Welcome to

DataCloak 4.3

Before you begin, don't forget to read the legal notice and registration information.

Introduction

What is DataCloak?

DataCloak is a utility that allows to you encrypt private data, including your files and e-mails. It has been designed for ease of use, but still with enough options and security you'd expect from higher-priced encryption software.

What sort of features does it have?

How about this:

- Select multiple files individually or by directory. This can be done through the buttons on the main box, through drag-and-drop, by right-clicking on selected files, or via command line options.
- Encrypt / decrypt clipboard data. This feature is designed mainly for use in e-mails - simply select and cut your text, encrypt or decrypt it, and paste it back.
- Full logging support. Logging can be done at various levels, from simply recording when DataCloak was started and closed, to exactly what happens to each file. Errors are also logged, allowing any mistakes or problems to be traced and solved.
- Code confirmation and hiding.
- Raw and string code included for compatibility with the older *FileCode* utility.
- Secure-delete files after encryption / decryption for total data security.
- Optional "just secure-delete" - allowing DataCloak to act like a separate secure-deleting program.
- Actual file name encryption and the ability to keep source file dates.
- Automatic re-encryption/re-decryption warning.
- Full command line support - totally control DataCloak's actions using a schedule program etc.
- Uses a unique encryption process.
- Advanced internal security - protection against potential DataCloak hackers.

Want to get going already? Check out the quick start!
If you want more to find out more, look in the "more detailed information" header in the help contents.

DataCloak on the Internet

Check out the DataCloak home page at
http://www.btinternet.com/~bennett/datacloak.html (Click here)

Advanced options box

Secure-delete options
Click here for more information on this.

Number of bytes allocated to file name store
This is an internal storage area used by DataCloak to store the names and locations of individually selected files. There is no really need to change this value from its default of 50k, unless you're planning on selecting a very large number of long-named files - in which case this value would need to be increased.

Always secure-delete decrypted log file
Make sure this option is checked for maximum security. It is recommended, as otherwise it may be possible for someone to view your log file even after it has been deleted "normally".

Pre-scan file name list for short names
When files are selected through the command line (for example), then some of these file names may be in "short" format. For example, "testingfilename.txt" would be shortened to "testin~1.txt". Turn this option on to enable DataCloak to "expand" any short file names to their proper, longer name.

Check and modify files for re-encryption/re-decryption
See the Advanced file options section for more information.

Pop-up "Done" box after process
If you don't want the visual (and audio) "Done" message box to pop-up after DataCloak has finished a particular job, uncheck this option. This is done automatically when using the command line options (it is assumed DataCloak has been called automatically from another program, so there is no need to confirm the job is done).

Add/remove .dce extension
See the Advanced file options section for more information.

Remember last source directory
If you want DataCloak to remember the last source directory you had selected, check this option. The directory name is automatically encrypted before it is stored, for added security.

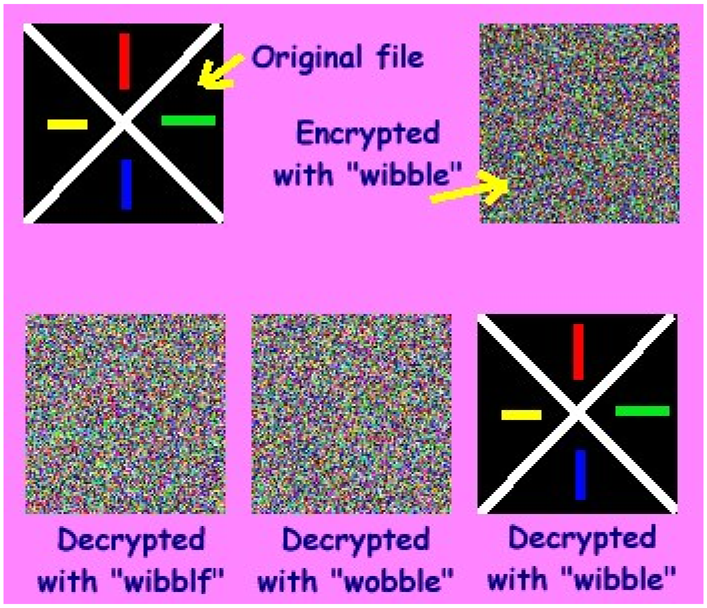
Colour gradient options
The gradient colours of the two graphical status bar displays can be set here. Just click the relevant button to display a standard colour-picking dialog.

How secure is this "unique encryption"?

Because DataCloak uses a unique process for encrypting / decrypting files, it's very hard to compare it with more well known methods such as BlowFish or DES. Still, a file encrypted just once can only be decrypted by one of a possible 2.9x10^48 combinations (that's 29 with 47 zeros after it!). This means someone would theoretically have to decrypt a file this many times, checking to see if it has been decrypted after each attempt (though how they could even do this would be hard to imagine), before they could possibly find the correct decryption combination. There is no other way to tell what it is from looking at the file, as obviously no hint of the decryption password is stored in the file itself. This is also, of course, assuming the file has only been encrypted once. Yet DataCloak has no problems encrypting a file twice, three or indeed any number of times (providing its automatic checking is disabled) - with each encryption the number of possible combinations increase so much that (even though there is certainly *no* reason why one encryption is not secure enough) after multiple encryptions the chances of an unauthorised decryption are even nearer to impossible. How can someone even tell how many times the file as been encrypted? They can't.

The fact that DataCloak uses a unique byte alteration process is also in favour of its security - someone has got to figure out just what goes on in DataCloak to even start an attempt at a decryption program (though as you've seen from above - there's not much point trying ;)

How about a graphical example? This mainly shows just how important the correct password is. A "raw" image is used to illustrate DataCloak's encryption / decryption. Normally you can't even open an encrypted image file in a viewer because it's "header" has been scrambled - so the viewer doesn't have a clue what it is. However, RAW images do not contain a header, so it's possible to use them as a visual display:



This simply demonstrates how vital the correct password is - and how even the slightest change in it will mean a totally unusable file.

Passwords and Passcodes

In order to encrypt a file, DataCloak needs to assign it between 3 and 5 numbers. Each of these numbers have a range of over 4.3 billion and are used in DataCloak's file alteration system. However, to save you having to type in and remember these numbers, you can simply enter a password. DataCloak can then turn this password into five numbers internally. Most people will use the *Easy* code type. This is simply a password consisting of whatever word(s) you want. However, there are two other types that can still be used - *String* and *Raw*. These are really only included for compatibility purposes with the older *FileCode* as the *Easy* code type is perfectly acceptable, and (as its name suggests ;) easier to use.

Use of each type

Easy

Simply enter any word (of even sentence) of your choice. It can contain any characters you can enter on your keyboard, and be virtually any length you like (it has a maximum of 8000 characters;). Please remember that it is **case sensitive** - so be careful. It must be entered exactly the same each time for correct results - though any mistakes can normally be found and corrected by using the log.
The minimum password length is 2 characters. Note that the length of the password you enter has very little relevance to the actual level of security on the file - a 3 character password has about the same security as a 20 character one.

String

This operates almost exactly like the *Easy* code type, but has either a "1" or a "2" in front of the password. This replaces the *"encrypt"* and *"decrypt"* options under *Easy* code (and you'll notice these buttons change to a single *"create target(s)"* button). The opposite number must be used to decrypt a file than was used to encrypt it. For example, a file encrypted with the *String* code of:

1mypassword

Must be decrypted by:

2mypassword

Raw

This is.. erm.. pretty pointless really :)
Still, one advantage of this type is that you specify the file alteration numbers directly. However, unlike both *Easy* and *String* types, only 3 numbers are supplied to the

alteration engine - and so is used slightly differently internally. *Raw* passcodes take the form:

A!B!C

Where "A" is either a "1" or a "2" and is used in the same way as the *String* type. "B" and "C" are numbers that can range from -2147483648 to +2147483647. Other than using the opposite alteration number in "A", the numbers in "B" and "C" must be exactly the same each time to obtain correct results. For example, a *Raw* code encryption of:

1!12345!123

Must be decrypted by:

2!12345!123

A minus (-) sign may be added to produce negative numbers.

Quick start

Want to get going straight away?   Follow these simple steps - and come back to the help if you need more information:

1)   Select the file(s) you want to encrypt or decrypt by pressing the *"individual file(s)"* button (Alt-I).   If you'd rather select all files in a directory, select it by pressing the *"all files in directory"* button (Alt-F).   If you want *everything* in the directory to be selected (including any directories within it, and all their files) check the *"recurse directories"* box - otherwise just the files in the root of that directory will be selected.

2)   The target directory will automatically be set equal to your source directory (meaning your old files will be replaced by the changed ones).   If, however, you'd rather leave your original files alone and have the changed files created in a new directory, select or create it by pressing the appropriate buttons.   If you've selected your files using the *"all files in directory"* button and have *"recurse directories"* selected, then you can choose to *"recreate source directories"* (Alt-O) or just dump all the source files in to one directory (this isn't really recommended though, as some files could be over-written).

3)   Type in the password you want to use in the top-left box (Alt-C).   Remember it is CaSe SeNsItIvE!

4)   Make sure everything is correct, and press *"Encrypt"* (Alt-E) or *"Decrypt"* (Alt-D) to encrypt or decrypt your files.

That's it!

Want to learn more? Check out the help contents :)

What is... Encryption?

Encryption is what happens to your data to make sure no-one else can read or understand it. You **Encrypt** data to hide it from others. The opposite to encryption is decryption.

Selecting your files

Selecting individual files

Via the main DataCloak box

This can be done by pressing the *"individual file(s)"* (Alt-I) button. A standard open box will appear. Either select one file just by clicking on it, or select multiple files by holding down *control* while clicking on your file names. To select a group of files click on the first one, hold down *shift* and click on the last one. Press OK to pass these file names on to DataCloak. A "file type" selector is also available allowing you to filter out specific files - zip, Word, DataCloak-encrypted (DCE), or text ones for example.

By drag-and-drop

Just select the files you want (in your file browsing program for example) and "drag" them over to the DataCloak program icon . This can be either on your desktop or as seen through a file browsing program such as *Explorer*. DataCloak will then start up with these files automatically selected.

This can be used as an alternative to the clipboard method for the transfer of encrypted e-mails. You use this method instead.

By right-clicking

Follow these instructions to make a shortcut to DataCloak in your Windows SendTo directory. When you have a selection of files, right-clicking on them will normally bring up a menu. On this menu, you should find a "Send To" option. Select this, then select DataCloak from the list of programs. DataCloak will start up with these files automatically selected.

Via DataCloak's command line options

See the topic on command line options.

Selecting all files in a directory

Via the main DataCloak box

Simply press the *"all files in directory"* (Alt-F) button. A standard browse for folder window will open, allowing you to select the directory you want. If you want to include any other directories within this directory, and all their files, check the *"recurse directories"* (Alt-R) box. Otherwise, just the files in the root of your chosen directory will be selected.

By drag-and-drop

Just drag the directory to a DataCloak program icon, as described in the previous section. Select *"recurse directories"* (Alt-R) if needed.

By right-clicking

Make sure you've got the directory name selected, and follow the instructions as described in the previous section. Select *"recurse directories"* (Alt-R) if needed.

Via DataCloak's command line options

See the topic on command line options.

After selection - setting the target

The selected file(s) will appear in the source display box. If this is the first selection you've made, then the target directory will also be set to your source. This means your old files will be replaced by the changed ones. You can also set this by pressing the *"set to source"* (Alt-T) button.

If, however, you'd rather leave your original files alone and have the changed files created in another directory, *"select"* (Alt-S) or *"create"* (Alt-A) it. If you've selected all files in a directory, and have *"recurse directories"* selected, then you can choose to *"recreate source directories"* (Alt-O). This will recreate the source's directory structure within the target directory. Otherwise all the source files will be placed in to the root of your target - this isn't recommended though, as some files could be over-written (where the source file names are the same but in different directories).

What is... Decryption?

Decryption is what happens to your encrypted data to make it readable again.   You must **Decrypt** your data before you can use it.   The opposite to decryption is encryption.

Selecting and using clipboard data

Select the text you want to use, and cut (or copy) it to the clipboard (normally by pressing Ctrl-X or Ctrl-C). Back in DataCloak, press the *"clipboard text"* (Alt-X) button. The *"select clipboard source"* dialog will appear. Most text you select (such as that from e-mails) will be "plain text" - so make sure this option is selected.

However, if your text has (or is meant to have) formatting (such as colours, bold and underline) then select either *"Rich Text Format (RTF)"* or (if the text is encrypted RTF), *"encrypted RTF"*. Please note RTF text encryption/decryption is *not* recommended for use in e-mails, due to the fact that text-wrapping cannot be used. Even if your e-mail is written as RTF (though this is not normally the case) it is strongly recommended you select the *"plain text"* option to convert to normal, unformatted text.

Providing you're using plain text, you can then select to wrap your text. This feature is included mainly for the benefit of e-mails. Before your e-mail client sends your letter, it normally wraps your text to a maximum line length of about 75 characters. However, if it does this to encrypted text the extra return characters it enters disrupts the code, stopping correct decryption. How do you get round this? Let DataCloak wrap your text to maximum 75 line length itself :)

For this reason, it is *strongly recommended* you have the *"wrap text before encrypting"* option turned **on** and the maximum line length set to 75 characters when encrypting e-mail text. If you're decrypting text, providing the text you're decrypting was also wrapped in this way, then this will have no effect. However, if you're having problems when decrypting text, try turning the wrap text option off.

Now, just enter your password and encrypt / decrypt your text as normal. Finally, paste your text back into your e-mail client (or whatever application you're using) - normally by Ctrl-V.

You could also use this method for encrypting / decrypting e-mails. It's perhaps not quite as quick and easy as the clipboard method (it was used before this was created) but some people might prefer it anyway :)

Other notes on clipboard encryption / decryption

The encrypted text outputted in this way contains no "illegal" characters, meaning it will always be displayed correctly on your recipient's computer. However, this also means the text alteration is slightly different to the file alteration process. This shouldn't be a problem - it just means you can't copy the contents of an encrypted file to the clipboard, and clipboard-decrypt it. As file-alteration and text-alteration aren't compatible, it won't work.

As encrypted text is sensitive to any character changes / additions, make sure you don't modify it afterwards by mistake!   Also, ensure your recipient knows exactly where to start selecting your text (such as saying "select everything below this line..").   Hopefully this is fairly obvious, but could still be a cause of decryption problems.

Another possible use for clipboard encryption could be on a web page - just paste your encrypted text into your HTML, and allow users to select your text from their browsers for clipboard decryption...   Sometimes *Netscape* tries to imitate the formatting on your web page by adding spaces to your copied text.   This can be avoided by ensuring your text doesn't have images, borders indents or frames around it - generally kept as plain as possible (though font and colour, for example, are ignored).   *Internet Explorer* does not appear to change your selected text in this way anyway :)

The drag-and-drop e-mail method

1) Right-click on the desktop, select new --> text document
2) Give the new text file a name, double click it and write your message.
3) Save the file and close the text window
4) Drag the text file's notepad icon to the DataCloak icon (or use the right-click --> send-to option).
5) DataCloak starts up with this file selected.   Type in your password and Encrypt (Alt-E).
6) Exit DataCloak - and there you are - your message has been encoded :)

You can then attach the file to your e-mail (it can be found from an open box in the top-most directory - "desktop").
The recipient simply drags the attached text file icon to the DataCloak icon to decrypt it.

Don't forget the clipboard method can also be used!

Legal Information

MATTHEW BENNETT IS THE AUTHOR OF DATACLOAK 4.3.

THE USER MUST ACCEPT THE FOLLOWING AGREEMENT:

DISCLAIMER:
"DATACLOAK 4.3 IS SUPPLIED AS IS. THE AUTHOR DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE WARRANTIES OF MERCHANTABILITY AND OF FITNESS FOR ANY PURPOSE.   THE AUTHOR ASSUMES NO LIABILITY FOR DAMAGES, INCLUDING THAT OF LOST OR DAMAGED DATA, BE IT DIRECT OR CONSEQUENTIAL, WHICH MAY RESULT FROM THE USE OF DATACLOAK 4.3."

DATACLOAK 4.3 IS THE PROPERTY OF MATTHEW BENNETT

THE DATACLOAK 4.3 EXECUTABLE AND ACCOMPANYING FILES (INCLUDING THIS FILE) MUST IN NO WAY BE ALTERED BY ANY MEANS, AND SO MUST REMAIN EXACT COPIES OF THOSE RELEASED BY THE AUTHOR.

DATACLOAK 4.3 IS RELEASED AS SHAREWARE.   THE UNREGISTERED USER MAY EVALUATE DATACLOAK 4.3 FOR THIRTY (30) DAYS STARTING FROM WHEN DATACLOAK 4.3 WAS FIRST RUN BY THE USER.   AFTER THIS PERIOD, THE USER MUST REGISTER DATACLOAK 4.3 TO CONTINUE USE, OR REMOVE DATACLOAK 4.3 (INCLUDING ALL COPIES) FROM THEIR SYSTEM.   DATACLOAK 4.3 MUST ONLY BE REGISTERED USING ONE OF TWO WAYS:
1) A VALID ACCESS KEY OBTAINED DIRECTLY FROM THE AUTHOR OR DIRECTLY FROM AN AUTHORISED REGISTRATION COMPANY AS SPECIFIED IN THE "HOW TO REGISTER" SECTION OF DATACLOAK 4.3.
2) A VALID RE-REGISTRATION DISK CREATED BY DATACLOAK 4.3 (OR LOWER VERSION OF DATACLOAK) FROM AN ACCESS KEY OBTAINED AS DESCRIBED IN WAY (1).

DATACLOAK 4.3 MAY ONLY BE REGISTERED TO ONE (1) COMPUTER AT A TIME PER REGISTERED USER, UNLESS THE USER HAS BEEN REGISTERED BY THE AUTHOR OR AN AUTHORISED REGISTRATION COMPANY TO BE ALLOWED TO DO OTHERWISE.

DATACLOAK 4.3 MAY BE FREELY DISTRIBUTED ACCORDING TO THE ABOVE AGREEMENT.

Any trade or registered names mentioned in this help document are hereby acknowledged to be the property of their respective owners.

Advanced file options

Keeping the original source file dates

If you wish to keep the original source file dates when creating your target files, be sure to check the *"keep original source file dates"* (Alt-K) option in the target section. This is aimed at users whose actual file dates are important, for storage purposes for example. It also means the date you created your encrypted files cannot be easily found out either.

Encrypting / decrypting file names

The actual file name can be encrypted / decrypted too. Simply check the *"include file name(s)"* (Alt-N) option. Now even the file names themselves can be hidden :)

Re-encryption / Re-decryption warning

By default, this option is turned on under the advanced settings. It allows DataCloak to check for, and add, four characters at the end of a file (DCEA). If these characters are present, it assumes the file is encrypted - if they're not, it assumes it has been decrypted (or simply untouched). However, this means the file's size is increased by 4 bytes. For this reason, this feature has been left as optional - though is still recommended as a safety warning for most users. Also, if this option is turned off, and DataCloak is used to decrypt a file encrypted when it was on (the file has the DCEA at the end) then this will **not** be removed upon decryption, resulting in 4 random characters at the end of the file. In most cases this shouldn't actually cause any problems - but is still to be avoided where possible. The best thing to do if unsure is to leave the option turned on.

Add / remove .dce extension

By default, this option is turned off under the advanced settings. It simply adds a .dce extension to files you encrypt, and removes it when they are decrypted. This is to allow users to easily see what files are encrypted. It also means they can double-click on a .dce file and launch DataCloak automatically.

Shareware and registering information

DataCloak 4.3 is shareware. You may use this program for 30 days - after which, you must either register DataCloak to obtain the fully registered version, or remove DataCloak from your system. The cost of registering is USD 15 - we hope you'll agree this is a very reasonable amount to pay for DataCloak!

Feel free to give as many people as you can the shareware version of DataCloak :)

For details on how to register, press the "how to register" button on the registration reminder screen. Your two UINs (Unique Identification Numbers) will also be shown here. These numbers are (very nearly) unique to your system, and mean DataCloak can only be registered on **your** computer with the access key you'll be given. This prevents people from registering DataCloak illegally. Please remember to keep your access key safe, as you will also need it to "unlock" your re-registration disk. Your user name is also important to remember when registering for the first time, and is *case sensitive*.

DataCloak registration site:
http://www.btinternet.com/~bennett/dcreg.html (Click here)
This site will contain a direct link to DataCloak's registration page on ShareIt.com.

ShareIt! registration site (allowing you to register DataCloak):
http://www.shareit.com/ (Click here)
Type "datacloak" in the Express Registration search box.

Re-registration

As your access key is only valid for the system you first register DataCloak to, this means DataCloak will recognise a problem if you upgrade your computer, for example. If your RAM, hard drive (the one with your operating system on) or your operating system change (or is re-installed), then you will need to re-register.

This is done using the re-registration disk that was created for you upon your initial registration. Please keep this disk **safe** and secure (to prevent any one other than you using it). You may make one back-up copy of the disk using the disk-copy feature on your operating system (such as right-clicking on your floppy disk icon and selecting "copy disk"). Please note the command-line version of "diskcopy" will *not* work.

You may only use your re-registration disk to register DataCloak on one computer at a time, **unless** you have been registered to do otherwise.

If a copy of your registered version is placed on another computer, DataCloak will give a warning and then revert back to the shareware version (the new user remains unregistered).

Registration problems or questions

If you're having troubles registering, or are unable to find an answer to a registration problem, e-mail me (the author) at bennett@btinternet.com and I'll do my best to help.

Adding a DataCloak SendTo Icon

For this example we'll be using Windows Explorer.

1) Right-click on the datacloak.exe file (the one with the small yellow and blue icon) in your DataCloak directory.   Select "Copy" from the menu that appears.

2) In your Windows directory, you'll find a folder called "SendTo".   Select it, and in the right-hand window right-click on a blank white area.   Select "Paste Shortcut".   Now, click *once* on the new file created (it should already be highlighted in blue), and rename it simply to "DataCloak".

You can now send files to DataCloak as described here!

DataCloak won't start up

If DataCloak quits the moment you run it, or doesn't run at all, then there are two possible causes:

1) The datacloak.sec file is not in the same directory as the DataCloak program. Copy the .sec file to the same directory and try again.

2) The DataCloak program file (datacloak.exe) has been modified. Delete this file and replace with an un-modifed version (or re-install). This could be a sign that someone has tried to hack DataCloak, or that your computer has a virus!

About the author

Hi :)

Firstly, thanks for using DataCloak!

Who am I?	Matthew Bennett
Where do I live?	Near Guildford, in the south-east of England
How old am I?	Well... I'm a student :)

Why did I start DataCloak?
DataCloak is the latest (and best) encryption program I've written. I first made one quite a few years ago, and have really just been improving it ever since. *FileCode* was released to the public as freeware, and was followed-up by the program you're using now about 6 months later. To be honest, I'm no great encryption enthusiast - I was just interesting in writing a program (originally text-based, and in Pascal) that could encrypt and decrypt text files. Things just went on from there, and when I had the chance I'd just add a bit more to my program. Now, finally, I've released *DataCloak* - a 32-bit Windows application written using the excellent (and free!) MinGW32 C/C++ compiler. The DataCloak "C" source file (excluding custom header and resource files) contains 164,511 characters in 4021 lines. It has probably taken around a year to write, though this includes the time taken writing *FileCode* (or which DataCloak is based).

How can you contact me?
My e-mail is bennett@btinternet.com. My ICQ UIN is 15594981 (though I don't have much time for checking ICQ at the moment..). You could also find me in the #tuna or #england IRC (IRCNET) channel as MattB :)

Bug reports

Nnnnooooo!!! You can't have found a bug!

OK.. if the impossible does happen ;) then please do e-mail me at **bennett@btinternet.com** with as much information as you can. Make sure you've read the help first though, to make sure it's not actually *meant* to be happening :)

Secure delete options

Why use *secure-delete* anyway?

When you normally delete a file, it normally goes to your "recycle bin". Only when you empty to bin are your files actually deleted. Sometimes (for example through the DOS prompt or by other programs) the file bypasses the recycle bin and is deleted straight away.

However, even when a file is deleted "properly" (and its file name disappears from file browsers), it is only the file system's pointer that has been removed. All the data from that file is **still** on your disk, just can't be seen. However, using a standard undelete program can replace the file's pointer - and up pops all the data again!

So how can this be stopped?

With *secure-delete* turned on, the file is over-written by 1's, 0's or random characters, **then** deleted. This means that even if the file was later recovered, the person would simply get an unusable file anyway - no trace of your original data could be seen. Note that using 1's or 0's is faster than using random characters, with all three being about as effective as each other.

Why have the option to over-write a file multiple times then?

This is only really necessary for people that want the very maximum of security. It is possible, using advanced data recovery techniques, to still trace the magnetic residue of your original file directly from your disk. However, each time a file is over-written, this original magnetic residue decreases - meaning the more over-writes, the less the chances of this advanced recovery succeeding. Still - given the noticeable speed decrease when using multiple over-writes (particularly when using random characters) multiple over-writes are only recommended for people that seriously believe their data could be examined using magnetic residue attempts. Otherwise, simply one over-write is perfectly acceptable!

How to I get DataCloak to secure-delete my files then?

Simply check the *"secure-delete file(s) afterwards"* (Alt-U) box. DataCloak will then secure-delete each source file after it has created the new target one. Note this also applies even when the source directory and target directory are the same. If you **just** want to secure-delete some files, simply select them as usual, and press the *"just secure-delete now"* (Alt-J) button - and they're gone :)

Secure-delete options are also available through the command line options.

Using the log

Overview

The log file can record anything from simply when DataCloak was started and closed, to exactly what happens to each individual file. The file itself is encrypted (both internally in DataCloak and as a file) with a password you specify. The exact level of recording written to the log can be controlled through the log options box.

Options

The log options dialog itself can only be accessed once the correct password has been entered. Once this is done, one of the things you'll be able to do it to set what is recorded in the log. You choices are:

Log start / close

This option is available if you want the time and date of each time DataCloak is started and closed. This is not enabled by default, as it could lead to a large log file - and would only be really necessary if many people have access to your computer.

Log all actions

This option is certainly recommended, and is on by default. All actions you perform (such as encrypting all files in a directory, or decrypting 4 files through drag-and-drop, etc.) will be recorded. However, each individual file is not recorded - so meaning the log doesn't become too large too quickly. This is one of the most useful options to leave on for "debugging".

Log individual files

If you want each individual file name to be logged, enable this. It is off by default to save on space (and to save having a too complicated-looking log file). Still, if you need to search for information on what has happened to a particular file - the file name itself will be recorded - instead of simply saying (for example) "all 20 files in....".

Log passwords / passcodes

This option is on by default, as mistyped passwords are one of the most common mistakes to be made. It also allows you to find a file's password you've forgotten. However, some people may not wish to have their passwords recorded in any way - even in the encrypted password-protected log file. Un-checking this option means the record of your password will never be written to the log - so there's nothing that can be done if you forget it!

Log errors

Once again, this option is on by default.   Any errors DataCloak encounters (such as being unable to read or write a file) will be recorded here.

Viewing and clearing the log

Simply press the relevant button.   When you wish to view the log, DataCloak will decrypt your log file and display it using your default text viewer (normally NotePad). The decrypted log will be deleted (secure-deleted by default) when DataCloak exits.   It is recommended you close your text viewer *before* closing DataCloak, to save any problems when trying to delete the file.   It is also recommended you do not modify this file (though any modifications will have no effect on your actual log file itself).   If DataCloak is terminated unexpectedly (such as through a "close program" termination) after you've viewed the log then your decrypted log file will *still be present* in your log directory as "log_zyi.txt".   Always ensure this file is deleted should this happen. Please note the log is never decrypted unless you wish to actually view it (or ask to change the log password).

If you're sure the information in your current log file will not be needed, then DataCloak can clear the log file.   The time this have occurred will be recorded at the top of your new log file.

Changing the log password

To do this, simply select it from the log options box.   Please note you will not be asked to enter the old log password, as this will have already been done upon accessing the options themselves.   Log passwords are case sensitive, and may have a maximum of 95 characters.

Other information

Whatever options are currently chosen will be displayed to the left of the log button on the main DataCloak box - to allow you to quickly check what is or is not being recorded. Other than a text description, "+P" shows your password is being recorded, and "+E" shows errors are being logged.   For security reasons, any attempts to access the log file with an incorrect password will be recorded to the log itself (the incorrect password itself will be recorded too, provided you have "log passwords/passcodes" checked).

If you with to *disable* the log, simply uncheck the "enable log" option.   Though this means nothing will be written to your log file, the file itself must still be present and accessible to DataCloak (as it holds the log options verification password, for example).

Please see this topic for further information on getting "lost" files back using the log file.

Security issues

If someone obtained a copy of your log file, it is always possible (though unlikely, due to various internal security measures) that a hacker could access the internal workings of DataCloak and obtain your log's password. Once they have this, it would be possibled for them to view your file's decryption passwords. How can you prevent this? You can either simply stop DataCloak logging the passwords you use, or disable the log all together. Provided you have the "confirm password" checked in DataCloak, the first option may be preferred to users who belive their systems have a high chance of being accessed by hackers. Disabling the log is not recommended due to the fact that any mistakes you make cannot be traced. However, another option is to store your log file on a floppy disk, that you keep safe yourself. You can do this simply by setting your log directory to "A:\" (or whatever drive letter you use).

Please remember though these precautions are only recommended for users who belive their log file has a reasonable chance of being found, copied and hacked. For most users however, storing your log file on your hard disk should pose no security problem at all. Your encrypted files themselves are obviously safe wherever they are :)

Lost files - common causes

Though uncommon to most users, sometimes things go wrong that means you can't access your files. What could have caused this, and what are the things to watch out for?

Re-encryption, re-decryption

One of the most common problems encountered by users of *FileCode* was that of re-encryption and/or re-decryption. For example, a user encrypts a file once. They then decrypt it back again. However, they later return to the file - forget it has already been decrypted - and re-decrypt it. They are then unable to access the file. Why?

There is very little difference, so far as DataCloak is concerned, between encrypting and decrypting a file. Simply put, for encryption DataCloak moves the file's bytes in one direction, and for decryption they're moved by the same amount but in the opposite direction. For example:

Normal:	OOOOOXOOOOOO	The X is the byte
Encrypted:	OOOOOOOOXOOO	The byte has changed by +3
Decrypted:	OOOOOXOOOOOO	The byte has been moved back by -3

However, problems arise during (in this case) re-encryption:

Normal:	OOOOOXOOOOOO	
Encrypted:	OOOOOOOOXOOO	+3
Re-encrypted:	OOOOOOOOOOOX	+3
Decrypted:	OOOOOOOOXOOO	-3

The user thinks the file has been decrypted, so it must be readable, but this is not the case. The byte is still out by 3 because of the re-encryption. It must be decrypted *again* to move it back by 3 again, and the file returns to normal. When looking at the diagram, this seems obvious - but some users may think just the action of pressing "decrypt" will always produce a normal file. As you can see above, when things go wrong this is not always the case.

The chances of this happening has however been greatly reduced by the new warning option in DataCloak. See the advanced file options for details.

Mis-typed or incorrect passwords

Many users are more cautious of this, and ensure "confirm password" is checked. This is particularly important for users who prefer their passwords to be hidden. However, as the password is the most important variable when decrypting your files, any mistakes will result in this being done incorrectly.   This happens because the bytes are not changed in the same way as they were when they were decrypted:

Correct:

Normal:	OOOOOXOOOOOO	
Encryption A	OOOOOOOOXOOO	+3
Decryption A	OOOOOXOOOOOO	-3

Incorrect:

Normal:	OOOOOXOOOOOO	
Encryption A	OOOOOOOOXOOO	+3
Decryption B	OOOXOOOOOOOO	-5

Other problems

Not selecting the correct source files, or sending their target files off to the wrong place, can mess things up.   Basically, it is up to you to ensure the source and target options are correct before starting - there is little DataCloak can do itself!

One other possible source of confusion could be if any of your files you wish to encrypt/decrypt have the extension "**_zx**".   This is a special extension used by DataCloak during the file alteration process, but it assumes no files have these letters as their normal extension.   If this is the case then DataCloak will simply ignore this file if it is doing an "all files in directory" process and the source directory matches the target one.   This may cause an error towards the end when DataCloak has altered all the files, but still thinks there's another one to do.   However, it is unlikey you *would* get a file with a "_zx" extension, and even if you did, the problem could be solved simply by renaming that file beforehand.

See this topic for details on solving common problems.

Lost files - how to get them back

If you've opened the DataCloak help in a panic to try and get your files back, I bet you're glad this one has been put in :)

If your text file is still a mess, or an application complains it still can't access your "decrypted" files, then it is DataCloak's **log file** that should be able to sort things out. This is the reason it was put in - if you've disabled it, or are not recording actions or individual files, then I'm afraid your chances of recovery are considerably reduced - just try and think back over what you've done is all that can be recommended in this case.

However, if you've kept with the log defaults, then follow this topic:

File recovery steps

1) Sounds obvious, but make sure your files *are* actually inaccessible. Check you're trying to load/read the correct ones - especially if your target directory is different from your source. Once you're sure your files have defiantly not been decrypted correctly, continue.

2) Open your log file in DataCloak (log-->enter password-->view)

3) Starting from the top, find the line just above the point you're certain the files were normal. This may simply be the start of the log file itself. Delete the irrelevant log entries above this point, to make things clearer. Don't worry - nothing you do here will actually effect the main log itself. Work through the log file, deleting any more irrelevant references that you're sure have no relevance to your file(s) in question. This is all to make the log clearer.

4) Starting from the very **last** line of the log file, and working **backwards**, copy each entry to *another* text file. You'll notice you're creating a *reverse* list of the log entries. Keep going up the log until you've copied the top-most line (the one where the trouble started..). There's no need to record the times or dates, and you can simplify the entries. For example, a log entry of:

[2/Nov/1998 12:08] All 25 files from 'C:\Private' --> 'C:\Private', using EasyCode Encrypt password "mypassword" (confirm and hide code)

Can be simplified and written to your list as:

Encrypt all 25 files from 'C:\Private' using "mypassword"

(Don't forget to keep the target directory if it's different to your source, though). When copying the password, make sure you copy *exactly* what it says - don't assume it's what it *should* be - a mistyped password could have been your problem. As you work up the log, it might be a good idea to mark the line you've just done, to save confusion. **Number** each entry you copy to your *new* list.

5) Now, work down your **new** list, but this time **reversing** the encrypt / decrypt references. Also, if the target directory is different to your source, **swap** these round too. For example, if an entry on your new list said something like:

```
1) Encrypt all 25 files from 'C:\Private' using "mypassword"
```

You should change it to read:

```
1) Decrypt all 25 files from 'C:\Private' using "mypassword"
```

It helps to make the "E" and "D" of encrypt and decrypt capital letters, to help make them more clear. It might be a good idea to print out your list now.

6) Now, in DataCloak, simply follow the instructions on your new list (reading from top (entry 1), to bottom as normal). Be *sure* to **check** everything it correct before encrypting/decrypting at each step. Mark (such as cross out) each step as you complete it, to save confusion. Once you've done this, your files should be back to normal.

Working example

Say this is what your log file said:

```
<<Files were normal>>
[2/Nov/1998 12:08] All 25 files from 'C:\Private' --> 'C:\Private', using EasyCode Encrypt password
"mypassword" (confirm and hide code)
[2/Nov/1998 12:08] DataCloak closed
[3/Nov/1998 9:22] DataCloak started
[3/Nov/1998 9:29] All 25 files from 'C:\Private' --> 'C:\Private', using EasyCode Encrypt password
"mypassword" (confirm and hide code)
[3/Nov/1998 9:30] All 25 files from 'C:\Private' --> 'C:\Private', using EasyCode Decrypt password "wibble"
(confirm and hide code)
[3/Nov/1998 9:31] All 25 files from 'C:\Private' --> 'C:\Private', using EasyCode Decrypt password
"mypassword" (confirm and hide code)
<<End of log>>
```

To create an "undo" list, you'd follow the instructions above. Here's what you should be doing:

1) and 2) ***done***

3) - Simplify log

```
<<Files were normal>>
[2/Nov/1998 12:08] All 25 files from 'C:\Private' --> 'C:\Private', using EasyCode Encrypt password
"mypassword" (confirm and hide code)
[3/Nov/1998 10:29] All 25 files from 'C:\Private' --> 'C:\Private', using EasyCode Encrypt password
"mypassword" (confirm and hide code)
[3/Nov/1998 10:30] All 25 files from 'C:\Private' --> 'C:\Private', using EasyCode Decrypt password
"wibble" (confirm and hide code)
[3/Nov/1998 10:31] All 25 files from 'C:\Private' --> 'C:\Private', using EasyCode Decrypt password
"mypassword" (confirm and hide code)
<<End of log>>
```

DataCloak start and close times removed - these were irrelevant

4) - Copy (and simplify) log entries to a new file, starting from the last log entry and working backwards.

New file:

1) Decrypt all 25 files from 'C:\Private' using "mypassword"
2) Decrypt all 25 files from 'C:\Private' using "wibble"
3) Encrypt all 25 files from 'C:\Private' using "mypassword"
4) Encrypt all 25 files from 'C:\Private' using "mypassword"

5) - Reverse Encrypts and Decrypts

1) Encrypt all 25 files from 'C:\Private' using "mypassword"
2) Encrypt all 25 files from 'C:\Private' using "wibble"
3) Decrypt all 25 files from 'C:\Private' using "mypassword"
4) Decrypt all 25 files from 'C:\Private' using "mypassword"

6) - Follow this list to "undo" the changes to your files

Why does this work?

All you've done is work backwards through the log, reversing the encryptions and decryptions. Simply, if you've done this:

Encrypt 'file.txt'
Encrypt 'file.txt'
Decrypt 'file.txt'

Then to get your file back, you do this:

1) Encrypt 'file.txt'
2) Decrypt 'file.txt'
3) Decrypt 'file.txt'

Though in this case you could also simply decrypt it once more, copying out every line individually and following it should prevent any mistakes, and allow you to solve even the most complicated mix-ups :)   It also means you can solve problems where the passwords are different/misspelt too.

If you're still having problems, and your files are ***very*** *important - it may be possible to contact the author at bennett@btinternet.com with a copy of your log file and what the problem is.   Please note however that the author has no obligation to do so, and so this really is a last resort.   Obviously there is no way the author (DataCloak programmer) or anyone else can decrypt your files without access to your log and password(s).*

Command line options

DataCloak allows you (or an external program) to totally control DataCloak from the command line. You can do just about any process through the command line that you could through the main DataCloak dialog. When you call DataCloak in command line mode, it will automatically exit after it has completed the job. Here are the switches to be entered after the program name:

/s "c:\files"	Select default **s**ource directory
/f "filename1" "filename2"	Select source **f**iles
/t "c:\encrypted"	Select **t**arget directory
/p "mypassword"	**P**assword / Passcode
/r	**R**aw code
/g	Strin**g** code
/e	Easy code **e**ncrypt
/d	Easy code **d**ecrypt
/h	**H**ide code
/c	Re**c**urse directories
/n	Recreate **n**ew source directories in target
/k	**K**eep source file date(s)
/l	Secure-de**l**ete source files
/a	Include file n**a**mes in encryption/decryption
/m	Run **m**inimised
/x	*JUST* secure-delete source files
/o	Add / remove .dce filename extensi**o**n
/y	No checking or modif**y**ing files for re-encryption/re-decryption
/w	Show no **w**arning / error message boxes

- If the default source directory is not specified, then the directory DataCloak is running in will be used.
- If no source files are specified, then ALL files in the source directory will be altered.
- You may include the file's full directory name if it is different from the default source directory.
- If the target directory is not specified, then DataCloak will assume you want to overwrite your source files (the target directory will match the source directory).
- If String code or Raw code is not specified, then DataCloak will default to Easy code, and you will need to include either the encrypt or decrypt option.
- If Hide code is not specified, then the code will be visible.
- DataCloak will *not* recurse directories (or recreate source directories in the target), keep the source file date(s), include file names in encryption/decryption, secure-delete source files or add / remove .dce filename extension by default.
- DataCloak *will* check and modify files for re-encryption / re-decryption and show warnings / errors by default.
- There is no need to specify a password or target when *just* secure-deleting.
- Switches are not case sensitive.

Command line examples

To encrypt "text.txt" in the DataCloak directory with the Easy code password "mypassword":

```
datacloak /f "text.txt" /p "mypassword" /e
```

To decrypt "thingy.zip" in "c:\encfiles" with the Easy code password "normalpass". Hide the code and minimise DataCloak:

```
datacloak /s "c:\encfiles" /f "thingy.zip" /p "normalpass" /d /h /m
```

or

```
datacloak /f "c:\encfiles\thingy.zip" /p "normalpass" /d /h /m
```

To encrypt everything in "c:\private" with the Easy code password "justdoit". Recurse the directories. Put the encrypted files in "c:\enc", and recreate the source directories:

```
datacloak /s "c:\private" /t "c:\enc" /c /n /p "justdoit" /e
```