

**PEMBUATAN PERANGKAT LUNAK SEBAGAI MEDIA PEMBELAJARAN
KRIPTOGRAFI ALGORITMA VIGENERE CIPHER DAN AES 128bit
(*ADVANCED ENCRYPTION STANDARD*)**

SKRIPSI



Disusun oleh

Gita Ramadanita Qamaril

11.11.5055

**JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2015**

**PEMBUATAN PERANGKAT LUNAK SEBAGAI MEDIA PEMBELAJARAN
KRIPTOGRAFI ALGORITMA VIGENERE CIPHER DAN AES 128bit
(ADVANCED ENCRYPTION STANDARD)**

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai derajat Sarjana S1
pada jurusan Teknik Informatika



Disusun oleh

Gita Ramadanita Qamaril

11.11.5055

**JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2015**

PERSETUJUAN

SKRIPSI

**PEMBUATAN PERANGKAT LUNAK SEBAGAI MEDIA
PEMBELAJARAN KRIPTOGRAFI ALGORITMA
VIGENERE CIPHER DAN AES 128bit
(ADVANCED ENCRYPTION STANDARD)**

yang dipersiapkan dan disusun oleh

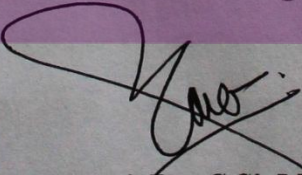
Gita Ramadanita Qamaril

11.11.5055

Telah disetujui oleh Dosen Pembimbing Skripsi

Pada tanggal 08 September 2015

Dosen Pembimbing



Ema Utami, Dr., S.Si, M.Kom
NIK. 190302037

PENGESAHAN

SKRIPSI

**PEMBUATAN PERANGKAT LUNAK SEBAGAI MEDIA
PEMBELAJARAN KRIPTOGRAFI ALGORITMA
VIGENERE CIPHER DAN AES 128bit
(ADVANCED ENCRYPTION STANDARD)**

yang disusun oleh

Gita Ramadanita Qamaril
11.11.5055

telah dipertahankan di depan Dewan Penguji
pada tanggal 15 September 2015

Susunan Dewan Penguji

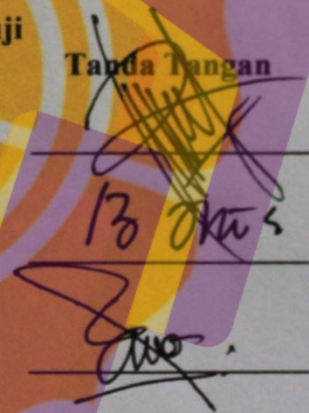
Nama Penguji

Robert Marco, M.T
NIK. 190302228

Barka Satva, M.Kom
NIK. 190302126

Ema Utami, Dr., S.Si, M.Kom
NIK. 190302037

Tanda Tangan



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 15 September 2015

KETUA STMIK AMIKOM YOGYAKARTA



Prof. Dr. M. Suvanto, M.M.
NIK. 190302001

PERNYATAAN

Saya yang bertandatangan di bawah 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 Instansi Pendidikan 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.

Yogyakarta, 15 September 2015



Gita Ramadanita Qamaril
11.11.5055

MOTTO

"Semua ini adalah rentetan dari sebuah proses, jalani semuanya dengan sabar maka kelak kamu akan mendapatkan hasil yang memuaskan"



HALAMAN PERSEMBAHAN

Segala puji hanyalah terucap bagi Allah SWT pencipta alam semesta ini yang telah menganugraahkan segala nikmat untuk semua umat-NYA , Serta shalawat dan salam selalu tercurah kepada junjungan kita Nabi Muhammad SAW .

Ku persembahkan karya ini untuk kedua orang tua ku tercinta

Ayahanda Amir Gapuri dan Ibunda Rukanah

Terima kasih yang tak terhingga dan segala dukungan serta cinta kasih yang tiada mungkin bisa kubalas hanya dengan selembar kertas yang bertuliskan kata cinta dan persembahan. Semoga ini menjadi langkah awal untuk membuat kalian bahagia. Terima kasih selalu membuat termotivasi dan selalu mendo'akan ku serta menasihati agar menjadi lebih baik.

dan

Keluarga besar ku

“Yang selalu memberi dukungan, semangat serta nasihat-nasihat”

KATA PENGANTAR

Assalamu 'alaikum wr.wb.

Puji syukur penulis panjatkan kepada Allah SWT , yang telah melimpahkan segala rahmat, karunia serta hidayah-Nya kepada penulis, dan sholawat serta salam tetap tercurahkan kepada Nabi Muhammad SAW, sehingga penulis dapat menyelesaikan serta menyusun Laporan Skripsi ini sebagai syarat untuk menyelesaikan studi Strata 1 Teknik Informatika STMIK AMIKOM Yogyakarta.

Penulis menyadari bahwa penyusunan skripsi ini tidak akan terselesaikan dengan baik, tanpa bantuan, petunjuk, bimbingan dan saran dari berbagai pihak. Oleh karenanya, pada kesempatan ini dengan kerendahan hati, penulis mengucapkan terima kasih yang sebesar-besarnya kepada :

1. Sang Khalik Allah Subhanahu Wa Ta'ala, yang selalu memberikan petunjuk, pencerahan, kemudahan serta ridho, dan kasih sayang yang tiada terkira kepada setiap hamba-Nya, dan tidak terkecuali kepada penulis.
2. Nabi besar Muhammad Shalallahu Alaihi Wa Sallam.
3. Bapak Prof. Dr. M. Suyanto, M.M. selaku Ketua STMIK AMIKOM Yogyakarta,
4. Bapak Sudarmawan, M.T, selaku Ketua Jurusan Teknik Informatika STMIK AMIKOM Yogyakarta,
5. Ibu Ema Utami, Dr., S.Si, M.Kom, selaku dosen pembimbing yang telah mendukung dan membimbing sampai laporan ini selesai,
6. Kepada seluruh dosen STMIK AMIKOM Yogyakarta, Terima kasih atas ilmu yang diberikan, semoga penulis dapat mengamalkan dan menjadikan sebagai amal jariyah,
7. Ayahanda Amir Gapuri dan Ibunda Rukanah selaku kedua orang tua penulis yang selalu memberikan dukungan dan motivasi selama penulisan laporan ini,
8. Muhammad Rizqiannor yang selalu menemani dan memberi semangat dalam menyelesaikan Skripsi ini,

9. Seluruh teman-teman S1TI-06, terkhusus Lutfi Fauziah, Nurul Hidayah, Elvira Devina N.F, yang selalu memberi masukan dalam penyelesaian Skripsi ini,
10. Teman-teman Asrama Himpunan Mahasiswa dan Pelajar Tabalong Putri “Kambang Tanjung” yang selalu mendukungku dan mendidik ku selama berada di Kota Yogyakarta ini.
11. Semua pihak yang tidak dapat disebutkan satu persatu atas perhatian dan curahan ide sehingga skripsi ini dapat diselesaikan dengan baik.

Menyadari bahwa laporan ini masih jauh dari sempurna maka penulis mengharapkan segala kritik dan saran dari para pembaca agar laporan ini dapat lebih sempurna sehingga dapat menjadi perbaikan untuk penyusunan laporan di masa mendatang. Semoga laporan ini dapat bermanfaat bagi para pembaca pada umumnya dan penulis pada khususnya.

Yogyakarta, 15 September 2015

Penulis,

Gita Ramadanita Qamaril

DAFTAR ISI

JUDUL	i
PERSETUJUAN	ii
PENGESAHAN	iii
PERNYATAAN	iv
MOTTO	v
HALAMAN PERSEMBAHAN	vi
KATA PENGANTAR	vii
DAFTAR ISI	ix
DAFTAR TABEL	xi
DAFTAR GAMBAR	xii
INTISARI	xvi
ABSTRACT	xvii
BAB I	1
1.1 Latar Belakang Masalah.....	1
1.2 Rumusan Masalah.....	2
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	4
1.6 Metode Pengumpulan Data	5
1.7 Sistematika Penulisan	5
BAB II LANDASAN TEORI	7
2.1 Tinjauan Pustaka.....	7
2.2 Kriptografi.....	8
1.1.1 Definisi Kriptografi	9
1.1.2 Tujuan Kriptografi.....	9
1.1.3 Komponen Kriptografi.....	11
1.1.4 Macam-Macam Kriptografi	12
2.3 Vigenere Cipher.....	14
2.4 Advanced Encryption Standard (AES)	14
1.1.5 Algoritma Advanced Encryption Standard (AES)	17

1.1.6	Transformasi-Transformasi AES.....	19
1.1.7	Ekspansi Kunci AES.....	26
2.5	UML (Unified Modeling Language)	28
1.1.8	Usecase Diagram	29
1.1.9	Class Diagram	32
1.1.10	Activity Diagram.....	33
1.1.11	Sequence Diagram.....	34
2.6	Delphi.....	35
1.1.12	IDE Delphi	36
BAB III	41
3.1	Gambaran Umum Aplikasi.....	41
3.1	Analisis SWOT.....	41
3.2	Analisis Kebutuhan Sistem	42
1.1.13	Analisis Kebutuhan Fungsional.....	42
5.1.1	Analisis Kebutuhan Non Fungsional	43
3.3	Analisis Kelayakan Sistem.....	44
5.1.2	Analisis Kelayakan Teknik	44
5.1.3	Analisis Kelayakan Operasional.....	45
5.1.4	Analisis Kelayakan Hukum.....	45
3.4	Analisis Data	45
3.5	Perancangan Sistem	65
5.1.5	Perancangan Uml.....	65
3.6	Rancangan Tampilan	73
BAB IV	76
4.1	Implementasi	76
4.1.1	Implementasi User Interface	76
4.2	Pembahasan.....	79
4.2.1	Pembahasan Kode Program.....	79
4.2.2	Pengujian Program	90
BAB V	104
5.1	Kesimpulan.....	104
5.2	Saran	105
DAFTAR PUSTAKA	106

DAFTAR TABEL

Tabel 2. 1 Parameter AES	17
Tabel 2. 2 Tabel Rcon pada AES	27
Tabel 2. 3 Simbol-simbol Use-case Diagram	30
Tabel 2. 4 Simbol-simbol Class Diagram	32
Tabel 2. 5 Simbol-simbol Activity Diagram	34
Tabel 2. 6 Simbol-simbol Sequence Diagram	35
Tabel 3. 1 Analisis SWOT	42
Tabel 3. 2 Spesifikasi computer	43
Tabel 3. 3 Perangkat Lunak	44
Tabel 3. 4 Hasil Proses Ekspansi Kunci untuk Setiap Ronde	55
Tabel 3. 5 Proses Enkripsi AES	62
Tabel 3. 6 Proses Dekripsi AES	64
Tabel 4. 1 Hasil Uji Coba.....	102

DAFTAR GAMBAR

Gambar 2.1 Proses Umum Enkripsi dan Dekripsi AES.....	19
Gambar 2.2 Tabel Substitusi untuk Transformasi SubBytes	20
Gambar 2.3 Tabel Substitusi untuk Transformasi InvSubBytes	21
Gambar 2.4 Transformasi ShiftRows	22
Gambar 2.5 Contoh Transformasi ShiftRows	22
Gambar 2.6 Transformasi InvShiftRows	23
Gambar 2.7 Transformasi MixColumns	24
Gambar 2.8 Operasi Transformasi MixColumns	24
Gambar 2.9 Transformasi InvMixColumns	25
Gambar 2.10 Proses Transformasi AddRoundKey	26
Gambar 2.11 Contoh Operasi AddRoundKey	26
Gambar 2.12 Proses Ekspansi Kunci AES.....	27
Gambar 2.13 Ekspansi Kunci AES.....	28
Gambar 2.14 Tampilan IDE Delphi 7.....	37
Gambar 2.15 Menu Utama Delphi 7.....	37
Gambar 2.16 Component Pallete.....	38
Gambar 2.17 Toolbar	38
Gambar 2.18 Object Inspector.....	39
Gambar 2.20 Form Editor	40
Gambar 2.21 Kode Editor	40

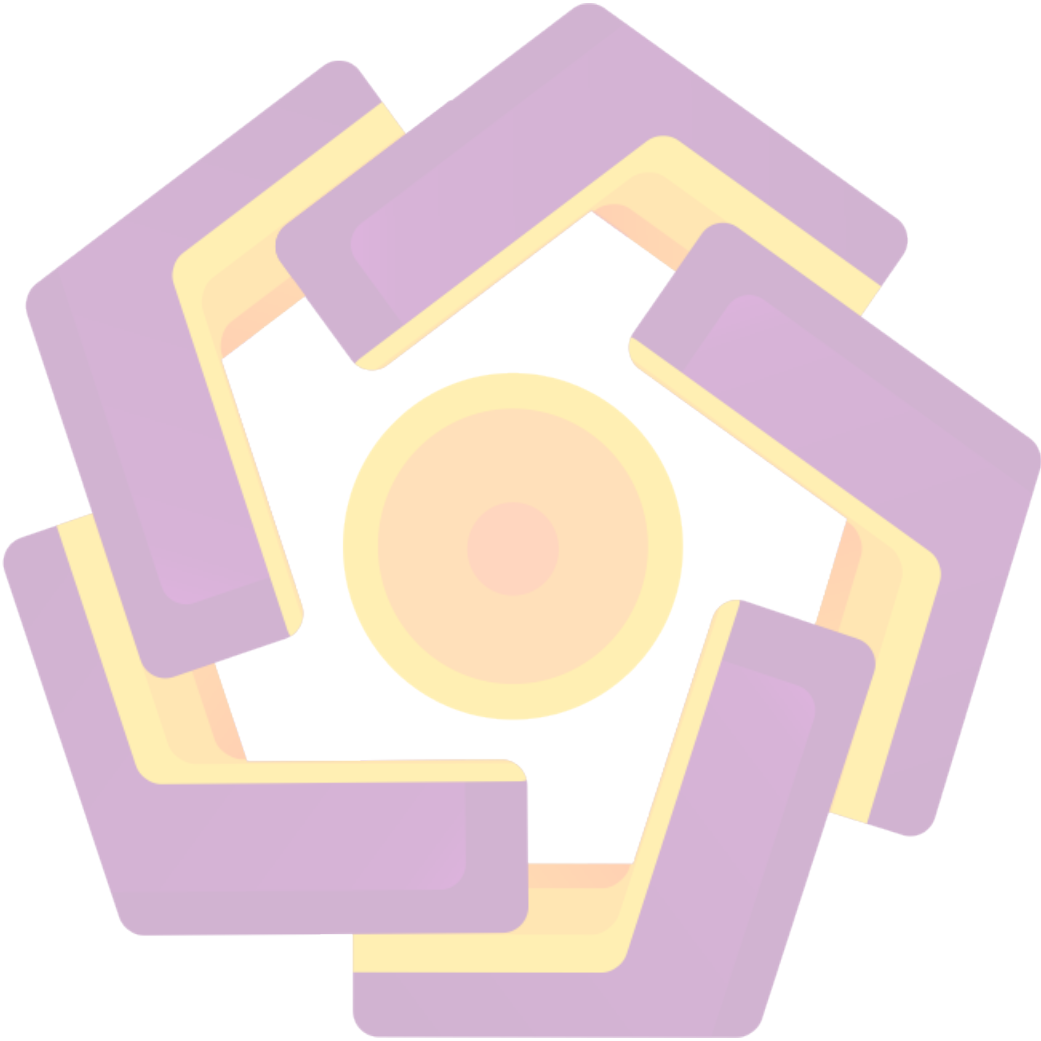
Gambar 3. 1 Proses Ekspansi Kunci Ronde Ke-1	52
Gambar 3. 2 Proses Ekspansi Kunci Ronde Ke-2	52
Gambar 3. 3 Proses Ekspansi Kunci Ronde Ke-3	52
Gambar 3. 4 Proses Ekspansi Kunci Ronde Ke-4	53
Gambar 3. 5 Proses Ekspansi Kunci Ronde Ke-5	53
Gambar 3. 6 Proses Ekspansi Kunci Ronde Ke-6	53
Gambar 3. 7 Proses Ekspansi Kunci Ronde Ke-7	54
Gambar 3. 8 Proses Ekspansi Kunci Ronde Ke-8	54
Gambar 3. 9 Proses Ekspansi Kunci Ronde Ke-9	54
Gambar 3. 10 Proses Ekspansi Kunci Ronde Ke-10	55
Gambar 3. 11 Diagram Use case Aplikasi Enkripsi	66
Gambar 3. 12 Diagram Use Case Aplikasi Dekripsi	67
Gambar 3. 13 Diagram Kelas Aplikasi Enkripsi dan Dekripsi Vigenere	68
Gambar 3. 14 Diagram Kelas Aplikasi Enkripsi dan Dekripsi AES	68
Gambar 3. 15 Activity Diagram Menu Enkripsi dan Dekripsi Algoritma Vigenere..	70
Gambar 3. 16 Activity Diagram Menu Enkripsi dan Dekripsi Algoritma AES.....	71
Gambar 3. 17 Diagram Sequence Aplikasi Enkripsi	72
Gambar 3. 18 Diagram Sequence Aplikasi Dekripsi.....	73
Gambar 3. 19 Rancang Tampil Menu Awal	74
Gambar 3. 20 Rancang Tampil Menu Algoritma Vigenere	74
Gambar 3. 21 Rancang Tampil Menu Algoritma AES	75
Gambar 4. 1 Tampilan Menu Utama	77

Gambar 4. 2 Tampilan Menu Algoritma Vigenere.....	78
Gambar 4. 3 Tampilan Menu Algoritma Aes.....	79
Gambar 4. 4 Tampilan Menu Enkripsi Vigenere Cipher	90
Gambar 4. 5 Tampilan input plainteks Vigenere Cipher	91
Gambar 4. 6 Tampilan input kunci enkripsi Vigenere Cipher	91
Gambar 4. 7 Tampilan proses enkripsi Vigenere Cipher.....	92
Gambar 4. 8 Tampilan input kunci enkripsi Vigenere Cipher	92
Gambar 4. 9 Tampilan Menu Dekripsi Vigenere Cipher	93
Gambar 4. 10 Tampilan cipherteks Vigenere Cipher	94
Gambar 4. 11 Tampilan input kunci dekripsi Vigenere Cipher	94
Gambar 4. 12 Tampilan proses dekripsi Vigenere Cipher	95
Gambar 4. 13 Tampilan proses dekripsi Vigenere Cipher	95
Gambar 4. 14 Tampilan Menu Enkripsi AES-128 bit	96
Gambar 4. 15 Tampilan input plainteks AES-128 bit	97
Gambar 4. 16 Tampilan input kunci enkripsi AES-128 bit	97
Gambar 4. 17 Tampilan proses enkripsi AES-128 bit	98
Gambar 4. 18 Tampilan input kunci enkripsi AES-128 bit	98
Gambar 4. 19 Tampilan Menu Dekripsi AES-128 bit	99
Gambar 4. 20 Tampilan cipherteks AES-128 bit	100
Gambar 4. 21 Tampilan input kunci dekripsi AES-128 bit	100
Gambar 4. 22 Tampilan proses dekripsi AES-128 bit	101
Gambar 4. 23 Tampilan proses dekripsi AES-128 bit	101

Gambar 4. 24 *Runtime Error*.....103

Gambar 4. 25 *Syntax Error*103

Gambar 4. 26 *Logic Error*.....103



INTISARI

Pengamanan sistem informasi memiliki beberapa dasar-dasar dan teori yang digunakan. Kriptografi, enkripsi dan dekripsi merupakan dasar dari pengamanan sistem informasi. Algoritma Vigenere Cipher dan AES merupakan beberapa algoritma pada kriptografi yang dapat digunakan atau diimplementasikan sebagai pengamanan sistem informasi.

Dikarenakan peranan kriptografi yang penting, oleh karena itu di dalam dunia pendidikan diperlukan suatu aplikasi untuk mempelajari kriptografi secara visual dan interaktif. Di beberapa tempat kuliah dan belajar sering sekali ditemukan pembelajaran kriptografi yang masih menggunakan teori-teori tanpa langsung melihat apa yang terjadi di dalam proses kriptografi tersebut.

Maka dari itu, akan dibuat suatu perangkat lunak pembelajaran kriptografi klasik yang dapat mempermudah dalam mempelajari proses dari beberapa algoritma kriptografi seperti vigenere dan AES, dengan visualisasi dan proses dalam perubahan data.

Kata kunci : Kriptografi, Vigenere, AES, perubahan data.

ABSTRACT

Information system security has some basics and theory are used. Cryptography, encryption and decryption is the Foundation of the security of information systems. Vigenere Cipher Algorithm and AES cryptographic algorithm on some of that can be used or implemented as information systems security.

Due to the role of cryptography are important, therefore in the educated world needed an application to learn Cryptography visually and interactively. In some places lecture and study often found still using cryptographic learning theories without directly see what is going on inside the cryptographic process.

Therefore, it will be created a classic Cryptography learning software that can ease in learning process of several cryptographic algorithms such as AES and vigenere, with visualization and data changes in the process.

Keywords: *Cryptography, Vigenere, AES, data changes*