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	Kasyful Amron, S.T, M.Sc
NIK. 201102 831228 2 001	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 menyeleseikan 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 terseleseikan 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 popular dikalangan pengguna telepon seluler di Indonesia. Celah keamanan terbesar pada komunikasi SMS adalah dapat terbacanya pesan yang dikirimkan dan simpan 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

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN