

# **PERBANDINGAN ALGORITMA KRIPTOGRAFI RIJNDAEL DAN TWOFISH PADA PENGAMANAN CITRA**

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



Oleh :

FRESSY ARLIND  
NIM : 09021381621106

**Jurusan Teknik Informatika  
FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA  
2019**

## **LEMBAR PENGESAHAN TUGAS AKHIR**

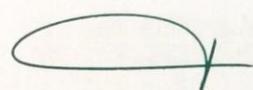
**PERBANDINGAN ALGORITMA KRIPTOGRAFI RIJNDAEL DAN TWOFISH  
PADA PENGAMANAN CITRA**

Oleh:

**FRESSY ARLIND  
NIM : 09021381621106**

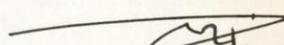
Palembang, Desember 2019

Pembimbing I,



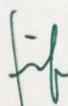
**Drs. Megah Mulya, M.T.  
NIP. 196602202006041001**

Pembimbing II,



**Osvari Arsalan, S.Kom., M.T.  
NIP. 198211082012122001**

Mengetahui,  
Ketua Jurusan Teknik Informatika,



**Rifkie Pramartha, MT  
NIP. 197708012009121004**

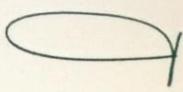
## TANDA LULUS UJIAN SIDANG TUGAS AKHIR

Pada hari Kamis tanggal 26 Desember 2019 telah dilaksanakan ujian sidang tugas akhir oleh Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.

Nama : Fressy Arlind  
NIM : 09021381621106  
Judul : Perbandingan Algoritma Kriptografi *Rijndael* dan *Twofish* pada Pengamanan Citra

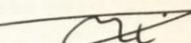
1. Pembimbing I

Drs. Megah Mulya, M.T  
NIP. 196602202006041001



2. Pembimbing II

Osvari Arsalan, S.Kom., M.T.  
NIP. 198806282018031001



3. Penguji I

Alvi Syahrini Utami, M.Kom  
NIP. 197812222006042003



4. Penguji II

Mastura Diana Marieska, S.T., M.T  
NIP. 198603212018032001



Mengetahui,  
Ketua Jurusan Teknik Informatika

  
Rifkie Primartha, MT  
NIP. 197706012009121004

## HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini:

Nama : Fressy Arlind  
NIM : 09021381621106  
Program Studi : Teknik Informatika  
Judul Skripsi : Perbandingan Algoritma Kriptografi *Rijndael* dan *Twofish*  
pada Pengamanan Citra  
Hasil Pengecekan Software *iThenticate/Turnitin* : 8%

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, 27 Desember 2019



Fressy Arlind  
NIM. 09021381621106

## MOTTO DAN PERSEMBAHAN

"To get a success, your courage must be greater than  
your fear"

"Never say

"Why I never get what I wanted?"!

It is possible that you dislike a thing which is good  
for you, and that you love a thing which is bad for  
you. But Allah knows, while you know not"

*Kupersembahkan karya tulis ini kepada :*

- *Kedua orangtuaku tercinta, kakak, dan  
keponakanku tersayang*
- *Keluarga besarku*
- *Teman - teman Tersayangku*
- *Fakultas Ilmu Komputer*
- *Universitas Sriwijaya*

## ABSTRACT

The advancement of information technology will certainly have an impact on information security along with the ease of accessing media communication in this modern era. Cryptography provides the secure guarantee of information in order to avoid those impacts. The main characteristics of a good data encryption and decryption are security and speed. This study provides a comparative analysis of security and speed between two cryptography algorithms, Rijndael and Twofish, on image security with different mode of operations (ECB and CBC). Security analysis can be seen by the value of Avalanche Effect and speed analysis can be seen by the execution time of its algorithm. Based on the results of tests conducted, it is known that both the Rijndael and Twofish cryptographic algorithms both produce the avalanche effect in accordance with the Strict Avalanche Effect (SAC) which is close to 50%. In testing the Avalanche Effect changes in plainimage obtained the results of the Rijndael algorithm has the highest Avalanche Effect value of 52.8125% with CBC operating mode and small change pixel RGB value categories. Testing the Avalanche Effect changes to the key also outperformed by Rijndael with a value of 49,98619% with CBC operating mode. While for execution time, it can be concluded that the resolution and mode of operation has an influence on the execution time.

**Keywords :** Avalanche Effect, Execution Time, Rijndael, Twofish, Data Encryption and Decryption, ECB, CBC

## ABSTRAK

Kemajuan teknologi informasi tentunya akan memberikan dampak bagi keamanan informasi seiring dengan mudahnya pengaksesan media komunikasi pada era modern ini. Kriptografi memberikan jaminan keamanan informasi yang dibutuhkan untuk menghindari dampak-dampak tersebut. Karakteristik utama dalam algoritma enkripsi dan dekripsi data yang baik adalah keamanan dan kecepatan. Penelitian ini memberikan analisis perbandingan keamanan dan kecepatan antar dua algoritma kriptografi, *Rijndael* dan *Twofish*, pada pengamanan citra dengan mode operasi yang berbeda (ECB dan CBC). Analisis keamanan dilihat dari nilai *Avalanche Effect* dan analisis kecepatan dilihat dari waktu eksekusi algoritma tersebut. Berdasarkan hasil pengujian yang dilakukan diketahui bahwa baik algoritma kriptografi *Rijndael* dan *Twofish* sama-sama menghasilkan nilai *avalanche effect* sesuai dengan *Strict Avalanche Effect* (SAC) yaitu mendekati 50%. Pada pengujian *Avalanche Effect* perubahan pada *plainimage* didapatkan hasil algoritma *Rijndael* memiliki nilai *Avalanche Effect* tertinggi sebesar 52.8125% dengan mode operasi CBC dan kategori nilai RGB pixel ubah kecil. Pengujian *Avalanche Effect* perubahan pada kunci juga diungguli oleh *Rijndael* dengan nilai sebesar 49.98619% dengan mode operasi CBC. Sedangkan untuk waktu eksekusi, didapatkan kesimpulan bahwa resolusi dan mode operasi memiliki pengaruh terhadap waktu eksekusi.

**Kata Kunci :** *Avalanche Effect*, Waktu Eksekusi, *Rijndael*, *Twofish*, Enkripsi dan Dekripsi Data, ECB, CBC

## KATA PENGANTAR

Puji syukur kepada Allah atas berkat dan rahmat-Nya yang telah diberikan kepada Penulis sehingga dapat menyelesaikan Tugas Akhir ini dengan baik. Tugas akhir ini disusun untuk memenuhi salah satu syarat guna menyelesaikan pendidikan program Strata-1 pada Fakultas Ilmu Komputer Program Studi Teknik Informatika di Universitas Sriwijaya.

Dalam menyelesaikan Tugas Akhir ini banyak pihak yang telah memberikan bantuan dan dukungan baik secara langsung maupun secara tidak langsung. Penulis ingin menyampaikan rasa terima kasih kepada:

1. Orang tuaku, Arsyad Hengry Bacik dan Herlinda, saudara-saudariku, Frizky Arlind, Freisha Arlind, dan Agung Hidayat, keponakanku, Aidan Ghally Hidayat, dan seluruh keluarga besarku yang selalu mendoakan serta memberikan dukungan baik moril maupun materil.
2. Bapak Jaidan Jauhari selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya, Bapak Rifkie Primartha selaku Ketua Jurusan Teknik Informatika, dan Ibu Hardini Novianti selaku Sekretaris Jurusan Teknik Informatika.
3. Bapak Megah Mulya selaku dosen pembimbing I dan Bapak Osvari Arsalan selaku pembimbing II yang telah membimbing, mengarahkan, dan memberikan motivasi penulis dalam proses perkuliahan dan pengeroaan Tugas Akhir.
4. Ibu Yunita selaku dosen pembimbing akademik, yang telah membimbing, mengarahkan dan memberikan motivasi penulis dalam proses perkuliahan dan pengeroaan Tugas Akhir.
5. Ibu Alvi Syahrini Utami selaku dosen penguji I, dan Ibu Mastura Diana Marieska selaku dosen penguji II yang telah memberikan masukan dan dorongan dalam proses pengeroaan Tugas Akhir.
6. Seluruh dosen Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.
7. Pak Tony, Mbak Anna, Mbak Wiwin dan seluruh staf tata usaha yang telah membantu dalam kelancaran proses administrasi dan akademik selama masa perkuliahan.

8. Sari Dwi Septiani dan Abdul Hafiz Muttaqien selaku sahabat yang telah menemani dan memotivasi selama proses menyelesaikan Tugas Akhir.
9. Teman-teman jurusan Teknik Informatika yang telah berbagi keluh kesah, motivasi, semangat, dan canda tawa selama masa perkuliahan.

Penulis menyadari dalam penyusunan Tugas Akhir ini masih terdapat banyak kekurangan disebabkan keterbatasan pengetahuan dan pengalaman, oleh karena itu kritik dan saran yang membangun sangat diharapkan untuk kemajuan penelitian selanjutnya. Akhir kata semoga Tugas Akhir ini dapat berguna dan bermanfaat bagi kita semua.

Palembang, Desember 2019

Fressy Arlind

## DAFTAR ISI

	Halaman
<b>HALAMAN JUDUL .....</b>	i
<b>HALAMAN PERSETUJUAN .....</b>	ii
<b>HALAMAN PERSETUJUAN KOMISI PENGUJI .....</b>	iii
<b>HALAMAN PERNYATAAN .....</b>	iv
<b>HALAMAN MOTTO DAN PERSEMBAHAN .....</b>	v
<b>ABSTRACT .....</b>	vi
<b>ABSTRAK.....</b>	vii
<b>KATA PENGANTAR.....</b>	viii
<b>DAFTAR ISI .....</b>	x
<b>DAFTAR TABEL.....</b>	xiv
<b>DAFTAR GAMBAR .....</b>	xvii
<b>DAFTAR ALGORITMA.....</b>	xx
<b>DAFTAR LAMPIRAN .....</b>	xxi

### **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-5
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 Citra Bitmap .....	II-1

2.2.2 Kriptografi .....	II-1
2.2.3 Enkripsi dan Dekripsi Data .....	II-2
2.2.4 <i>Stream</i> dan <i>Block Cipher</i> .....	II-4
2.2.5 Mode Operasi .....	II-5
2.2.6 <i>S-Box</i> .....	II-6
2.2.7 Algoritma <i>Rijndael</i> .....	II-8
2.2.8 Matriks <i>Maximum Distance Separable</i> (MDS).....	II-12
2.2.9 <i>Pseudo-Hadamard Transformation</i> (PHT) .....	II-12
2.2.10 Jaringan Feistel .....	II-13
2.2.11 Fungsi F.....	II-13
2.2.12 Fungsi G .....	II-14
2.2.13 Algoritma <i>Twofish</i> .....	II-15
2.2.14 <i>Avalanche Effect</i> .....	II-21
2.2.15 <i>Unified Modeling Language</i> (UML).....	II-21
2.2.16 <i>Rational Unified Process</i> (RUP) .....	II-22
2.3 Penelitian Terdahulu yang Relevan.....	II-24
2.4 Kesimpulan .....	II-29

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

3.1 Pedahuluan .....	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 Menetapkan Kerangka Kerja.....	III-2
3.3.2 Menetapkan Kriteria Pengujian .....	III-5
3.3.3 Menetapkan Format Data Pengujian.....	III-9
3.3.4 Menetukan Alat yang Digunakan dalam Pelaksanaan Penelitian.....	III-9
3.3.5 Melakukan Pengujian Penelitian .....	III-10

3.3.6 Melakukan Analisa Hasil Pengujian dan Membuat Kesimpulan Penelitian .....	III-10
3.4 Metode Pengembangan Perangkat Lunak.....	III-12
3.5 Manajemen Proyek Penelitian.....	III-14

## **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 .....	IV-2
4.2.3 Analisis dan Desain.....	IV-2
4.2.4 Implementasi .....	IV-5
4.3 Fase Elaborasi .....	IV-6
4.3.1 Pemodelan Bisnis.....	IV-6
4.3.2 Kebutuhan .....	IV-21
4.3.3 Analisis dan Desain.....	IV-21
4.3.4 Implementasi .....	IV-21
4.4 Fase Konstruksi .....	IV-22
4.4.1 Pemodelan Bisnis.....	IV-22
4.4.2 Kebutuhan .....	IV-24
4.4.3 Analisis dan Desain.....	IV-24
4.4.4 Implementasi .....	IV-27
4.5 Fase Transisi.....	IV-29
4.5.1 Pemodelan Bisnis.....	IV-29
4.5.2 Kebutuhan .....	IV-29
4.5.3 Analisis dan Desain.....	IV-29
4.5.4 Implementasi .....	IV-31
4.6 Kesimpulan .....	IV-36

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

5.1 Pendahuluan .....	V-1
-----------------------	-----

5.2 Data Hasil Percobaan.....	V-1
5.2.1 Data Hasil Pengujian <i>Avalanche Effect</i> Perubahan pada <i>Plainimage</i> .....	V-1
5.2.2 Data Hasil Pengujian <i>Avalanche Effect</i> Perubahan pada Kunci.....	V-10
5.2.3 Data Hasil Pengujian Waktu Eksekusi.....	V-11
5.3 Analisis Hasil Penelitian.....	V-12
5.4 Kesimpulan .....	V-22

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

6.1 Pendahuluan .....	VI-1
6.2 Kesimpulan .....	VI-1
6.3 Saran .....	VI-3

<b>DAFTAR PUSTAKA.....</b>	xxii
----------------------------	------

## DAFTAR TABEL

Halaman

Tabel II-1. Contoh <i>S-Box</i> dengan Kasus .....	II-8
Tabel II-2. Hasil Perbandingan Kecepatan Enkripsi dalam Pengamanan Citra.....	II-24
Tabel II-3. Hasil Perbandingan Kecepatan Dekripsi dalam Pengamanan Citra.....	II-25
Tabel II-4. Hasil Perbandingan Kecepatan Algoritma <i>Rijndael</i> dan <i>Twofish</i> .....	II-26
Tabel II-5. Hasil Perbandingan Ukuran Data Setelah Enkripsi.....	II-26
Tabel II-6. Hasil Perbandingan Ketahanan Algoritma .....	II-26
Tabel II-7. Hasil Perbandingan <i>Avalanche Effect</i> .....	II-27
Tabel II-8. Hasil Perbandingan Nilai <i>Avalanche Effect</i> pada Mode ECB .....	II-28
Tabel II-9. Hasil Perbandingan Nilai <i>Avalanche Effect</i> pada Mode CBC .....	II-28
Tabel III-1. <i>Plainimage</i> pada Waktu Eksekusi.....	III-3
Tabel III-2. <i>Plainimage</i> pada <i>Avalanche Effect</i> .....	III-4
Tabel III-3. Kunci pada Waktu Eksekusi.....	III-5
Tabel III-4. Kunci pada <i>Avalanche Effect</i> Perubahan pada Kunci .....	III-5
Tabel III-5. Rancangan Tabel Hasil Pengujian AE Perubahan pada <i>Plainimage</i> .....	III-9
Tabel III-6. Rancangan Tabel Hasil Pengujian AE Perubahan pada Kunci ..	III-9
Tabel III-7. Rancangan Tabel Hasil Pengujian Waktu Eksekusi .....	III-9
Tabel III-8. Rancangan Tabel Analisa Hasil AE Perubahan pada <i>Plainimage</i> .....	III-10
Tabel III-9. Rancangan Tabel Analisa Hasil AE Perubahan pada Kunci .....	III-11
Tabel III-10. Rancangan Tabel Analisa Hasil Perbandingan Waktu Eksekusi .....	III-11
Tabel III-11. Tabel <i>Work Breakdown Structure</i> (WBS) Penelitian.....	III-14
Tabel IV-1. Kebutuhan Fungsional Perangkat Lunak .....	IV-2
Tabel IV-2. Kebutuhan Non Fungsional Perangkat Lunak .....	IV-2

Tabel IV-3. Definisi Aktor pada Diagram <i>Use Case</i> .....	IV-7
Tabel IV-4. Definisi <i>Use Case</i> .....	IV-7
Tabel IV-5. Skenario <i>Use Case</i> Melakukan Perhitungan AE Perubahan pada <i>Plainimage</i> .....	IV-7
Tabel IV-6. Skenario <i>Use Case</i> Melakukan Perhitungan AE Perubahan pada Kunci.....	IV-9
Tabel IV-7. Skenario <i>Use Case</i> Melakukan Perhitungan Waktu Eksekusi ...	IV-10
Tabel IV-8. Spesifikasi kebutuhan Perangkat Keras dan Lunak .....	IV-22
Tabel IV-9. Daftar Implementasi Kelas pada Perangkat Lunak.....	IV-25
Tabel IV-10. Skenario Pengujian Melakukan Perhitungan AE Perubahan pada <i>Plainimage</i> .....	IV-27
Tabel IV-11. Skenario Pengujian Melakukan Perhitungan AE Perubahan pada Kunci.....	IV-28
Tabel IV-12. Skenario Pengujian Melakukan Perhitungan Waktu Eksekusi.	IV-28
Tabel IV-13. Hasil Pengujian Melakukan Perhitungan AE Perubahan pada <i>Plainimage</i> .....	IV-31
Tabel IV-14. Hasil Pengujian Melakukan Perhitungan AE Perubahan pada Kunci.....	IV-32
Tabel IV-15. Hasil Pengujian Melakukan Perhitungan Waktu Eksekusi .....	IV-33
Tabel V-1. Tabel Hasil Pengujian AE <i>Rijndael</i> Mode ECB dan Perubahan pada <i>Plainimage</i> dengan Kategori Nilai RGB Pixel Ubah Kecil.....	V-2
Tabel V-2. Tabel Hasil Pengujian AE <i>Rijndael</i> Mode CBC dan Perubahan pada <i>Plainimage</i> dengan Kategori Nilai RGB Pixel Ubah Kecil.....	V-3
Tabel V-3. Tabel Hasil Pengujian AE <i>Rijndael</i> Mode ECB dan Perubahan pada <i>Plainimage</i> dengan Kategori Nilai RGB Pixel Ubah Besar .....	V-4
Tabel V-4. Tabel Hasil Pengujian AE <i>Rijndael</i> Mode CBC dan Perubahan pada <i>Plainimage</i> dengan Kategori Nilai RGB Pixel Ubah Besar .....	V-5
Tabel V-5. Tabel Hasil Pengujian AE <i>Twofish</i> Mode ECB dan Perubahan pada <i>Plainimage</i> dengan Kategori Nilai RGB Pixel Ubah Kecil .....	V-6
Tabel V-6. Tabel Hasil Pengujian AE <i>Twofish</i> Mode CBC dan Perubahan pada <i>Plainimage</i> dengan Kategori Nilai RGB Pixel Ubah Kecil .....	V-7

Tabel V-7. Tabel Hasil Pengujian AE <i>Twofish</i> Mode ECB dan Perubahan pada <i>Plainimage</i> dengan Kategori Nilai RGB Pixel Ubah Besar .....	V-8
Tabel V-8. Tabel Hasil Pengujian AE <i>Twofish</i> Mode CBC dan Perubahan pada <i>Plainimage</i> dengan Kategori Nilai RGB Pixel Ubah Besar .....	V-9
Tabel V-9. Tabel Hasil Pengujian AE Perubahan pada <i>Plainimage</i> .....	V-10
Tabel V-10. Tabel Hasil Pengujian AE Perubahan pada Kunci.....	V-10
Tabel V-11. Tabel Hasil Pengujian Waktu Eksekusi .....	V-11
Tabel V-12. Tabel Analisis Hasil Pengujian AE Perubahan pada <i>Plainimage</i> di Kategori Nilai RGB Pixel Kecil .....	V-12
Tabel V-13. Tabel Analisis Hasil Pengujian AE Perubahan pada <i>Plainimage</i> di Kategori Nilai RGB Pixel Besar.....	V-12
Tabel V-14. Hasil Pengukuran Jitter dari Nilai AE Perubahan pada <i>Plainimage</i> di Kategori Nilai RGB Pixel Kecil .....	V-14
Tabel V-15. Hasil Pengukuran Jitter dari Nilai AE Perubahan pada <i>Plainimage</i> di Kategori Nilai RGB Pixel Besar .....	V-14
Tabel V-16. Tabel Analisis Hasil Pengujian AE Perubahan pada Kunci .....	V-16

## DAFTAR GAMBAR

	Halaman
Gambar II-1. Skema Proses Enkripsi dan Dekripsi Algoritma Simetris.....	II-3
Gambar II-2. Skema Proses Enkripsi dan Dekripsi Algoritma Asimetris .....	II-3
Gambar II-3. Skema Mode ECB .....	II-5
Gambar II-4. Skema Mode CBC .....	II-6
Gambar II-5. <i>S-Box</i> .....	II-7
Gambar II-6. <i>Inverse S-Box</i> .....	II-7
Gambar II-7. Skema Algoritma <i>Rijndael</i> .....	II-9
Gambar II-8. Struktur Jaringan Feistel .....	II-13
Gambar II-9. Skema Algoritma <i>Twofish</i> .....	II-17
Gambar II-10. Diagram Proses <i>Rational Unified Process</i> (RUP) .....	II-23
Gambar III-1. Diagram Tahapan Penelitian .....	III-2
Gambar III-2. Skema Pengujian AE Perubahan pada <i>Plainimage</i> .....	III-6
Gambar III-3. Skema Pengujian AE Perubahan pada Kunci .....	III-7
Gambar III-4. Skema Pengujian Waktu Eksekusi .....	III-8
Gambar III-5. <i>Gantt Chart</i> Penjadwalan Penelitian Fase Insepsi .....	III-19
Gambar III-6. <i>Gantt Chart</i> Penjadwalan Penelitian Fase Elaborasi.....	III-20
Gambar III-7. <i>Gantt Chart</i> Penjadwalan Penelitian Fase Konstruksi .....	III-21
Gambar III-8. <i>Gantt Chart</i> Penjadwalan Penelitian Fase Transisi .....	III-22
Gambar IV-1. Diagram Alir Perhitungan AE Perubahan pada <i>Plainimage</i> .....	IV-3
Gambar IV-2. Diagram Alir Perhitungan AE Perubahan pada Kunci.....	IV-4
Gambar IV-3. Diagram Alir Perhitungan Waktu Eksekusi .....	IV-5
Gambar IV-4. Diagram <i>Use Case</i> Fase Elaborasi .....	IV-6
Gambar IV-5. Diagram Aktivitas Melakukan Perhitungan AE Perubahan pada <i>Plainimage</i> .....	IV-12
Gambar IV-6. Diagram Aktivitas Melakukan Perhitungan AE Perubahan pada Kunci.....	IV-13
Gambar IV-7. Diagram Aktivitas Melakukan Perhitungan Waktu Eksekusi ..	IV-14
Gambar IV-8. Diagram Kelas Analisis Melakukan Perhitungan AE	

Perubahan pada <i>Plainimage</i> .....	IV-15
Gambar IV-9. Diagram Kelas Analisis Melakukan Perhitungan AE	
Perubahan pada Kunci .....	IV-15
Gambar IV-10. Diagram Kelas Analisis Melakukan Perhitungan Waktu Eksekusi .....	IV-16
Gambar IV-11. Diagram Sub-Sekuensial Set Data Pilih .....	IV-16
Gambar IV-12. Diagram Sekuensial Melakukan Perhitungan AE Perubahan pada <i>Plainimage</i> .....	IV-17
Gambar IV-13. Diagram Sekuensial Melakukan Perhitungan AE Perubahan pada Kunci.....	IV-18
Gambar IV-14. Diagram Kelas Analisis Melakukan Perhitungan Waktu Eksekusi .....	IV-19
Gambar IV-15. Diagram Kelas.....	IV-21
Gambar IV-16. Rancangan Antarmuka Perangkat Lunak <i>Tab “Avalanche Effect – Plainimage”</i> .....	IV-23
Gambar IV-17. Rancangan Antarmuka Perangkat Lunak <i>Tab “Avalanche Effect – Kunci”</i> .....	IV-23
Gambar IV-18. Rancangan Antarmuka Perangkat Lunak <i>Tab “Waktu Eksekusi”</i> .....	IV-24
Gambar IV-19. Tampilan Antarmuka Perangkat Lunak <i>Tab “Avalanche Effect – Plainimage”</i> .....	IV-29
Gambar IV-20. Tampilan Antarmuka Perangkat Lunak <i>Tab “Avalanche Effect – Kunci”</i> .....	IV-29
Gambar IV-21. Tampilan Antarmuka Perangkat Lunak <i>Tab “Waktu Eksekusi”</i> .....	IV-30
Gambar V-1. Perbandingan Nilai AE Perubahan pada <i>Plainimage</i> di Kategori Nilai RGB Pixel Kecil.....	V-13
Gambar V-2. Perbandingan Nilai Jitter dari Nilai AE Perubahan pada <i>Plainimage</i> di Kategori Nilai RGB Pixel Kecil .....	V-14
Gambar V-3. Perbandingan Nilai AE Perubahan pada <i>Plainimage</i> di Kategori Nilai RGB Pixel Besar .....	V-15

Gambar V-4. Perbandingan Nilai Jitter dari Nilai AE Perubahan pada <i>Plainimage</i> di Kategori Nilai RGB Pixel Besar .....	V-17
Gambar V-5. Perbandingan Nilai AE Perubahan pada <i>Plainimage</i> .....	V-18
Gambar V-6. Perbandingan Nilai Jitter dari Nilai AE Perubahan pada <i>Plainimage</i> .....	V-18
Gambar V-7. Perbandingan Nilai AE Perubahan pada Kunci .....	V-20
Gambar V-8. Perbandingan Waktu Eksekusi.....	V-21

## **DAFTAR ALGORITMA**

	Halaman
Algoritma II-1. <i>Pseudocode</i> Enkripsi Algoritma <i>Rijndael</i> .....	II-10
Algoritma II-2. <i>Pseudocode</i> Dekripsi Algoritma <i>Rijndael</i> .....	II-10
Algoritma II-3. <i>Pseudocode</i> Ekspansi Kunci Algoritma <i>Rijndael</i> .....	II-11
Algoritma II-4. <i>Pseudocode</i> Enkripsi Algoritma <i>Twofish</i> .....	II-18
Algoritma II-5. <i>Pseudocode</i> Dekripsi Algoritma <i>Twofish</i> .....	II-19
Algoritma II-6. <i>Pseudocode</i> Ekspansi Kunci Algoritma <i>Twofish</i> .....	II-20

## **DAFTAR LAMPIRAN**

Lampiran 1. Koding Program..... L-1

# **BAB I**

## **PENDAHULUAN**

### **1.1 Pendahuluan**

Pada bab ini diuraikan tentang pokok-pokok pikiran yang melandasi rencana skripsi. Pokok-pokok pikiran yang dimaksud diatas antara lain latar belakang masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah.

### **1.2 Latar Belakang Masalah**

Kriptografi merupakan cabang ilmu yang dikembangkan untuk mengamankan data atau informasi (Lusiana, 2011). Kemunculan kriptografi merupakan bentuk perhatian dari ancaman yang akan dihadapi seiring berkembangnya teknologi informasi. Ancaman-ancaman yang dimaksud adalah berbagai tindak kejahatan yang dapat mempengaruhi informasi dari segi kerahasiaan, otentikasi, integritas, dan ketersediaan data. Berbagai sektor seperti pemerintahan, militer, badan keuangan, rumah sakit, dan lain sebagainya menjadikan informasi sebagai peranan penting dalam menjalankan tugasnya (Kristoforus JB & Aditya BP, 2012). Hal tersebutlah yang membuat kriptografi mendapatkan perhatian lebih pada era digital seperti saat ini. Informasi yang diamankan bisa berupa teks, gambar, suara, video, dan lain sebagainya.

Salah satu algoritma kriptografi adalah algoritma kriptografi kunci simetris. Algoritma kunci simetris ini menggunakan satu kunci yang sama dalam

proses enkripsi dan dekripsinya. Beberapa algoritma dari kunci simetris adalah DES, Blowfish, *Twofish*, LOKI, *Rijndael*, dan lain sebagainya. Algoritma *Rijndael* dan *Twofish* merupakan dua dari lima finalis dalam pemilihan standar *Advances Encryption Standard* (AES) sebagai pengganti *Data Encryption Standard* (DES) oleh *National Institute of Standard and Technology* (NIST). Algoritma *Rijndael* dan *Twofish* memiliki beberapa karakteristik yang sama dikarenakan ada beberapa syarat yang harus dipenuhi untuk menjadi kandidat AES yaitu merupakan algoritma kriptografi simetris berbasis *chiper block*, panjang kunci fleksibel (128, 192, dan 256 bit), ukuran block enkripsi yaitu 128 bit, dan mudah diimplementasikan. Tetapi, ada berbagai perbedaan juga antara kedua algoritma *Rijndael* dan *Twofish* seperti proses, kerumitan, waktu pemrosesan, dan lain-lain yang menyebabkan dipilihnya *Rijndael* sebagai pemenang AES.

Terdapat penelitian mengenai perbandingan antara algoritma kriptografi *rijndael* dan *twofish* untuk mengetahui perbedaan karakteristik antar kedua algoritma ini. Penelitian yang menganalisis perbandingan dengan parameter kecepatan, ukuran data setelah enkripsi, dan ketahanan terhadap serangan antara algoritma *Rijndael* dan *Twofish* pada file teks (Shulhan, 2018). Hasil dari penelitian tersebut adalah algoritma *rijndael* lebih unggul pada kecepatan dan ukuran data setelah enkripsi sedangkan algoritma *twofish* lebih unggul pada ketahanannya terhadap serangan. Hasil penelitian tersebut telah membuktikan bahwa algoritma pemenang (*Rijndael*) tidak selalu unggul dari algoritma finalis (*Twofish*). Oleh karena itu diperlukannya analisa lebih antara kedua algoritma *rijndael* dan *twofish*.

untuk lebih memahami perbedaan karakteristik tersebut. Salah satu parameter pembanding yang dapat digunakan adalah pengukuran kekuatan.

Pengukuran kekuatan suatu algoritma kriptografi bisa dilakukan dengan cara melihat nilai perubahan kecil baik pada *plaintext* maupun kunci yang dapat mempengaruhi *chipertext* atau biasa disebut sebagai *avalanche effect* (Shi, Deng, & Yu, 2011). Kriteria algoritma kriptografi yang memiliki *Avalanche Effect* yang memuaskan adalah pada saat *chipertext* yang dihasilkan mengalami perubahan paling sedikit sebanyak 50% akibat terjadinya perubahan satu bit pada *plaintext* ataupun kunci (Bhoge & Chatur, 2014). Semakin tinggi nilai *avalanche effect* maka semakin bagus algoritma kriptografi tersebut.

Terdapat beberapa penelitian mengenai *avalanche effect* untuk mengukur keamanan suatu algoritma kriptografi. Salah satunya telah dilakukan oleh (Putra, Budiman, & Andini, 2015) yang menganalisis *avalanche effect* dari algoritma kriptografi *Rijndael* (AES) dengan mode *Electronic Code Book* (ECB). Dari hasil percobaan penelitian tersebut doloat dilihat nilai *avalanche effect* yang didapat baik dari perubahan *plaintext* ataupun kunci diatas 50%. Hal itu berarti untuk AES memiliki *avalanche effect* yang memuaskan. Efek yang lebih berpengaruh kuat adalah ketika terjadi perubahan pada *plaintext* dibandingkan adanya perubahan pada kunci. Tetapi, pada penelitian ini hanya menggunakan *plaintext* yang relatif pendek.

Penelitian lain mengenai *avalanche effect* juga telah dilakukan oleh (Mahamat et al. 2016) melakukan perbandingan nilai *avalanche effect* antara algoritma kriptografi AES, Blowfish, CAST-128, dan DES menggunakan mode

*Electronic Code Book* (ECB) dan *Cipher Block Chaining* (CBC). Hasil yang didapatkan adalah pada mode ECB dan CBC, DES memiliki *avalanche effect* paling besar diantara yang lainnya. Akan tetapi untuk urutan keduanya, pada mode ECB AES memiliki *avalanche effect* yang paling tinggi dibandingkan Blowfish dan CAST-128. Sedangkan untuk mode CBC, nilai *avalanche effect* Blowfish lebih baik dari pada AES.

Berdasarkan penelitian yang telah dilakukan sebelumnya didapatkan hasil bahwa mode operasi ECB dan CBC akan memberikan hasil *avalanche effect* yang berbeda. Untuk itulah, pada penelitian ini akan dilakukan perbandingan algoritma *Rijndael* dan *Twofish* pada pengamanan citra dengan menggunakan mode operasi ECB dan CBC berdasarkan nilai *avalanche effect* dan waktu eksekusi.

### 1.3 Rumusan Masalah

Berdasarkan latar belakang di atas dapat diidentifikasi permasalahan yang muncul adalah bagaimana perbandingan keamanan antara algoritma *Rijndael* dan *Twofish* pada pengamanan citra dengan menggunakan mode operasi ECB dan CBC berdasarkan nilai *avalanche effect*. Dari rumusan masalah yang telah dikemukakan, maka pertanyaan penelitian adalah bagaimana hasil perhitungan *avalanche effect* dan waktu eksekusi dari perbandingan algoritma kriptografi *Rijndael* dan *Twofish* pada pengamanan citra dengan mode operasi ECB dan CBC.

## 1.4 Tujuan Penelitian

Adapun tujuan yang hendak dicapai dari penelitian ini adalah:

1. Mengembangkan perangkat lunak perbandingan algoritma kriptografi *Rijndael* dan *Twofish* pada pengamanan citra.
2. Mengetahui nilai hasil perbandingan keamanan antara algoritma kriptografi *Rijndael* dan *Twofish* dengan mode operasi ECB dan CBC pada citra berdasarkan nilai *avalanche effect*.
3. Mengetahui nilai hasil perbandingan waktu eksekusi antara algoritma kriptografi *Rijndael* dan *Twofish* dengan mode operasi ECB dan CBC pada citra.

## 1.5 Manfaat Penelitian

Manfaat yang hendak dicapai dalam pelaksanaan penelitian ini adalah:

1. Mengetahui mode operasi yang lebih tepat digunakan pada algoritma kriptografi *rijndael* dan *twofish* sehingga memberikan nilai *avalanche effect* yang tinggi.
2. Mengetahui pengaruh resolusi citra terhadap perubahan waktu eksekusi.

## 1.6 Batasan Masalah

Karena keterbatasan waktu dan pengetahuan penulis, maka ruang lingkup permasalahan dalam penelitian ini dibatasi pada bidang kajian yang dibahas yaitu:

1. Algoritma kriptografi yang dibandingkan adalah *rijndael* dan *twofish* dengan panjang kunci 128 bit.

2. Data yang digunakan berupa citra bitmap dengan resolusi 32 x 32, 128 x 128, 256 x 256, 512 x 512, dan 1024 x 1024.
3. Satuan untuk nilai *avalanche effect* menggunakan persen (%).
4. Mode operasi yang digunakan adalah ECB dan CBC.
5. Proses enkripsi dekripsi *block* dilakukan menggunakan *library Bouncy Castle* yang di-support oleh *Australian Charitable Organization* yaitu *Legion of the Bouncy Castle Inc.*

## 1.7 Sistematika Penulisan

Sistematika penulisan laporan tugas akhir ini adalah sebagai berikut:

## BAB I. PENDAHULUAN

Pada bab ini diuraikan tentang pokok-pokok pikiran yang melandasi rencana skripsi. Pokok-pokok pikiran yang dimaksud diatas antara lain latar belakang masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah.

## BAB II. KAJIAN LITERATUR

Pada bab ini akan dibahas dasar-dasar teori yang digunakan dalam penelitian, seperti citra bitmap, kriptografi, enkripsi dan dekripsi data, *stream* dan *blok cipher*, mode operasi, *S-Box*, algoritma *rijndael*, Matriks *Maximum Distances Separable* (MDS), *Pseudo-Hadamard Transformation*

(PHT), jaringan feistel, fungsi f, fungsi g, algoritma *twofish*, dan *avalanche effect*, serta penelitian terdahulu yang relevan.

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

Pada bab ini akan dijelaskan data yang akan digunakan pada penelitian ini dan bagaimana cara pengumpulan datanya. Lalu, akan dijelaskan tahapan penelitian yang akan diimplementasikan, metode pengembangan perangkat lunak serta manajemen proyek penelitian.

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

Pada bab ini diuraikan tahapan yang dilakukan dalam proses pengembangan perangkat lunak yang merupakan alat penelitian yang digunakan untuk melakukan perbandingan algoritma kriptografi *Rijndael* dan *Twofish* dalam pengaman citra dengan menggunakan metode *Rational Unified Process* (RUP).

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

Pada bab ini akan diuraikan hasil pengujian dan analisis hasil pengujian dari pengembangan perangkat lunak.

## BAB VI. KESIMPULAN DAN SARAN

Pada bab ini akan dijabarkan kesimpulan penelitian dan saran yang diharapkan dapat dijadikan sebagai acuan untuk penelitian lain di bidang yang sama kedepannya.

### 1.8 Kesimpulan

Penelitian yang akan dijadikan rencana tugas akhir adalah penelitian tentang perbandingan algoritma *twofish* dan *rijndael* pada pengamangan citra dengan mode operasi ECB dan CBC berdasarkan nilai *avalanche effect* dan waktu eksekusi.

## DAFTAR PUSTAKA

- Bhoge, Jayant P, dan Prashant N Chatur. 2014. "Avalanche Effect of AES Algorithm." *International Journal of Computer Science and Information Technologies* 5 (3): 3101–3.
- Kristoforus JB, R., dan Stefanus Aditya BP. 2012. "Implementasi Algoritma Rijndael Untuk Enkripsi Dan Deskripsi Pada Citra Digital" 2012 (Snati): 15–16.
- Lusiana, Veronica. 2011. "Implementasi Kriptografi Pada File Dokumen Menggunakan Algoritma Aes-128." *Jurnal Dinamika Informatika* 3: 79–84. <https://doi.org/10.1108/02683940510579731>.
- Mahamat, Youssouf, Siti Hajar Othman, Maheyzah Siraj, dan Herve Nkiam. 2016. "Comparative Study Of AES , Blowfish , CAST-128 And DES Encryption Algorithm International Organization of Scientific Research International Organization of Scientific Research" 06 (06): 1–7.
- Muhathir, Muhathir. 2019. "Perbandingan Algoritma Blowfish Dan Twofish Untuk Kriptografi File Gambar." *Journal of Informatics and Telecommunication Engineering* 2 (1): 23. <https://doi.org/10.31289/jite.v2i1.1673>.
- Putra, Fadlan, Gelar Budiman, dan Nur Andini. 2015. "COMPARATION AND ANALYSIS OF PERFORMANCE OF ENCRYPTION- DECRYPTION OF TEXT USING AES ALGORITHM AND MODIFIED AES BASED ON ANDROID" 2 (2): 3022–30.
- Sharif, Suhaila Orner, dan S P Mansoor. 2010. "Performance Analysis of Stream and Block Cipher Algorithms," 522–25.
- Shi, Hui, Yuanqing Deng, dan Guan Yu. 2011. "Analysis of the Avalanche Effect of the AES S Box." *2011 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce, AIMSEC 2011 - Proceedings*, 5425–28. <https://doi.org/10.1109/AMSEC.2011.6009935>.
- Shulhan, Izzat. 2018. "Analisis Perbandingan Antara Algoritma Rijndael Dan Algoritma Twofish Dalam Penyandian Teks." *Jurnal Teknik Informatika Unika St. Thomas (JTIUST)* 03.
- Silva, Mathieu Da, Emanuele Valea, Marie-lise Flottes, Sophie Dupuis, Giorgio Di Natale, dan Bruno Rouzeyre. 2018. "Encryption of Test Data : Which Cipher Is Better ?" *2018 14th Conference on Ph.D. Research in Microelectronics and Electronics (PRIME)*, 85–88.