**LAPORAN TUGAS KRIPTOGRAFI**

**TEKNIK KRIPTOGRAFI MENGGUNAKAN ALGORITMA BLOWFISH**



**DisusunSOleh :**

Fahmi Anwar A11.2016.09916

**Kelompok : A11.4601**

**FAKULTASIILMUIKOMPUTER**

**UNIVERSITASIDIAN NUSWANTORO**

**SEMARANG**

**2019**

# BAB I

# PENDAHULUAN

## Latar Belakang

Perkembangan teknologi khususnya internet mempermudah untuk proses pertukaran informasi. Proses pertukaran ini tidak dapat menjamin bahwa file yang dikirimkan terbebas dari pengaksesan oleh orang – orang yang tidak berwenang. File yang dapat diakses oleh orang yang tidak berwenang dapat disalahgunakan sehingga akan merugikan pihak orang lain. Oleh karena itu dibutuhkan pengamanan file yang memungkinkan orang lain tidak dapat mengakses file tersebut, yaitu dengan cara menerapkan sebuah mekanisme algoritma kriptografi. Dengan demikian. Metode ini dapat membantu seseorang dalam mengamankan data informasi yang dikirim.

Kriptografi merupakan ilmu dan seni yang memperlajari cara untuk menjaga sebuah data atau pesan teks agar tetap aman saat dikirim dan menerimanya tanpa mengalami gangguan dari pihak yang tidak bertanggung jawab. Teknik kriptografi modern didasarkan pada sejumlah teori dengan menggunakan konsep aljabar. Kriptografi memiliki 2 tipe kunci, yang pertama menggunakan Asymmetric key Cryptography dan yang kedua menggunakan Symmetric Key Cryptography. Dalam Asymmetric Key Cryptography terdapat 2 kunci yang harus digunakan, yaitu public key dan private key, Sedangkan pada Symmetric Key Cryptography dapat menggunakan kunci yang sama untuk melakukan proses enkripsi dan dekripsi. Dalam metode Symmetric key terdapat 2 jenis tipe cipher, yaitu stream cipher dan block cipher. Untuk metode stream cipher mengenkripsi 1 bit pada plaintext terhadap suatu waktu yang di compare ke block cipher dengan mengambil sejumlah bit. Dalam hal ini algoritma blowfish termasuk menggunakan Symmetric Key [1] [2].

Algoritma Blowfish merupakan rancangan Bruce Schneider pada tahun 1993 sebagai algoritma alternative untuk enkripsi cepat. Blowfish juga termasuk kedalam enkripsi cipher block 64-bit yang memiliki panjang kunci 32-bit hingga 448-bit [3]. Blowfish merupakan salah satu algoritma yang belum dipatenkan dan cukup kuat karena memiliki ruang kunci yang besar dan panjangnya pun bisa beragam, sehingga algoritma ini lebih sulit untuk diserang pada bagian kuncinya.

Beberapa studi mencoba menggunakan algoritma algoritma Blowfish untuk pengamanan informasinya. Dalam hal ini, tujuan penelitian ini untuk memperoleh pengetahuan dengan metode algoritma Blowfish melalui perancangan system yang dapat digunakan untuk mengamankan data atau informasi berupa file atau text.

# BAB II

# STUDI LITERATUR

## Tinjauan Studi

Dalam penelitian yang penulis lakukan untuk menyusun laporan dan mengimplementasikan algoritmanya, penulis menggunakan beberapa referensi yang ada. Referensi tersebut berfungsi sebagai pendukung untuk membuat system dan melakukan analisa agar dapan direalisasikan.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| No | Tahun | Judul | Masalah | Metode | Hasil |
| 1  [4] | 2013 | Security Analysis of Blowfish Algorithm | Menganalisis Algoritma Blowfish dalam hal Avalanhce effect dan Correlation Coefficient | Algoritma Blowfish | Mendapatkan nilai yang bagus pada untuk pengujian avalanche effect dari round kedua. Namun algoritma ini memiliki hubungan non-linier yang bagis antara plaintext dan cipher text |
| 2  [5] | 2016 | Enkripsi dan Dekripsi File dengan Algoritma Blowfish pada perangkat Mobile berbasis Android | Menggunakan Algoritma Blowfish untuk mengenkripsi data yang berjalan pada sistem operasi android | Algoritma Blowfish | Tingkat keamanan pada OS android versi 2.3, 4.0, 4.1 cukup aman dengan menggunakan kunci berjumlah 72 bit atau 9 karakter membutuhkan waktu 1,49x109 tahun untuk membongkarnya |
| 3  [1] | 2017 | Design and Implementation of Blowfish Algorithm using Reconfigurable Platform | Mengevaluasi kinerja algoritma Blowfish pada platform yang dapat dikonfigurasi ualng dalam hal konsumsi daya dan throughput | Algoritma Blowfish dengan pengujian data gambar dan data ECG yang telah digunakan sebagai plaintext | Panjang kunci dapat ditingkatkan untuk membuat Algoritma Blowfish lebih aman, namun akan meningkatkan sumber daya dan konsumsi daya |
| 4 [6] | 2011 | Penerapan Enkripsi Algoritma Blowfish Pada Proses Steganografi Metode EOF | Mengimplementasi algoritma blowfish untuk mengenkripsi informasi yang akan dikirim lalu diproses menggunakan teknik steganografi metode End Of File untuk menyamartkan informasi. | Algoritma Blowfish dan LSB dengan metode End Of File | Pada ukuran File menjadi lebih besar 16 bytes yang berbanding lurus dengan waktu proses penyisipan. Waktu yang diperoleh untuk penyisipan lebih cepat dibandingkan dengan lama proses ekstraksi |
| 5  [7] | 2015 | Analisa Pebandingan Kinerja Algoritma Blowfish dan Algoritma Twofish pada Proses Enkripsi dan Dekripsi | Menganalisis Perbandingan kinerja dari algoritma Blowfish dan algoritma Twofish | Algoritma Blowfish dan Algoritma Twofish | Ukuran file yang didapatkan memiliki nilai sama besar, tetapi untuk lama prosesnya Blowfish lebih cepat dibandingkan dengan Twofish |