IMPLEMENTASI ALGORITMA AES DAN MODIFIKASI VIGENERE UNTUK PENGAMANAN PESAN SMS DENGAN NOMOR PENGIRIM DAN PENERIMA SEBAGAI KUNCI TAMBAHAN

IMAM PRAYOGO PUJIONO
Program Studi Teknik Informatika - S1, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro Semarang
URL : http://dinus.ac.id/
Email : 111201106408@mhs.dinus.ac.id

ABSTRAK

Salah satu faktor maraknya penyadapan informasi adalah lemahnya pengamanan sarana pertukaran informasi yang ada. Salah satu sarana pertukaran informasi yang banyak digunakan adalah dengan menggunakan SMS (Short Message Service). Pesan yang dikirim melalui SMS dapat berupa informasi yang sifatnya rahasia dan tidak boleh diketahui oleh umum. Pengirim pesan seringkali tidak menyadari bahwa pesan yang dikirim memiliki tingkat keamanan yang rendah dari penyadapan. Untuk menjaga keamanan dan kerahasiaan pesan maka diperlukan sebuah Aplikasi yang dapat digunakan untuk mengamankan pesan. Dalam penelitian ini penulis menggunakan Algoritma AES (Advanced Encryption Standard) untuk melakukan enkripsi terhadap pesan yang akan dikirim dan modifikasi Algoritma Vigenere untuk membuat kunci enkripsi baru yang dihasilkan dari kombinasi kunci yang diinputkan, nomor pengirim dan penerima. Nomor pengirim dan penerima yang digunakan dalam pembentukan kunci enkripsi baru berfungsi untuk memastikan bahwa isi pesan hanya dapat dibaca maknanya pada handphone penerima asli dengan memasukkan kunci yang benar. Dari hasil penelitian ini meskipun seorang penyadap mendapatkan ciphertext (pesan enkripsi) dan mengetahui kunci pengamanan pesan, pesan tetap tidak terbaca maknanya di handphone penyadap karena nomor pengirim atau penerima pesan sudah berubah.

Kata Kunci : Aplikasi pengamanan, SMS, Kriptografi, AES, Vigenere.

IMPLEMENTATION OF AES ALGORITHM AND VIGENERE MODIFICATION FOR SMS SECURITY WITH SENDER AND RECEIVER NUMBER AS ADDITION KEY

IMAM PRAYOGO PUJIONO
Program Studi Teknik Informatika - S1, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro Semarang
URL : http://dinus.ac.id/
Email : 111201106408@mhs.dinus.ac.id

ABSTRACT

One of the factor in the rise of information interception is the weak security in the information exchange. One means of information exchange that is widely used is to use SMS (Short Message Service). Messages sent through SMS can be any information which is confidential and may not be noticed by the public. The sender of the message is often not aware that message sent have a low level of security from eavesdropping. To maintain the security and confidentiality of message, an application to secure the message is needed. In this research, the author uses AES (Advanced Encryption Standard) algorithm to encrypt the message which will be sent and the modification of Vigenere algorithm to generate a new encryption key which is generated from the inputed key combination, the number of sender and receiver. The number of the sender and the receiver that are used to generate the new encryption key is to ensure that the content of the message will be known only from the handphone of the receiver by inputing the correct key. From the results of this research, eventhough another people able to get the ciphertext and knows the key, ita bug gets the ciphertext messages (encryption) and knowing the key safety message, the message remains unreadable due to a bug in mobile, meaning the number of the sender or recipient of the message has changed.

Keyword : Security application, SMS, Cryptography, AES, Vigenere.