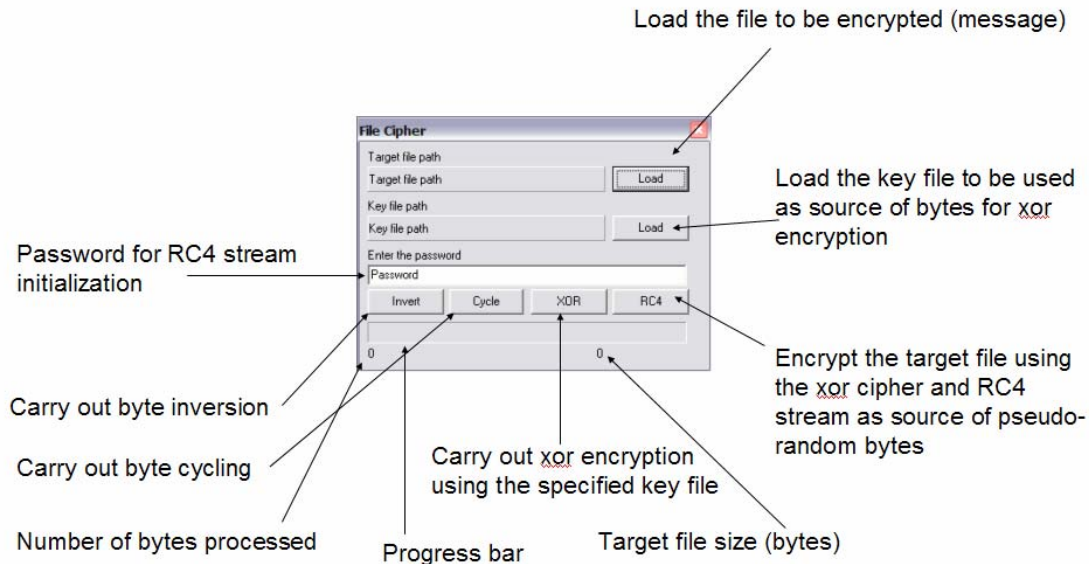


File Protector

Version 1.0.0.10

User Interface Description



Mechanics of File Encryption

The program is designed to work with extremely large files. The target file is opened in random access mode which implies that program can read any part of the file in the RAM. When encryption is started, the program reads consecutive blocks of 65536 bytes of target file in the RAM and carries out encryption using selected method (see below.) After the block is processed, the program records it back on the drive. Thus File Protector never reads the whole file in the RAM and the amount of memory needed by the program is kept minimal.

Caution: in the event of abrupt program termination while in process of encrypting target file, it will be impossible to know at what point did the program stop and how many bytes were encrypted. The target file will be completely corrupted without any possibility of recovery. The user is advised to run the program under conditions of stable power supply and stable operating system environment.

Encryption Methodology

File Protector is designed to carry out four operations on files.

- A) Byte inversion
- B) Byte cycling
- C) xor cipher
- D) RC4 cipher

- A.** Each byte can be represented as a sequence of zeros and ones. Byte inversion literally means that cipher will process every byte in the file by inverting its bit sequence. This kind of file protection is very fast. Inverted file will become unreadable to programs that are designed to read the file format. For example, an inverted M.S. Word document will fail to open by the Word processor. An inverted mp3 file fail to open by Windows Multimedia Player and other programs designed for music playback.
- B.** Byte cycling takes every two consecutive bits in a given byte and rotates their positions. Some examples of byte cycling are below.

Decimal value	Original sequence	Cycled sequence	Decimal value
096	01 10 00 00	10 01 00 00	144
202	11 00 10 10	11 00 01 01	197
085	01 01 01 01	10 10 10 10	170

- C.** Exclusive-Or (xor) is a binary operator which modifies identity of the one byte while leaving the other intact. An example is below.

$M \text{ xor } N = P$
 $P \text{ xor } N = M$
 $128 \text{ xor } 047 = 175$
 $175 \text{ xor } 047 = 128$

The operation is symmetric which implies that application of the xor operator can be reversed. This procedure is used in typical cipher designs. Cipher would generate a stream of bytes as a product of an algorithm and apply the resulting stream to the target file. In case if the stream contains a truly random sequence of bytes (high entropy physical source), there is no way to reproduce the key stream. Consequently this provides 100% protection. If used properly, this cipher is one-time-pad. The key file has to be larger than the target file. User is strongly advised to use key file only once per protection.

- D.** RC4 (pronounced Arc 4) is a xor stream cipher invented by Ron Rivest. The algorithm for the cipher has been used in Internet security and numerous other applications. The stream is initialized by password sequence. The password has to be less than 256 characters in length.