Rancang Bangun Aplikasi Pesan Menggunakan Algoritma Vigenere Cipher dan One Time Pad

SUGENG SUTRISNO
Program Studi Teknik Informatika - S1, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro Semarang
URL : http://dinus.ac.id/
Email : 111201106032@mhs.dinus.ac.id

ABSTRAK

Dalam penelitian ini dirumuskan masalah tentang bagaimana merancang dan mengimplementasikan metode Vigenere Cipher dan One Time Pad untuk keamanan pada pesan pesan agar dapat menjadi lebih aman. Sedangkan tujuan dari penelitian ini adalah untuk merancang keamanan Pesan dengan menggunakan metode Vigenere Cipher dan One Time Pad, merancang enkripsi dan dekipsi dengan metode Vigenere Cipher dan One Time Pad pada Pesan agar menjadi lebih aman untuk digunakan serta merancang enkripsi dan dekripsi Pesan agar dapat diterapkan menggunakan bahasa pemrograman PHP. Vigenere cipher dan one time pad adalah bagian dari algoritma kriptografi klasik. Pada kedua algoritma ini menggunakan kunci simetrik untuk proses enkripsi dan dekripsinya, yang mana kunci yang digunakan untuk proses enkripsi sama dengan kunci yang digunakan untuk proses dekripsi. Penggunaan algoritma Vigenere cipher dan one time pad membuat kunci yang digunakan untuk proses enkripsi ataupun dekripsi berjumlah 2 kunci. Dengan adanya 2 kunci ini menjadikan kriptanalisis membutuhkan waktu untuk menemukan kunci yang digunakan sebelum melakukan dekripsi pada ciphertext. Hasil dari keamanan Pesan pada sistem enkripsi Pesan menggunakan algoritma Vigenere Cipher dan One Time Pad untuk membuat Pesan menjadi lebih aman digunakan.

Kata Kunci : Kata kunci : Vigenere Cipher, One Time Pad, Enkripsi, Dekripsi, Pesan

DESIGN OF MESSENGER APPLICATION USING VIGENERE CIPHER AND ONE TIME PAD ALGORITHM

SUGENG SUTRISNO
Program Studi Teknik Informatika - S1, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro Semarang
URL : http://dinus.ac.id/
Email : 111201106032@mhs.dinus.ac.id

ABSTRACT

The way to make and apply Vigenere Cipher and One Time Pad has been formulated in this research for making Message became more secure. The main purpose of this reseach is to create Messaging security system using Vigenere Cipher and One Time Pad method, and compile it using PHP so we can encrypt and decrypt in order to make that method work properly. Vigenere Cipher and One Time Pad are part of classic cryptographic algorithm. Both of those algorithm are using symmetrical key on the encryption and decryption progress, which is the key is identical between those two progresses. With the existence of those two key, cryptanalytic needs time for encrypting the Message on ciphertext, the result of this method in to make Message (text, in this case) become more secure.

Keyword : Keywords: Vigenere Cipher, One Time Pad, Encryption, Decryption, Message