

**IMPLEMENTASI *HYBRID CRYPTOSYSTEM*  
MENGGUNAKAN ALGORITMA AES DAN LUC UNTUK  
KEAMANAN PESAN**

Diajukan Sebagai Syarat Untuk Menyelesaikan  
Pendidikan Program Strata-1 Pada  
Jurusan Teknik Informatika



Oleh :

Muhammad Farhan  
NIM : 09021181722012

**Jurusan Teknik Informatika  
FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA  
2021**

## **LEMBAR PENGESAHAN SKRIPSI**

**Implementasi *Hybrid Cryptosystem* Menggunakan Algoritma AES  
dan LUC untuk Keamanan Pesan**

**Oleh :**

**MUHAMMAD FARHAN**

**NIM : 09021181722012**

Palembang, 10 Januari 2022

**Pembimbing I**



Alfarissi, M.Comp.Sc.  
NIP. 198512152014041001

**Pembimbing II,**



M. Naufal Rachmatullah, M.T.  
NIP. 1671060112920006

**Mengetahui,  
Ketua Jurusan Teknik Informatika**



Alvi Syahrini Utami, M.Kom.  
NIP. 197812222006042003

## TANDA LULUS UJIAN SIDANG SKRIPSI

Pada hari Rabu tanggal 05 Januari 2022 telah dilaksanakan ujian sidang skripsi oleh Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya

Nama : Muhammad Farhan  
NIM : 09021181722012  
Judul : Implementasi *Hybrid Cryptosystem* Menggunakan Algoritma AES dan LUC untuk Keamanan Pesan

1. Ketua

Alvi Syahrini Utami, M.Kom.  
NIP. 197812222006042003



2. Pembimbing I

Alfanissi, M.Comp.Sc  
NIP. 198512152014041001

3. Pembimbing II

M. Naufal Rachmatullah, M.T.  
NIP. 198908062015042002



4. Penguji I

Osvari Arsalan, M.T.  
NIP. 1601142806880003

5. Penguji II

Anggina Primanita, M.I.T., Ph.D.  
NIP. 198908062015042002



Mengetahui,  
Ketua Jurusan Teknik Informatika



Alvi Syahrini Utami, M.Kom.  
NIP. 197812222006042003

## **HALAMAN PERNYATAAN**

Yang bertanda tangan dibawah ini : :

Nama : Muhammad Farhan  
NIM : 09021181722012  
Program Studi : Teknik Informatika Reguler  
Judul Skripsi : Implementasi *Hybrid Cryptosystem*  
Dengan Menggunakan Algoritma  
AES dan LUC untuk Keamanan Pesan

Hasil Pengecekan Software *iThenticate /Turnitin* : 11%

Menyatakan bahwa Laporan Projek saya merupakan hasil karya sendiri dan bukan hasil penjiplakan/plagiat. Apabila ditemukan unsur penjiplakan/plagiat dalam laporan projek ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian pernyataan ini saya buat dengan sebenarnya dan tidak ada paksaan oleh siapapun.

Palembang, 5 Januari 2021



(Muhammad Farhan)

NIM. 09021181722012

## **MOTTO DAN PERSEMPAHAN**

Motto:

- If at first, you don't succeed, try, try again and don't forget to take a breath.
- Where there's a will, there's a way.
- Progress, not perfection.
- If you keep thinking and do nothing, you will be left far behind

Kupersembahkan Karya Tulis ini kepada:

- Allah SWT
- Alm Ayah, Ibu, dan kakakku yang selalu mendukung.
- Dosen-dosen pengajarku yang selalu sabar dan membimbing dengan ikhlas.
- Teman-teman seperjuangan yang selalu ada untuk membantu dalam pembuatan skripsi, tidak bisa disebut satu persatu, tetapi saya ucapkan terima kasih atas bantuannya

**HYBRID CRYPTOSYSTEM IMPLEMENTATION  
USING AES AND LUC ALGORITHM FOR MESSAGE SECURITY**

By  
Muhammad Farhan  
09021181722012

**ABSTRACT**

In data and telecommunications, cryptography is required when communicating over untrusted media which includes almost all communication networks especially on the Internet. This study applies a cryptography technique called hybrid cryptosystem, which is a technique of combining the symmetric and asymmetric algorithms of cryptography, using the security and speed of the symmetric algorithm along with the strength of the asymmetric algorithm in distributing secure keys. The symmetry algorithm used is the AES algorithm while the asymmetric algorithm used is the LUC algorithm. Based on the test results, it can be concluded that the combination of the AES and LUC algorithms in this hybrid cryptosystem method can work well and is considered strong in terms of security because it has an avalanche effect value that meets the criteria with a value of 49.97% for the AES algorithm and 53.52% for the LUC algorithm.

*Keywords:* Cryptography, Hybrid Cryptosystem, AES Algorithm, LUC Algorithm, Avalanche Effect

**IMPLEMENTASI HYBRID CRYPTOSYSTEM MENGGUNAKAN  
ALGORITMA AES DAN LUC UNTUK KEAMANAN PESAN**

Oleh  
Muhammad Farhan  
09021181722012

**ABSTRAK**

Dalam data dan telekomunikasi, kriptografi diperlukan ketika berkomunikasi melalui media yang tidak dapat dipercaya yang mencakup hampir semua jaringan komunikasi terutama di Internet. Penelitian ini menerapkan teknik kriptografi *hybrid cryptosystem* yaitu teknik menggabungkan algoritma simetri dan asimetri dari kriptografi, menggunakan keamanan dan kecepatan algoritma simetri bersama dengan kekuatan algoritma asimetri dalam mendistribusikan kunci yang aman. Algoritma simetri yang digunakan adalah algoritma AES sedangkan algoritma asimetri yang digunakan adalah algoritma LUC. Berdasarkan hasil percobaan pengujian dapat disimpulkan bahwa perpaduan algoritma AES dan LUC dalam metode hybrid cryptosystem ini dapat bekerja dengan baik dan termasuk kuat dari segi keamanan karena memiliki nilai avalanche effect yang memenuhi kriteria dengan nilai 49.97% untuk algoritma AES dan 53.52% untuk algoritma LUC.

Kata kunci: Kriptografi, Hybrid Cryptosystem, Algoritma AES, Algoritma LUC, *Avalanche Effect*

## KATA PENGANTAR

Puji syukur kepada Allah SWT atas segala rahmat dan karunia-Nya penulis dapat menyelesaikan Skripsi ini dengan baik. Skripsi ini disusun untuk memenuhi salah satu syarat dalam menyelesaikan pendidikan program Strata-1 Program Studi Teknik Informatika pada Fakultas Ilmu Komputer, Universitas Sriwijaya.

Penulis ingin mengucapkan terima kasih kepada seluruh pihak yang telah memberikan bantuan dan dukungan baik dalam materil maupun moril selama proses pembuatan skripsi ini.

Semoga skripsi ini dapat bermanfaat bagi penulis khususnya maupun pembaca pada umumnya. Serta dapat menjadi referensi dan rujukan bagi hal-hal yang bermanfaat. Penulis menyadari bahwa dalam proses penyelesaian skripsi ini, terdapat beberapa penjelasan yang kurang sempurna. Oleh karena itu penulis mengharapkan kritik dan saran yang membangun agar skripsi ini menjadi karya tulis yang sempurna supaya terciptanya bekal pengetahuan yang baik bagi peneliti di masa depan.

Palembang, 30 Desember 2021



Muhammad Farhan

## **DAFTAR ISI**

	Halaman
HALAMAN JUDUL .....	i
LEMBAR PENGESAHAN SKRIPSI .....	ii
TANDA LULUS UJIAN SIDANG SKRIPSI.....	iii
MOTTO DAN PERSEMBERAHAN.....	iv
HALAMAN PERNYATAAN .....	vi
ABSTRACT .....	vi
ABSTRAK .....	vii
KATA PENGANTAR .....	viii
DAFTAR ISI .....	viii
DAFTAR TABEL .....	xiii
DAFTAR GAMBAR .....	xv
BAB I PENDAHULUAN	
1.1 Pendahuluan.....	I-1
1.2 Latar Belakang.....	I-1
1.3 Rumusan Masalah.....	I-4
1.4 Tujuan Penelitian .....	I-5
1.5 Manfaat Penelitian .....	I-5
1.6 Batasan Masalah .....	I-6
1.7 Sistematika Penulisan.....	I-6
1.8 Kesimpulan.....	I-8
BAB II KAJIAN LITERATUR	
2.1 Pendahuluan.....	II-1
2.2 Landasan Teori .....	II-1
2.2.1 Kriptografi .....	II-1
2.2.2 Algoritma Simetri .....	II-2
2.2.3 Algoritma Asimetri .....	II-3

2.2.4	<i>Hybrid Cryptosystem</i> .....	II-3
2.2.5	Algoritma AES .....	II-5
2.2.5.1	Proses Enkripsi AES.....	II-7
2.2.5.2	Proses Dekripsi AES.....	II-10
2.2.5.3	Proses Ekspansi kunci AES .....	II-12
2.2.5.4	Mode Operasi AES.....	II-13
2.2.6	Algoritma LUC .....	II-14
2.2.6.1	Proses Pembangkitan Kunci LUC .....	II-16
2.2.6.2	Proses Enkripsi LUC .....	II-17
2.2.6.3	Proses Dekripsi LUC .....	II-18
2.2.7	Pengkodean Karakter .....	II-18
2.2.8	Avalanche Effect.....	II-19
2.3	Penelitian Terdahulu yang Relevan .....	II-20
2.3.1	<i>Hybrid Implementation of Twofish, AES, ElGamal and RSA Cryptosystems</i> .....	II-20
2.3.2	<i>Comparative Study of LUC, ElGamal, and RSA Algorithm in Encoding Texts</i> .....	II-21
2.4	Kesimpulan.....	II-22

### BAB III METODOLOGI PENELITIAN

3.1	Pendahuluan.....	III-1
3.2	Pengumpulan Data.....	III-1
3.2.1	Jenis Data .....	III-1
3.2.2	Sumber Data .....	III-1
3.3	Tahapan Penelitian.....	III-2
3.3.1	Kerangka Kerja .....	III-2
3.3.2	Kriteria Pengujian .....	III-2
3.3.3	Format Data Pengujian.....	III-4
3.3.4	Alat yang Digunakan dalam Pelaksanaan Penelitian.....	III-5
3.3.5	Pengujian Penelitian.....	III-6
3.3.6	Analisis Hasil Pengujian dan Kesimpulan .....	III-6
3.4	Metode Pengembangan Perangkat Lunak .....	III-8
3.4.1	Rational Unified Process.....	III-8

3.4.2 Fase Insepsi .....	III-10
3.4.3 Fase Elaborasi.....	III-10
3.4.4 Fase Konstruksi .....	III-10
3.4.5 Fase Transisi.....	III-11
3.5 Manajemen Proyek Penelitian.....	III-11
3.6 Kesimpulan.....	III-20

#### BAB IV PENGEMBANGAN PERANGKAT LUNAK

4.1 Pendahuluan.....	IV-1
4.2 Fase Insepsi.....	IV-1
4.2.1 Pemodelan Bisnis.....	IV-1
4.2.2 Kebutuhan Sistem .....	IV-3
4.2.3 Analisis dan Desain.....	IV-5
4.2.3.1 Analisis Kebutuhan Perangkat Lunak.....	IV-5
4.2.3.2 Desain Perangkat Lunak .....	IV-6
4.3 Fase Elaborasi.....	IV-20
4.3.1 Pemodelan Bisnis.....	IV-20
4.3.3.1 Desain Data .....	IV-20
4.3.3.2 Desain Antarmuka .....	IV-21
4.3.2 Kebutuhan Sistem .....	IV-24
4.3.3 Diagram <i>Sequence</i> .....	IV-25
4.4 Fase Konstruksi.....	IV-28
4.4.1 Kebutuhan Sistem .....	IV-29
4.4.2 Diagram Kelas .....	IV-29
4.4.3 Implementasi .....	IV-30
4.4.3.1 Implementasi Kelas .....	IV-30
4.4.3.2 Implementasi Antarmuka.....	IV-32
4.5 Fase Transisi.....	IV-35
4.5.1 Pemodelan Bisnis.....	IV-35
4.5.2 Kebutuhan Sistem .....	IV-35
4.5.3 Rencana Pengujian.....	IV-36
4.5.3.1 Rencana Pengujian <i>Use Case</i> Mengenkripsi Pesan....	IV-36

4.5.3.2 Rencana Pengujian <i>Use Case</i> Mendekripsi Pesan.....	IV-36
4.5.3.3 Rencana Pengujian <i>Use Case</i> Pembangkitan Kunci...IV-36	
4.5.3.4 Rencana Pengujian dari <i>Use Case</i> Menguji <i>Avalanche Effect</i> .....	IV-37
4.5.3.5 Rencana Pengujian dari <i>Use Case</i> Menguji Enkripsi ..... Kelompok .....	IV-37
4.5.4 Implementasi .....	IV-38
4.5.4.1 Pengujian <i>Use Case</i> Mengenkripsi Pesan.....	IV-38
4.5.4.2 Pengujian dari <i>Use Case</i> Mendekripsi Pesan.....	IV-40
4.5.4.3 Pengujian dari <i>Use Case</i> Pembangkitan Kunci.....	IV-43
4.5.4.4 Pengujian <i>Use Case</i> Menguji Avalanche Effect .....	IV-45
4.5.4.5 Pengujian <i>Use Case</i> Menguji Enkripsi Kelompok ....	IV-48
4.6 Kesimpulan.....	IV-52

## BAB V HASIL DAN ANALISA PENELITIAN

5.1 Pendahuluan.....	V-1
5.2 Hasil Percobaan Penelitian .....	V-1
5.2.1 Hasil Skenario 1.....	V-2
5.2.2 Hasil Skenario 2.....	V-9
5.2.3 Hasil Skenario 3.....	V-16
5.3 Analisis Hasil Penelitian .....	V-23
5.4 Kesimpulan.....	V-27

## BAB VI KESIMPULAN DAN SARAN .....

6.1 Kesimpulan.....	VI-1
6.2 Saran.....	VI-1

## DAFTAR PUSTAKA .....

xvi

## LAMPIRAN

## DAFTAR TABEL

	Halaman
Tabel II-1. Tabel Perbandingan Jumlah Round dan Key Algoritma AES.....	II-6
Tabel II-2. Nilai Awal Dari Barisan Lucas .....	II-15
Tabel II-3. Tabel Perbedaan UTF-16BE dan UTF-16LE .....	II-19
Tabel II-4. Perbandingan Waktu Enkripsi Algoritma Kriptografi .....	II-20
Tabel III-1. Hasil Uji Avalanche Effect AES .....	III-4
Tabel III-2. Hasil Uji Avalanche Effect LUC .....	III-4
Tabel III-3. Hasil Uji Lama Waktu Proses Enkripsi dan Dekripsi.....	III-5
Tabel III-4. Analisis Hasil Uji Avalanche Effect AES .....	III-7
Tabel III-5. Analisis Hasil Uji Avalanche Effect LUC .....	III-7
Tabel III-6. Analisis Hasil Uji Total Perubahan Bit.....	III-7
Tabel III-7. Analisis Hasil Uji Lama Waktu Proses Enkripsi dan Dekripsi .....	III-7
Tabel III-5. Tabel Penjadwalan Penelitian dalam Bentuk <i>Work Breakdown Structure</i> (WBS) .....	III-12
Tabel IV-1. Kebutuhan Fungsional Software Perangkat Lunak .....	IV-2
Tabel IV-2. Kebutuhan Non-Fungsional Perangkat Lunak .....	IV-2
Tabel IV-3. Definisi Aktor <i>Use Case Diagram</i> .....	IV-7
Tabel IV-4. Definisi <i>Use Case Diagram</i> .....	IV-7
Tabel IV-5. Skenario <i>Use Case</i> Mengenkripsi Pesan.....	IV-9
Tabel IV-6. Skenario <i>Use Case</i> Mendekripsi Pesan.....	IV-10
Tabel IV-7. Skenario <i>Use Case</i> Membangkitkan Kunci .....	IV-11
Tabel IV-8. Skenario <i>Use Case</i> Menguji <i>Avalanche Effect</i> .....	IV-12
Tabel IV-9. Menguji Enkripsi Kelompok .....	IV-13
Tabel IV-10. Daftar Implementasi Kelas .....	IV-30
Tabel IV-11. Rencana Pengujian <i>Use Case</i> Mengenkripsi Pesan .....	IV-36
Tabel IV-12. Rencana Pengujian <i>Use Case</i> Mendekripsi Pesan .....	IV-36
Tabel IV-13. Rencana Pengujian <i>Use Case</i> Pembangkitan Kunci .....	IV-36
Tabel IV-14. Rencana Pengujian <i>Use Case</i> Menguji <i>Avalanche Effect</i> .....	IV-37
Tabel IV-15. Rencana Pengujian <i>Use Case</i> Menguji Enkripsi Kelompok .....	IV-37
Tabel IV-16. Pengujian <i>Use Case</i> Mengenkripsi Pesan .....	IV-39
Tabel IV-17. Pengujian <i>Use Case</i> Mengenkripsi Pesan .....	IV-41
Tabel IV-18. Pengujian dari <i>Use Case</i> Pembangkitan Kunci .....	IV-44
Tabel IV-19. Pengujian <i>Use Case</i> Menguji <i>Avalanche Effect</i> .....	IV-46
Tabel IV-20. Pengujian <i>Use Case</i> Menguji Enkripsi Kelompok .....	IV-49
Tabel V- 1. Skenario 1 Uji Avalanche Effect AES .....	V-2
Tabel V- 2. Skenario 1 Uji Avalanche Effect LUC.....	V-5
Tabel V- 3. Skenario 1 Uji Enkripsi Kelompok .....	V-6
Tabel V- 4. Skenario 2 Uji Avalanche Effect AES .....	V-9
Tabel V- 5. Skenario 2 Uji Avalanche Effect LUC.....	V-12
Tabel V- 6. Skenario 2 Uji Enkripsi Kelompok .....	V-14

Tabel V- 7. Skenario 3 Uji Avalanche Effect AES .....	V-16
Tabel V- 8. Skenario 3 Uji Avalanche Effect LUC.....	V-19
Tabel V- 9. Skenario 3 Uji Enkripsi Kelompok.....	V-21
Tabel V-10. Analisis Hasil Uji Avalanche Effect AES .....	V-23
Tabel V-11. Analisis Hasil Uji Avalanche Effect LUC.....	V-23
Tabel V-12. Analisis Hasil Uji Total Perubahan Bit.....	V-25
Tabel V- 13. Analisis Hasil Uji Lama Waktu Proses AES+LUC .....	V-26

## DAFTAR GAMBAR

	Halaman
Gambar II-1. Diagram Proses Enkripsi dan Dekripsi Kriptografi.....	II-1
Gambar II-2. Diagram Proses Enkripsi dan Dekripsi Algoritma Simetri.....	II-2
Gambar II-3. Diagram Proses Enkripsi dan Dekripsi Algoritma Asimetri.....	II-3
Gambar II-4. Diagram Proses Enkripsi Hybrid Cryptosystem (Jintcharadze dan Iavich, 2020).....	II-4
Gambar II-5. Diagram Proses Enkripsi Algoritma AES.....	II-7
Gambar II-6. Tabel <i>S-Box</i> .....	II-8
Gambar II-7. Ilustrasi Proses <i>Shiftrows</i> Pada State Matriks 4x4 .....	II-9
Gambar II-8. Ilustrasi Proses <i>Mixcolumns</i> Pada State Matriks 4x4 .....	II-9
Gambar II-9. Diagram Proses Dekripsi Algoritma AES .....	II-10
Gambar II-10. Ilustrasi Proses <i>Shiftrows</i> Pada State Matriks 4x4.....	II-11
Gambar II-11. Tabel <i>Invers S-Box</i> .....	II-11
Gambar II-12. Ilustrasi Proses <i>Mixcolumns</i> Pada State Matriks 4x4 .....	II-12
Gambar II-13. Artisitktur Mode Enkripsi <i>Electroic Codebook (ECB)</i> .....	II-13
Gambar II-14. Definisi Bilangan Lucas atau $L_n$ .....	II-14
Gambar II-15. Perbandingan Ukuran File Enkripsi AES dan Twofish .....	II-21
Gambar II-16. Perbandingan Waktu Enkripsi dan Dekripsi Algoritma Asimetri.....	II-21
Gambar III-1. Diagram Kerangka Kerja Penelitian.....	III-2
Gambar III-2. Diagram Tahap Pengujian Penelitian .....	III-6
Gambar III-3. Arsitektur Rational Unified Process (Kruchten, 2000) .....	III-9
Gambar III-4. Penjadwalan Untuk Tahap Identifikasi Masalah.....	III-16
Gambar III-5. Penjadwalan Untuk Studi Literatur dan Menentukan Kriteria..... Pengujian.....	III-17
Gambar III-6. Penjadwalan Untuk Tahap Pengembangan Perangkat Lunak Fase Insepsi .....	III-17
Gambar III-7. Penjadwalan Untuk Tahap Pengembangan Perangkat Lunak Fase Elaborasi.....	III-18
Gambar III-8. Penjadwalan Untuk Tahap Pengembangan Perangkat Lunak Fase Konstruksi .....	III-18
Gambar III-9. Penjadwalan Untuk Tahap Pengembangan Perangkat Lunak Fase Transisi.....	III-19
Gambar III-10. Penjadwalan Untuk Tahap Analisis Hasil Pengujian danKesimpulan .....	III-19
Gambar IV-1. <i>Use Case Diagram</i> .....	IV-6
Gambar IV-2. <i>Activity Diagram</i> Mengenkripsi Pesan.....	IV-15
Gambar IV-3. <i>Activity Diagram</i> Mendekripsi Pesan.....	IV-16
Gambar IV-4. <i>Activity Diagram</i> Pembangkitan Kunci.....	IV-17
Gambar IV-5. <i>Activity Diagram</i> Pengujian <i>Avalanche Effect</i> .....	IV-18
Gambar IV-6. <i>Activity Diagram</i> Pengujian Enkripsi Kelompok.....	IV-19

Gambar IV-7. Data Teks <i>8192 Byte</i> .....	IV-20
Gambar IV-8. Desain Antar Muka Beranda.....	IV-21
Gambar IV-9. Desain Antar Muka Enkripsi .....	IV-22
Gambar IV-10. Desain Antar Muka Dekripsi .....	IV-22
Gambar IV-11. Desain Antar Muka Pembangkitan Kunci .....	IV-23
Gambar IV-12. Desain Antar Muka Pengujian Avalanche Test .....	IV-23
Gambar IV-13. Desain Antar Muka Pengujian Enkripsi Kelompok (1) .....	IV-24
Gambar IV-14. Desain Antar Muka Pengujian Enkripsi Kelompok (2) .....	IV-24
Gambar IV-15. Diagram Sequence Mengenkripsi Pesan .....	IV-26
Gambar IV-16. Diagram Sequence Mendekripsi Pesan .....	IV-26
Gambar IV-17. Diagram Sequence Pembangkitan Kunci .....	IV-27
Gambar IV-18. Diagram Sequence Pengujian <i>Avalanche Effect</i> .....	IV-27
Gambar IV-19. Diagram Sequence Pengujian Enkripsi Kelompok .....	IV-28
Gambar IV-20. Diagram Kelas Hybrid Cryptosystem AES dan LUC .....	IV-29
Gambar IV-21. Antarmuka Menu Dashboard.....	IV-32
Gambar IV-22. Antarmuka Menu Enkripsi .....	IV-32
Gambar IV-23. Antarmuka Menu Dekripsi .....	IV-33
Gambar IV-24. Antarmuka Menu Pembangkitan Kunci .....	IV-33
Gambar IV-25. Antarmuka Menu Pengujian <i>Avalanche Effect</i> .....	IV-34
Gambar IV-26. Antarmuka Menu Pengujian Enkripsi Kelompok.....	IV-34
Gambar V-1. Skenario 1 Diagram Waktu Enkripsi AES, LUC dan AES+LUC .....	V-8
Gambar V-2. Skenario 1 Diagram Waktu Dekripsi AES, LUC dan AES+LUC .....	V-8
Gambar V-3. Skenario 2 Diagram Waktu Enkripsi AES, LUC dan AES+LUC .....	V-15
Gambar V-4. Skenario 2 Diagram Waktu Dekripsi AES, LUC dan AES+LUC .....	V-15
Gambar V-5. Skenario 3 Diagram Waktu Enkripsi AES, LUC dan AES+LUC .....	V-22
Gambar V-6. Skenario 3 Diagram Waktu Dekripsi AES, LUC dan AES+LUC .....	V-22
Gambar V-7. Grafik Perubahan Bit AES Tiap Putaran .....	V-24

# **BAB I**

## **PENDAHULUAN**

### **1.1 Pendahuluan**

Bab ini berisi pokok-pokok pikiran yang melandasi pembuatan skripsi. Pokok-pokok pikiran tersebut meliputi latar belakang, rumusan masalah, tujuan, dan manfaat yang diperoleh dalam melakukan penelitian serta batasan masalah.

### **1.2 Latar Belakang**

Kerahasiaan dan keamanan data penting untuk pengguna teknologi informasi sehingga datanya aman dan tidak diketahui oleh pihak yang tidak berkepentingan. Kejahatan informasi seperti penyadapan dan penyalahgunaan data untuk tujuan ilegal juga dapat membahayakan dan merugikan orang lain. Salah satu metode untuk mengamankan data dari tindak kejahatan adalah dengan menerapkan ilmu kriptografi.

Kriptografi (*cryptography*) merupakan ilmu sekaligus seni untuk menjaga kerahasiaan pesan (data atau informasi) yang mempunyai pengertian, dengan cara menyamarkannya (mengacak) menjadi bentuk yang tidak dapat dimengerti menggunakan suatu algoritma tertentu (Mulya, 2014). Metode yang digunakan dalam kriptografi adalah enkripsi dan dekripsi. Pada dasarnya, enkripsi dan dekripsi merupakan dua fungsi penting dari kriptografi itu sendiri. Dalam enkripsi, pesan sederhana (*plaintext*) diubah menjadi bentuk yang tidak terbaca atau biasa disebut

*ciphertext*, sedangkan dalam dekripsi, *ciphertext* tersebut diubah kembali ke bentuk semula yaitu *plaintext*.

Kriptografi memiliki dua jenis algoritma, yaitu algoritma simetri dan asimetri. Algoritma simetri atau kunci simetris adalah algoritma yang menggunakan kunci yang sama dalam proses enkripsi dan dekripsinya, sedangkan algoritma asimetri atau kunci publik adalah algoritma yang menggunakan kunci yang berbeda (pasangan kunci) untuk keperluan enkripsi dan dekripsi. Algoritma simetri memiliki kelebihan dalam kecepatan namun lemah terhadap pendistribusian kunci karena distribusi kunci memerlukan saluran khusus yang aman. Masalah pendistribusian kunci dapat diatasi dengan menggunakan algoritma asimetri namun kecepatan prosesnya tergolong lebih lambat dari algoritma simetri.

Berdasarkan uraian permasalahan tersebut, maka penelitian ini menerapkan teknik kriptografi *hybrid cryptosystem*. *Hybrid cryptosystem* adalah teknik menggabungkan algoritma simetri dan asimetri, menggunakan keamanan dan kecepatan algoritma simetri bersama dengan kekuatan algoritma asimetri dalam mendistribusikan kunci yang aman (Torkaman et al., 2011). Algoritma simetri digunakan untuk mengenkripsi pesan sedangkan algoritma asimetri digunakan untuk keperluan pengamanan dan distribusi kunci pada algoritma simetri.

Algoritma simetri yang digunakan pada penelitian ini adalah algoritma AES atau dapat disebut juga sebagai algoritma Rijndael. Algoritma AES (*Advanced Encryption Standard*) merupakan algoritma kriptografi simetri yang menjadi standar enkripsi saat ini. Algoritma AES dikembangkan oleh Joan Daemen dan

Vincent Rijmen dan dipublikasikan oleh NIST (National Institute of Standard and Technology) pada tahun 2001.

Berdasarkan penelitian yang dilakukan oleh Jintcharadze dan Iavich (2020), mereka membandingkan antara algoritma AES dengan algoritma Twofish sebagai salah satu kombinasi algoritma simetri dalam *hybrid cryptosystem*. Hasil penelitian tersebut adalah algoritma Twofish lebih unggul dalam kecepatan untuk enkripsi file kecil sedangkan AES lebih unggul untuk enkripsi file besar. Selain itu Twofish juga menghasilkan ukuran file enkripsi yang 6,2674 lebih besar dari AES.

Algoritma asimetri yang digunakan untuk mengenkripsi kunci AES pada penelitian ini adalah algoritma LUC. Algoritma LUC adalah algoritma asimetris yang dikembangkan oleh Peter Smith dan Michael Lennon berdasarkan Lucas Function. Algoritma LUC memiliki dua kunci yang berbeda yang berarti keamanan dari algoritma ini tidak bergantung pada kuncinya (Rachmawati et al., 2018).

Menurut Sari, Nababan, dan Zarlis (2020) algoritma LUC memiliki kesamaan proses kalkulasi dengan algoritma Elgamal dan RSA yaitu pembangkitan kuncinya berupa bilangan prima dan hasil dari pengacakan kunci public dan kunci privat. Berdasarkan pengujian yang mereka lakukan, algoritma dengan enkripsi tercepat adalah algoritma RSA dengan waktu 0,19 ms dan 0,17 ms sedangkan untuk dekripsi tercepat algoritma LUC lebih unggul dengan waktu 0,31 ms dan 0,17 ms. Selain kecepatan, salah satu parameter pembanding lain yang dapat digunakan adalah pengukuran kekuatan algoritma.

Kekuatan suatu algoritma kriptografi dapat diukur dengan cara melihat nilai perubahan kecil baik pada *plaintext* maupun kunci yang dapat mempengaruhi

chipertext atau biasa disebut dengan avalanche effect (Shi, Deng, & Yu, 2011).

Algoritma kriptografi bisa dikatakan kuat apabila algoritma tersebut memenuhi kriteria *avalanche effect* yaitu ketika satu *input* bit pada *plaintext* atau kunci diubah, maka *ciphertext* yang dihasilkan paling tidak mengalami setengah bit perubahan dari hasil sebelumnya (Bhoge & Chatur, 2014). Semakin tinggi nilai *avalanche effect* maka semakin kuat algoritma kriptografi tersebut.

### 1.3 Rumusan Masalah

Berdasarkan permasalahan yang diuraikan pada latar belakang diatas maka dapat dirumuskan masalah dari penelitian ini adalah sebagai berikut.

1. Bagaimana mengimplementasikan *hybrid cryptosystem* dengan menggunakan algoritma AES dan LUC dalam mengamankan suatu pesan?
2. Bagaimana hasil penerapan *hybrid cryptosystem* AES dan LUC terhadap keamanan data berdasarkan hasil uji *avalanche effect* terhadap *ciphertext* hasil enkripsi?
3. Bagaimana hasil pengujian *hybrid cryptosystem* AES dan LUC berdasarkan jenis teks yang digunakan dan lama waktu proses di berbagai ukuran *file* yang berbeda?

#### **1.4 Tujuan Penelitian**

Berdasarkan rumusan masalah di atas, maka tujuan dari penelitian ini adalah sebagai berikut.

1. Mengimplementasikan dan mengembangkan perangkat lunak *hybrid cryptosystem* dengan menggunakan algoritma AES dan LUC dalam suatu pesan.
2. Mengetahui hasil penerapan *hybrid cryptosystem* AES dan LUC terhadap keamanan data berdasarkan hasil uji *avalanche effect* terhadap *ciphertext* hasil enkripsi.
3. Mengetahui hasil pengujian *hybrid cryptosystem* AES dan LUC berdasarkan jenis teks yang digunakan dan lama waktu proses di berbagai ukuran *file* yang berbeda.

#### **1.5 Manfaat Penelitian**

Manfaat yang dihasilkan dari penelitian ini adalah sebagai berikut.

1. Menghasilkan perangkat lunak *hybrid cryptosystem* yang memungkinkan user melakukan enkripsi dan dekripsi pesan.
2. Hasil penelitian dapat digunakan untuk meningkatkan kerahasiaan dan keamanan data dalam berkomunikasi.

## 1.6 Batasan Masalah

Batasan masalah dari penelitian ini adalah sebagai berikut.

1. Data atau pesan yang digunakan adalah *file* dokumen dengan ekstensi \*.txt.
2. Perangkat lunak yang dikembangkan berbasis *desktop* dan menggunakan bahasa pemrograman Java.
3. Pengkodean karakter yang digunakan adalah *UTF-16BE* dan satu *string* karakter dihitung sebagai dua *byte* mengikuti standarisasi pemrograman Java.

## 1.7 Sistematika Penulisan

Penelitian ini disusun berdasarkan prosedur penulisan berikut.

### **BAB I. PENDAHULUAN**

Bab ini menguraikan tentang ide utama yang melandasi pembuatan penelitian, seperti latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah dan sistematika penulisan.

### **BAB II. KAJIAN LITERATUR**

Bab ini membahas landasan teori yang akan digunakan dalam penelitian, seperti definisi kriptografi, jenis kriptografi, *hybrid cryptosystem*, algoritma AES, algoritma LUC, *avalanche effect* dan beberapa kajian literatur mengenai penelitian lain yang relevan.

### **BAB III. METODOLOGI PENELITIAN**

Bab ini membahas tentang tahapan yang akan dilaksanakan pada penelitian, seperti pengumpulan data, tahapan penelitian, metode perangkat lunak, dan manajemen proyek perangkat lunak. Masing-masing rencana tahapan penelitian dideskripsikan dengan rinci dan mengacu pada suatu kerangka kerja.

### **BAB IV. PENGEMBANGAN PERANGKAT LUNAK**

Bab ini menjelaskan mengenai proses pengembangan perangkat lunak yang akan digunakan sebagai alat penelitian. Perangkat lunak yang dikembangkan menggunakan metode pemrograman yang berorientasi objek yang menyesuaikan dengan metode pengembangan perangkat lunak yang akan digunakan.

### **BAB V. HASIL DAN ANALISA PENELITIAN**

Bab ini akan membahas tentang hasil penelitian dan analisis hasil penelitian dari alat penelitian yang dihasilkan. Analisis ini akan digunakan sebagai dasar kesimpulan yang dapat diambil dalam penelitian.

### **BAB VI. KESIMPULAN DAN SARAN**

Bab ini memuat kesimpulan dari semua penjelasan pada bab-bab sebelumnya dan saran berdasarkan hasil dari penelitian.

## **1.8 Kesimpulan**

Bab ini telah menguraikan tentang ide utama yang melandasi pembuatan penelitian, seperti latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah dan sistematika penulisan.

## DAFTAR PUSTAKA

- A. Latif. 2015. Implementasi Kriptografi Menggunakan Metode *Advanced Encryption Standar* (AES) untuk Pengamanan Data Teks. Jurnal Ilmiah Mustek Anim Ha, Vol. 4 No. 2, Agustus 2015.
- A. Singh. 2014. *A New Approach to Enhance Avalanche Effect in Aes to Improve Computer Security*. J Inform Tech Softw Eng 2015, 5:143. DOI: 10.4172/2165-7866.1000143
- D. Ariyus. 2006. Kriptografi (Keamanan Data dan Komunikasi). Graha Ilmu, Yogyakarta.
- D. Surian. 2016. Algoritma Kriptografi Aes Rijndael. Jurnal Teknik Elektro, TESLA Vol. 8. No. 2, 97–101.
- E. Jintcharadze & M. Iavich. 2020. *Hybrid Implementation of Twofish, AES, ElGamal and RSA Cryptosystems*. IEEE East-West Design & Test Symposium (EWDTS), 1–5, Sep. 2020.
- F. Muhamarram, H. Aziz & A. R. Manga. 2018. Analisis Algoritma pada Proses Enkripsi dan Dekripsi File Menggunakan *Advanced Encryption Standard* (AES). Prosiding Seminar Nasional Ilmu Komputer dan Teknologi Informasi Vol. 3, No. 2, Desember 2018.
- H. Shi, Y. Deng, Y. Guan. 2011. *Analysis of The Avalanche Effect of The AES S Box*. IEEE 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC), 5425–5428, Aug. 2011.

- M. Mulya. 2014. Bahan Ajar Kriptografi S-1 Edisi Revisi. Fakultas Ilmu Komputer, Universitas Sriwijaya, Palembang.
- M. R. N. Torkaman, P. Nikfard, N. S. Kazazi, M. R. Abbasy, and S. F. Tabatabaiee. 2011. *Improving Hybrid Cryptosystems with DNA Steganography*. E. Ariwa and E. El-Qawasmeh (Eds.), DEIS 2011, Vol 194, 42–52.
- P. P. Sari, E. B. Nababan & M. Zarlis. 2020. *Comparative Study of LUC, ElGamal and RSA Algorithms in Encoding Texts*. 3rd International Conference on Mechanical, Electronics, Computer, and Industrial Technology (MECnIT), 148–151, June 2020.
- Rachmawati, A. Sharif, Jaysilen, & M. A. Budiman. 2018. *Hybrid Cryptosystem Using Tiny Encryption Algorithm and LUC Algorithm*. IOP Conf. Ser.: Mater. Sci. Eng. 300 012042, 1–8.
- R. Saputra, B. Yismianto & Suhartono. 2006. Kriptografi Teks dengan Menggunakan Algoritma LUC. Prosiding Seminar Nasional SPMIPA 2006.
- S. A. Pradana. 2013. *Lucas Sequence and the Application for Cryptography*. Makalah IF3058 Kriptografi – Sem. II Tahun 2012/2013, Informatics Engineering School of Electrical Engineering and Informatics (SEEI), Bandung Institute of Technology (ITB), Bandung.
- S. A. M. Rizvi, S. Z. Hussain and N. Wadhwa. 2011. *Performance Analysis of AES and TwoFish Encryption Schemes*. International Conference on Communication Systems and Network Technologies (CSNT), 76-79, June 2011.

S. Sharma & Y. Gupta. 2017. Study on Cryptography and Techniques. International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), 249–252, Feb. 2017.

Y. Anshori, D.W. Nugraha & A. Pratomo. 2021. Implementasi Algoritma LUC Pada Aplikasi Keamanan *Short Message Service* (SMS) Berbasis Android. CESS (Journal of Computer Engineering System and Science), Vol. 6 No. 1, Januari 2021.