

IMPLEMENTASI ALGORITMA AES 256 BIT DAN ALGORITMA DES UNTUK ENKRIPSI DAN DESKRIPSI PESAN TEKS BERBASIS ANDROID

HARIS MUFTI MAULANA

(Pembimbing : DR Pulung Nurtantio Andono, S.T, M.Kom)

Teknik Informatika - S1, FIK, Universitas Dian Nuswantoro

www.dinus.ac.id

Email : 111201206631@mhs.dinus.ac.id

ABSTRAK

Pada era teknologi dan informasi serba modern sekarang ini, keamanan pesan teks sangatlah penting apalagi berkaitan dengan sebuah informasi yang sangat berharga sekali. Kriptografi menjadi teknik alternatif untuk mengubah pesan menjadi pesan sandi yang mungkin tidak bisa dibaca oleh orang yang tidak berhak. Salah satunya data Encryption Standard menjadi standard kriptografi sebelum ditemukannya serangan terhadap algoritma DES. Tetapi seiring berjalannya waktu telah ditemukan celah enchipering salah satu serangan oleh pihak yang tidak berhak. Saat ini, AES (Advanced Encryption Standard) digunakan sebagai standar untuk algoritma kriptografi. Pada salah satu penelitian, Algoritma AES merupakan algoritma yang terbaik dibandingkan dengan algoritma DES, Triple DES dan Blowfish. Oleh karena itu, algoritma AES dapat dikombinasikan pada aplikasi enkripsi DES berbasis android. Metode penelitian ini menggunakan metode RAD (Rapid Application Development). Hasil pengujian menunjukkan bahwa aplikasi dapat melakukan enkripsi pada pesan teks serta mengirim ke nomor tujuan dan dekripsi pada sisi penerima pesan teks dengan tingkat keberhasilan sebesar 100 %. Aplikasi ini dapat membantu pengguna untuk mengamankan pesan teks yang dikirim melalui SMS.

Kata Kunci : Kriptografi, SMS , AES 256 bit , AES , DES , Android

AES 256 BIT ALGORITHM IMPLEMENTATION AND DES ALGORITHM FOR ENCRYPTION AND DESCRIPTION OF TEXT MESSAGE BASED ON ANDROID

HARIS MUFTI MAULANA

(Lecturer : DR Pulung Nurtantio Andono, S.T, M.Kom)

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

www.dinus.ac.id

Email : 111201206631@mhs.dinus.ac.id

ABSTRACT

In the era of information technology and modern department today, security is mainly a text message that is very important related information invaluable. Cryptography become an alternative technique to change the message into the message that allows the password can not be read by unauthorized people. One of them became the standard Data Encryption Standard cryptography before the invention of the attack on the DES algorithm. But over time it has been found loopholes enchipering an attack by unauthorized parties. Currently, AES (Advanced Encryption Standard) is used as the standard for cryptographic algorithms. In one study, the AES algorithm is an algorithm that is best compared with algorithms DES, Triple DES and Blowfish. Therefore, the AES algorithm can be combined on DES encryption application based on Android. This method of research using RAD (Rapid Application Development). The test results showed that the application can encrypt a text message and sent to the destination number and decrypted on the receiver side a text message with a success rate of 100%. This application can help users to secure text messages sent via SMS.

Keyword : Cryptography, SMS, AES 256 bit, DES, Android