James Grant

Prof.Arias

CMPT 220

10/26/18

File Encryption Program

The program I will be working on is a file encryption program. Encryption works by making a file unintelligible to unintended parties unless the computer has the key(ex. Having the user type a password to access their files). This is done through encryption algorithms. Some of the most common algorithms include Triple DES, RSA, Blowfish, Twofish, and AES.For this program I will be using the Blowfish method. The Blowfish method is a method of encryption that has a 64- bit block size and a key length from 32 bits up to 448 bits. It is a symmetric-key block cipher designed in 1993 by Bruce Schneier. A symmetric-key algorithm is an algorithm that use the same cryptographic keys for both encryption of plain text and decryption of ciphertext. For this program the user will input a file they need encrypted and the computer will encrypt it. The user will give the computer a key to encrypt the file and will use that key to decrypt the file. If the user does not have a key and tries to open the file it will return what basically can be described as undecipherable string. But when the user has a key it will allow the user access to their files unaffected. There are certain weaknesses that Blowfish has but for the purpose of this program we will be ignoring them. In terms of effectiveness the Blowfish program is very effective as it has a good encryption rate but is outshined by the Advanced Encryption Standard (AES). A system of encryption used by the government. It is recommended by the GnuPG project recommends that Blowfish not be used to encrypt files larger than 4gb due to its small block size.