

# **APLIKASI KRIPTOGRAFI KOMPOSISI *ONE TIME PAD CIPHER* DAN *AFFINE CIPHER***

**oleh**  
**Ivan Luckiyana Firdaus**

## **ABSTRAK**

Kriptografi *one time pad cipher* memiliki kelemahan pada kurangnya keefisienan dalam pembentukan dan pengiriman kuncinya jika menggunakan cara manual untuk menentukan kuncinya. Salah satu cara agar pembentukannya lebih mudah dengan menggunakan aturan barisan Fibonacci terhadap teks asli (*plaintext*) sehingga menghasilkan kunci untuk *one time pad cipher*. Untuk lebih mempersulit pemecahan, *one time pad cipher* dikomposisikan dengan *affine cipher* yang merupakan dasar dari algoritma kriptografi klasik yang menggunakan metode substitusi. Skripsi ini membahas bagaimana pengkonstruksian kunci untuk *one time pad cipher* dan pembuatan program aplikasi komposisi *one time pad cipher* dan *affine cipher*. Hasil dalam penulisan skripsi ini berupa program aplikasi untuk mempermudah enkripsi dan dekripsi komposisi *one time pad cipher* dan *affine cipher* yang dibuat menggunakan bahasa pemrograman Delphi 7.0.

**Kata kunci:** program aplikasi, *one time pad cipher*, *affine cipher*

# **APPLICATION CRYPTOGRAPHY COMPOSITION OF ONE TIME PAD CIPHER AND AFFINE CIPHER**

*by*  
**Ivan Luckiyana Firdaus**

## **ABSTRACT**

*One time pad cipher has a weakness on generating it's key. There are many ways to cover it's weakness, such as using Fibonacci series formula on the plaintext to generate one time pad cipher's key. One time pad cipher is an encryption technique that difficult to be cracked. One way for a cipher to become more difficult to resolve is by composing two encryption technique. One time pad cipher which is difficult to be cracked will be composed by affine cipher which is the base of classic cryptography whose using substitution methode. This paper aimed to discuss how to generate one time pad cipher's key with Fibonacci series formula and how to make application program crptography composition of one time pad cipher and affine cipher. And the result of this paper is a program application cryptography composition of one time pad cipher and affine cipher using Borland Delphi 7.0, which made encrypting and decrypting became easier.*

**Keyword: application program, one time pad cipher, affine cipher**