

**ANALISIS PERBANDINGAN ALGORITMA ADVANCED  
ENCRYPTION STANDARD UNTUK ENKRIPSI SHORT MESSAGE  
SERVICE (SMS) PADA ANDROID**

**SKRIPSI**

Untuk memenuhi sebagian persyaratan  
memperoleh gelar Sarjana Komputer

Disusun oleh:  
Fredianto  
125150200111069



PROGRAM STUDI TEKNIK INFORMATIKA  
JURUSAN TEKNIK INFORMATIKA  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS BRAWIJAYA  
MALANG  
2018

# PENGESAHAN

ANALISIS PERBANDINGAN ALGORITMA ADVANCED ENCRYPTION STANDARD  
UNTUK ENKRIPSI SHORT MESSAGE SERVICE (SMS) PADA ANDROID

SKRIPSI

Diajukan untuk memenuhi sebagian persyaratan  
memperoleh gelar Sarjana Komputer

Disusun Oleh:  
Fredianto  
125150200111069

Skripsi ini telah diuji dan dinyatakan lulus pada  
15 Januari 2018  
Telah diperiksa dan disetujui oleh:

Dosen Pembimbing I

Dosen Pembimbing II

Ari Kusyanti, S.T, M.Sc  
NIK. 201102 831228 2 001

Kasyful Amron, S.T, M.Sc  
NIP. 19750803 200312 1 003

Mengetahui  
Ketua Jurusan Teknik Informatika

Tri Astoto Kurniawan, S.T, M.T, Ph.D  
NIP: 19710518 200312 1 001

## **PERNYATAAN ORISINALITAS**

Saya menyatakan dengan sebenar-benarnya bahwa sepanjang pengetahuan saya, di dalam naskah skripsi ini tidak terdapat karya ilmiah yang pernah diajukan oleh orang lain untuk memperoleh gelar akademik di suatu perguruan tinggi, dan tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis disitasi dalam naskah ini dan disebutkan dalam daftar pustaka.

Apabila ternyata didalam naskah skripsi ini dapat dibuktikan terdapat unsur-unsur plagiasi, saya bersedia skripsi ini digugurkan dan gelar akademik yang telah saya peroleh (sarjana) dibatalkan, serta diproses sesuai dengan peraturan perundang-undangan yang berlaku (UU No. 20 Tahun 2003, Pasal 25 ayat 2 dan Pasal 70).

Malang, 15 Januari 2018

Fredianto

NIM: 125150200111069

## KATA PENGANTAR

Puji dan syukur penulis panjatkan kepada Tuhan Yang Maha Esa atas berkat, rahmat, ridho dan karunia-Nya sehingga penulis dapat menyelesaikan tugas akhir yang berjudul **“Analisis Perbandingan Algoritma Advanced Encryption Standard untuk Enkripsi Short Message Service (SMS) Berbasis Android”** sebagai salah satu persyaratan untuk menyelesaikan studi di Jurusan Informatika, Fakultas Ilmu Komputer Universitas Brawijaya.

Penulis menyadari bahwa tugas akhir ini dapat terselesaikan berkat bantuan, petunjuk, bimbingan dan dukungan dari berbagai pihak yang telah banyak membantu proses penyelesaian tugas akhir ini. Oleh karena itu penulis ingin menyampaikan terima kasih yang sebesar-besarnya kepada:

1. Ari Kusyanti, S.T, M.Sc selaku pembimbing I dan Kasyful Amron, S.T, M.Sc selaku pembimbing II yang telah membimbing dan mengarahkan penulis sehingga dapat menyelesaikan skripsi ini.
2. Orang tua penulis, Ibu Maria Lucia Sri Astuti yang tak henti-hentinya memberikan dukungan moril dan materil serta dan semangat demi terselesaikanya skripsi ini.
3. Saudara penulis, Kristina Yuliani, Aufrida Yanti Dwi Lestari, serta Alm. Antonius Rudi Trianto yang telah memberikan motivasi dan semangat demi terselesaikanya skripsi ini
4. Bapak Nicolaas Tirtadinata dan Ibu Hani, Bapak dan Ibu Katrin, Ibu Budi, serta Bapak Basuki yang telah memberikan dukungan moril dan materil selama penulis mengenyam pendidikan
5. Seluruh dosen Program Teknologi Informasi dan Ilmu Komputer Universitas Brawijaya atas kesediaan membagi ilmunya kepada penulis sehingga penulis dapat menyelesaikan skripsi ini.
6. Sahabat penulis Moh. Irfan Haris, Lulus Bagos H, Rian Deka, yang senantiasa menemani, bertukar ilmu, serta memberikan semangat dan motivasi dalam penyelesaian skripsi.
7. Teman-teman KMK Filkom, serta UAKKat Universitas Brawijaya yang telah memberi pengalaman berharga dalam kehidupan kampus
8. Teman-teman seperjuangan Program Teknologi Informasi dan Ilmu Komputer angkatan 2012 yang telah memberikan bantuan selama masa studi hingga penyelesaian skripsi ini.
9. Dan semua pihak yang tidak bisa disebutkan satu per satu. Terima kasih atas segala bantuannya.

Penulis sadar bahwa skripsi ini masih banyak kekurangan, oleh karena itu kritik dan saran yang bersifat membangun sangat diharapkan untuk menyempurnakan

skripsi ini. Penulis berharap skripsi ini dapat bermanfaat khususnya bagi diri sendiri dan bagi semua pihak.

Malang, 15 Januari 2018

Penulis

Fredianto.agustinus@gmail.com

## **ABSTRAK**

Short Message Service (SMS) merupakan suatu layanan yang populer dikalangan pengguna telepon seluler di Indonesia. Celah keamanan terbesar pada komunikasi SMS adalah dapat terbacanya pesan yang dikirimkan dan disimpan pada Short Message Service Center (SMSC) ketika terjadi serangan pada SMSC. Salah satu solusi menanggulangi masalah tersebut adalah dengan melakukan penyandian pesan yang dikirimkan atau lebih dikenal dengan enkripsi. Pada penelitian ini dilakukan analisis perbandingan antar algoritma AES, yaitu AES 128 bit, AES 192 bit, serta AES 256 bit untuk enkripsi pesan SMS pada Android. Protokol Elliptic Curve Diffie-Hellman (ECDH) digunakan dalam mekanisme pertukaran kunci untuk proses enkripsi dan dekripsi pesan. Pada penelitian ini didapatkan hasil semakin panjang data maka akan semakin lama waktu proses enkripsi dan dekripsi. Pada penelitian ini tidak ditemukan perbedaan performansi yang signifikan, hal ini dibuktikan dengan pengujian ANOVA yang telah dilakukan dengan masing-masing panjang data.

## **ABSTRACT**

*Short Message Service (SMS) is a popular service among mobile phone users in Indonesia. The biggest security gap in SMS communications is that it can read messages and save them to the Short Message Service Center (SMSC) when an SMSC attack occurs. One solution to solve the problem is by encoding messages that are sent or better known as encryption. In this research, AES 128 AES, AES 192 bits AES and AES 256 bits are used for SMS message encryption on Android. The Elliptic Curve Diffie-Hellman (ECDH) protocol is used in key exchange mechanisms for encryption and decryption of messages. In this study obtained the longer the data will be the longer the process of encryption and decryption. In this research, there is no significant performance difference, it is proved by ANOVA test which has been done with each data length.*

## DAFTAR ISI

PENGESAHAN .....	ii
PERNYATAAN ORISINALITAS .....	iii
KATA PENGANTAR.....	iv
ABSTRAK.....	vi
ABSTRACT .....	vii
DAFTAR ISI.....	viii
DAFTAR TABEL.....	xi
DAFTAR GAMBAR.....	xiii
DAFTAR LAMPIRAN .....	xv
BAB 1 PENDAHULUAN.....	1
1.1 Latar belakang.....	1
1.2 Rumusan masalah .....	2
1.3 Tujuan .....	2
1.4 Manfaat.....	2
1.5 Batasan masalah .....	3
1.6 Sistematika pembahasan .....	3
BAB 2 LANDASAN KEPUSTAKAAN .....	5
2.1 Kajian Pustaka .....	5
2.2 SMS .....	6
2.2.1 Struktur SMS .....	6
2.2.2 Arsitektur SMS.....	7
2.3 Android .....	7
2.3.1 Konsep Platform Android.....	8
2.3.2 Konsep Pengembangan Android.....	9
2.4 Kriptografi .....	9
2.4.2 Algoritma Kriptografi.....	10
2.5 Diffie-Hellman Key Exchange .....	11
2.5.1 Elliptic Curve Cryptography (ECC) .....	12
2.5.2 Elliptic Curve Domain Parameter .....	13
2.5.3 Elliptic Curve Diffie-Hellman Key Exchange .....	14



2.6 AES .....	15
2.6.1 Input dan Output .....	15
2.6.2 <i>byte</i> .....	15
2.6.3 <i>Array bytes</i> .....	16
2.6.4 <i>State</i> .....	17
2.6.5 Algoritma kriptografi AES.....	18
2.6.6 Proses Inisialisasi Kunci Internal .....	18
2.6.7 Contoh proses inisialisasi kunci internal .....	20
2.6.8 Proses enkripsi .....	23
2.6.9 Proses Dekripsi .....	27
2.6.10 Perbedaan AES 128 bit, AES 192 bit dan AES 256 bit .....	29
BAB 3 METODOLOGI .....	31
3.1 Studi Literatur .....	31
3.2 Analisa Kebutuhan .....	32
3.3 Perancangan Sistem.....	32
3.4 Implementasi .....	33
3.5 Pengujian dan Analisis Hasil.....	33
3.6 Pegambilan Kesimpulan.....	33
BAB 4 PERANCANGAN.....	34
4.1 Perancangan Proses Algoritma.....	34
4.1.1 Proses Tukar Kunci .....	34
4.1.2 Proses Enkripsi .....	35
4.1.3 Proses Dekripsi .....	40
4.2 Perancangan Sistem.....	41
4.2.1 Perancangan Antar Muka Perangkat Lunak Pengujian.....	41
4.3 Perancangan Lingkungan Pengujian .....	42
BAB 5 implementasi .....	43
5.1 Implementasi Algoritma .....	43
5.1.1 Implementasi Proses Tukar Kunci .....	43
5.1.2 Implementasi Proses Enkripsi .....	44
5.1.3 Implementasi Proses Dekripsi.....	45
5.2 Implementasi Antar Muka .....	46

5.2.1 Antar Muka Halaman Awal .....	46
5.2.2 Antar Muka Buat Pesan.....	47
5.3 Implementasi Lingkungan Pengujian.....	48
5.3.1 Perangkat Lingkungan Pengujian.....	49
BAB 6 Pengujian dan Analisis .....	51
6.1 Pengujian .....	51
6.1.1 Pengujian Performansi.....	51
6.1.2 Pengujian Analisis Variansi (ANOVA) .....	52
6.2 Hasil dan Analisis .....	53
6.2.1 Analisis Variansi Pada Enkripsi dengan Panjang Data 12.....	53
6.2.2 Analisis Variansi Pada Enkripsi dengan Panjang Data 16.....	55
6.2.3 Analisis Variansi Pada Enkripsi dengan Panjang Data 32.....	56
6.2.4 Analisis Variansi Pada Enkripsi dengan Panjang Data 160.....	57
6.2.5 Analisis Variansi Pada Enkripsi dengan Panjang Data 300.....	58
6.2.6 Analisis Variansi Pada Dekripsi dengan Panjang Data 12 .....	60
6.2.7 Analisis Variansi Pada Dekripsi dengan Panjang Data 16 .....	61
6.2.8 Analisis Variansi Pada Dekripsi dengan Panjang Data 32 .....	63
6.2.9 Analisis Variansi Pada Dekripsi dengan Panjang Data 160 .....	64
6.2.10 Analisis Variansi Pada Dekripsi dengan Panjang Data 300 .....	65
BAB 7 Penutup .....	67
7.1 Kesimpulan.....	67
7.2 Saran .....	67
DAFTAR PUSTAKA.....	68
LAMPIRAN A TABEL S-BOX DAN INVERSE S-BOX AES .....	70

## DAFTAR TABEL

Tabel 2.1 Tabel Kajian Pustaka.....	5
Tabel 2.2 Representasi heksadesimal dari suatu bit.....	16
Tabel 2.3 Tabel <i>Rcon</i> untuk 10 <i>round key</i> AES.....	20
Tabel 2.4 Perbandingan Jumlah Round dan Key.....	30
Tabel 5.1 Implementasi Proses Tukar Kunci .....	43
Tabel 5.2 Implementasi Fitur Enkripsi.....	44
Tabel 5.3 Implementasi Fitur Dekripsi .....	45
Tabel 6.1 Skenario Pengujian Performansi .....	51
Tabel 6.2 Prosedur Pengujian Performansi.....	52
Tabel 6.3 <i>Descriptive Table</i> dengan Panjang Data 12 .....	54
Tabel 6.4 Tabel <i>Test of Homogeneity of Variances</i> Panjang Data 12.....	54
Tabel 6.5 Tabel Pengujian ANOVA dengan Panjang Data 12.....	54
Tabel 6.6 <i>Descriptive Table</i> dengan Panjang Data 16.....	55
Tabel 6.7 Tabel <i>Test of Homogeneity of Variances</i> Panjang Data 16.....	55
Tabel 6.8 Tabel Pengujian ANOVA dengan Panjang Data 16.....	56
Tabel 6.9 <i>Descriptive Table</i> dengan Panjang Data 32 .....	56
Tabel 6.10 Tabel <i>Test of Homogeneity of Variances</i> Panjang Data 32.....	57
Tabel 6.11 Tabel Pengujian ANOVA dengan Panjang Data 32.....	57
Tabel 6.12 <i>Descriptive Table</i> dengan Panjang Data 160.....	57
Tabel 6.13 Tabel <i>Test of Homogeneity of Variances</i> Panjang Data 160.....	58
Tabel 6.14 Tabel Pengujian ANOVA dengan Panjang Data 160.....	58
Tabel 6.15 <i>Descriptive Table</i> dengan Panjang Data 300.....	59
Tabel 6.16 Tabel <i>Test of Homogeneity of Variances</i> Panjang Data 300.....	59
Tabel 6.17 Tabel Pengujian ANOVA dengan Panjang Data 300.....	60
Tabel 6.18 <i>Descriptive Table</i> dengan Panjang Data 12 .....	60
Tabel 6.19 Tabel <i>Test of Homogeneity of Variances</i> Panjang Data 12.....	61
Tabel 6.20 Tabel Pengujian ANOVA dengan Panjang Data 12.....	61
Tabel 6.21 <i>Descriptive Table</i> dengan Panjang Data 16.....	61
Tabel 6.22 Tabel <i>Test of Homogeneity of Variances</i> Panjang Data 16.....	62
Tabel 6.23 Tabel Pengujian ANOVA dengan Panjang Data 16.....	62

Tabel 6.24 <i>Descriptive Table</i> dengan Panjang Data 32 .....	63
Tabel 6.25 Tabel <i>Test of Homogeneity of Variances</i> Panjang Data 32 .....	63
Tabel 6.26 Tabel Pengujian ANOVA dengan Panjang Data 32 .....	64
Tabel 6.27 <i>Descriptive Table</i> dengan Panjang Data 160 .....	64
Tabel 6.28 Tabel <i>Test of Homogeneity of Variances</i> Panjang Data 160 .....	65
Tabel 6.29 <i>Descriptive Table</i> dengan Panjang Data 300 .....	65
Tabel 6.30 Tabel <i>Test of Homogeneity of Variances</i> Panjang Data 300 .....	66
Tabel 6.31 Tabel Pengujian ANOVA dengan Panjang Data 300 .....	66

## DAFTAR GAMBAR

Gambar 2.1 Struktur SMS (Prihartini, 2006) .....	6
Gambar 2.2 Perkembangan Android .....	7
Gambar 2.3 Simulasi konsep pekerjaan Android (Vogel, 2014) .....	8
Gambar 2.4 Enkripsi dan dekripsi pada <i>plaintext</i> (Schneier, 1996).....	10
Gambar 2.5 Enkripsi dan dekripsi algoritma kunci simetris (Schneier, 1996) .....	10
Gambar 2.6 Enkripsi dan dekripsi algoritma kunci asimetris (Schneier, 1996) ....	11
Gambar 2.7 Mekanisme Diffie-Hellman (Schneier, 1996) .....	12
Gambar 2.8 Proses Elliptic Curve Diffie-Hellman (Hendra, 2014) .....	15
Gambar 2.9 <i>State array</i> , Input dan Output.....	18
Gambar 2.10 Skema proses inisialisasi kunci pada AES.....	19
Gambar 2.11 Skema proses <i>RotCol</i> pada AES.....	19
Gambar 2.12 Contoh <i>array</i> kunci eksternal.....	20
Gambar 2.13 Contoh transformasi <i>RotCol</i> .....	20
Gambar 2.14 Contoh transformasi <i>SubBytes</i> .....	21
Gambar 2.15 Cara memperoleh kolom pertama <i>round key 1</i> .....	21
Gambar 2.16 Cara memperoleh kolom kedua <i>round key 1</i> .....	22
Gambar 2.17 Cara memperoleh kolom ketiga <i>round key 1</i> .....	22
Gambar 2.18 Cara memperoleh kolom keempat <i>round key 1</i> .....	23
Gambar 2.19 Kunci eksternal dan <i>round key</i> .....	23
Gambar 2.20 Skema proses enkripsi AES (Kurniawan, 2007) .....	24
Gambar 2.21 Transformasi <i>AddRoundKey</i> (Gladman, 2001).....	25
Gambar 2.22 Tranformasi <i>SubBytes</i> (Gladman, 2001) .....	26
Gambar 2.23 Transformasi <i>ShiftRows</i> (Gladman, 2001).....	26
Gambar 2.24 Transformasi <i>MixColumns</i> (Gladman, 2001).....	27
Gambar 2.25 Skema global proses dekripsi AES (Kurniawan, 2007) .....	28
Gambar 2.26 Transformasi <i>InvShiftRows</i> (Kurniawan, 2007) .....	29
Gambar 2.27 Transformasi <i>InvMixColumns</i> (Gladman, 2001).....	29
Gambar 3.1 Diagram Alir Metode Penelitian.....	31
Gambar 4.1 Proses Tukar Kunci .....	34
Gambar 4.2 Proses Enkripsi .....	35

Gambar 4.3 Tahapan <i>RotCol</i> pada <i>Round key 1</i> .....	36
Gambar 4.4 Tahapan <i>SubBytes</i> pada <i>Round key 1</i> .....	36
Gambar 4.5 Tahapan XOR dengan Round Constant dan kunci Eksternal.....	37
Gambar 4.6 Tahapan XOR Round Constant dengan Kunci Eksternal .....	37
Gambar 4.7 <i>Round key 1</i> .....	37
Gambar 4.8 <i>Initial round</i> .....	38
Gambar 4.9 Proses <i>SubBytes</i> terhadap <i>State array</i> Round 1 .....	38
Gambar 4.10 Transformasi <i>ShiftRows</i> pada <i>State array</i> Round 1 .....	39
Gambar 4.11 Transformasi <i>MixColumn</i> pada <i>State array</i> Round 1 .....	39
Gambar 4.12 Transformasi <i>AddRoundKey</i> pada <i>State array</i> Round 1.....	39
Gambar 4.13 <i>Ciphertext</i> Hasi dari Proses Enkripsi.....	40
Gambar 4.14 Proses Dekripsi .....	40
Gambar 4.15 Tampilan Halaman Awal .....	41
Gambar 4.16 Tampilan Halaman Buat Pesan .....	42
Gambar 4.17 Rancangan lingkungan pengujian .....	42
Gambar 5.1 Antar Muka Halaman Awal .....	46
Gambar 5.2 Antar Muka Halaman Awal – Pengguna belum melakukan obrolan	47
Gambar 5.3 Antar Muka List Pesan.....	47
Gambar 5.4 Antar Muka Buat Pesan.....	48
Gambar 5.5 Implementasi Lingkungan Pengujian .....	49

## DAFTAR LAMPIRAN

LAMPIRAN A TABEL S-BOX DAN INVERSE S-BOX AES .....	70
A.1 Tabel S-Box AES .....	70
A.2 Tabel Inverse S-Box AES .....	71