memberikan banyak masukan – masukan dalam penulisan skripsi ini.
3. Bapak, ibu dosen, dan seluruh staf pegawai di prodi informatika yang telah menjadi bagian dari pembelajaran studi penulis.
4. Bapak dan ibu tercinta yang selalu memberikan doanya setiap hari kepada penulis.
5. Serta semua pihak yang telah membantu dan bekerjasama dalam pelaksanaan skripsi ini.

Penulis menyadari masih begitu banyak kekurangan dalam penyusunan laporan skripsi ini. Untuk itu, kritik dan saran adalah sesuatu yang sangat penulis harapkan demi kemajuan bersama.

Yogyakarta, 7 Mei 2018

Penulis



## DAFTAR ISI

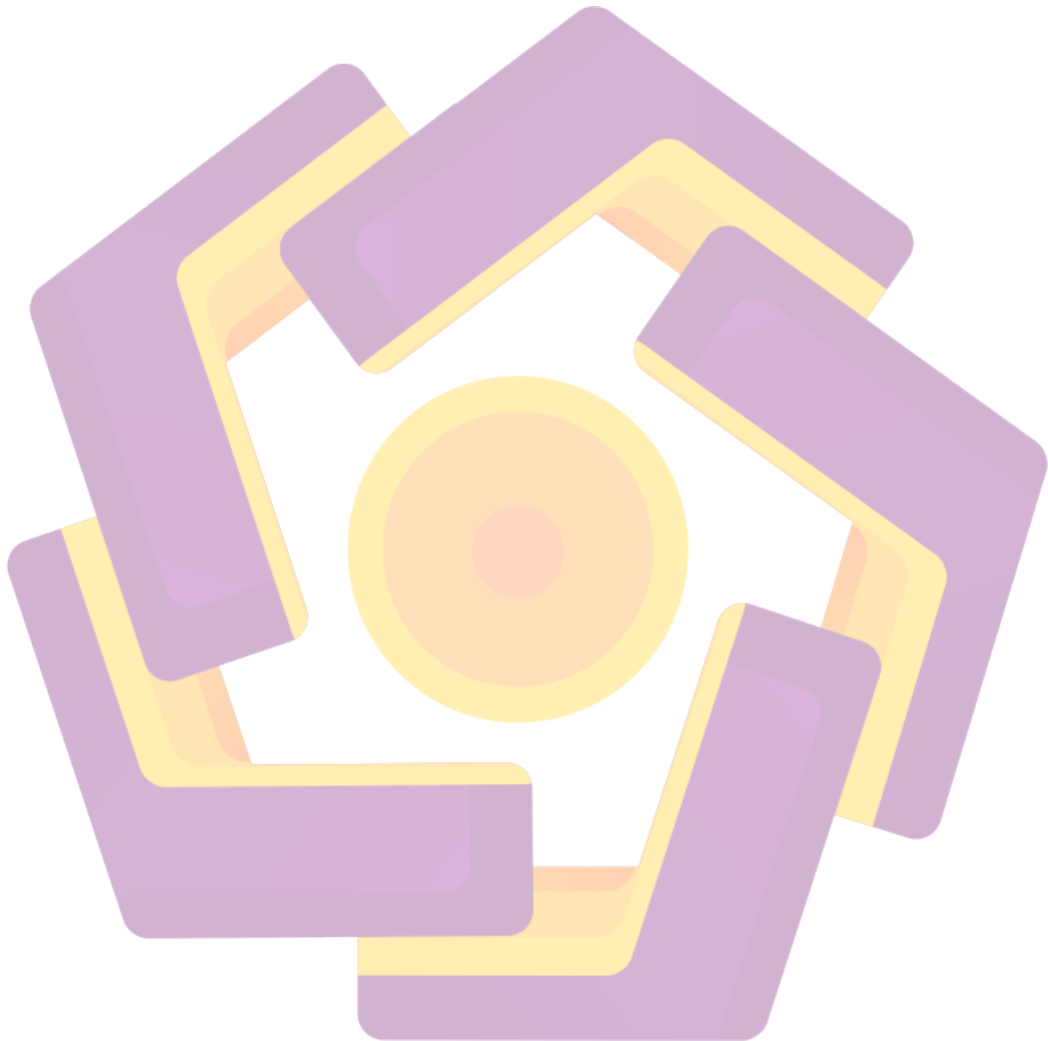
HALAMAN JUDUL.....	i
PERSETUJUAN .....	ii
PENGESAHAN .....	iii
PERNYATAAN.....	iv
MOTTO .....	v
PERSEMBAHAN .....	vi
KATA PENGANTAR .....	vii
DAFTAR ISI.....	viii
DAFTAR TABEL.....	xiv
DAFTAR GAMBAR .....	xv
INTISARI.....	xvii
ABSTRACT .....	xviii
BAB I .....	1
PENDAHULUAN .....	1
<b>1.1 Latar Belakang Masalah</b> .....	1
<b>1.2 Rumusan Masalah</b> .....	3
<b>1.3 Batasan Masalah</b> .....	3
<b>1.4 Maksud dan Tujuan Penelitian</b> .....	4
<b>1.5 Manfaat Penelitian</b> .....	4
<b>1.6 Metode Penelitian</b> .....	5
1.6.1 Metode Pengumpulan Data.....	5
1.6.1.1 Metode Observasi.....	5
1.6.1.2 Metode Studi Kepustakaan .....	5
1.6.1.3 Metode Internet .....	5

1.6.2	Metode Analisis .....	6
1.6.2.1	Analisis Kebutuhan Sistem .....	6
1.6.2.2	Analisis Kelayakan Sistem.....	6
1.6.3	Metode Perancangan .....	6
<b>1.7</b>	<b>Sistematika Penulisan .....</b>	<b>6</b>
<b>BAB II</b> .....		<b>8</b>
<b>LANDASAN TEORI</b> .....		<b>8</b>
<b>2.1</b>	<b>Tinjauan Pustaka .....</b>	<b>8</b>
<b>2.2</b>	<b>Teori Matematika dalam Kriptografi .....</b>	<b>10</b>
2.2.1	Divisibility .....	10
2.2.2	Division Algorithm .....	11
2.2.3	Modulus .....	11
2.2.4	Proper Congruences .....	12
<b>2.3</b>	<b>Konsep Keamanan Komputer.....</b>	<b>13</b>
<b>2.4</b>	<b>Pengertian Kriptografi.....</b>	<b>16</b>
<b>2.5</b>	<b>Sejarah Kriptografi.....</b>	<b>18</b>
<b>2.6</b>	<b>Algoritma Kriptografi.....</b>	<b>22</b>
2.6.1	Algoritma Kriptografi Classic.....	23
2.6.1.1	Substitution Cipher .....	23
2.6.1.2	Shift Cipher .....	25
2.6.1.3	The Polyalphabetic Cipher .....	26
2.6.1.4	Kerckhoffs Principle .....	29
2.6.2	Algoritma Kriptografi Modern.....	30
2.6.2.1	Vernam Cipher atau Steam Cipher .....	30
2.6.2.2	One-Time Pad .....	33

2.6.2.3	Block Cipher .....	34
<b>2.7</b>	<b>Symmetric Encryption .....</b>	<b>35</b>
<b>2.8</b>	<b>Asymmetric Encryption.....</b>	<b>36</b>
<b>2.9</b>	<b>Caesar Cipher .....</b>	<b>37</b>
<b>2.10</b>	<b>Advanced Encryption Standard (AES) .....</b>	<b>44</b>
2.10.1	Input dan Output .....	46
2.10.2	Bytes.....	47
2.10.3	Byte Array.....	48
2.10.4	State.....	49
2.10.5	State sebagai Array dari Kolom .....	50
2.10.6	Rincian Algoritma.....	50
2.10.7	Cipher.....	51
2.10.8	SubByte Transformation .....	52
2.10.9	ShiftRows Transformation.....	54
2.10.10	MixColumns Transformation.....	55
2.10.11	AddRoundKey Transformation.....	56
2.10.12	Key Expansion .....	57
2.10.13	Inverse Cipher .....	57
2.10.14	InvShiftRows Transformation.....	58
2.10.15	InvSubBytes Transformation .....	59
2.10.16	InvMixColumns Transformation.....	59
2.10.17	Inverse AddRoundKey Transformation .....	60
<b>2.11</b>	<b>UML.....</b>	<b>61</b>
2.11.1	Pengenalan UML .....	62
2.11.2	Diagram UML.....	63

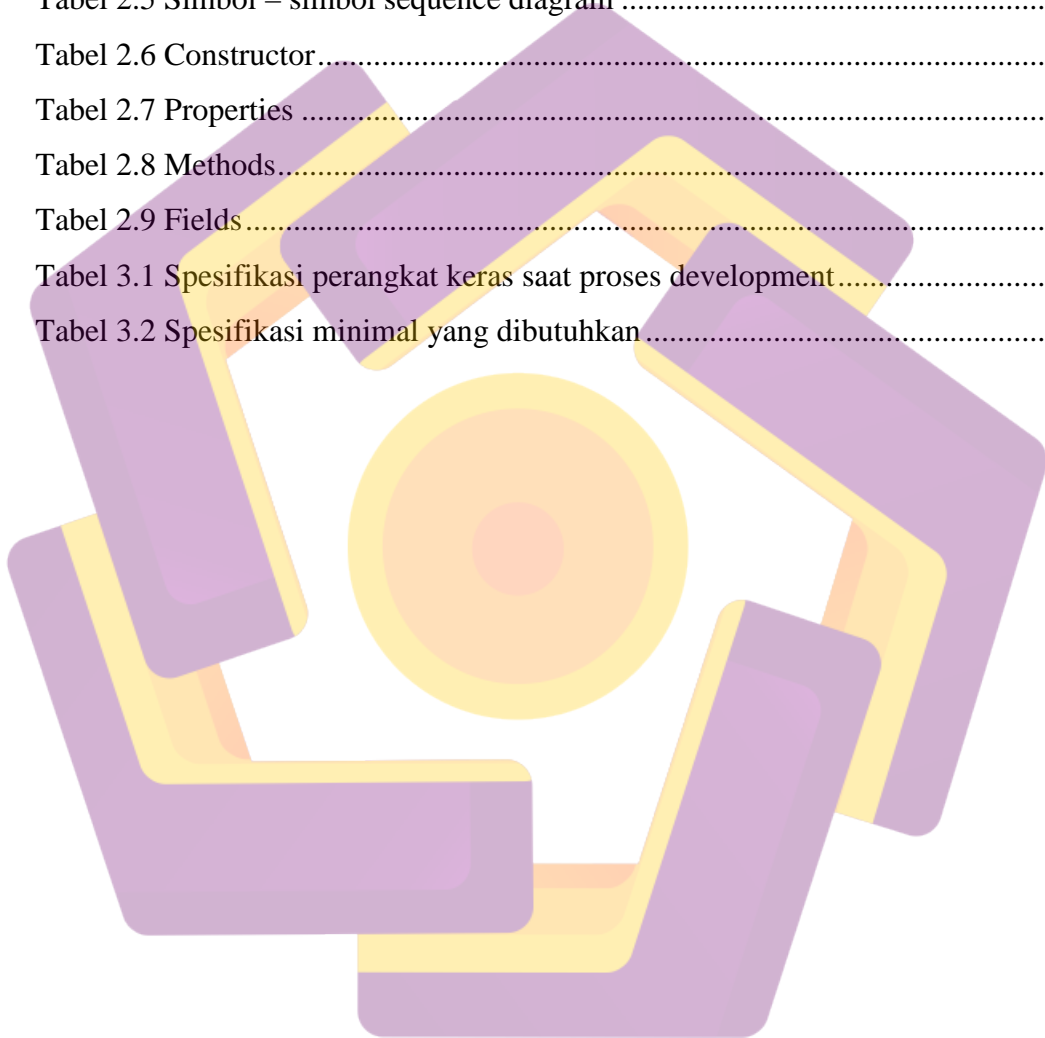
2.11.3	Class Diagram .....	64
2.11.4	Use Case Diagram.....	66
2.11.5	Activity Diagram.....	67
2.11.6	Sequence Diagram .....	69
<b>2.12</b>	<b>Pengujian Pada File Photo.....</b>	<b>71</b>
<b>2.13</b>	<b>Pengujian Pada File Video.....</b>	<b>71</b>
<b>2.14</b>	<b>Implementasi Kriptografi di dalam C# .....</b>	<b>72</b>
<b>BAB III</b>	<b>.....</b>	<b>77</b>
<b>ANALISIS DAN PERANCANGAN</b>	<b>.....</b>	<b>77</b>
<b>3.1</b>	<b>Gambaran Aplikasi .....</b>	<b>77</b>
<b>3.2</b>	<b>Analisis Kebutuhan Sistem.....</b>	<b>77</b>
3.2.1	Analisis Kebutuhan Fungsional .....	77
3.2.2	Analisis Kebutuhan Non-Fungsional .....	78
3.2.2.1	Analisis Kebutuhan Perangkat Keras.....	78
3.2.2.2	Analisis Kebutuhan Perangkat Lunak.....	79
<b>3.3</b>	<b>Analisis Kelayakan Sistem.....</b>	<b>80</b>
3.3.1	Kelayakan Teknis.....	80
3.3.2	Kelayakan Operasional .....	80
3.3.3	Kelayakan Hukum.....	80
<b>3.4</b>	<b>Skema Program .....</b>	<b>80</b>
<b>3.5</b>	<b>Perancangan Sistem .....</b>	<b>82</b>
3.5.1	Use Case Diagram.....	82
3.5.2	Activity Diagram.....	83
3.5.3	Sequence Diagram .....	83
3.5.4	Class Diagram .....	84

<b>3.6 Perancangan Interface</b> .....	84
<b>BAB IV</b> .....	93
<b>IMPLEMENTASI DAN PEMBAHASAN</b> .....	93
<b>4.1 Implementasi</b> .....	93
4.1.1 Implementasi User Interface .....	93
4.1.1.1 Pembahasan Program User Interface .....	95
4.1.2 Implementasi Algoritma Enkripsi Caesar Cipher .....	96
4.1.2.1 Pembahasan Algoritma Caesar Cipher.....	96
4.1.3 Implementasi Algoritma Enkripsi AES .....	98
4.1.3.1 Pembahasan Algoritma Enkripsi AES .....	98
4.1.4 Implementasi Algoritma Dekripsi AES .....	100
4.1.4.1 Pembahasan Algoritma Dekripsi AES.....	101
4.1.5 Implementasi Input File .....	101
4.1.5.1 Pembahasan Input File .....	102
4.1.6 Implementasi Save File .....	102
4.1.6.1 Pembahasan Save File.....	102
<b>4.2 Pengujian Program</b> .....	102
4.2.1 Pengujian Pada File Photo .....	103
4.2.2 Pengujian Pada File Video.....	104
<b>4.3 Pemeliharaan Sistem</b> .....	105
<b>BAB V</b> .....	106
<b>PENUTUP</b> .....	106
<b>5.1 Kesimpulan</b> .....	106
<b>5.2 Saran</b> .....	107
<b>DAFTAR PUSTAKA</b> .....	108



## DAFTAR TABEL

Tabel 2.1 Substitution cipher sederhana .....	23
Tabel 2.2 Simbol – simbol class diagram .....	64
Tabel 2.3 Simbol – simbol use case diagram .....	66
Tabel 2.4 Simbol – simbol activity diagram .....	68
Tabel 2.5 Simbol – simbol sequence diagram .....	70
Tabel 2.6 Constructor .....	73
Tabel 2.7 Properties .....	73
Tabel 2.8 Methods .....	74
Tabel 2.9 Fields .....	76
Tabel 3.1 Spesifikasi perangkat keras saat proses development .....	78
Tabel 3.2 Spesifikasi minimal yang dibutuhkan .....	79

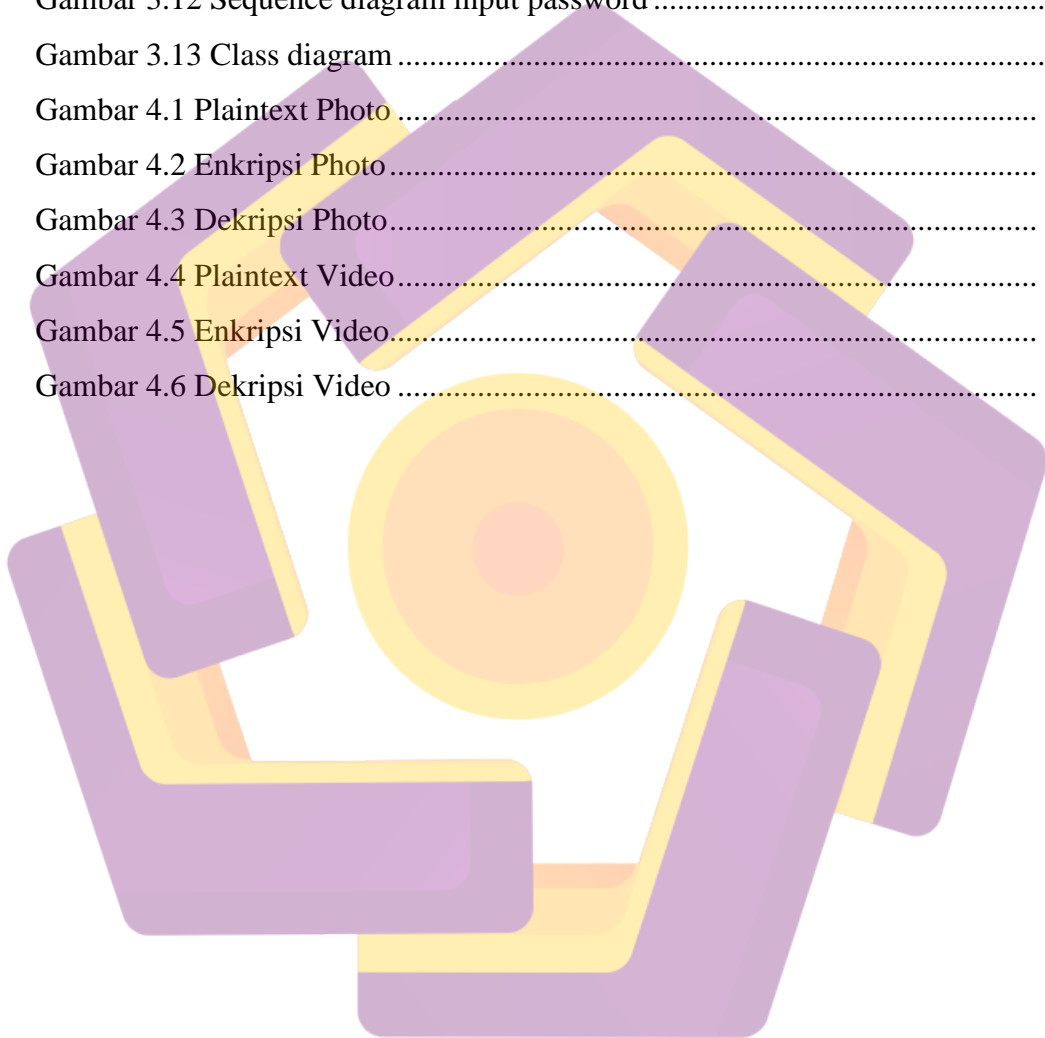


## DAFTAR GAMBAR

Gambar 2.1 CIA triad.....	14
Gambar 2.2 Herbern electric coding machine.....	19
Gambar 2.3 Enigma .....	20
Gambar 2.4 Siemens and Halske T52 .....	21
Gambar 2.5 Pergeseran huruf alphabet .....	25
Gambar 2.6 Vigenere tableau.....	27
Gambar 2.7 Cara kerja algoritma polyalphabetic .....	28
Gambar 2.8 Gulungan kertas pita atau paper tape untuk enkripsi dan dekripsi....	31
Gambar 2.9 Paper tape of baudot system.....	32
Gambar 2.10 Modern cipher disk dari nasional cyptography museum .....	39
Gambar 2.11 Tampilan bit dalam hexadecimal .....	47
Gambar 2.12 Petunjuk untuk byte dan bits .....	48
Gambar 2.13 State array input dan output .....	49
Gambar 2.14 Kombinasi key-block-round.....	51
Gambar 2.15 Tranformasi affine elemen s-box .....	52
Gambar 2.16 SubByte yang digunakan di s-box pada state.....	53
Gambar 2.17 Substitusi nilai x y dalam hexadecimal .....	53
Gambar 2.18 ShiftRows menukar tiga barsi terakhir di state .....	54
Gambar 2.19 Transformasi MixColumns bekerja kolom demi kolom .....	56
Gambar 2.20 AddRoundKey operasi xor pada kolom state dengan word yang berasal dari key schedule .....	57
Gambar 2.21 InvShiftRows menggeser atau menukar tiga baris terakhir di dalam State.....	58
Gambar 2.22 Pembalikan S-box: substitusi nilai xy dalam format hexadecimal .	59
Gambar 3.1 Skema proses enkripsi.....	81
Gambar 3.2 Skema proses dekripsi.....	81
Gambar 3.3 Inteface program .....	85
Gambar 3.4 Use case diagram.....	85
Gambar 3.5 Activity diagram input file .....	86
Gambar 3.6 Activity diagram save file .....	87



Gambar 3.7 Activity diagram input password .....	87
Gambar 3.8 Activity diagram enkripsi .....	88
Gambar 3.9 Activity diagram dekripsi .....	89
Gambar 3.10 Sequence diagram input file .....	90
Gambar 3.11 Sequence diagram save file .....	90
Gambar 3.12 Sequence diagram input password .....	91
Gambar 3.13 Class diagram .....	92
Gambar 4.1 Plaintext Photo .....	103
Gambar 4.2 Enkripsi Photo .....	103
Gambar 4.3 Dekripsi Photo .....	103
Gambar 4.4 Plaintext Video .....	104
Gambar 4.5 Enkripsi Video .....	104
Gambar 4.6 Dekripsi Video .....	104



## INTISARI

Saat ini komputer sudah menjadi barang umum yang sudah dimiliki oleh masyarakat. Komputer digunakan untuk membantu mengerjakan berbagai macam tugas, mulai dari tugas yang memiliki tingkat kesulitan yang tinggi atau tugas yang memiliki tingkat kesulitan yang rendah. Komputer membantu dengan cara membuat file, menampilkan file, menghapus file, membagikan file, hingga menyimpan file. File tersebut terbagi kedalam kedalam beberapa jenis yaitu, file text, file image, file video, file audio, dan juga file konfigurasi.

Banyak sekali masalah yang sering terjadi berkaitan dengan file yang ada di dalam komputer, satu masalah yang sering terjadi adalah masalah privasi. Masalah ini terjadi karena orang lain berhasil mengakses file, merubah file, atau menghapus file tanpa seizin dan sepengetahuan penulis. Dampak yang dihasilkan dari masalah ini adalah rusaknya kerahasiaan file, hilangnya integritas file karena file sudah mengalami perubahan, hingga kerugian ekonomi.

Kriptografi adalah solusi yang dapat digunakan untuk mengatasi masalah diatas, dengan menggunakan algoritma AES dan modifikasi algoritma Caesar cipher.

**Kata kunci :** *Kriptografi, Advanced Encryption Standard (AES), Caesar Cipher, Modifikasi Caesar Cipher.*

## **ABSTRACT**

*Currently computers have become common goods that are owned by the community. The computer used to perform a variety of tasks, the tasks that have a high degree of difficulty or the tasks that have low levels of difficulty. The computer itself is helping the community by the way of creating file, displaying file, deleting file, sharing file, and also up to save file. The file are divided into several types, for example is text file, image files, video files, audio files, and also configuration files.*

*A great many of the problems that often occur with regards to the files that are in the computer, one of the problems that often occurs is a matter of privacy. This problem happened because the other person can successfully access files, change file, or delete file without permission and knowledge of the file's owner. The impact caused from this privacy issue is the destruction of the confidentiality of the data, discuss the destruction of the integrity of the file, as well as material losses.*

*Cryptography is a solution that can be used to solve the problem above by using the AES algorithm and algorithm Caesar cipher modified.*

**Keywords :** *Cryptography, Advanced Encryption Standard (AES), Caesar Cipher, Modification of the Caesar Cipher.*