

**IMPLEMENTASI ALGORITMA BLOWFISH DAN RSA
UNTUK ENKRIPSI DAN
DEKRIPSI FILE**

SKRIPSI

Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar

SARJANA TEKNIK

Program Studi Teknik Informatika – Strata 1



OLEH:

NAMA : RIKI ISMAYANA

NIM : 011201573125003

FAKULTAS : TEKNIK

UNIVERSITAS SATYA NEGARA INDONESIA

JAKARTA

2016

ABSTRAK

Implementasi Algoritma *Blowfish* dan *RSA* untuk Enkripsi dan Dekripsi File

Dibawah bimbingan **Berlin Siotrus, S.Kom, M.Kom** dan **Faizal Zuli, S.Kom., M.Kom, MTA.**

Penelitian ini dilatarbelakangi oleh permasalahan *file .txt* merupakan format *file* teks yang sangat populer dalam dunia komputer. Format ini bisa dijalankan di berbagai sistem operasi seperti windows, linux, macos, dan lain-lain. Dalam sistem operasi windows format *.txt* bisa dibuka dengan program notepad dan wordpad. File *.txt* salah satunya digunakan dalam game sebagai kumpulan perintah yang akan dijalankan ketika bermain game, diantaranya: menaikkan level, memunculkan boss monster, mendapatkan item di dalam game, dan masih banyak lagi. Untuk melindungi *file .txt* yang terdapat pada komputer atau tempat penyimpanan data dari akses ilegal salah satu caranya adalah dengan menggunakan kriptografi. *Blowfish* merupakan salah satu algoritma yang tidak dipatenkan dan cukup kuat karena memiliki ruang kunci yang besar dan panjangnya bisa beragam, sehingga tidak mudah diserang pada bagian kuncinya. Suatu sistem kriptografi yang baik terletak pada kerahasiaan kunci dan bukan pada kerahasiaan algoritma yang digunakan. *RSA* (*RivestShamirAdleman*) adalah singkatan dari para pembuatnya yaitu *RonRivest*, *Adi Shamir*, dan *Leonard Adleman* yang dibuat pada tahun 1977. *RSA* merupakan sistem kriptografi asimetrik. Tujuan dari penelitian ini adalah dapat merancang dan mengimplementasikan algoritma *Blowfish* dan *RSA* pada aplikasi kriptografi *file*. Adapun manfaat dari perancangan dan implementasi aplikasi ini adalah dapat mengamankan dan menjaga kerahasiaan data dengan menggunakan kriptografi *Blowfish* dan *RSA* serta sebagai referensi untuk penelitian yang berhubungan dengan kriptografi selanjutnya.

Kata Kunci: Kriptografi, *Blowfish*, *RSA*

ABSTRACK

Implementation Blowfish algorithm and RSA for Encryption and Decryption File

*Under the guidance of **Berlin Siotrus, S. Kom, M. Kom and Faizal Zuli, Kom., M. Kom, MTA.***

This research is motivated by the problems in the .txt file is a text file format that is very popular in the world of computers. This format can be run on various operating systems such as Windows, Linux, MacOS, and others. In the windows operating system .txt format can be opened with Notepad and WordPad program. .txt File one of which is used in the game as a set of commands to be executed when playing games, such as: raising the level, raises the boss, get an item in the game, and much more. To protect .txt files contained on a computer or data storage from unauthorized access one way is by using cryptography. Blowfish is one of the algorithms are not patentable and strong enough because it has a large key space and the length can vary, so it is not vulnerable on the key. A cryptographic system that is well located on the secrecy of the key and not on secrecy algorithm used. RSA (Rivest Shamir Adleman) is an abbreviation of the authors is that Ron Rivest, Adi Shamir, and Leonard Adleman created in 1977. RSA is an asymmetric cryptography system. The purpose of this study was able to design and implement the Blowfish algorithm and RSA cryptography application file. The benefits of the design and implementation of these applications are able to secure and maintain the confidentiality of data using Blowfish cryptography and RSA as well as a reference for research related to cryptography next.

Keywords: cryptography, Blowfish, RSA