# ABSTRAK

Blowfish, merupakan sebuah kunci rahasia yang dibuat dengan menggunakan blok cipher. Di dalamnya terdapat jaringan Feistel, iterasinya hanya menggunakan fungsi enkripsi sederhana sebanyak 16 putaran. Ukuran blok adalah 64 bit, dan kunci dapat berupa panjang hingga 448 bit. Meskipun ada fase inisialisasi yang kompleks diperlukan sebelum enkripsi dilakukan, tetapi sebenarnya enkripsi data yang dilakukan sangat efisien jika digunakan pada mikroprosesor besar. Blowfish merupakan metoda enkripsi yang mirip dengan DES (DES-like cipher) dan diciptakan oleh Bruce Schneier yang ditujukan untuk mikroposesor besar (32 bit ke atas dengan cache data yang besar). Blowfish dioptimasikan untuk aplikasi dimana kunci tidak sering berubah, seperti jalur komunikasi atau enkripsi file otomatis. Blowfish jauh lebih cepat dari DES bila diimplementasikan pada 32 bit mikroprosesor dengan cache data yang besar, seperti Pentium dan Power PC, Blowfish tidak cocok untuk aplikasi seperti packet switching, dengan perubahan kunci yang sering, atau sebagai fungsi hash satu arah.

**Kata Kunci** : Blowfish, Enkripsi, Cryptographi

# ABSTRACT

Blowfish, constitute one clue which is made by use of block cipher. In it available network Feistel, it iteration just utilize encryption function plain as much 16 laps. Measure obstructs is 64 bits, and key gets as length until 448 bits. Even available complex initials phase needful before encryption is done, but actually encryption data that is done so efficient if is utilized on big microprocessor. Blowfish constituting kindred encryption method with DES (DES like cipher) and created by Bruce Schneier which is attributed for microprocessor to outgrow (32 bits onto with cache big data). Blowfish is optimal for application where changed unfrequented key, as band of communication or Encryption is automatic file. Blowfish goes away faster from DES if take on 32 microprocessor bit with cache big data, as Pentium and Power Is PC, Incompatible Blowfish for application as packet switching, with key change that often, or as logistic as hash one way.

**Kata Kunci** : Blowfish, Encripsi, Cryptographi