View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Udinus Repo

IMPLEMENTASI ALGORITMA DIFFIE-HELLMAN, CAESAR CIPHER DAN AES UNTUK PENGAMANAN PESAN SMS PADA TELEPON SELULER BERBASIS ANDROID

REZA AKBAR SETYAWAN

(Pembimbing : Ahmad Zainul Fanani, SSi, M.Kom)

Teknik Informatika - S1, FIK, Universitas Dian Nuswantoro

www.dinus.ac.id

Email : 111201106401@mhs.dinus.ac.id

ABSTRAK

Penyadapan informasi sering kali terjadi karena lemahnya pengamanan sarana pertukaran informasi. SMS (Short Message Service) adalah salah satu pertukaran informasi yang paling banyak digunakan saat ini karena dengan SMS kita dapat melakukan komunikasi jarak dekat maupun jauh dengan mudah dan cepat. Pesan yang dikirim melalui SMS pada telepon seluler dapat berupa informasi yang bersifat rahasia dan tidak boleh diketahui umum, tetapi dengan majunya teknologi saat ini maka informasi yang seharusnya bersifat rahasia dengan mudah disadap oleh pihak lain. Untuk mengurangi lemahnya keamanan pada layanan SMS diperlukan suatu algoritma kriptografi pada sebuah aplikasi yang dapat digunakan untuk mengamankan pesan. Dalam penelitian ini penulis menggunakan gabungan antara Algoritma pertukaran kunci Diffie-Hellman, Algoritma Caesar Cipher dan Algoritma Advanced Encryption Standard untuk melakukan enkripsi terhadap pesan yang akan dikirimkan. Berdasarkan pengujian sistem dapat dilihat bahwa sistem dapat berjalan dengan baik dan dapat diimplementasikan untuk enkripsi SMS pada telepon seluler berbasis android. Dalam penelitian ini, pengujian pertukaran kunci pada aplikasi yang dibuat tidak dapat berjalan dengan baik karena tipe data yang digunakan adalah double yang hanya bisa menyimpan 15 digit angka dan panjang pesan menjadi bertambah panjang setelah di enkripsi dengan metode yang diusulkan.

Kata Kunci : Aplikasi Pengamanan SMS, Kriptografi, AES, Caesar Cipher, Diffie-Hellman.

Generated by SiAdin Systems ï¿½ PSI UDINUS 2016

Repository | Thesis | Bachelor of Informatics Engineering - S1 | Faculty of Computer Science | DINUS University | 2016

IMPLEMENTATION OF DIFFIE-HELLMAN, CAESAR CIPHER AND AES ALGORITHM FOR SMS SECURITY ON ANDROID BASED CELLULAR PHONE

REZA AKBAR SETYAWAN
(Lecturer : Ahmad Zainul Fanani, SSi, M.Kom)
Bachelor of Informatics Engineering - S1, Faculty of Computer Science, DINUS University
www.dinus.ac.id
Email : 111201106401@mhs.dinus.ac.id

ABSTRACT

Tapping the information often occurred because of weak security of the means of information exchange. SMS (Short Message Service) is one of the exchanges of information most widely used today because SMS can communicate near and far too easily and quickly. Messages sent via SMS on mobile phones contain information that is confidential and may not be common knowledge, but with the advancement of technology, today is the confidential information that should easily be intercepted by others. To reduce the security situation on the SMS service requires a cryptographic algorithm in an application that can be used to secure the message. In this study, the authors used a combination of algorithm Diffie-Hellman key exchange, Caesar Cipher Algorithm, and Advanced Encryption Standard algorithm to encrypt the message to be delivered. Based on the test system can be seen that the system can work well and can be implemented for the encryption of SMS on mobile phones based on Android. In this study, testing the key exchange in applications created can not walk properly because of the type of data used is double that could only store 15-digit number and length of the message be to increase long after encrypted with the proposed method.

Keyword : SMS Application Security , Cryptography , AES , Caesar Cipher , Diffie - Hellman .

Generated by SiAdin Systems ï¿½ PSI UDINUS 2016