

IMPLEMENTASI ALGORITMA ENKRIPSI AES UNTUK APLIKASI SMS BERBASIS SISTEM OPERASI GOOGLE ANDROID

Awang Maristyono
(06.04.111.00862)

Pembimbing I : Cucun Very Angkoso, ST., MT.

Pembimbing II : Moch.Kautsar Sophan, S.Kom., M.MT

ABSTRAK

Pengiriman informasi *Short Message Service (SMS)* merupakan sesuatu hal yang di butuhkan pada masa modern, Layanan *SMS* memiliki kerentanan dalam keamanan data. Kelemahan layanan *SMS* salah satunya disebabkan pada pengguna standard pengkodean yang universal, *SMS* dibangun dengan sistem bahasa program yang sejenis dengan bahasa program *hardware* seperti komputer dan ponsel dapat menerjemahkan semua data dalam frekuensi tertentu yang terbuka. Untuk menjamin keamanan dan kerahasiaan informasi saat pengiriman, dilakukan proses enkripsi dan dekripsi terhadap informasi yang akan dikirimkan. Enkripsi dilakukan pada saat pengiriman dengan cara mengkonversi informasi asli menjadi informasi sementara sedangkan dekripsi dilakukan pada saat penerimaan dengan cara mengkonversi informasi sementara menjadi informasi asli. Jadi informasi yang dikirimkan selama proses pengiriman adalah data informasi sementara, sehingga informasi asli tidak dapat diketahui oleh pihak yang tidak berkepentingan. Informasi asli hanya dapat diketahui oleh penerima dengan menggunakan kunci rahasia. Dari 50 *sample* hasil Pengujian sistem di peroleh akurasi 40% menggunakan *plaintext* dan *key valid* 128bit menghasilkan 100% *output ciphertext* dan *plaintext* yang sama, 60% menggunakan *plaintext* dan *key tidak valid* menghasilkan 100% *output ciphertext* dan *plaintext* yang berbeda dengan menggunakan metode *Advanced Encryption Standard*.

Kata kunci : *Advanced Encryption Standard, AES, SMS, Android*

IMPLEMENTATION OF AES ENCRYPTION ALGORITHM FOR SMS APPLICATION BASED ON GOOGLE ANDROID OPERATION SYSTEM

Awang Maristyono
(06.04.111.00862)

Preceptor I : Cucun Very Angkoso, ST., MT.

Preceptor II : Moch.Kautsar Sophan, S.Kom., M.MT

ABSTRAK

Short Message Service (SMS) information delivery is needed in modern era like these days. However, SMS service has security vulnerability in the data. One of the SMS service's weakness caused by universal coding standard users, SMS system is built with a programming language which is similar to the language programs and computer hardware such as mobile phones can translate all the data in a specific open frequency. To ensure the security and confidentiality of the information during transmission, encryption and decryption are carried out on the information that will be delivered. Encryption is done at the time of delivery by converting original information into temporary information, while decryption is done at the time of reception by converting temporary information into original information. Therefore, information which delivered through delivery process is temporary information data, so that the original information can not be known by unauthorized parties. Original information only be known by the receiver by using secret key. From 50 samples, the test results of the system obtained 40% accuracy using plaintext and 128bit valid key obtained 100% the same ciphertext and plaintext output, 60% using plaintext and invalid key obtained 100% different ciphertext and plaintext output by using Advanced Encryption Standard (AES) method.

Keywords : Advanced Encryption Standard, AES, SMS, Android

DAFTAR ISI

ABSTRAK.....	ix
KATA PENGANTAR	xi
DAFTAR ISI.....	xiii
DAFTAR GAMBAR	xv
DAFTAR TABEL.....	xv
DAFTAR LAMPIRAN.....	xvii
DAFTAR ISTILAH	xxi

BAB I PENDAHULUAN

1.1.Latar Belakang	1
1.2.Perumusan Masalah.....	2
1.3.Tujuan dan Manfaat	2
1.4.Batasan Masalah.....	2
1.5.Metodologi Pengerjaan Tugas Akhir.....	2
1.6.Sistematika Penulisan.....	3

BAB II TINJAUAN PUSTAKA

2.1 Penelitian Sebelumnya	5
2.1.1 Aplikasi Kriptografi Untuk Pertukaran Pesan Menggunakan Teknik Steganografi dan Algoritma AES	5
2.1.2 Implementasi Enkripsi Data Dengan Algoritma <i>Blowfish</i> Menggunakan Java Pada Aplikasi Email	5
2.1.3 Perancangan aplikasi <i>SMS emotisound</i> pada perangkat Android.....	6
2.2 Sejarah SMS.....	7
2.3 Kriptografi	9
2.4 <i>Advanced Encryption Standard (AES)</i>	9
2.5 Android	10
2.6 Eclipse.....	16
2.7 Metode Algoritma Lain Sebelum AES.....	17

BAB III METODOLOGI PENELITIAN

3.1 Analisis Awal	19
3.1.1 Analisis Kebutuhan Sistem (<i>Requirement</i>).....	19
3.1.2 Arsitektur Enkripsi SMS Global.....	22
3.1.3 Analisis Struktur SMS	22
3.2 Pemrograman Pada Android	24
3.3 Pembahasan <i>Class</i> Program	25
3.3.1 <i>Splash Class</i>	25
3.3.2 <i>Main Class</i>	25
3.3.3 <i>Service Class</i>	25
3.3.4 <i>Inbox Class</i>	25
3.3.5 <i>AES Class</i>	25
3.4 Sistem Utama	26
3.5 Algoritma AES.....	28
3.6 Use Case	32
3.7 Teori Algoritma AES	33
3.8 Analisa Perhitungan.....	33

BAB IV IMPLEMENTASI SISTEM

4.1 Lingkungan Pengembangan	39
4.2 Implementasi Antarmuka	39
4.2.1 Tampilan Awal/ <i>Splash Screen</i>	40
4.2.2 Tampilan <i>Home Menu</i>	41
4.2.3 Tampilan <i>Compose</i> Pesan	42
4.2.4 Tampilan Halaman Enkripsi	43
4.2.5 Tampilan Proses Enkripsi	44
4.2.6 Tampilan <i>Inbox</i>	45
4.2.7 Menu <i>Help</i>	46
4.3 Pengujian Proses	47

BAB V PENUTUP

5.1 Kesimpulan	65
5.2 Saran.....	66
DAFTAR PUSTAKA	67
DAFTAR RIWAYAT HIDUP.....	97

DAFTAR GAMBAR

Gambar 2.4	Proses <i>Shift</i> pada algoritma AES	10
Gambar 3.1.2	Arsitektur Enkripsi SMS Global.....	22
Gambar 3.4.1	<i>Flowchart</i> Pengiriman Pesan	26
Gambar 3.4.2	<i>Flowchart</i> Penerimaan Pesan.....	26
Gambar 3.5	<i>Flowchart</i> Proses algoritma AES	28
Gambar 3.5.1	<i>Transformasi SubBytes</i>	31
Gambar 3.5.2	<i>Transformasi ShiftRows</i>	31
Gambar 3.6	<i>Use Case</i>	32
Gambar 4.2.1	Tampilan awal <i>splash screen</i>	40
Gambar 4.2.2	Tampilan <i>Home Menu</i>	41
Gambar 4.2.3	Tampilan <i>Compose</i> Pesan	42
Gambar 4.2.4	Tampilan Halaman Enkripsi	43
Gambar 4.2.5	Tampilan Proses Enkripsi	44
Gambar 4.2.6	Tampilan <i>Inbox</i>	45
Gambar 4.2.7	Tampilan <i>Help</i>	46
Gambar 5.1	Pengujian <i>Splash Screen</i>	48
Gambar 5.2	Pengujian <i>Menu</i> Pada <i>Gadget</i>	49
Gambar 5.3	Pengujian <i>Input</i> Pesan Baru	50
Gambar 5.4	Pengujian <i>Menu</i> Enkripsi.....	51
Gambar 5.5	Pengujian Hasil Enkripsi.....	52
Gambar 5.6	Pengujian <i>Inbox</i>	53
Gambar 5.7	Pengujian Isi <i>Inbox</i>	54
Gambar 5.8	Pengujian Deskripsi Pesan.....	55
Gambar 5.9	Pengujian Hasil Deskripsi Pesan.....	56
Gambar 6.0	Pengujian Enkripsi Pesan dengan <i>AES Test Vector</i>	62
Gambar 6.1	Pengujian Pengujian Deskripsi Pesan dengan <i>AES Test Vector</i>	62

DAFTAR TABEL

Tabel 3.5.1	Perbandingan jumlah <i>Round</i> dan <i>Key</i>	29
Tabel 3.5.2	Substitusi (<i>S-Box</i>).....	30
Tabel 4.1	Lingkungan Pengembangan Aplikasi.....	39
Tabel 4.2	Tabel RCON.....	57

DAFTAR LAMPIRAN

Lampiran 1. Pengujian <i>sample</i>	69
Lampiran 2. Perhitungan Sistematis Manual Program.....	74
Lampiran 3. <i>Source Code</i>	83

DAFTAR ISTILAH

<i>Kriptografi,</i>	adalah sebuah cara atau metode untuk menjadikan informasi asli menjadi informasi yang tidak dapat dibaca
<i>Enkripsi,</i>	yaitu proses untuk menjadikan informasi asli menjadi informasi yang tidak dapat diartikan dalam proses kriptografi.
<i>Dekripsi,</i>	yaitu proses pengembalian dari informasi yang terenkripsi menjadi informasi asli.
<i>Plaintext</i>	Informasi asli/data masukan
<i>Chypertext,</i>	adalah informasi yang telah disandikan atau informasi yang tidak dapat dibaca karena telah dienkripsi menggunakan metode kriptografi tertentu.
<i>AES,</i>	Advanced Encryption Standard (standart enkripsi)
<i>Emulator,</i>	adalah suatu perangkat lunak yang memungkinkan kita untuk menjalankan suatu program komputer di dalam sistem komputer lain yang berbeda.
<i>Smartphone,</i>	Telepon cerdas adalah telepon genggam yang mempunyai kemampuan tingkat tinggi, Terkadang dengan fungsi menyerupai computer

