

PROGRAM APLIKASI KRIPTOGRAFI PENYANDIAN *ONE TIME PAD* MENGUNAKAN SANDI *VIGENERE*

**oleh
Lis Endah Pratiwi**

ABSTRAK

Penggabungan konsep algoritma kriptografi sandi *Vigenere* dan *one time pad* memiliki keunggulan dalam hal peringkasan/pemadatan data. Pada sandi *one time pad*, kunci yang digunakan untuk proses enkripsi dan dekripsi mempunyai panjang yang sama dengan data awal, sedangkan dalam penggabungan konsep ini kunci sandi yang digunakan cukup memiliki panjang kunci setengah dari panjang data awal. Teori dasar matematika yang digunakan dalam penggabungan konsep dua sandi kriptografi ini yang menjadi masalah yang perlu dibahas, juga merancang dan membuat program aplikasi kriptografi gabungan dua sandi tersebut dalam penulisan skripsi ini. Metodologi penelitian yang diterapkan dalam penulisan skripsi ini berupa studi literatur, pengembangan program, pembuatan program serta pengujian program aplikasi kriptografi. Hasil dalam penulisan skripsi ini berupa program aplikasi kriptografi yang dapat mempermudah proses enkripsi dan dekripsi sandi kriptografi tersebut. Sehingga dapat disimpulkan bahwa algoritma dari penggabungan dua sandi kriptografi dapat dijelaskan secara matematis dan program aplikasi kriptografi dapat dibuat menggunakan bahasa pemrograman Delphi 7.

Kata kunci: program aplikasi, sandi *one time pad*, sandi *Vigenere*

CRYPTOGRAPHIC APPLICATION PROGRAM ONE TIME PAD ENCRYPTION USING THE VIGENERE CIPHER

**by
Lis Endah Pratiwi**

ABSTRACT

The integration of the concept of cryptographic algorithms vigenere cipher and one time pad has advantages in terms of data compression. At one time pad cipher, the key used for encryption and decryption process has a length that is equal to the initial data, whereas in this integration, the key used enough to have half of its key length the length of the initial data. At this writing there are problem that needs to be discussed, basic theory of mathematics of the integration and designing and creating application program. Research methodology which is applied in the form of study literature, program development, program creation, and program testing of cryptographic application. The result in this writing is in the form of a cryptography application program that can ease the process of encryption and decryption of the cryptography cipher. So it can be inferred that the algorithm form the integration of the two cipher cryptography can be described mathematically and cryptographic application program can be created using the programming language Delphi 7.

Keyword: application program,one time pad cipher, Vigenere cipher