

**IMPLEMENTASI ALGORITMA KRIPTOGRAFI  
DENGAN S-BOX DINAMIS BERGANTUNG PADA KUNCI UTAMA  
BERBASIS *ADVANCED ENCRYPTION STANDARD* (AES)**



**SKRIPSI**

**Disusun Sebagai Salah Satu Syarat  
Untuk Memperoleh Gelar Sarjana Komputer  
Pada Jurusan Ilmu Komputer/Informatika**

**Disusun Oleh :  
HERDAYA ADIYASA  
J2F009084**

**JURUSAN ILMU KOMPUTER/INFORMATIKA  
FAKULTAS SAINS DAN MATEMATIKA  
UNIVERSITAS DIPONEGORO**

**2014**

## HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Saya yang bertanda tangan di bawah ini :

Nama : Herdaya Adiyasa  
NIM : J2F009084  
Judul : Implementasi Algoritma Kriptografi  
dengan S-box Dinamis Bergantung pada Kunci Utama  
Berdasarkan *Advanced Encryption Standard* (AES)

Dengan ini saya menyatakan bahwa dalam tugas akhir / skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu perguruan tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Semarang, 24 September 2014



Herdaya Adiyasa  
J2F009084

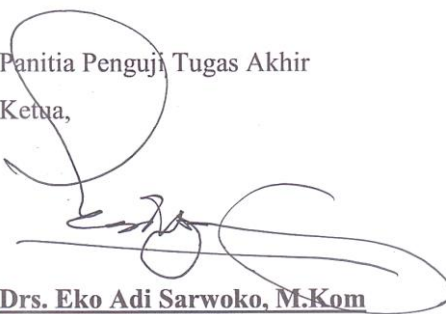
## HALAMAN PENGESAHAN

Judul : Implementasi Algoritma Kriptografi dengan S-box Dinamis Bergantung pada  
Kunci Utama Berbasis *Advanced Encryption Standard* (AES)  
Nama : Herdaya Adiyasa  
NIM : J2F009084

Telah diujikan pada sidang tugas akhir pada tanggal 12 September 2014 dan dinyatakan  
lulus pada tanggal **22 September 2014**.

Mengetahui,  
Ketua Jurusan Ilmu Komputer/Informatika  
FSM JUNDIP  
  
**Nurdin Bahriar, S.Si, M.T**  
NIP. 19790720 200312 1 002

Semarang, 24 September 2014

Panitia Penguji Tugas Akhir  
Ketua,  
  
**Drs. Eko Adi Sarwoko, M.Kom**  
NIP. 19651107 199203 1 003

## HALAMAN PENGESAHAN

Judul : Implementasi Algoritma Kriptografi dengan S-box Dinamis Bergantung pada  
Kunci Utama Berbasis *Advanced Encryption Standard* (AES)

Nama : Herdaya Adiyasa

NIM : J2F009084

Telah diujikan pada sidang tugas akhir pada tanggal 12 September 2014

Pembimbing I



Drs. Putut Sri Wasito, M.Kom

NIP. 19530628 198003 1 001

Semarang, 24 September 2014

Pembimbing II



Satriyo Adhy, S.Si, M.T

NIP. 19830203 200604 1 002

## ABSTRAK

*Advanced Encryption Standard* (AES) merupakan sebuah algoritma kriptografi yang ditetapkan *National Institute of Standards and Technology* (NIST) Amerika sebagai standar untuk algoritma enkripsi data elektronik. Penelitian tentang penggunaan S-box yang dinamis pada AES telah dilakukan sebelumnya dan disimpulkan dapat meningkatkan kompleksitas algoritma AES. Penelitian ini mengimplementasikan penggunaan S-box dinamis dalam algoritma AES tanpa melakukan perubahan operasi dasar AES. Implementasi dilakukan pada berkas citra BMP dengan menggunakan dua mode operasi. Hasil implementasi pada penelitian ini menunjukkan bahwa perubahan S-box AES menjadi S-box dinamis tidak mempengaruhi efektivitas dari algoritma AES. Hal tersebut dibuktikan dengan uji kemiripan citra asli dengan citra hasil dekripsi yang menunjukkan hasil 100 % pada semua citra uji. Penelitian ini juga membuktikan bahwa penggunaan S-box dinamis pada AES dapat diimplementasikan pada berkas citra. Implementasi pada berkas multimedia jenis lain masih memungkinkan untuk penelitian selanjutnya.

**Kata Kunci** : kriptografi, AES, S-box dinamis, ECB, CBC, citra BMP.

## **ABSTRACT**

Advanced Encryption Standard (AES) is a cryptographic algorithm which standardized by the U.S National Institute of Standards and Technology (NIST) as a standard for electronic data encryption algorithm. A research about Dynamic S-box application in AES algorithm has been done previously and might increase the complexity of the AES algorithm. This study implements the use of Dynamic S-box in AES algorithm without changing the basic operation of AES. The implementation has been done on BMP image files by using two modes of operation. The result of the implementation in this study indicate that the changes of S-box to be Dynamic S-box does not affect the effectivity of AES algorithm. It is proven by the similarity test of the original images compared to decrypted cipher images that show the results of 100 % on all of the test images. This study also proves that the use of the Dynamic S-box could be implemented on an image file. Implementation in other types of multimedia files is still opened for further research.

**Keywords** : cryptography, AES, dynamic S-box, ECB, CBC, BMP image.

## KATA PENGANTAR

Puji syukur penulis sampaikan atas limpahan rahmat, hidayah dan kesempatan yang telah diberikan oleh Allah SWT sehingga penulis dapat menyelesaikan laporan tugas akhir ini.

Tugas akhir yang berjudul “Implementasi Algoritma Kriptografi dengan S-box Dinamis Bergantung pada Kunci Utama Berbasis Advanced Encryption Standard (AES)” ini disusun sebagai salah satu syarat untuk memperoleh gelar sarjana strata satu pada Jurusan Ilmu Komputer / Informatika Fakultas Sains dan Matematika Universitas Diponegoro Semarang.

Penulis dalam penyusunan tugas akhir ini mendapatkan banyak bimbingan, bantuan dan dukungan dari berbagai pihak. Oleh karena itu, dengan ketulusan dan kerendahan hati, penulis menyampaikan terimakasih kepada :

1. Dr. Muhammad Nur, DEA, selaku Dekan FSM UNDIP
2. Nurdin Bahtiar, S.Si, M.T, selaku Ketua Jurusan Ilmu Komputer / Informatika UNDIP
3. Indra Waspada, S.T, M.TI, selaku Koordinator Tugas Akhir
4. Drs. Putut Sri Wasito, M.Kom, selaku dosen pembimbing I tugas akhir ini
5. Satriyo Adhy, S.Si, M.T, selaku dosen pembimbing II tugas akhir ini
6. Serta semua pihak yang telah membantu selesainya tugas akhir ini, yang tidak dapat penulis sebutkan satu persatu. Semoga Allah SWT membalas segala kebaikan yang telah dilakukan.

Penulis sadar bahwa dalam penulisan laporan ini tentu masih banyak kekurangan baik dalam penyampaian materi maupun isi dari materi itu sendiri. Hal ini dikarenakan keterbatasan kemampuan dan pengetahuan penulis. Oleh karena itu, kritik dan saran yang membangun sangat penulis harapkan.

Semoga laporan tugas akhir ini dapat membawa manfaat bagi penulis dan semua pembaca.

Semarang, September 2014

Herdaya Adiyasa

## DAFTAR ISI

HALAMAN PERNYATAAN KEASLIAN SKRIPSI.....	ii
HALAMAN PENGESAHAN .....	iii
HALAMAN PENGESAHAN .....	iv
ABSTRAK .....	v
ABSTRACT .....	vi
KATA PENGANTAR.....	vii
DAFTAR ISI .....	viii
DAFTAR GAMBAR.....	x
DAFTAR TABEL .....	xii
DAFTAR ALGORITMA .....	xiv
BAB I PENDAHULUAN .....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	2
1.3 Tujuan dan Manfaat.....	2
1.4 Ruang Lingkup .....	3
1.5 Sistematika Penulisan .....	3
BAB II TINJAUAN PUSTAKA .....	5
2.1 Definisi Kriptografi .....	5
2.2 Algoritma <i>Advanced Encryption Standard</i> .....	7
2.3 Transformasi pada <i>Advanced Encryption Standard</i> .....	8
2.3.1 Proses Enkripsi <i>Advanced Encryption Standard</i> .....	8
2.3.2 Proses Dekripsi <i>Advanced Encryption Standard</i> .....	11
2.4 Algoritma Kriptografi dengan S-box Dinamis .....	13
2.4.1 Pembentukan S-box Dinamis untuk Enkripsi.....	14
2.4.2 Pembentukan <i>Invers</i> S-box Dinamis untuk Dekripsi.....	14
2.5 Mode Operasi <i>Block Cipher</i> .....	15
2.5.1 Mode <i>Electronic Code Book</i> .....	15
2.5.2 Mode <i>Cipher Block Chaining</i> .....	15
2.6 Berkas Citra BMP.....	17
2.7 <i>Unified Modeling Language</i> .....	18
2.7.1 <i>Use Case Diagram</i> .....	19



2.7.2	<i>Class Diagram</i> .....	20
2.7.3	<i>Sequence Diagram</i> .....	22
2.7.4	<i>Activity Diagram</i> .....	24
2.8	Model Proses <i>Unified Process</i> .....	26
2.8.1	Struktur <i>Unified Process</i> .....	26
2.8.2	Fase <i>Inception</i> .....	28
2.8.3	Fase <i>Elaboration</i> .....	28
2.8.4	Fase <i>Construction</i> .....	28
2.8.5	Fase <i>Transition</i> .....	28
2.9	Pengujian Citra Berdasarkan Perubahan Nilai <i>Pixel</i> .....	29
2.10	Bahasa Pemrograman <i>C#</i> .....	29
BAB III FASE <i>INCEPTION</i> DAN FASE <i>ELABORATION</i> .....		31
3.1	Rencana Iterasi .....	31
3.2	Fase <i>Inception</i> .....	31
3.2.1	Deskripsi Sistem .....	32
3.2.2	<i>Business Rules</i> .....	33
3.2.3	Kebutuhan Non-fungsional .....	33
3.2.4	Model <i>Use case</i> .....	34
3.3	Fase <i>Elaboration</i> .....	39
3.3.1	<i>Elaboration</i> Iterasi Pertama .....	39
3.3.2	<i>Elaboration</i> Iterasi Kedua .....	44
3.3.3	<i>Elaboration</i> Iterasi Ketiga .....	57
BAB IV FASE <i>CONSTRUCTION</i> DAN FASE <i>TRANSITION</i> .....		63
4.1	Implementasi Perangkat Lunak .....	63
4.1.1	Implementasi Objek .....	63
4.1.2	Implementasi Antarmuka .....	68
4.2	Pengujian Perangkat Lunak .....	71
4.2.1	Lingkungan Pengujian .....	71
4.2.2	Pelaksanaan Pengujian .....	71
4.3	Analisis Hasil Pengujian .....	72
4.4	Rilis Perangkat Lunak .....	72
BAB V PENUTUP .....		75
DAFTAR PUSTAKA .....		76
LAMPIRAN .....		78

## DAFTAR GAMBAR

Gambar 2. 1 Proses enkripsi .....	6
Gambar 2. 2 Proses dekripsi .....	6
Gambar 2. 3 Proses <i>SubBytes</i> .....	9
Gambar 2. 4 Proses <i>ShiftRows</i> .....	9
Gambar 2. 5 Proses <i>MixColumns</i> .....	10
Gambar 2. 6 Operasi perkalian dan penjumlahan.....	10
Gambar 2. 7 Proses <i>AddRoundKey</i> .....	11
Gambar 2. 8 Matriks pengali pada tahap <i>InvMixColumns</i> .....	13
Gambar 2. 9 Mode <i>Electronic CodeBook</i> .....	16
Gambar 2. 10 Mode <i>Cipher Block Chaining</i> .....	16
Gambar 2. 11 Contoh berkas citra BMP.....	17
Gambar 2. 12 Format berkas BMP .....	17
Gambar 2. 13 Contoh <i>use case diagram</i> .....	20
Gambar 2. 14 Contoh <i>class diagram</i> .....	22
Gambar 2. 15 Contoh <i>sequence diagram</i> .....	24
Gambar 2. 16 Contoh <i>activity diagram</i> .....	26
Gambar 2. 17 Siklus hidup <i>unified process</i> .....	27
Gambar 2. 18 Hubungan fase dengan <i>workflow</i> dalam <i>unified process</i> .....	27
Gambar 3. 1 Alur proses aplikasi implementasi algoritma kriptografi .....	32
Gambar 3. 2 <i>Use case diagram</i> aplikasi .....	35
Gambar 3. 3 <i>Class diagram</i> aplikasi .....	39
Gambar 3. 4 <i>Sequence diagram</i> Input Berkas Citra .....	40
Gambar 3. 5 <i>Sequence diagram</i> Mengenkripsi Citra .....	41
Gambar 3. 6 <i>Sequence diagram</i> Mendekripsi Citra .....	42
Gambar 3. 7 <i>Sequence diagram</i> Atur Mode Operasi.....	43
Gambar 3. 8 <i>Sequence diagram</i> Simpan Citra Hasil .....	43
Gambar 3. 9 <i>Activity diagram</i> aplikasi .....	44
Gambar 3. 10 <i>Flowchart</i> enkripsi dan dekripsi .....	45
Gambar 3. 11 <i>Flowchart</i> mesin enkripsi .....	46
Gambar 3. 12 <i>Flowchart</i> mesin dekripsi .....	47

Gambar 3. 13 Alur algoritma AES .....	55
Gambar 3. 14 Antarmuka menu proses kriptografi bagian enkripsi.....	59
Gambar 3. 15 Antarmuka menu proses kriptografi bagian dekripsi.....	59
Gambar 3. 16 Antarmuka menu proses kriptografi bagian pengujian.....	60
Gambar 3. 17 Antarmuka menu pengaturan.....	60
Gambar 4. 1 Implementasi antarmuka menu proses kriptografi bagian enkripsi.....	69
Gambar 4. 2 Implementasi antarmuka menu proses kriptografi bagian dekripsi.....	69
Gambar 4. 3 Implementasi antarmuka menu proses kriptografi bagian pengujian.....	70
Gambar 4. 4 Implementasi antarmuka menu pengaturan .....	70

## DAFTAR TABEL

Tabel 2. 1 Perbandingan ukuran kunci dan jumlah ronde pada AES .....	7
Tabel 2. 2 Tabel S-box .....	8
Tabel 2. 3 Tabel <i>invers</i> S-box.....	12
Tabel 2. 4 Perbandingan AES 128 bit dan algoritma oleh Sliman Arrag, dkk.....	14
Tabel 2. 5 Komponen <i>use case diagram</i> .....	19
Tabel 2. 6 Komponen <i>class diagram</i> .....	21
Tabel 2. 7 Komponen <i>sequence diagram</i> .....	23
Tabel 2. 8 Komponen <i>activity diagram</i> .....	25
Tabel 3. 1 Daftar aktor.....	34
Tabel 3. 2 Daftar <i>use case</i> .....	34
Tabel 3. 3 Detail <i>Use Case Input</i> Berkas Citra.....	36
Tabel 3. 4 Detail <i>Use Case</i> Mengenkripsi Citra.....	36
Tabel 3. 5 Detail <i>Use Case</i> Mendekripsi Citra.....	37
Tabel 3. 6 Detail <i>Use Case</i> Atur Mode Operasi .....	37
Tabel 3. 7 Detail <i>Use Case</i> Simpan Citra Hasil .....	38
Tabel 3. 8 Tabel S-box $\oplus$ 6f .....	53
Tabel 3. 9 Tabel <i>invers</i> S-box $\oplus$ 6f .....	54
Tabel 3. 10 Rencana pengujian struktur aplikasi.....	61
Tabel 3. 11 Rencana pengujian kriptografi citra .....	62
Tabel 4. 1 Tabel implementasi kelas .....	63
Tabel 4. 2 Implementasi atribut kelas GUI.....	64
Tabel 4. 3 Implementasi operasi kelas GUI .....	65
Tabel 4. 4 Implementasi atribut kelas Enkripsi .....	65
Tabel 4. 5 Implementasi operasi kelas Enkripsi .....	65
Tabel 4. 6 Implementasi atribut kelas Dekripsi .....	66
Tabel 4. 7 Implementasi operasi kelas Dekripsi.....	66
Tabel 4. 8 Implementasi atribut kelas ModeOperasi.....	66
Tabel 4. 9 Implementasi operasi kelas ModeOperasi.....	67
Tabel 4. 10 Implementasi atribut kelas Crypto.....	67
Tabel 4. 11 Implementasi operasi kelas Crypto .....	68

Tabel 4. 12 Spesifikasi perangkat lunak rilis.....	72
Tabel 4. 13 Hasil pengujian struktur aplikasi .....	73

## DAFTAR ALGORITMA

Algoritma 3. 1 Algoritma penanganan khusus berkas BMP .....	48
Algoritma 3. 2 Algoritma <i>padding</i> pada mode operasi .....	49
Algoritma 3. 3 Algoritma ECB untuk enkripsi.....	49
Algoritma 3. 4 Algoritma ECB untuk dekripsi.....	50
Algoritma 3. 5 Algoritma CBC untuk enkripsi .....	50
Algoritma 3. 6 Algoritma CBC untuk dekripsi .....	51
Algoritma 3. 7 Algoritma pembentukan S-box dinamis.....	51
Algoritma 3. 8 Algoritma pembentukan <i>invers</i> S-box dinamis.....	52
Algoritma 3. 9 Algoritma enkripsi kriptografi dengan S-box dinamis.....	56
Algoritma 3. 10 Algoritma dekripsi kriptografi dengan S-box dinamis.....	57

# BAB I

## PENDAHULUAN

Bab ini memaparkan latar belakang, rumusan masalah, tujuan dan manfaat, ruang lingkup dan sistematika dalam penelitian tugas akhir mengenai implementasi algoritma kriptografi dengan S-box dinamis bergantung pada kunci utama berbasis AES.

### 1.1 Latar Belakang

Perkembangan teknologi informasi yang pesat memberikan kemudahan kepada penggunaannya dalam melakukan pertukaran informasi. Data atau informasi dalam pertukarannya tidak hanya disajikan dalam bentuk teks, tetapi juga dapat berupa gambar (citra), audio dan video. Keempat macam data atau informasi ini sering disebut multimedia. Citra sebagai salah satu komponen multimedia memegang peranan penting sebagai bentuk informasi dalam bentuk *visual*. Citra kaya akan informasi secara *visual* sehingga sebuah citra dapat memberikan informasi yang lebih banyak daripada jika suatu informasi disajikan dalam bentuk teks. Tidak heran jika pertukaran informasi menggunakan citra kini begitu populer digunakan di media internet. (Munir, 2004)

Pertukaran informasi yang tidak aman dapat meningkatkan kerentanan terhadap akses suatu informasi yang bersifat pribadi atau rahasia. Kriptografi merupakan solusi untuk menyembunyikan informasi asli dari suatu berkas. Menurut Paar pada buku "*Understanding Cryptography*", kriptografi adalah ilmu penulisan rahasia dengan tujuan menyembunyikan arti dari pesan (Paar & Pelzl, 2010). Proses kriptografi untuk mengubah dari berkas asli (*plaintext*) menjadi berkas yang dirahasiakan (*ciphertext*) disebut enkripsi dan sebaliknya disebut dekripsi. Sebuah sistem enkripsi terdiri dari serangkaian transformasi yang mengubah *plaintext* menjadi *ciphertext*. Kriptografi memiliki berbagai algoritma yang semakin berkembang seiring dengan teknologi informasi.

Seiring peningkatan kecepatan perangkat keras komputer dibutuhkan pula algoritma-algoritma kriptografi yang lebih aman untuk mencegah terbongkarnya suatu *ciphertext*. Tahun 2001, *National Institute of Standard and Technology* (NIST) Amerika Serikat menetapkan sebuah algoritma bernama *Rijndael* untuk menjadi sebuah standar yang disebut *Advanced Encryption Standard* (AES) sebagai pengganti

algoritma DES. Algoritma DES dianggap tidak dapat digunakan lagi karena kunci yang digunakan dapat dibobol hanya dalam empat hari pada waktu itu. (NIST, 2001)

Tahun 2013, Sliman Arrag, dkk melakukan penelitian berjudul, “*Implementation of Stronger AES by Using Dynamic S-box Dependent of Master Key*”. Sliman Arrag, dkk mengusulkan sebuah algoritma yang berbasis AES untuk diimplementasikan pada sebuah perangkat FPGA. Penelitian tersebut melakukan modifikasi tabel substitusi yang digunakan pada transformasi algoritma AES (Arrag, et al., 2013). Algoritma AES mempunyai tabel substitusi (S-box) pada transformasinya yang bernilai selalu sama pada setiap proses enkripsi atau dekripsi algoritma tersebut (Daemen & Rijmen, 2001). Penelitian Sliman Arrag, dkk menggunakan tabel S-box dinamis yang dibentuk ulang bergantung pada *Master Key* (pada penelitian ini disebut dengan kunci utama) dalam setiap proses enkripsi atau dekripsi. Penelitian tersebut menyebutkan bahwa penggunaan S-box dinamis dapat meningkatkan keamanan algoritma AES. Oleh karena itu penulis berinisiatif untuk membuat sebuah implementasi algoritma dengan S-box dinamis yang bergantung pada kunci utama untuk diimplementasikan pada berkas citra. Implementasi tersebut adalah sebagai solusi untuk pengamanan berkas citra yang diharapkan bisa menjadi lebih baik daripada implementasi dengan algoritma AES biasa.

## **1.2 Rumusan Masalah**

Berdasarkan uraian latar belakang di atas, dapat dirumuskan permasalahan yang dihadapi yaitu bagaimana mengimplementasikan algoritma kriptografi dengan S-box dinamis bergantung pada kunci utama berbasis AES pada berkas citra.

## **1.3 Tujuan dan Manfaat**

Tujuan yang ingin dicapai dalam penelitian tugas akhir ini adalah menghasilkan sebuah implementasi algoritma kriptografi dengan S-box dinamis bergantung pada kunci utama berbasis AES pada berkas citra.

Manfaat dari penelitian tugas akhir ini adalah

1. Aplikasi hasil implementasi pada tugas akhir ini dapat dijadikan solusi untuk pengamanan berkas citra dan dapat sebagai acuan untuk pengembangan kriptografi pada citra.
2. Hasil pengujian aplikasi ini dapat menjadi acuan untuk melihat performa algoritma kriptografi yang digunakan jika diimplementasikan pada berkas citra.



## 1.4 Ruang Lingkup

Penyusunan laporan tugas akhir ini diberikan ruang lingkup yang jelas agar pembahasan lebih terarah dan tidak menyimpang dari tujuan penulisan. Ruang lingkup implementasi algoritma kriptografi dengan S-box dinamis bergantung pada kunci utama berbasis AES pada berkas citra adalah sebagai berikut:

1. *Input* proses enkripsi berupa *file* citra BMP (\*.bmp) dan output berupa *file* citra BMP (\*.bmp).
2. Berkas citra BMP yang digunakan adalah format BMP versi baru dari *Microsoft*
3. Algoritma kriptografi yang digunakan sebagai basis adalah *Advanced Encryption Standard (AES)*.
4. Ukuran kunci AES yang digunakan adalah 128 bit, 192 bit dan 256 bit.
5. S-box dinamis yang dibuat adalah sebagai pengganti S-box standar dari AES.
6. *Invers* S-box dinamis sebagai hasil *invers* dari S-box dinamis yang dibuat adalah pengganti *invers* S-box standar dari AES.
7. Mode operasi yang digunakan adalah *Electronic Code Book (ECB)* dan *Cipher Block Chaining (CBC)*.
8. Implementasi dibuat dengan berbasis *desktop* menggunakan bahasa pemrograman *C# IDE Visual Studio 2010*.

## 1.5 Sistematika Penulisan

Sistematika penulisan yang digunakan dalam tugas akhir ini terbagi dalam beberapa pokok bahasan, yaitu :

### BAB I PENDAHULUAN

Bab ini memaparkan latar belakang, rumusan masalah, tujuan dan manfaat, ruang lingkup dan sistematika dalam pembuatan tugas akhir mengenai implementasi algoritma kriptografi dengan S-box dinamis bergantung pada kunci utama berbasis AES.

### BAB II TINJAUAN PUSTAKA

Bab ini menyajikan kumpulan studi pustaka yang berhubungan dengan topik tugas akhir. Tinjauan pustaka yang digunakan dalam penyusunan tugas akhir ini meliputi, definisi kriptografi, algoritma AES, transformasi pada AES, algoritma kriptografi dengan S-box dinamis, mode operasi *block cipher*, berkas citra BMP, *Unified Modeling Language*, model

proses *Unified Process*, bahasa pemrograman *C#* dan pengujian citra berdasarkan perubahan nilai *pixel*.

### BAB III FASE *INCEPTION* DAN FASE *ELABORATION*

Bab ini menyajikan tahapan proses pembangunan perangkat lunak menggunakan model pengembangan *Unified Process*. Bab ini menyajikan dua fase awal yaitu fase *inception* dan fase *elaboration*.

### BAB IV FASE *CONSTRUCTION* DAN FASE *TRANSITION*

Bab ini menyajikan tahapan proses pembangunan perangkat lunak menggunakan model pengembangan *Unified Process*. Bab ini menyajikan fase *construction* dan fase *transition*.

### BAB V PENUTUP

Bab ini berisi kesimpulan dari pengerjaan penelitian tugas akhir ini dan saran-saran penulis untuk pengembangan lebih lanjut dari penelitian serupa.