

IMPLEMENTASI ALGORITMA ENKRIPSI RIJNDAEL PADA PEMBUATAN KUNCI LISENSI PROGRAM PENGUBAH ATRIBUT FILE

Budiantoro, Nanan Rohman
STMIK Mardira Indonesia, Bandung

Abstract

Promotion is important thing in retail system obtain for introducing a product, and it same with retail in business software. In promotion there is something can do to introduce our product, with trial system that gift along with a file that has a function as a source for recognize program status are they trial or no. To protect content of license file so it used encryption rijndael technique that have international standardize encryption.

Once of newest encryption algorithm is rijndael algorithm. The rijndael algorithm is the winner of open prize contest by NIST (National Institute of Standards and Technology) in 2000. Rijndael algorithm become dominant standarize of cryptografi at least 10 year. Rijndael cryptografi algorithm that desain by Vincent Rijmen dan John Daemen from Belgia is one of famous that used by simetrik key cryptografi.

In implementation benefit of rijndael algorithm it will used for secure license key where this key will be used for promotion our product, so it will take to our program that can be change attribute of file like hidden, archive, system, normal or read only in windows operation system.

In this study we try to observe about implementation rijndael encryption algorithm in license key process maker that is program that will be tested and will research about steps in encryption and decryption process use rijndael algorithm like addroundkey, subbytes, shiftrows, mixcolumn process and will be research about implementation in license maker program that wil be produce encrypted licensi file use this algorithm.

Keywords: *Promotion, Encryption, Decryption.*

Abstrak

Promosi merupakan hal yang penting dalam sistem ritel mendapatkan untuk memperkenalkan produk, dan sama dengan ritel dalam bisnis perangkat lunak. Dalam promosi ada sesuatu yang bisa dilakukan untuk memperkenalkan produk, dengan sistem trial yang menawarkan hadiah bersama dengan file yang memiliki fungsi sebagai sumber untuk mengenali status program yang di uji coba. Untuk melindungi isi dari file lisensi sehingga menggunakan teknik enkripsi rijndael yang memiliki enkripsi standar internasional. Setelah algoritma enkripsi terbaru adalah algoritma Rijndael. Algoritma rijndael adalah pemenang kontes hadiah terbuka oleh NIST (National Institute of Standards and Technology) pada tahun 2000. Algoritma Rijndael menjadi standar dominan cryptografi dalam 10 tahun. Algoritma Rijndael yang cryptografi desain oleh

Vincent Rijmen Dan John Daemen dari Belgia merupakan salah satu yang terkenal yang digunakan oleh cryptografi kunci simetrik.

Dalam pelaksanaan manfaat algoritma rijndael akan digunakan untuk kunci lisensi yang aman di mana kunci ini akan digunakan untuk promosi produk, sehingga waktu yang dibutuhkan untuk program yang dapat merubah atribut file seperti arsip, sistem, normal atau hanya membaca di sistem operasi windows.

Dalam penelitian ini kami mencoba untuk mengamati tentang algoritma enkripsi pelaksanaan rijndael di kunci lisensi pembuat proses yang program yang akan diuji dan akan penelitian tentang langkah-langkah dalam enkripsi dan dekripsi menggunakan proses rijndael algoritma seperti *AddRoundKey*, *subbytes*, *ShiftRows*, *mixcolumn process* dan akan dilakukan penelitian tentang pelaksanaan program pembuat lisensi yang akan menghasilkan enkripsi menggunakan berkas lisensi algoritma ini .

Kata Kunci: Promosi, *Encryption*, *Decryption*

REFERENSI

- Edwin NC Mui, Practical Implementation of Rijndael S-Box Using Combinational Logic, <http://www.comms.scitech.susx.ac.uk/fft/crypto/rijndael-sbox.pdf>
- Greg Perry & Ian Spencer, 1995, Visual C++, Andi, Yogyakarta
- Halvorson, Michael,. 2000, *Step by step Microsoft Visual Basic 6.0*, Elex Media Komputindo, Jakarta.
- Joan Daemen & Vincent Rijmen, AES Proposal : Rijndael, <http://www.esat.kuleuvalen.ac.be/~rizmen/>
- Petroustos, Evangelos, 1998, *Mastering Visual Basic Basic 6* , Sybex, California
- Pressman. Roger 2005, Software Engineering, McGrawHill , Singapore
- Rinaldi Munir, 2006, Kriptografi, Informatika, Bandung.