CRYPTOMAThIC

Cryptomathic File2File Desktop 2.1
User's Guide

Trademarks

All brand names and product names are trademarks or registered trademarks of their respective owners.

Copyrights

Under the copyright law, neither the Cryptomathic File2File software nor documentation may be copied, photocopied, reproduced, translated or reduced to any electronic medium or machine readable form, in whole or in part, without the prior written consent of Cryptomathic A/S.

Disclaimer

This document is provided "as is" without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the document. Cryptomathic may make improvements of and/or changes to the product described in this document at any time.

Contact

If you wish to obtain further information on this product or any other Cryptomathic product, you are always welcome to contact us. Contact information can be found on page 3. For applications regarding support matters, please use the relevant e-mail address or telephone number, which can also be found on page 3.

Date: 2003-09-30

Doc. title: Cryptomathic File2File Desktop 2.1 User's Guide
Doc. version: 1.1

Contact Information

General Information

If you wish to obtain further information on this product or any other Cryptomathic product, please visit our web site or contact your regional Cryptomathic branch.

www.cryptomathic.com

Nordic:
HQ
Cryptomathic A/S
Jægergårdsgade 118
DK-8000 Aarhus C
Denmark
Tel.: +45 8676 2288
Fax: +45 8620 2975

Nordic & Baltic Sales:
Cryptomathic A/S
Christians Brygge 28
DK-1559 Copenhagen V
Denmark
Tel.: +45 8676 2288
Fax: +45 3333 9756

Germany:
Postal Address:
Cryptomathic GmbH
P.O. Box 800 949
Balanstr. 73
D- 81609 Munich
Germany

Visitor Address:
Cryptomathic GmbH
Rosenheimer Str. 116
GB91-9/11
D- 81669 Munich
Germany
Tel.: +49 (89) 234-20931
Fax: +49 (89) 234-20932

BeNeLux:
Cryptomathic NV
Lei 8A
B-3000 Leuven
Belgium
Tel.: +32 (0) 16 300 880
Fax: +32 (0) 16 389 452

UK/Ireland:
Cryptomathic Ltd
329 Cambridge Science Park
Milton Road
Cambridge CB4 0WG
United Kingdom
Tel.: +44 (0) 1223 225350
Fax: +44 (0) 1223 225351

France:
Cryptomathic France
264 Avenue Victor Hugo
94120 Fontenay-Sous-Bois France
Tel.: +33 (0)1 41 95 53 25
Fax: +33 (0)1 41 95 01 98

Italy:
Cryptomathic S.p.A.
Via Bligny 11
I-10122 Turin
Italy
Tel.: +39 011 7509527
Fax: +39 011 7509535

Support

For applications regarding support matters, please use your local contact e-mail address or telephone number.

support-nordic@cryptomathic.com
+45 8676 2288

support-uk@cryptomathic.com
support-usa@cryptomathic.com
support-asia@cryptomathic.com
support-austr@cryptomathic.com
support-mdleast@cryptomathic.com
support-africa@cryptomathic.com
+44 1223 225366

support-leuven@cryptomathic.com
support-be@cryptomathic.com
support-fr@cryptomathic.com
support-lux@cryptomathic.com
support-nl@cryptomathic.com
+32 16300882

support-it@cryptomathic.com
+39 0117509527

Table of Contents

CRYPTOMAThIC

1 Introduction

Over the last decade, the amount of electronic information to be stored or exchanged has increased tremendously, and handling various kinds of electronic data has become a still more integrated part of our daily life – in private as well as business related contexts. Alongside this development, the aspect of security has become crucial as ever, and still more people realize that privacy and confidentiality can no longer be taken for granted in the world of networked communication.

We face the dilemma that not only do we wish to store our information in a secure way; we also wish to be able to share it fairly easily – though, only with those for whom it was intended! Most people realize that precautionary measures are necessary – but for everyday-use they, should not be based on onerous procedures or complicated tools that take up valuable time and defocus the actual tasks.
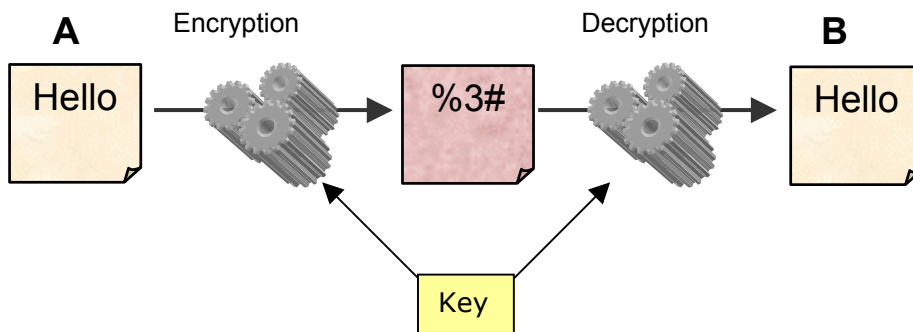
With File2File, Cryptomathic offers a simple solution to this problem: File2File is an easy-to-use encryption solution, which enables you to secure the confidentiality of data for personal storage as well as for exchange with colleagues, partners, customers or personal relations. With its basic but effective authentication relying on only one password shared by all initiated parties, File2File is the perfect ad-hoc solution independent of any specialized security infrastructure.

2 What You Can Do with File2File

File2File is based on the Advanced Encryption Standard (AES), which is a symmetric-key cryptosystem. This means that encryption and decryption is performed by means of the same key or password:
When you wish to encrypt a file, you enter a password as a key. When you wish to decrypt the file, you simply enter the same password again. And so, only users who know the password are able to open an encrypted file.

With File2File it is possible to secure single files as well as full directory structures on your personal hard disk, on a shared network drive, on a floppy disc or on some other kind of file store.
You may also use File2File to secure your files before sending them via e-mail: in this case, remember to inform the recipient about the password through an alternative "channel", e.g. a phone.
You may send encrypted files to users who also have File2File installed, and they will, of course, be able to decrypt the file by means of the password and the facilities in File2File. But it is also possible to send an encrypted file to a user, who does not have File2File installed, and he or she will still be able to decrypt the file: You do this by encrypting the file into an executable file (EXE-file), which is an encrypted file that contains the code necessary for decrypting the encrypted text. The receiver then only needs to enter the password.

3 How to Get Started

Once you have installed File2File, a manual for the program will be available in the *Start* menu under *Programs - Cryptomathic File2File*.

The program itself, however, cannot be started from the *Start* menu, as it is a so-called **Shell Extension** program, i.e. a program that you start from the **context menu**. You open the context menu by right-clicking the mouse.

After installation of File2File, the context menu for files and directories will have a File2File item: This means that whenever you wish to encrypt a file or a directory, you select the file or directory from Windows File Explorer, right-click it and open File2File by choosing *File2File*, see Figure 1.
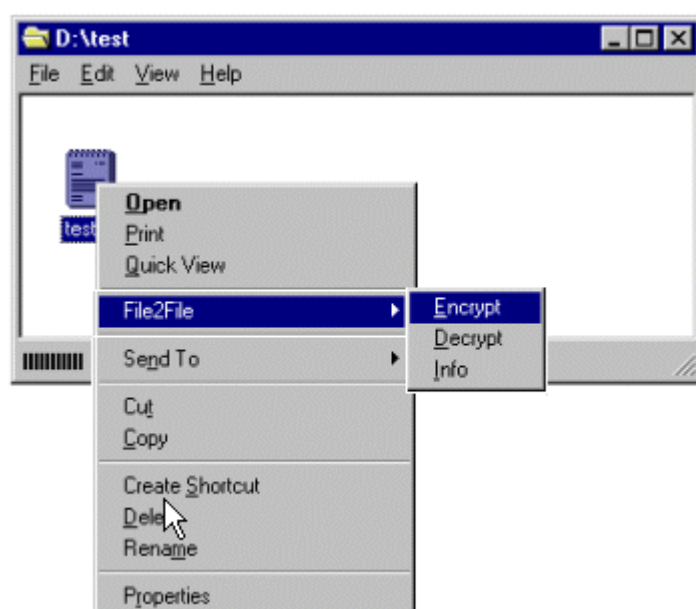

Figure 1

Encrypted files and directories will keep their original name and the extension *.F2F will be added.

4 How to Use File2File

4.1 Encrypt a File

To encrypt a file:

1. Open Windows File Explorer

2. Select the file and right-click it

    This will open up the context menu as shown in figure 1 above

3. Choose *File2File* and then *Encrypt*

4. Enter your password - at least 8 characters (characters, numbers and blanks are valid)

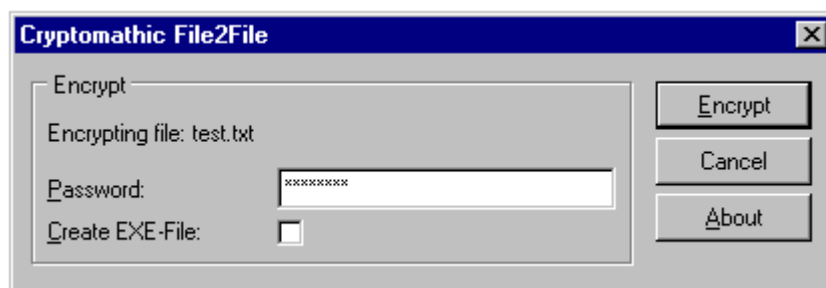5. Click the *Encrypt* button

Figure 2

It is possible to select more than one file at a time and then encrypt all selected files in one operation.

After the encryption, you will still be able to see your file in Windows File Explorer, but now the icon has changed into a Cryptomathic logo signalling that the file has been encrypted successfully, see Figure 3.
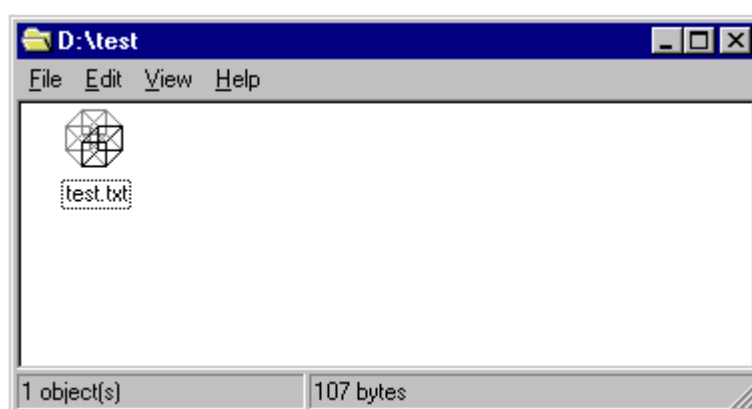
CRYPTOMAThIC

Figure 3

4.2 Make an Encrypted Executable File

To make an encrypted executable file:

1. Open Windows File Explorer

2. Select the file and right-click it

   This will open up the context menu as shown in figure 1 above

3. Choose *File2File* and then *Encrypt*

4. Enter a password - at least 8 characters (characters, numbers and blanks are valid

5. Check the box *Create EXE-File*

6. Click the *Encrypt* button

After the executable file has been made, you will still be able to see your file in Windows File Explorer, but now the icon has changed into a Cryptomathic logo and an '.exe' as been added to the file extension signalling that the file has been encrypted and made executable successfully, see Figure 4.
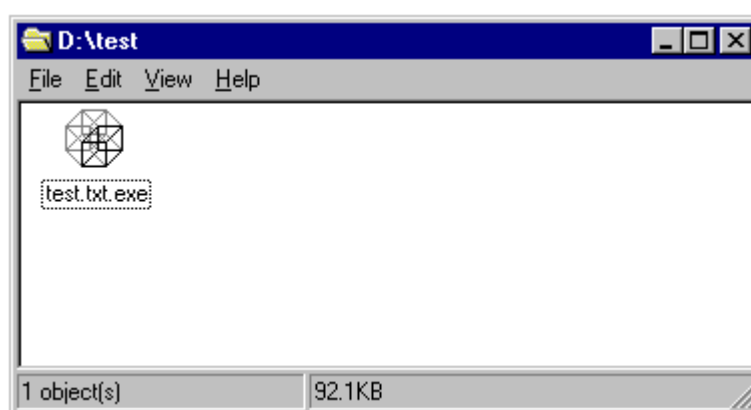

Figure 4

CRYPTOMATHIC

9

Passwords

Unlike many other encryption utilities, File2File does not require a password to be entered twice for confirmation. Instead, it offers to recognize your "default password" as a safeguard against mistyping.

The first time you enter a password for encryption, a message will tell you that File2File is storing a secure one-way hash, a "fingerprint" of your password. The password is now your default password, and so you will be allowed to perform a number of subsequent encryptions without having to enter the password twice each time.

The password should be at least 8 characters. (Characters, numbers and blanks are valid.)

If you use a password that is *not* your default password, a dialogue will pop up and ask you to confirm the password. This measure protects you from encrypting files with a mistyped password, e.g. if you use a unique password for encrypting files to be exchanged via e-mail.

4.3 Encrypt a Directory

To encrypt a directory:

1. Open Windows File Explorer

2. Select the directory and right-click it

   This will open up the context menu as shown in figure 1 above

3. Choose *File2File* and then *Encrypt*

4. Enter your password

5. Click the *Encrypt* button

File2File will now encrypt all files and subdirectories in the directory by reading the directory and encrypting the files one by one.

If the directory contains any files that have already been encrypted with File2File, these files will not be encrypted again.

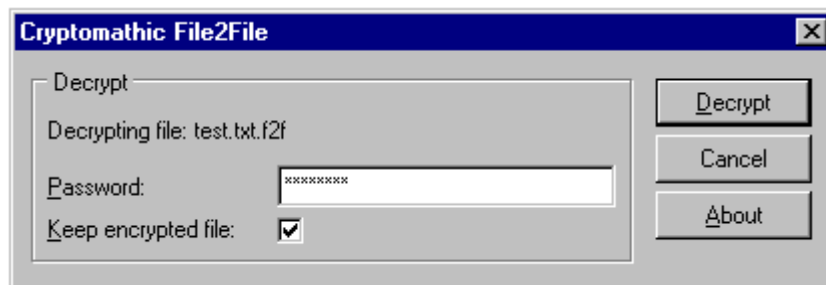It is *not* possible to create executables when you encrypt a directory.

4.4 Decrypt a File or a Directory

To decrypt a file or a directory:

1. Open Windows File Explorer

2. Select the file or the directory and right-click it

This will open up the context menu as shown in figure 1 above

3. Choose *File2File* and then *Decrypt*

4. Enter the password that was used for encrypting the file or directory

CRYPTOMATHIC

5. If you wish to keep the encrypted file or directory, check the ***Keep Encrypted File*** box

6. Click the ***Decrypt*** button

Figure 5

The original file or directory will now be restored.

The original file or directory will ***not*** be restored, if you have used the wrong password or if the content of the file or directory has been changed.

4.5 Open an Executable Encrypted File, EXE-file

The EXE-version of an encrypted file contains the code necessary for decrypting its content – the user only has to enter the right password. This enables extraction of an encrypted file from a computer where File2File is not installed.

To open an EXE-version of a decrypted a file:

1. Double-click the file

    This will bring up a modified "Save As" Windows dialogue

2. Enter the right password in the dialogue and specify where you want to save the file, see Figure 6 below

3. Click the ***Save*** button

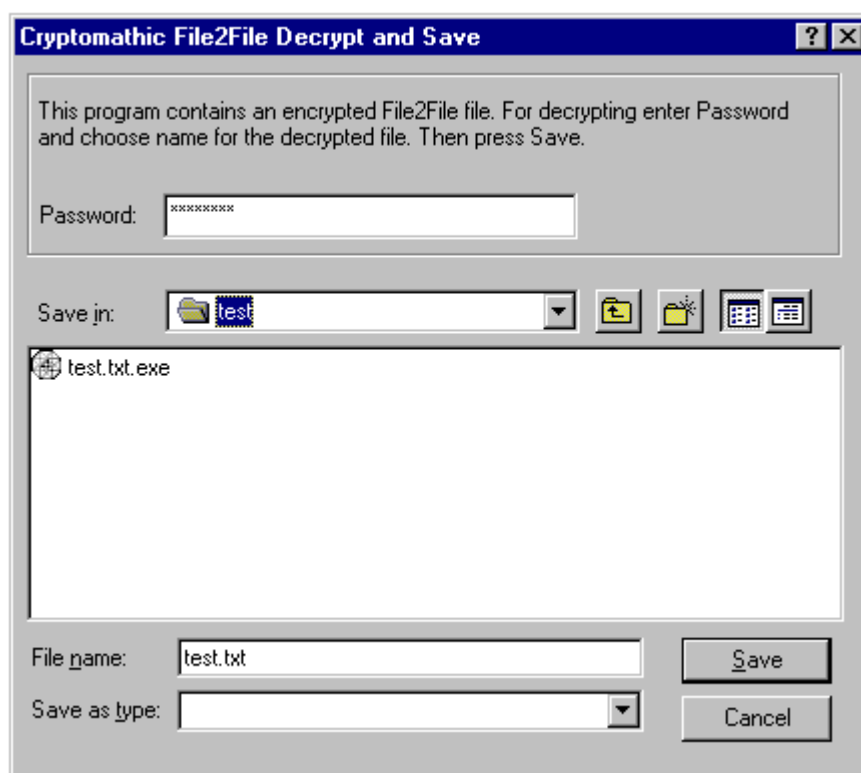The decrypted file will be launched in the application associated with its file type.

Figure 6

5 Terminology

Encryption

Encrypting a text means converting a plain text into a crypto-text, i.e. a text, which has either no meaning or a meaning different from that of the plain text. In this way, only those who have the key to convert the text back into the original plain text will have access to its actual content.

Decryption

Decrypting a text means converting an encrypted text back into the original plain text.

Executable encrypted files

The EXE-version of an encrypted file contains a small program that includes the code for decrypting the file. When opening the file, the user only has to enter the right password.

The EXE-file enables extraction of an encrypted file from a computer where File2File is not installed.

Default Password

The first time you enter a password for encryption, a message will tell you that File2File is storing a secure one-way hash, a "fingerprint" of your password. File2File will now recognize this password as your default password for future encryptions, which serves as a safeguard against encrypting a file with a mistyped password.

It is, however, possible to use another password than your default password: In this case, File2File will ask for a confirmation of the entered password.

Encrypted files and directories must always be decrypted with the password with which they were encrypted.