

# CyProtect File Encryption

File Encryption with 512 Bit Polymorphic Cipher

Version 2.2

**Documentation**

July 23, 2004

# Contents

<b>1 Introduction.....</b>	<b>3</b>
1.1 RIPEMD-160.....	3
<b>2 Installation.....</b>	<b>4</b>
2.1 Windows.....	4
2.2 Linux.....	4
<b>3 Licensing.....</b>	<b>5</b>
<b>4 Encryption.....</b>	<b>6</b>
<b>5 Decryption.....</b>	<b>8</b>
<b>6 FilePMC - Console application.....</b>	<b>9</b>
<b>7 Version history.....</b>	<b>10</b>
7.1 Version 2.0 (15-Jan-2004).....	10
7.2 Version 2.1 (23-Apr-2004).....	10
7.3 Version 2.2 (23-Jul-2004).....	10
<b>8 Contact.....</b>	<b>11</b>

# 1 Introduction

With *CyProtect File Encryption* you can encrypt single files with the revolutionary and ultra-fast 512 Bit Polymorphic Cipher, additionally standard AES/Rijndael can be applied. You can use normal passwords as well as keys from a SafeNet iKey (only with *CyProtect Key Administration*).

The software consists of 2 components:

- **Encryption** (short: *CyFile*) for encrypting files
- **Decryption** (short: *CyDecrypt*) for decryption

## 1.1 RIPEMD-160

If you encrypt a file you have the possibility to save a hash code (RIPEMD-160) of the password or key. This will provide a chance to check the password while you enter it for decryption.

Today's state of science does not give you an opportunity to compute the original password or key from the given hash code. But you have to keep in mind that the convenience this feature offers may cause a security hole. So we recommend not to use this feature for those users who attach great importance to security.

## 2 Installation

Please consider the following system requirements:

- Pentium compatible PC
- 64 MB RAM
- 25 MB harddisk space
- 800x600 pixel screen resolution or higher, min. 256 colors

Please note that for each Rainbow iKey series there is a special software version. It is not possible to use iKeys of different series with one version of *CyProtect File Encryption*.

### 2.1 Windows

Please start the setup program and follow the instructions shown on the screen.

### 2.2 Linux

Please note that with the Linux version only Rainbow iKeys 3000 are supported.

## 3 Licensing

In order to activate the software you need a license key file (cyfile.key) which you will get from us (see chapter ) when you license the software. Please copy the license key file into the installation directory of this software or into the following directory:

C:\Program files\Common files\CyProtect

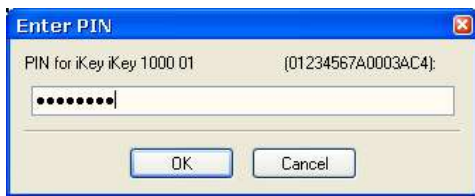
# 4 Encryption

With the component *CyProtect File Encryption* you encrypt files with a password or a key from a Rainbow iKey. Optionally you can choose to compress the file during encryption.

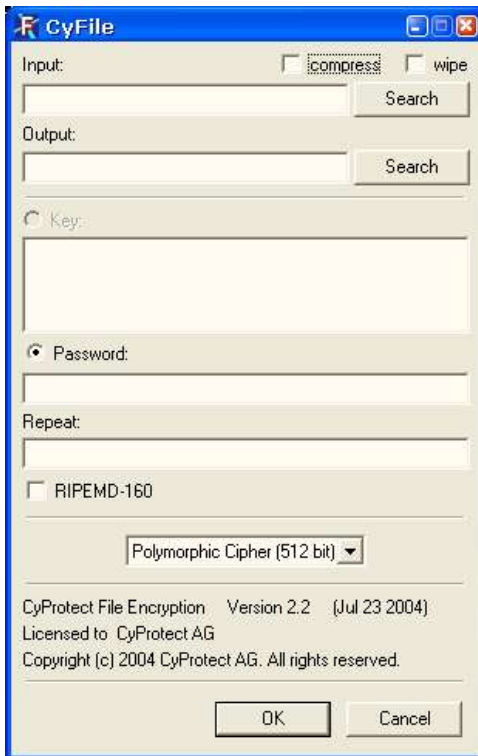
After starting the program it will first of all check for connected iKeys. If there are more than one iKeys connected you will have to choose which one to use:



Now you have to enter the PIN for the selected iKey:



You will see the main dialog of the program:



In the field „Input“ you select the file to encrypt. Alternatively you can use the „Search“ button to search for the appropriate file.

If you want the file to be compressed during encryption, select „compress“.

If „wipe“ is checked, the unencrypted input file will be securely deleted after successful encryption.

In the field „Output“ you select a name for the encrypted output file. Alternatively you can use the „Search“ button as well.

If you want to use a key from an Rainbow iKey for the encryption please choose „Key“ and select the desired key.

Should you want to use a normal password instead then choose „Password“ and enter the password twice.

If you select „RIPEMD-160“ then the hash code of the chosen password or key is saved with the encrypted file (see chapter 1.1).

As algorithm Polymorphic Cipher and AES/Rijndael are available.

Now you can start the encryption with „OK“.

## 5 Decryption

With the component *CyProtect File Decryption* you can decrypt files.

You are allowed to distribute this component for free. If you want to send for example a sensitive file via email, the recipient does not have to buy our software in order to decrypt your file. Instead he can download this decryption tool from our web site or you can send the tool with the encrypted file via email

The handling of connected iKey is similar to the encryption (s. above).

In the main dialog of the program:



you primarily select the encrypted file (Input) via the „Search“ button. Depending on the information saved with the encrypted file you now have to enter the password or the connected iKey is searched for the appropriate key.

With „OK“ you start the decryption (and wipe) process if everything is all right.

## 6 FilePMC - Console application

In addition to the above mentioned GUI applications you get the similar functionality in a simple console application: „FilePMC.exe“.

With this program you can encrypt and decrypt file, presently without access to Rainbow iKeys so you are limited to passwords at the moment.

The calling syntax is really simple:

- -e FILENAME Encrypt given file
- -d FILENAME Decrypt given file
- -o FILENAME Name of output file
- -p PASSWORD The password in quotation marks „“
- -s SEQUENCE Sequence of hex values (a1:01:3f:00:cc) as key
- -k KEYNAME Name of used key (max. 100 characters)
- -c Compress file during encryption
- -r Save RIPEMD-160 of password/hex key as checksum
- -w Overwrite input file after successful encryption (3 passes: 0xe6, 0x15 (complement) and random bytes)
- -a Algorithm (0: Polymorphic Cipher (default), 1: AES/Rijndael)
- -q Suppress messages
- -v Show version
- -h Show help

Examples:

- *FilePMC.exe -e sample.dat -p „1234“ -c*  
Encrypt the file „sample.dat“ with the password „1234“. The file will be compressed during encryption. The output will be (automatically) „sample.dat.pmc“
- *FilePMC.exe -d sample.dat.pmc -p „1234“*  
Decrypt the file „sample.dat.pmc“ with the password „1234“. The output file will be (automatically) „sample.dat“. If decompression is necessary this will be done automatically.
- *FilePMC.exe -e „sample.dat“ -s 12:34:56:78:9A:BC:DE -r -o „sample.encrypted“*  
Encrypt the file „sample.dat“ with the sequence of hex values „12:34:56:78:9A:BC:DE“. Additionally the RIPEMD-160 message digest of these hex values will be saved as well. The name of the encrypted output file is „sample.encrypted“.

## 7 Version history

Legend:

- [+] Additional feature
- [\*] Changed feature
- [-] Bugfix

### 7.1 Version 2.0 (15-Jan-2004)

First public release.

### 7.2 Version 2.1 (23-Apr-2004)

- [\*] Search for license key also in the installation directory
- [-] Fixes crash when input file missing (FilePMC)
- [+] Added possibility for secure file removal of input file after successful encryption
- [-] Fixed disabled OK button in CyDecrypt

### 7.3 Version 2.2 (23-Jul-2004)

- [-] License key is really found in installation directory
- [+] AES/Rijndael as alternative for PMC
- [\*] Dialog remains open after successful encryption/decryption
- [\*] Whirlpool hashcode for key derivation from password

## 8 Contact

For orders, questions, commendation, criticism, hints and proposals please contact:

CyProtect AG  
*A company of IT & More GmbH*  
Schatzbogen 58  
D-81829 Munich  
Germany  
Phone: +49-(0)89-420447-0  
Fax: +49-(0)89-420447-79  
E-Mail: [info@cyprotect.com](mailto:info@cyprotect.com)  
Internet: [www.cyprotect.com](http://www.cyprotect.com)

