Implementasi MD5 pada Algoritma Kriptografi GOST untuk Keamanan Penyandian Data

MOHAMMAD NUR DIYATAN
(Pembimbing : Aisyatul Karima, S.Kom, MCS)
Teknik Informatika - S1, FIK, Universitas Dian Nuswantoro
www.dinus.ac.id
Email : 111201207059@mhs.dinus.ac.id

ABSTRAK

Keamanan dan kerahasiaan data merupakan suatu hal yang penting dalam pertukaran informasi. salah satu solusi yang dapat digunakan untuk mengamankan data adalah menggunakan metode kriptografi. kriptografi merupakan ilmu yang mempelajari cara mengamankan data atau pesan. Gost merupakan salah satu algoritma kriptografi yang prosesnya memiliki putaran sebanyak 32 kali dan menggunakan Fiestel Newtork serta panjang kunci 256 bit. Algoritma ini memiliki struktur yang sama dalam enkripsi dan dekripsi. Perbedaannya terletak pada penjadwalan kunci (key-schedule). Pembentukan kunci yang sederhana pada algoritma gost menyebabkan rentan terhadap serangan. Salah satu cara untuk menutupinya yaitu dengan menambahkan proses lain pada saat pembentukan kunci. MD5 merupakan salah satu fungsi hash yang memiliki panjang output 128 bit. Algoritma MD5 dipilih dalam penelitian sebagai komponen tambahan dalam pembentukan kunci algoritma GOST. Setelah dilakukan penelitian, GOST yang sudah disubtitusi dengan MD5 mempunyai rata-rata nilai avalanche effect yang cukup ungggul dengan nilai 52.34% sedangkan untuk GOST memiliki nilai avalanche effect 46.72%.

Kata Kunci : Kriptografi, Algoritma GOST, algoritma MD5, avalanche effect

MD5 Implementation on GOST Cryptography Algorithm to Secure Data Encryption

MOHAMMAD NUR DIYATAN
(Lecturer : Aisyatul Karima, S.Kom, MCS)
Bachelor of Informatics Engineering - S1, Faculty of Computer Science, DINUS University
www.dinus.ac.id
Email : 111201207059@mhs.dinus.ac.id

ABSTRACT

The security and confidentiality of data are an important exchange on the information system. one of the solutions can be used to secure data is cryptographic methods. Cryptography is the science that studies how to secure data or messages. GOST is cryptographic algorithms which the process has the round as much as 32 times and use Feistel Network with 256 bits the key of length. These algorithms have the same structure in the encryption and decryption process. The differences on the key scheduling. The simple key generates process, causes vulnerable to attack. In order to safe, by adding another process at the key generate process. The MD5 hash function has 128 bits the output of length. The MD5 algorithm is chosen in this study as additional components on the key generate process of GOST algorithm. In this study shows that the GOST substituted with MD5 has 52.34% of average avalanche effect, it is higher than GOST which has 46.72% of average avalanche effect.

Keyword : Cryptography,GOST Algorithm,MD5 algorithms, avalanche effect