

CyProtect File Encryption

Dateiverschlüsselung mit 512 Bit Polymorphic Cipher

Version 2.2

Dokumentation

23. Juli 2004

Inhaltsverzeichnis

1 Einführung	3
1.1 RIPEMD-160.....	3
2 Installation	4
2.1 Windows.....	4
2.2 Linux.....	4
3 Lizenzierung	5
4 Encryption	6
5 Decryption	8
6 FilePMC - Konsolenanwendung	9
7 Versionsgeschichte	10
7.1 Version 2.0 (15.01.2004).....	10
7.2 Version 2.1 (23.04.2004).....	10
7.3 Version 2.2 (23.07.2004).....	10
8 Kontakt	11

1 Einführung

Mit *CyProtect File Encryption* können Sie einzelne Dateien mit dem revolutionären und ultraschnellen 512 Bit Polymorphic Cipher verschlüsseln, zusätzlich steht der Standard AES/Rijndael zur Verfügung. Dabei können Sie sowohl normale Paßwörter benutzen, als auch (nur im Zusammenspiel mit der *CyProtect Key Administration*) Schlüssel von einem SafeNet iKey einsetzen.

Die Software besteht aus 2 Komponenten:

- **Encryption** (kurz: *CyFile*) zur Verschlüsselung von Dateien
- **Decryption** (kurz: *CyDecrypt*) zur Entschlüsselung

1.1 RIPEMD-160

Beim Verschlüsseln einer Datei haben Sie die Möglichkeit einen Hashcode (RIPEMD-160) des Paßworts bzw. Schlüssels mitzuspeichern. Dies gibt Ihnen z.B. bei Verwendung eines Paßworts die Möglichkeit, die Korrektheit des Paßworts bereits bei der Eingabe zu prüfen.

Nach heutigem Stand der Wissenschaft kann man von dem gespeicherten Hashcode des Paßworts/Schlüssels nicht auf das tatsächliche Paßwort (oder den Schlüssel) schließen. Es kann jedoch nicht ausgeschlossen werden, daß durch den Komfort, den diese Funktion bietet, ein mögliches Sicherheitsloch geöffnet wird. Daher empfehlen wir denjenigen Benutzern, die besonderen Wert auf Sicherheit legen, auf die Verwendung dieser Funktion zu verzichten.

2 Installation

Bitte beachten Sie unbedingt die folgenden Installationsvoraussetzungen:

- Pentium kompatibler PC
- 64 MB RAM
- 25 MB verfügbarer Festplattenplatz
- 800x600 Punkte Bildschirmauflösung oder höher, mindestens 256 Farben

Bitte beachten Sie, daß für jede Modellreihe eine eigenständige Softwareversion notwendig ist. Es ist also nicht möglich, mit einer Version der *CyProtect File Encryption* iKeys unterschiedlicher Modellreihen zu verwenden.

2.1 Windows

Starten Sie das Setup-Programm und folgen Sie den Anweisungen auf dem Bildschirm.

2.2 Linux

Bitte beachten Sie, daß unter Linux derzeit ausschließlich SafeNet iKeys 3000 unterstützt werden.

3 Lizenzierung

Zur Freischaltung der Software benötigen Sie eine Schlüsseldatei (cyfile.key), die Sie bei der Lizenzierung (Bezugsquelle s. Kapitel 8) von uns erhalten. Diese Datei müssen Sie dann in das Verzeichnis

C:\Programme\Gemeinsame Dateien\CyProtect

oder in das Installationsverzeichnis der Software kopieren.

4 Encryption

Mit der Komponente *CyProtect File Encryption* verschlüsseln Sie Dateien mit einem Paßwort oder einem Schlüssel von einem iKey. Gleichzeitig können Sie wählen, ob die Datei bei der Verschlüsselung auch komprimiert werden soll.

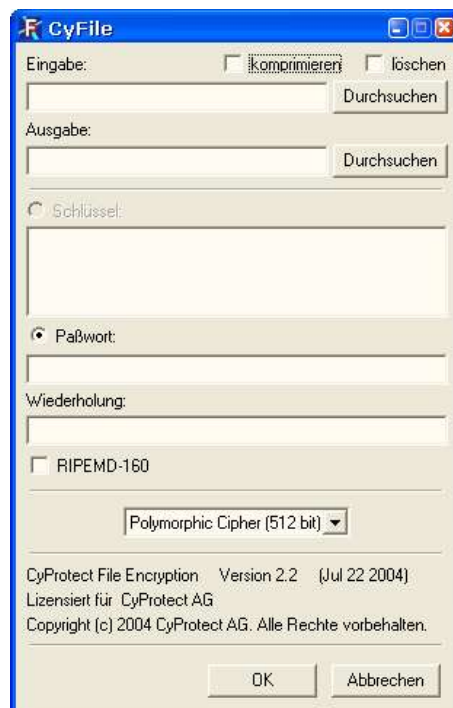
Nach dem Start des Programms wird zunächst geprüft, ob ein SafeNet iKey angeschlossen ist. Sind mehrere iKey angeschlossen, werden Sie aufgefordert, einen auszuwählen:



Anschließend müssen Sie die PIN für den gewählten (oder den einzig angeschlossenen iKey) eingeben:



Nun sehen Sie den Hautpdialog des Programms:



Im Feld „Eingabe“ wählen Sie die zu verschlüsselnde Datei aus. Wahlweise können Sie auch den Dateiauswahldialog über „Suchen“ aufrufen.

Wenn Sie die Datei beim Verschlüsseln komprimieren möchten, wählen Sie „komprimieren“.

Sofern „löschen“ angewählt wurde, wird die ursprüngliche, unverschlüsselte Datei nach erfolgreicher Verschlüsselung sicher gelöscht. Dabei wird die Datei in 3 Durchläufen überschrieben: mit 0xe6, mit 0x0a (Komplement) und mit Zufallswerten.

Im Feld „Ausgabe“ wählen Sie den Namen der verschlüsselten Datei aus. Wahlweise können Sie auch hier den Dateiauswahldialog über „Suchen“ aufrufen.

Wenn Sie zur Verschlüsselung einen Schlüssel auf einem SafeNet iKey nutzen wollen, wählen Sie bitte „Schlüssel“ sowie den gewünschten Schlüssel aus.

Sollten Sie ein normales Paßwort zur Verschlüsselung verwenden wollen, so wählen Sie „Paßwort“ und geben das Paßwort und zur Sicherheit (Tippfehler) die Wiederholung des Paßworts in den entsprechenden Feldern ein.

Wenn Sie zusätzlich das Feld „RIPEMD-160“ anwählen, wird der entsprechende Hashcode des Paßworts oder Schlüssels mitgespeichert (s. Kapitel 1.1).

Als Algorithmen stehen Polymorphic Cipher und AES/Rijndael zu Auswahl.

Mit „OK“ starten Sie nun die Verschlüsselung und ggf. das sichere Löschen der Eingabedatei..

5 Decryption

Mit der Komponente *CyProtect File Decryption* werden Dateien wieder entschlüsselt.

Dieses Programm dürfen Sie unverändert beliebig weitergeben. Wenn Sie zum Beispiel eine vertrauliche Datei per E-Mail verschicken wollen, muß der Empfänger die Software nicht unbedingt auch lizenziert haben. Er kann sich die Komponente zum Entschlüsseln entweder von der CyProtect Website (s. Kapitel 8) herunterladen oder Sie hängen die Komponente einfach mit an die E-Mail.

Die Handhabung angeschlossener iKeys verläuft analog der Encryption (s.o.).

Im Hauptdialog des Programms



wählen Sie zunächst die verschlüsselte Datei (Eingabe) über „Suchen“ aus. Je nach den dort gespeicherten Informationen müssen Sie nun das Paßwort eingeben oder der iKey wird nach einem passenden Schlüssel durchsucht.

Mit „OK“ starten Sie, wenn alles in Ordnung ist, die Entschlüsselung.

6 FilePMC - Konsolenanwendung

Zusätzlich zu den o.g. GUI-Anwendungen erhalten Sie die entsprechende Funktionalität in Form einer Konsolenanwendung: „FilePMC.exe“.

Mit diesem Programm können Sie Dateien ver- und entschlüsseln, zur Zeit jedoch noch ohne Zugriff auf SafeNet iKeys. Beim Einsatz dieses Programms sind Sie im Moment also auf die Verwendung von Paßwörtern beschränkt.

Nützlich ist dieses Tool zum Beispiel bei der skriptgesteuerten Verschlüsselung und anschließenden Sicherung von Daten auf einem Sicherungsmedium.

Die Aufrufsyntax ist bewußt einfach gehalten:

- -e FILENAME Verschlüssele angegebene Datei
- -d FILENAME Entschlüssele angegebene Datei
- -o FILENAME Name der Ausgabedatei
- -p PASSWORD Das Paßwort in Hochkommata „“
- -s SEQUENCE Folge von Hex-Werten (a1:01:3f:00:cc) als Schlüssel
- -k KEYNAME Name des verwendeten Schlüssels (max. 100 characters)
- -c Komprimiere Datei bei Verschlüsselung
- -r Speichere RIPEMD-160 vom Paßwort/Hex-Schlüssel als Prüfsumme
- -w Lösche die ursprüngliche, unverschlüsselte Datei nach erfolgreicher Verschlüsselung (3 Durchläufe: Überschreibe mit 0xe6, überschreibe mit 0x0a (Komplement) und überschreibe mit Zufallswerten)
- -a Algorithmus (0: Polymorphic Cipher (default), 1: AES/Rijndael)
- -q Keinerlei Nachrichten zeigen
- -v Versionsinfo anzeigen
- -h Hilfe anzeigen

Beispiele:

- *FilePMC.exe -e beispiel.dat -p „1234“ -c*
Verschlüsselt die Datei „beispiel.dat“ mit dem Paßwort „1234“. Die Datei wird beim Verschlüsseln komprimiert. Die Ausgabedatei ist (automatisch) „beispiel.dat.pmc“
- *FilePMC.exe -d beispiel.dat.pmc -p „1234“*
Entschlüsselt die Datei „beispiel.dat.pmc“ mit dem Paßwort „1234“. Die Ausgabedatei ist (automatisch) „beispiel.dat“. Eine evtl. notwendige Dekomprimierung wird automatisch durchgeführt.
- *FilePMC.exe -e „beispiel.dat“ -s 12:34:56:78:9A:BC:DE -r -o „beispiel.encrypted“*
Verschlüsselt die Datei „beispiel.dat“ mit der Folge der Hex-Werte „12:34:56:78:9A:BC:DE“. Zusätzlich wird der RIPEMD-160 Message Digest dieser Hex-Werte als Hashcode mitgespeichert. Der Name der Ausgabedatei ist „beispiel.encrypted“.

7 Versionsgeschichte

Legende:

- [+] Zusätzliche Funktionalität
- [*] Geänderte Funktionalität
- [-] Bugfix

7.1 Version 2.0 (15.01.2004)

Erste freigegebene Version.

7.2 Version 2.1 (23.04.2004)

- [*] Suche Lizenzschlüssel jetzt auch im Installationsverzeichnis der Software.
- [-] Kein Absturz mehr bei nicht vorhandener Eingabedatei (FilePMC)
- [+] Möglichkeit zum sicheren Löschen der (unverschlüsselten) Eingabedatei
- [-] Gesperrter OK-Button in CyDecrypt behoben.

7.3 Version 2.2 (23.07.2004)

- [-] Lizenzschlüssel wird jetzt tatsächlich im Installationsverzeichnis gefunden
- [+] AES/Rijndael als Alternative zu PMC
- [*] Dialog bleibt nach erfolgreicher Ver-/Entschlüsselung offen
- [*] Whirlpool Hashcode zur Ableitung des Schlüssels aus dem Paßwort

8 Kontakt

Bestellungen, Fragen, Lob, Kritik, Hinweise und Anregungen richten Sie bitte an:

CyProtect AG
Ein Unternehmen der IT & More GmbH
Schatzbogen 58
D-81829 München
Tel.: +49-(0)89-420447-0
Fax: +49-(0)89-420447-79
E-Mail: info@cyprotect.com
Internet: www.cyprotect.com

