

**IMPLEMENTASI ALGORITMA KRIPTOGRAFI HYBRID (DES, AES,
DAN ELGAMAL) PADA APLIKASI DESKTOP
BERBASIS PHYTON**

SKRIPSI



disusun oleh

M. Urfa Nurfathan

11.11.5341

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

**IMPLEMENTASI ALGORITMA KRIPTOGRAFI HYBRID (DES, AES,
DAN ELGAMAL) PADA APLIKASI DESKTOP
BERBASIS PHYTON**

SKRIPSI

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



disusun oleh

M. Urfa Nurfathan

11.11.5341

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

PERSETUJUAN

SKRIPSI

**IMPLEMENTASI ALGORITMA KRIPTOGRAFI HYBRID (DES, AES,
DAN ELGAMAL) PADA APLIKASI DESKTOP
BERBASIS PYTHON**

yang dipersiapkan dan disusun oleh

M. Urfa Nurfathan

11.11.5341

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 10 Maret 2015

Dosen Pembimbing



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

NIK. 190302037

PENGESAHAN
SKRIPSI
IMPLEMENTASI ALGORITMA KRIPTOGRAFI HYBRID (DES, AES,
DAN ELGAMAL) PADA APLIKASI DESKTOP
BERBASIS PYTHON

yang disusun oleh

M. Urfa Nurfathan

11.11.5341

yang telah dipertahankan di depan Dewan Penguji
pada tanggal 17 April 2015

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Windha Mega Pradnya D, M.Kom
NIK. 190302185



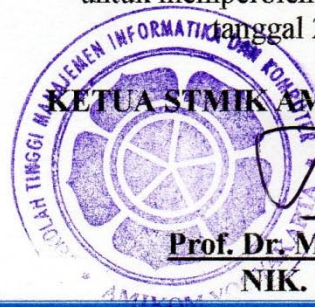
Hartatik, ST, M.Cs
NIK. 190302232




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



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
tanggal 25 April 2015



KETUA STMIK AMIKOM YOGYAKARTA


Prof. Dr. M. Suyanto, M.M
NIK. 190302001

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, 25 April 2015



M. Urfa Nurfathan
NIM. 11.11.5341

MOTTO

Ibnu Abbas ra berkata : “Sulaiman bin Dawud as disuruh memilih antara ilmu, harta dan kerajaan maka beliau memilih ilmu, lalu beliau diberi harta dan kerajaan”.

Abul Aswad berkata : “Tidak ada sesuatu yang lebih utama dari pada ilmu. Para raja itu memerintah manusia (orang kebanyakan), sedangkan para ahli ilmu itu memerintah para raja”.

”sebaik-baiknya manusia adalah yang paling bermanfaat bagi manusia lainnya.” [HR. Thabrani & Daruquthni]

Berusahalah untuk tidak menjadi manusia yang berhasil, tapi berusaha untuk menjadi manusia yang berguna. [Albert Einstein]

”Rahasia didalam kehidupan ini, meskipun anda terjatuh hingga tujuh kali, anda harus bangkit hingga delapan kali.” (Paulo Cuelho)

Kecerdasan bukan penentu kesuksesan, tetapi kerja keras merupakan penentu kesuksesan yang sebenarnya. (Anonymous)

”Tidak ada kata terlambat untuk belajar, belajar bersyukur dalam hidup kepada yang memberi hidup”

[Penulis]

"Ku olah kata, ku baca makna, ku ikat dalam alinea, ku bingkai dalam bab sejumlah lima, jadilah makarya, gelar sarjana ku terima, orang tua, calon istri, calon mertua pun bahagia"

[Penulis]

"Jadilah seperti karang di lautan yang kuat dihantam ombak dan kerjakanlah hal yang bermanfaat untuk diri sendiri dan orang lain, karena hidup di dunia hanyalah sekali. Ingat hanya pada Allah apapun dan dimanapun kita berada kepada Dia-lah tempat meminta dan memohon"

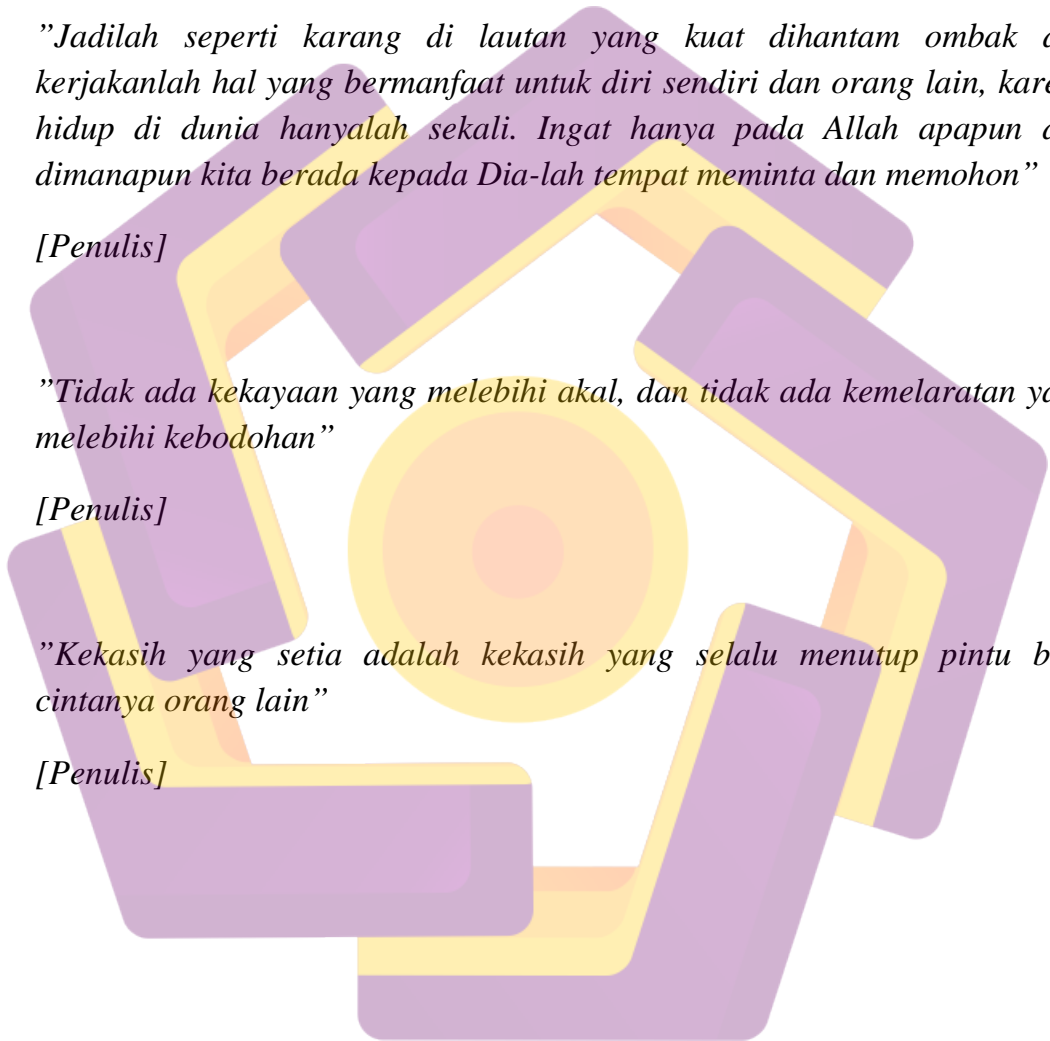
[Penulis]

"Tidak ada kekayaan yang melebihi akal, dan tidak ada kemelaratan yang melebihi kebodohan"

[Penulis]

"Kekasih yang setia adalah kekasih yang selalu menutup pintu buat cintanya orang lain"

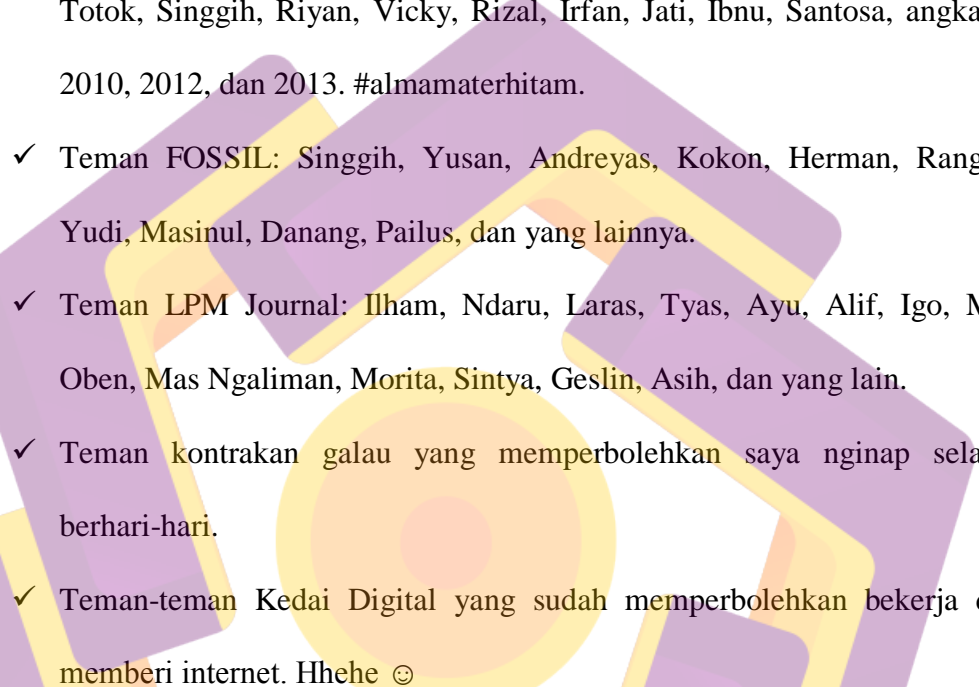
[Penulis]



PERSEMBAHAN

Sembah sujud serta syukur kepada Allah SWT. Taburan cinta dan kasih sayang-Mu telah memberikanku kekuatan, membekaliku dengan ilmu serta memperkenalkanku dengan cinta. Atas karunia serta kemudahan yang Engkau berikan akhirnya skripsi yang sederhana ini dapat terselesaikan. Sholawat dan salam selalu terlimpahkan keharibaan Rasulullah SAW. Kupersembahkan karya sederhana ini kepada orang yang sangat kukasihi dan kusayangi.

- ✓ Kedua orang tua Paino dan Nur Aisyati yang tak lelah salalu mendo'akan, mencintai dan mengasih sayangi tak terhingga. Takkan pernah mampu aku membalas keikhlasan kalian, walaupun dengan gunung emas sekalipun.
- ✓ Adik-adikku Zulfa Fikriana Rahma dan Faiz Salman Ar-Rosiid. Semoga kita selalu membuat Abah dan Umi bahagia dan bangga, dan kita adalah penerus keluarga kita harus jadi orang yang berguna. ☺
- ✓ Calon istri (Amin) Afriyanti Irawati Utami yang sudah setia memberikan semangat dan mempercayaku. Sudah lama kita tak bertemu, semoga kita dipertemukan dalam janji dihadapan Allah SWT dalam sebuah pernikahan.
- ✓ Dosen Pembimbing Ema Utami, Dr., S.Si, M.Kom yang sudah sangat membantu dalam proses pengerjaan laporan skripsi saya.
- ✓ Dosen Penguji 1 dan 2 Bu Windha dan Bu Hartatik yang sudah bersedia meluangkan waktu dalam proses ujian skripsi saya. (A)lhamdulillah.
- ✓ Rekan seperjuangan, Kelas 11-S1TI-10 yang tidak bisa saya sebutkan namanya satu persatu, sukses selalu buat kita semua, jaga silaturahmi.

- 
- ✓ Organisasi mahasiswa STMIK Amikom Yogyakarta. HMJTI mengajarkan manajemen dan tanggung jawab, FOSSIL memberikan banyak ilmu dan relasi, LPM Journal arti seni dalam segala hal serta kejujuran.
 - ✓ Teman HMJTI: Ira, Nafi, Ita, Yayan, Laela, Vidia, Tesa, Rose, Bobby, Totok, Singgih, Riyan, Vicky, Rizal, Irfan, Jati, Ibnu, Santosa, angkatan 2010, 2012, dan 2013. #almamaterhitam.
 - ✓ Teman FOSSIL: Singgih, Yusan, Andreyas, Kokon, Herman, Rangga, Yudi, Masinul, Danang, Pailus, dan yang lainnya.
 - ✓ Teman LPM Journal: Ilham, Ndaru, Laras, Tyas, Ayu, Alif, Igo, Mas Oben, Mas Ngaliman, Morita, Sintya, Geslin, Asih, dan yang lain.
 - ✓ Teman kontrakan galau yang memperbolehkan saya nginap selama sehari-hari.
 - ✓ Teman-teman Kedai Digital yang sudah memperbolehkan bekerja dan memberi internet. Hhehe ☺

KATA PENGANTAR

Alhamdulillahirabbil'alamiin, segala puji bagi Allah SWT Tuhan semesta alam. Atas berkat, rahmat, taufik serta hidayah-Nya yang tiada terkira besarnya, sehingga penulis dapat menyelesaikan skripsi dengan judul "**IMPLEMENTASI ALGORITMA KRIPTOGRAFI HYBRID (DES, AES, DAN ELGAMAL) PADA APLIKASI DESKTOP BERBASIS PHYTON**".

Dalam penyusunannya, penulis memperoleh banyak bantuan dari berbagai pihak, oleh karena itu penulis mengucapkan terima kasih yang sebesar-besarnya kepada :

1. Bapak Prof. Dr. M. Suyanto, MM selaku ketua STMIK AMIKOM Yogyakarta.
2. Bapak Sudarmawan, MT selaku ketua jurusan Teknik Informatika STMIK AMIKOM Yogyakarta.
3. Ibu Ema Utami, Dr., S.Si, M.Kom selaku dosen pembimbing yang telah memberikan arahan, bimbingan, motivasi, waktu dan masukan yang sangat membantu dalam pembuatan laporan skripsi ini.
4. Bapak Ibu dosen, staff dan karyawan STMIK AMIKOM Yogyakarta yang telah memberikan ilmu dan bantuan yang bermanfaat.
5. Kedua orang tua beserta keluarga tercinta yang senantiasa mendoakan dan memberi dukungan penuh kepada penulis.

6. Semua teman-teman kelas 11-S1-TI 10, teman-teman organisasi, sahabat-sahabat, dan kekasih tercinta yang membantu secara tidak langsung hingga skripsi ini dapat diselesaikan dengan sebaik-baiknya.
7. Semua pihak yang telah membantu dalam penyusunan tugas skripsi ini yang tidak dapat penulis sebutkan satu persatu.

Penulis menyadari bahwa dalam penyusunan skripsi ini masih jauh dari sempurna karena keterbatasan dan minimnya pengalaman penulis. Meskipun demikian penulis berharap segala laporan skripsi ini bermanfaat bagi yang membacanya dan penulis dengan senang hati menerima kritik dan saran yang membangun dari para pembaca.

Akhirnya, semoga laporan skripsi ini dapat bermanfaat bagi penulis dan para pembaca.

Wassalamu'alaikum Wr. Wb.

Yogyakarta, 25 April 2015

M. Urfa Nurfathan

DAFTAR ISI

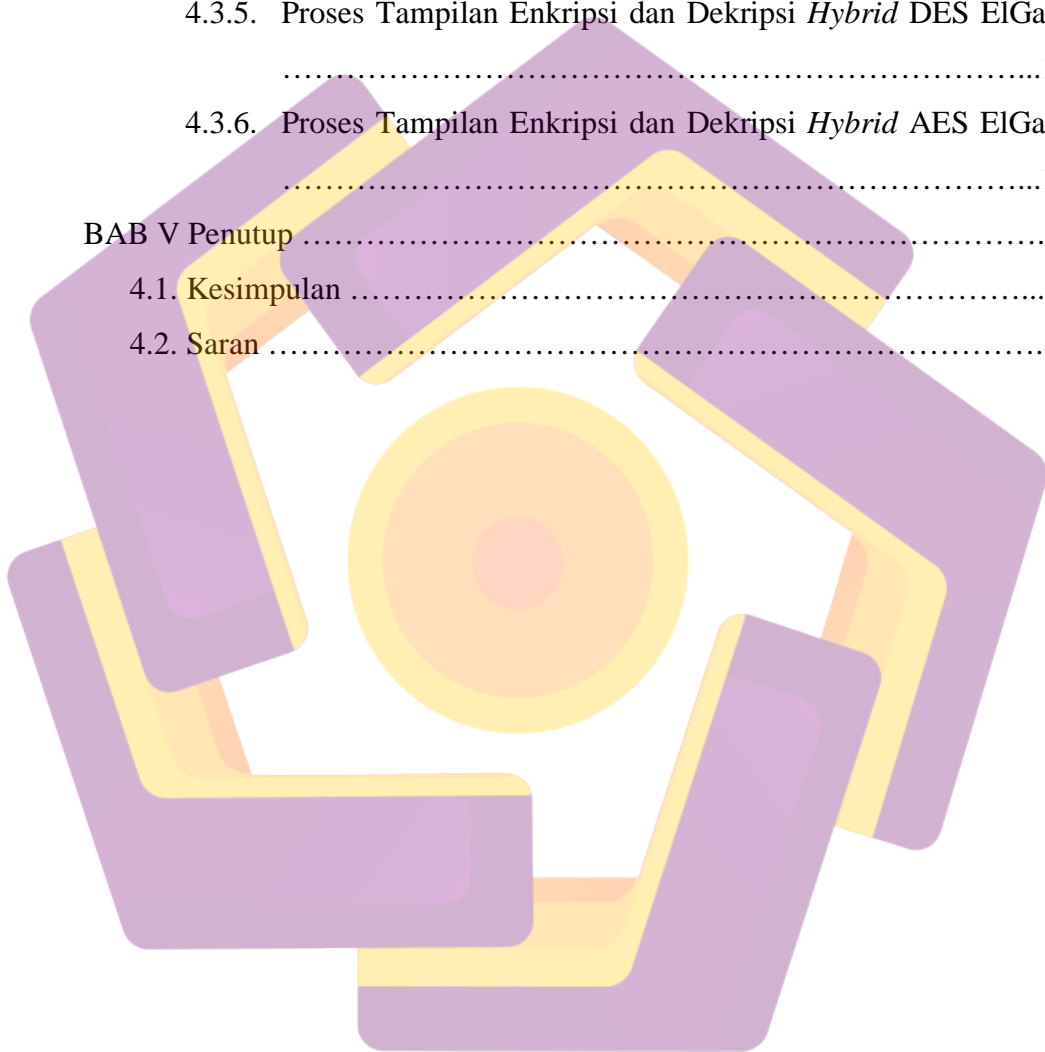
JUDUL	i
PERSETUJUAN	ii
PENGESAHAN	iii
PERNYATAAN	iv
MOTTO	v
PERSEMBAHAN	vii
KATA PENGANTAR	ix
DAFTAR ISI	xi
DAFTAR TABEL	xvi
DAFTAR GAMBAR	xvii
INTISARI	xxiii
ABSTACT	xxiv
BAB I Pendahuluan	1
1.1. Latar Belakang	1
1.2. Rumusan Masalah	3
1.3. Batasan Masalah	4
1.4. Maksud dan Tujuan Penelitian	5
1.4.1. Internal	5
1.4.2. Eksternal	6
1.5. Manfaat Penelitian	7
1.6. Metode Penelitian	8
1.6.1. Metode Analisis	8
1.6.1.1. Analisis SWOT	8
1.6.1.2. Analisis Kebutuhan Sistem	8
1.6.1.3. Analisis Kelayakan Sistem	8
1.6.2. Metode Pengumpulan Data	9
1.6.2.1. Metode Studi Kepustakaan	9
1.6.2.2. Metode Browsing	9
1.6.2.3. Metode Wawancara	9

1.6.3. Metode Perancangan	9
1.6.3.1. UML	10
1.6.3.2. Flowchart	10
1.7. Sistematika Penulisan	10
BAB II Landasan Teori	13
2.1. Tinjauan Pustaka	13
2.2. Kriptografi	15
2.2.1. Konsep Dasar Kriptografi	15
2.2.1.1. Pengertian Kriptografi	15
2.2.1.2. Sejarah Perkembangan Sistem Kriptografi	19
2.2.1.3. Penerapan Kriptografi di Indonesia	25
2.2.2. Komponen Kriptografi	26
2.2.3. Teknik Dasar Kriptografi	27
2.2.4. Algoritma Kriptografi	31
2.2.4.1. Algoritma Simetri	32
2.2.4.2. Algoritma Asimetri	33
2.2.4.3. Hash Function	33
2.2.5. Sistem Kriptografi	34
2.3. DES (<i>Data Encryption Standart</i>)	36
2.3.1. Sejarah DES	36
2.3.2. Algoritma DES	37
2.3.2.1. <i>Initial Permutation</i>	43
2.3.2.2. Pembangkitan Kunci Internal	44
2.3.2.3. Enkripsi dan Dekripsi DES	47
2.4. AES (<i>Advanced Encryption Standart</i>)	48
2.4.1. Sajarah AES	48
2.4.2. Algoritma AES	51
2.4.3. Ekspansi Kunci AES	55
2.4.3.1. Karakteristik Algoritma Ekspansi Kunci AES	58
2.4.4. Enkripsi dan Dekripsi AES	59
2.5. ElGamal	59

2.5.1. Sejarah ElGamal	59
2.5.2. Algoritma ElGamal	60
2.5.3. Pembangkit Kunci ElGamal	61
2.5.4. Enkripsi dan Dekripsi ElGamal	61
2.6. Algoritma Kriptografi Hibrida (<i>Hybrid</i>)	62
2.6.1. Pengertian Kriptografi <i>Hybrid</i>	62
2.6.2. Gambaran Umum Sistem	63
2.7. UML (<i>Unified Modeling Language</i>)	64
2.7.1. Pengenalan UML	64
2.7.2. Konsep Dasar UML	64
2.8. <i>Flowchart</i> (Bagan Alir)	67
2.8.1. <i>Flowchart System</i>	67
2.8.2. <i>Flowchart Program</i>	68
2.9. Pengenalan Perangkat Lunak	69
2.9.1. Sistem Operasi Linux Mint	69
2.9.2. Sejarah Linux Mint	70
2.9.3. Mengetahui Linux Mint	70
2.9.3.1. Tujuan Linux Mint	70
2.9.3.2. Nomor Versi dan Nama Sandi Linux Mint	71
2.9.3.3. Edisi	73
2.10. Bahasa Pemrograman Python	73
2.10.1. Sejarah Bahasa Pemrograman Python	73
2.10.2. Konsep OOP (<i>Object Oriented Programming</i>) pada Python	74
2.10.2.1. <i>Inheritance</i>	75
2.10.2.2. <i>Composition</i>	75
2.10.3. Tentang Bahasa Pemrograman Python	76
2.10.4. Instruksi Bahasa Pemrograman Python	77
2.10.5. Kekurangan dan Kelebihan Bahasa Pemrograman Python	78
BAB III Analisis dan Perancangan	81
3.1. Analisis Sistem	81
3.1.1. Identifikasi Masalah	81

3.1.2.	Analisis SWOT	81
3.1.2.1.	Analisis Kekuatan (<i>Strengths</i>)	82
3.1.2.2.	Analisis Kelemahan (<i>Weakness</i>)	83
3.1.2.3.	Analisis Peluang (<i>Opportunities</i>)	83
3.1.2.4.	Analisis Ancaman (<i>Threats</i>)	84
3.1.3.	Analisis Kebutuhan Sistem	85
3.1.3.1.	Analisis Kebutuhan Fungsional	85
3.1.3.2.	Analisis Kebutuhan Non-Fungsional	86
3.1.4.	Analisis Kelayakan Sistem	88
3.1.4.1.	Analisis Kelayakan Teknologi	88
3.1.4.2.	Analisis Kelayakan Operasional	88
3.1.4.3.	Analisis Kelayakan Hukum	89
3.1.5.	Analisis Pengumpulan Data	89
3.2.	Perancangan Sistem	101
3.2.1.	Perancangan UML	101
3.2.1.1.	<i>Use Case Diagram</i>	102
3.2.1.2.	<i>Activity Diagram</i>	103
3.2.1.3.	<i>Sequence Diagram</i>	109
3.2.1.4.	<i>Class Diagram</i>	112
3.2.2.	Perancangan <i>Flowchart</i>	114
3.2.3.	Perancangan GUI (<i>Graphical User Interface</i>)	116
BAB IV	Implementasi dan Pembahasan	122
4.1.	Implementasi Sistem	122
4.1.1.	Manual Instalasi	122
4.1.1.1.	Instalasi Sublime Text	122
4.1.1.2.	Instalasi PyQt4	125
4.1.1.3.	Instalasi Program Aplikasi	126
4.2.	Pembahasan Program	127
4.2.1.	Pembahasan Main Aplikasi	128
4.2.2.	Pembahasan Tampilan Aplikasi (GUI)	128
4.2.3.	Pembahasan <i>PyCrypto</i> untuk Enkripsi dan Dekripsi	146

4.3. Implementasi dan Pembahasan Tampilan	152
4.3.1. Proses Tampilan Awal	153
4.3.2. Proses Tampilan Enkripsi dan Dekripsi DES	154
4.3.3. Proses Tampilan Enkripsi dan Dekripsi AES	156
4.3.4. Proses Tampilan Enkripsi dan Dekripsi ElGamal	158
4.3.5. Proses Tampilan Enkripsi dan Dekripsi <i>Hybrid</i> DES ElGamal	162
4.3.6. Proses Tampilan Enkripsi dan Dekripsi <i>Hybrid</i> AES ElGamal	164
BAB V Penutup	166
4.1. Kesimpulan	166
4.2. Saran	167



DAFTAR TABEL

Tabel 2.1 <i>Expansion Permutation (E)</i>	39
Tabel 2.2 <i>DES S-Box</i>	40
Tabel 2.3 <i>Permutasi P</i>	41
Tabel 2.4 <i>Boks Permutasi IP</i>	44
Tabel 2.5 <i>Boks Permutasi IP^{-1}</i>	44
Tabel 2.6 <i>Boks Permutasi IP^1</i>	45
Tabel 2.7 <i>Jumlah Pergeseran Bit pada Setiap Putaran</i>	45
Tabel 2.8 <i>Permutasi Pilihan Dua (PC-2)</i>	46
Tabel 2.9 <i>Hubungan antara Panjang Ronde dan Panjang Kunci AES</i>	52
Tabel 2.10 <i>S-Box Rijndael</i>	53
Tabel 2.11 <i>Konstan RC dalam Hexadesimal</i>	57
Tabel 2.12 <i>Simbol-simbol Use Case Diagram</i>	65
Tabel 2.13 <i>Simbol-simbol Activity Diagram</i>	65
Tabel 2.14 <i>Simbol-simbol Sequence Diagram</i>	66
Tabel 2.15 <i>Simbol-simbol Class Diagram</i>	66
Tabel 2.16 <i>Versi, Nama Sandi dan Keterangan dalam Linux Mint</i>	72
Tabel 3.1 <i>Analisis SWOT</i>	84

DAFTAR GAMBAR

Gambar 2.1 (a) Sebuah scytale; (b) Pesan ditulis secara horizontal, baris per baris. Bila kertas dilepaskan, maka pesan yang terbentuk adalah <i>cipher text</i>	20
Gambar 2.2 Mesin enkripsi Enigma yang digunakan oleh tentara Jerman pada masa Perang Dunia ke-2. Enigma <i>cipher</i> berhasil dipecahkan oleh Sekutu	22
Gambar 2.3 Mesin Kriptografi yang pernah digunakan	25
Gambar 2.4 Contoh Teknik Substitusi Algoritma <i>Caesar Cipher</i>	28
Gambar 2.5 Contoh Teknik Blocking	29
Gambar 2.6 Pembagian Blok pada Teknik Permutasi	30
Gambar 2.7 Proses Enkripsi dengan Teknik Permutasi	30
Gambar 2.8 Contoh Teknik Ekspansi	31
Gambar 2.9 Contoh Teknik Pemampatan	31
Gambar 2.10 Sistem Kriptografi Konvensional	35
Gambar 2.11 Putaran Pertama Enkripsi DES	38
Gambar 2.12 Rincian DES fungsi <i>f</i>	39
Gambar 2.13 Pemakaian Kunci pada DES	41
Gambar 2.14 Gambaran Umum Algoritma DES	42
Gambar 2.15 Proses Pembangkitan Kunci Internal	47
Gambar 2.16 Unit Data AES	52
Gambar 2.17 Transformasi Pergeseran Baris	53
Gambar 2.18 Transformasi Percampuran Kolom	54
Gambar 2.19 Transformasi Penambahan Kunci dengan Operasi XOR	55

Gambar 2.20 Ekspansi Kunci AES 128 bit	57
Gambar 2.21 Proses Umum Enkripsi dan Dekripsi Algoritma AES	59
Gambar 2.22 Sistem Kriptografi dengan Kunci Publik ElGamal	60
Gambar 2.23 Enkripsi Hibrida	63
Gambar 2.24 Dekripsi Hibrida	63
Gambar 2.25 <i>Interpreter Python</i>	76
Gambar 2.26 <i>Compiler Python</i>	77
Gambar 3.1 <i>Use Case Diagram</i>	103
Gambar 3.2 <i>Activity Diagram</i> Enkripsi dan Dekripsi Kriptografi DES	104
Gambar 3.3 <i>Activity Diagram</i> Enkripsi dan Dekripsi Kriptografi AES	105
Gambar 3.4 <i>Activity Diagram</i> Enkripsi dan Dekripsi Kriptografi ElGamal	106
Gambar 3.5 <i>Activity Diagram</i> Enkripsi dan Dekripsi Kriptografi Hybrid (DES ElGamal)	107
Gambar 3.6 <i>Activity Diagram</i> Enkripsi dan Dekripsi Kriptografi Hybrid (AES ElGamal)	108
Gambar 3.7 <i>Sequence Diagram</i> Enkripsi dan Dekripsi Kriptografi DES	109
Gambar 3.8 <i>Sequence Diagram</i> Enkripsi dan Dekripsi Kriptografi AES	110
Gambar 3.9 <i>Sequence Diagram</i> Enkripsi dan Dekripsi Kriptografi ElGamal ...	110
Gambar 3.10 <i>Sequence Diagram</i> Enkripsi dan Dekripsi Kriptografi Hybrid (DES ElGamal)	111
Gambar 3.11 <i>Sequence Diagram</i> Enkripsi dan Dekripsi Kriptografi Hybrid (AES ElGamal)	111
Gambar 3.12 <i>Class Diagram</i> Aplikasi Kriptografi	113

Gambar 3.13 <i>Flowchart</i> Algoritma Kriptografi DES dalam Aplikasi Kriptografi	114
Gambar 3.14 <i>Flowchart</i> Algoritma Kriptografi AES dalam Aplikasi Kriptografi	114
Gambar 3.15 <i>Flowchart</i> Algoritma Kriptografi ElGamal dalam Aplikasi Kriptografi	115
Gambar 3.16 <i>Flowchart</i> Algoritma Kriptografi DES dan ElGamal dalam Aplikasi Kriptografi	115
Gambar 3.17 <i>Flowchart</i> Algoritma Kriptografi AES dan ElGamal dalam Aplikasi Kriptografi	116
Gambar 3.18 Rancangan Enkripsi dan Dekripsi Kriptografi DES	117
Gambar 3.19 Rancangan Enkripsi dan Dekripsi Kriptografi AES	118
Gambar 3.20 Rancangan Enkripsi dan Dekripsi Kriptografi ElGamal	119
Gambar 3.21 Rancangan Enkripsi dan Dekripsi Kriptografi Hybrid (DES ElGamal)	120
Gambar 3.22 Rancangan GUI Enkripsi dan Dekripsi Kriptografi Hybrid (AES ElGamal)	121
Gambar 4.1 Tampilan <i>Terminal</i>	123
Gambar 4.2 Proses Penambahan <i>Repository</i>	124
Gambar 4.3 Proses <i>Update Package Install</i> Sublime Text	124
Gambar 4.4 Proses Konfirmasi untuk Melanjutkan Instalasi Sublime Text	125
Gambar 4.5 Proses PyQt4 yang sudah ter- <i>install</i>	126
Gambar 4.6 Proses Menjalankan <i>mainApps.py</i> dengan Terminal	127

Gambar 4.7 <i>Source Code</i> mainApps.py	128
Gambar 4.8 Modul-modul yang dimasukkan dalam <i>File</i> mainWidget.py	129
Gambar 4.9 Potongan <i>Source Code</i> dalam <i>Method</i> setupUI	130
Gambar 4.10 Potongan <i>Source Code</i> dalam <i>Method</i> retranslateUI	130
Gambar 4.11 <i>Source Code</i> dalam <i>Method</i> initialize dan <i>Method</i> hideComponent	131
Gambar 4.12 Potongan <i>Source Code</i> dalam <i>Method</i> setButtonSignal	132
Gambar 4.13 <i>Method</i> doEncryptDES untuk Proses Enkripsi DES	133
Gambar 4.14 <i>Method</i> doDecryptDES untuk Proses Dekripsi DES	133
Gambar 4.15 <i>Method</i> doEncryptAES untuk Proses Enkripsi AES	134
Gambar 4.16 <i>Method</i> doDecryptAES untuk Proses Dekripsi AES	134
Gambar 4.17 <i>Method</i> generateKeyElGamal untuk Proses Pembuatan <i>Public Key</i> dan <i>Private Key</i> ElGamal	135
Gambar 4.18 <i>Method</i> loadPrivateKeyElgamal dan <i>Method</i> loadPublicKeyElgamal untuk Proses Pengambilan <i>File</i> Kunci yang Pernah Dibuat	136
Gambar 4.19 <i>Method</i> doEncryptElgamal untuk Proses Enkripsi ElGamal	137
Gambar 4.20 <i>Method</i> doDecryptElgamal untuk Proses Dekripsi ElGamal	138
Gambar 4.21 <i>Method</i> generateKeyDesElGamal untuk Proses Pembuatan <i>Public Key</i> dan <i>Private Key</i> DES ElGamal	138
Gambar 4.22 <i>Method</i> loadPrivateKeyDesElgamal dan <i>Method</i> loadPublicKeyDesElgamal untuk Proses Pengambilan <i>File</i> Kunci yang Pernah Dibuat	139

Gambar 4.23 <i>Method doEncryptDesElgamal</i> untuk Proses Enkripsi DES ElGamal	140
Gambar 4.24 <i>Method doDecryptDesElgamal</i> untuk Proses Dekripsi DES ElGamal	140
Gambar 4.25 <i>Method Method generateKeyAesElGamal</i> untuk Proses Pembuatan <i>Public Key</i> dan <i>Private Key</i> AES ElGamal	141
Gambar 4.26 <i>Method loadPrivateKeyAesElgamal</i> dan <i>Method</i> <i>loadPublicKeyAesElgamal</i> untuk Proses Pengambilan <i>File</i> Kunci yang Pernah Dibuat	142
Gambar 4.27 <i>Method doEncryptAesElgamal</i> untuk Proses Enkripsi AES ElGamal	143
Gambar 4.28 <i>Method doDecryptAesElgamal</i> untuk Proses Dekripsi AES ElGamal	143
Gambar 4.29 <i>Method moreThanMaxElgamalPlaintextAllowed</i> dalam Proses Enkripsi Dekripsi ElGamal	144
Gambar 4.30 <i>Method moreThanMaxDesPasswordAllowed</i> dalam Proses Enkripsi Dekripsi DES	145
Gambar 4.31 <i>Method showError</i> dan <i>method showInfo</i>	146
Gambar 4.32 Tampilan Awal Aplikasi dijalankan	153
Gambar 4.33 Tampilan Enkripsi Dekripsi DES	155
Gambar 4.34 Tampilan Implementasi dari Perhitungan Manual DES	156
Gambar 4.35 Tampilan Enkripsi Dekripsi AES	157
Gambar 4.36 Tampilan Implementasi dari Perhitungan Manual AES	158

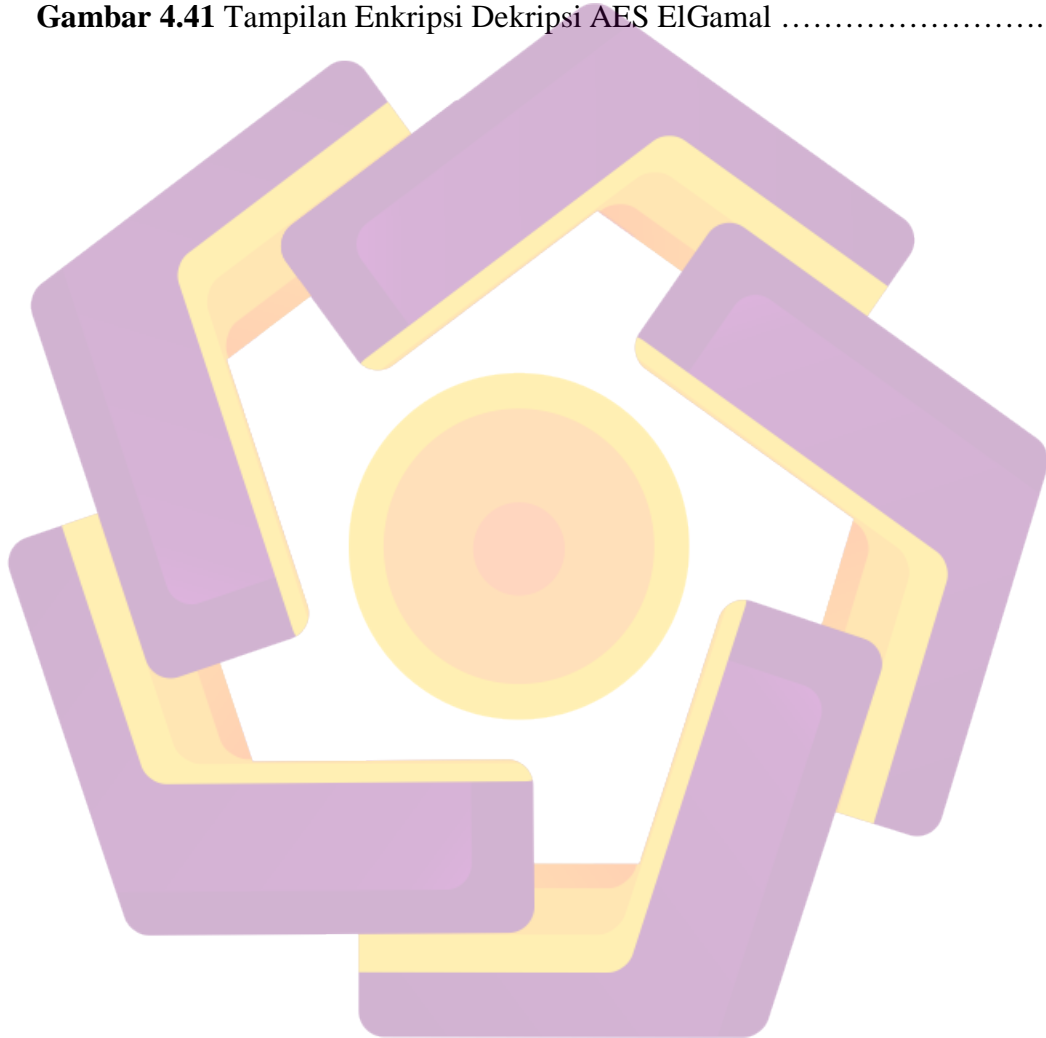
Gambar 4.37 Tampilan Proses Pembuatan *Public Key* dan *Private Key*160

Gambar 4.38 Tampilan Enkripsi Dekripsi ElGamal161

Gambar 4.39 Tampilan Implementasi dari Perhitungan Manual ElGamal162

Gambar 4.40 Tampilan Enkripsi Dekripsi DES ElGamal164

Gambar 4.41 Tampilan Enkripsi Dekripsi AES ElGamal165



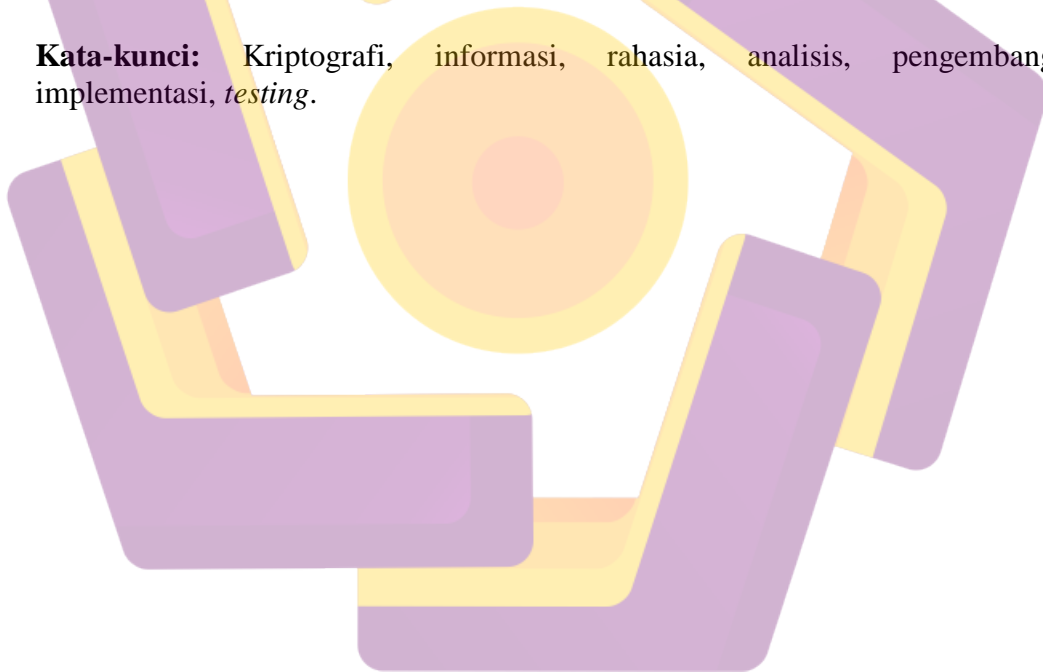
INTISARI

Informasi di era globalisasi ini merupakan peran penting dalam kehidupan sehari-hari, khususnya dalam dunia bisnis. Hal penting yang menjadi bahan analisis yang dilakukan oleh peneliti adalah tentang informasi rahasia. Selama ini informasi-informasi yang seharusnya rahasia masih dapat diketahui orang lain. Adapun langkah yang diupayakan untuk merahasiakan informasi tersebut sudah dilakukan. Beberapa pertanyaan yang muncul: Upaya apa lagi yang dilakukan untuk merahasiakan informasi? Bagaimana cara merahasiakannya?

Pada skripsi ini, peneliti mencoba untuk menganalisis dan mengusulkan solusi guna menyelesaikan pokok-pokok masalah yang ada. Menggunakan metode analisis sistem SWOT. Melakukan perancangan model proses menggunakan ERD dan Flowchart.

Aplikasi yang dihasilkan berbentuk prototype base-on desktop “PyCryptoTools”, yang ditujukan untuk memberikan solusi dalam pengiriman maupun penerimaan informasi rahasia. Di samping itu, peneliti juga menambahkan agar informasi yang sudah dirahasiakan selalu berubah-ubah dengan tujuan keamanan yang terjamin tanpa mengubah informasi aslinya.

Kata-kunci: Kriptografi, informasi, rahasia, analisis, pengembangan, implementasi, *testing*.



ABSTRACT

Information in this era of globalization is an important role in everyday life, especially in the business world. It is important that the subject of the analysis conducted by researchers is about confidential information. So far, the information confidential should still be known to others. The steps that attempted to conceal the information was done. Several questions arise: What other efforts are being made to conceal information? How do I keep it a secret?

In this thesis, the researcher tried to analyze and propose solutions to resolve the issues of the present. SWOT system analysis method. Do the designing process models using the ERD and Flowchart.

Generated application form on the desktop prototype base "PyCryptoTools", which is intended to provide a solution in the delivery and receipt of confidential information. In addition, the researchers also added that the information that has been withheld always changing with guaranteed security purposes without change original information.

Keywords: *Cryptography, information, confidential, analysis, development, implementation, testing.*

