

Implementasi Kriptografi Advanced Encryption Standard(AES) Dengan 2 Kunci Pada Berbentuk Teks Berbasis Android

ARIE AGUNG SETYA BUDI

(Pembimbing : ARIPIN, M.Kom)

Teknik Informatika - S1, FIK, Universitas Dian Nuswantoro

www.dinus.ac.id

Email : 111201206933@mhs.dinus.ac.id

ABSTRAK

Salah satu dampak negatif dalam perkembangan teknologi adalah adanya penyadapan dan peretasan, yang merupakan salah satu masalah yang paling ditakuti oleh para pengguna smartphone. Keamanan file tentu menjadi sangat penting agar tidak ada pihak-pihak yang tidak berwenang meretas atau memanipulasi informasi yang ada didalam smartphone. Salah cara untuk mengamankan suatu informasi agar informasi itu tidak bocor kepada pihak yang tidak berwenang, yaitu dengan menggunakan kriptografi. Secara umum kriptografi dapat diartikan sebagai ilmu dan seni penyandian yang bertujuan untuk menjaga keamanan dan kerahasiaan suatu data. Kriptografi merupakan salah satu solusi atau metode pengamanan data yang tepat untuk menjaga kerahasiaan dan keaslian data, serta dapat meningkatkan aspek keamanan suatu data atau informasi. Pada penelitian ini kriptografi yang digunakan adalah Advanced Encryption Standard(AES). AES menggunakan komponen yang selalu memiliki invers dengan panjang blok 128, 192 dan 256 bit. Penyandian AES menggunakan proses yang berulang-ulang yang biasa disebut dengan ronde dan jumlah perulangannya tergantung dengan panjang kunci yang digunakan. Setiap ronde AES memerlukan kunci ronde dan kunci ronde berikutnya dibangkitkan berdasarkan kunci yang diberikan. Kriptografi AES memiliki keamanan yang baik, karena setiap ada perubahan dibagian key maupun plaintext maka hasil ciphertext akan berbeda. Fokus penelitian ini adalah pembuatan aplikasi kriptografi AES 128 bit pada data berbentuk teks berbasis android. Berdasarkan hasil pengujian dengan menggunakan default teks, spesial character dan emoticon. Aplikasi berhasil melakukan enkripsi dan dekripsi dengan baik.

Kata Kunci : Advanced Encryption Standard , Android, Kriptografi, Teks.

Implementation of Cryptography Advanced Encryption Standard(AES) with 2 keys For Text Based On Android

ARIE AGUNG SETYA BUDI

(Lecturer : ARIPIN, M.Kom)

*Bachelor of Informatics Engineering - S1, Faculty of Computer
Science, DINUS University*

www.dinus.ac.id

Email : 111201206933@mhs.dinus.ac.id

ABSTRACT

One of the negative impacts on the development of technology is the tapping and hacking, which is one of the issues most feared by smartphone users. Security file would be very important that there are no parties not authorized to hack or manipulate the information that is inside the smartphone. One way to secure the information that it does not leak information to unauthorized parties, that is with using cryptography. In general, cryptography can be defined as the science and art encryption that aims to maintain the security and confidentiality of the data. Cryptography is one solution or method of securing data is appropriate to maintain the confidentiality and authenticity of data and can increase the security aspects of the data or information. In this study cryptography used is Advanced Encryption Standard (AES). AES uses components that always has an inverse to the length of blocks 128, 192 and 256 bits. AES Encryption using an iterative process which is called the round and the number of recurrences depends on the key length used. Each round requires a key AES round and the next round keys generated by a given key. AES cryptography has good security, because any changes key section ciphertext and plaintext, the results will be different. The focus of this research is the creation of applications on a 128 bit AES cryptographic data in the form of text-based android. Based on test results using the default text, special characters, and emotions. Application successfully performs encryption and decryption well.

Keyword : Advanced Encryption Standard, Android, Cryptography, Text.