Instructions for CODER program

CODER is a dedicated encryption program with a number of front-end facilities to make the tasks associated with secure communications easier.

Starting Coder

Place the CODER Program Disk in drive A: and at the DOS prompt type

>A:TECOD

If you have copied CODER to your hard drive (not recommended) you will still need to have the CODER Program Disk in drive A: in order to launch it.

If you are using Windows and have installed CODER as an icon, click on the icon to start the program. You will need to have the CODER Program Disk in drive A: for the program to launch.

Using Coder

When you invoke CODER you will get the following main menu:

C O D E R

MAIN MENU

F1: Copy files
F2: Rename/Move files
F3: Delete files

F4: Encipher files
F5: Decipher files

F6: Type a new document
F7: Edit/Read documents
F8: Configure
F9: Terminal

F10: Quit

In addition to these ten functions, CODER has an additional set of functions - an 'ALT' menu - which are accessed by pressing Alt F1 to Alt F10.

The complete set of functions is as follows:

F1	Copy Files	Alt F1	Merge Files
F2	Rename/Move files	Alt F2	Wipe Disk
F3	Delete Files	Alt F3	Wipe Files
F4	Encipher Files	Alt F4	Compress Files
F5	Decipher Files	Alt F5	Decompress Files
F6	Type a New Document	Alt F6	Store Files
F7	Edit/Read Documents	Alt F7	Retrieve Stored Files
F8	Configure	Alt F8	Configure
F9	Terminal	Alt F9	Run a Program
F10	Quit	Alt F10	Go to DOS

Accessing functions: The various modules (functions or facilities) of CODER are reached by pressing the requisite function keys (F1 to F10, Alt F1 to Alt F10). On pressing the required key you are taken to a screen from where you may select files to be worked on.

Most screens look similar, with a listing of the files on or in the current drive or directory in the upper part of the screen and the name of the module in the lower part of the screen. Also shown in the lower part of the screen is the name and size of the file highlighted in the file listing.

To go to another module it is not necessary to go back to the Main Menu to reach it; you can press the function key of any module from any other module. Once a module has been selected the menu options are listed across the bottom of the screen (note that '1' at the bottom means 'F1', '2' means 'F2', '0' means 'F10' and so on).

Selecting drives and directories: In most instances when a function key is pressed from the Main Menu you are taken to a screen which lists the files in the default drive or directory specified in the configuration of CODER. To select another drive the drive letter can be typed at the flashing cursor in the bottom screen. On pressing Enter the files on the new drive are listed on the screen. A directory path can be included with the drive letter but it is easier to access directories on the drive by selecting (highlighting) the directory with the arrow keys and pressing Enter. Directories are names bounded by ‘<>’ brackets. On pressing Enter when one of these names are highlighted you will be taken into the directory; to return to the parent or root directories select the ‘<..>’ and ‘<.>’ entries respectively.

Selecting files: A particular file is selected by highlighting it with the arrow keys. Pressing Enter starts the action which is pertinent to the function. Many modules allow you to select multiple files for the program to work on. Multiple files are selected by ‘tagging’ them with the space bar. This puts a little pointer next to the filename to inform the program that it is to be included in the action. Pressing the space bar again ‘untags’ a tagged file. Pressing CTRL Enter begins the action on the tagged files.

In some modules only one file can be worked on at a time so tagging has no effect.

The following is a description of how to use each of the modules (F1 to F10, Alt F1 to Alt F10).

F1: Copy Files

This is a simple file copy facility for copying files from one location to another.

Copying single files: To copy a single file simply highlight it using the arrow keys and press Enter. You will be asked for a path (destination) for the file. If you type the path only the file will be copied to the new location with the same name; if you give a path and a new name (or new name only) the file will be copied with the new name.

Copying multiple files: If you want to copy a number of files in one go tag the files with the space bar and press CTRL Enter. Specify a destination for the files and they will all be copied one after the other. If a file being copied exists at the destination you will be prompted to overwrite or ignore (Y/N/A - ***Y***es, ***N***o, overwrite ***A***ll and don't ask again).

F2: Rename/Move Files

Renaming files: To rename a file simply highlight it and press Enter. The cursor will jump to the 'To:' box at the bottom right. Type in the new name and press Enter. It is not possible to tag files for a mass rename.

Moving files: It is possible to rename files across directories and drives. This is the same as moving files. If you specify only a path in the 'To:' box the file is moved to the new location with the same name. If you give a new name as well, the file is moved with the new name. It is possible to tag files for mass moving. Use CTRL Enter to move tagged files.

Note: The move facility of CODER copies files and then deletes the originals. When an original is deleted it is wiped (overwritten) before being deleted so that it cannot be undeleted and recovered. This is slower than a normal DOS move but is more secure.

F3: Delete Files

To delete a single file simply highlight it and press Enter. You will be asked to confirm the delete. If you press 'Y' for yes or just Enter it will be deleted.

To delete multiple files tag them and press CTRL Enter.

Note: The delete facility of CODER wipes (overwrites) files before it deletes them so that they cannot be undeleted and recovered. This is slower than a normal DOS delete but is more secure. The original filename is also deleted so that an attempted unerasure will lead to nothing.

For a really secure wipe of files use the WIPE facility (Alt F3) which overwrites files with different character patterns as many times as is specified in the configuration (*F8 - see below).*

F4: Encipher Files

Press F4 to encipher one or more files.

Security levels: Before enciphering, choose a security level that will be used for the encryption. Levels are chosen by pressing Alt 1, 2, 3 or 4. The higher the level the more secure the encryption. The chosen level will be indicated next to the 'Encipher Files' heading in the bottom window and also on the Main Menu. (*See below for details of the security levels.*)

Level 1 uses a key which is typed in from the keyboard; the other levels take their keys from a separate Data Disk that contains a large amount of random data.

Enciphering a single file: Once a level has been chosen enciphering works in much the same way as the other modules of CODER. Highlight the file you wish to encipher and press Enter. What follows next will depend on which level of encryption has been chosen (*see below*).

Enciphering multiple files: If you wish to encipher a number of separate files, tag them by pressing the space bar and press CTRL Enter. You will be asked to provide an output name as the individual files are enciphered together into a single file. Do not provide a path (files are enciphered in the same place as the plaintext file(s)) and the name should not contain an extension as this is provided by the program. What follows next will depend on which level of encryption has been chosen (*see below*).

The levels are as follows:

Level 1: This level uses a keyword that is typed in by hand. The keyword (or rather, key phrase) can be one which is mutually agreed with the other side or taken from a book which is held by both communicating parties. The keyword (phrase) length is 36 characters. It is not possible to type a shorter key.

There is no restriction on the length of files that may be enciphered with Level 1.

Level 1 is a fallback level that should only be used when a Data Disk has been used up and there is no replacement or the Data Disk has become damaged or corrupted.

Whenever possible Level 2 should be chosen in preference to Level 1. The former automatically draws its keys from the Data Disk so there is no possibility of typing errors. In addition, Level 2 keys are stronger as they contain random data as opposed to language phrases in Level 1 keys.

If using a book for the key, choose a page from which the key will be taken and count down the required number of lines to the chosen line. Do not count blank lines. Type the page and line numbers into the appropriate boxes, press Enter after each, and

type in the key from the beginning of the chosen line.

The key must be typed exactly as it appears in the book. Do not type upper case characters where there are lower case and vice versa. If the line is indented or contains what appear to be double spaces, do not type these. The key should start with an ordinary keyboard character; spaces at the start are likely to cause confusion. Agree with the other side what conventions will be used as different interpretations will ensue if this is not done. Usually it is best to use keys with simple text rather than ones with punctuation, abbreviations and uncommon characters. The use of these leads to confusion and typing errors.

When choosing keys from a book do not always choose the first or second lines simply because it is easier to count down a few lines. This will likely result in the same lines being chosen and thus the same keys being used. Try to ensure that a different key is used each time. Do not mark which lines have been used as this will attract attention to the book if anyone is looking for such a book.

If the key being used is a mutually agreed one (i.e. not from a book), type in any page and line numbers and then the actual key. If such keys are being used it is recommended that the communicating parties have a number of different keys so that the same ones are not used over and over. It is far preferable, however, to use a book to ensure that the same keys are never used.

Having typed the key, press Enter to start the enciphering. The file(s) will be compressed and enciphered in one go and the enciphered file will appear alongside the plaintexts. The enciphered file will have the extension specified in the configuration (F8).

Level 2: Level 2 uses the same algorithm as Level 1 but takes its key data from the Data Disk instead of the keyboard. For this reason Level 2 is more secure than Level 1 as its keys contain random data and not structured language phrases. In addition, keys are used once and are then erased. The size of the key is fixed by the program.

There is no restriction on the length of files that may be enciphered with Level 2.

Level 2 should be set as the default level in the configuration (F8) as it will probably be the level most frequently used. Level 2 should not, however, be used for the most sensitive files. Use Levels 3 or 4 depending on sensitivity.

After having chosen your file(s) for enciphering you will be asked to place the Data Disk in the drive. The program will read a key from the disk and use it for the enciphering. The file will be compressed before enciphering and after enciphering the program will wipe (overwrite) the data used for the key. For this reason do not remove the Data Disk while the enciphering is taking place.

Level 3: Level 3 uses a more secure algorithm than Levels 1 and 2. Like Level 2, keys are taken from the Data Disk.

The length of the key depends on the length of the file being enciphered and is

proportional in length to the file. Since the key gets longer with the length of the file there is a limit to the size of files that may be enciphered with this level. The maximum length of files is approximately 160,000 bytes. This is the length after compression so files may be up to 320,000 bytes or more before enciphering starts. However, it should be noted that files of this length will use a lot of data and the Data Disk will quickly be used up.

Use Level 3 for files of high sensitivity but which are fairly long.

After having chosen your file(s) for enciphering you will be asked to place the Data Disk in the drive. The program will read a key from the disk and use it for the enciphering. The file will be compressed before enciphering and after enciphering the program will wipe (overwrite) the data used for the key. For this reason do not remove the Data Disk while the enciphering is taking place.

Level 4: Use this level for files which contain information of the highest confidentiality.

Level 4 takes its key data from the Data Disk like Levels 2 and 3. The length of the key is always exactly the same length as the file being enciphered. For this reason, use Level 4 sparingly as it consumes key data at a high rate.

The maximum length of files under Level 4 is 32,750 bytes after compression, meaning that they can be twice this length or more before enciphering starts.

The most economical way to use Level 4 is to encipher only the most sensitive parts of a document with this Level. The Level 4 enciphered file may then be re-enciphered with the remainder of the document(s) at Levels 1, 2 or 3.

After having chosen your file(s) for enciphering you will be asked to place the Data Disk in the drive. The program will read a key from the disk and use it for the enciphering. The file will be compressed before enciphering and after enciphering the program will wipe (overwrite) the data used for the key. For this reason do not remove the Data Disk while the enciphering is taking place.

Super-enciphering: Enciphered files may be re-enciphered as many times as you wish, with all levels and across levels. Doing this increases security but can cause confusion at the other end. If you re-encipher an enciphered file the receiving party should know that you are doing this. Using appropriate filenames can advise that a file is super-enciphered. For example, an enciphered file that you intend to re-encipher can be renamed ‘AGAIN.DEC’. When the recipient deciphers the received enciphered file, ‘AGAIN.DEC’ will come out of it and advise that the file needs to be deciphered again.

In order to save key matter, shorter files enciphered with higher levels of security can be super-enciphered with plaintext files at Level 1 or 2.

F5: Decipher Files

Press F5 to decipher files. Only one enciphered file may be deciphered at a time as each file requires its unique decryption key.

Security levels: The CODER program is able to detect which level of security was used to encipher a file.

If the file was enciphered with Level 1 you will be shown from which page and line of the codebook the key was taken. Take note of these numbers and seek the key line in the codebook. Type in the key and press Enter.

If the file was enciphered with Levels 2, 3 or 4 you will be asked to place the Data Disk in the drive. Do this and press a key to proceed.

With all levels the enciphered file will be deciphered and decompressed in one go. The deciphered file(s) will end up alongside the enciphered file.

F6: Type a new document

This module asks you for a name for the file you are about to type. A path can also be specified but if none is specified the file will end up in the directory shown on screen (current path shown at the top). On pressing Enter you will be taken to the wordprocessor/editor specified in the setup (F8) where you can prepare your message(s). On exiting from the wordprocessor/editor you will find yourself back in the F7 ('Edit/Read a document') module from where you can access the document again in order to edit it.

F7: Edit/Read a Document

This module allows you to edit documents that have previously been opened or that have come out of enciphered files that have been sent to you. Highlight the file to be edited and press Enter. This will take you into your wordprocessor/editor with the file on screen.

F8: Configuration

CODER as supplied should be correctly configured for your system. However, if ever you want to change anything this is how to do it.

Press F8 and you will see something like (*see over*):

A	Colour, B&W or LCD	-	B&W
B	Default level (1 - 4)	-	2
C	Path for data/message disk	-	B:
D	Path for work area	-	D:
E	Path for editor program	-	C:\WP51
F	Name of editor program	-	WP.EXE
G	Path for comms program	-	C:\CSERVE\DOSCIM
H	Name of comms program	-	CIM.EXE
I	Path for utilities	-	C:\CSERVE
J	Wipe count	-	6
K	Encrypted file extension	-	.ENC
L	Storage key	-	MY+PASSWORD

Type the letter of the option you wish to change (A - L). This will bring the cursor onto the line that you want to change. Simply type the new setting and press Enter.

Option A sets the way CODER is displayed on your screen. Type 'COLOUR' or 'B&W' or 'LCD' depending on whether you have a colour screen, a black and white screen or an LCD screen.

Option B sets the default encryption level. This is the level that will show when CODER is loaded. It is recommended that the default level is set to 2 as this will be the level most frequently used.

Option C is the drive for the Data Disk. This is usually A: or B:.

Option D is the work drive/directory where you would normally do your enciphering and deciphering. It is also where you would have your files for sending with your communications program (your default upload directory) and to which files are received (your default download directory).

Option E is the path for your editor or wordprocessor.

Option F is the name of your editor or wordprocessor program. Give the full name (eg: WP.EXE). If the program requires switches these may be added too.

Option G is the path for your communications program.

Option H is the name of your communications program. Give the full name (eg. PCPLUS.EXE). If the program requires switches these may be added too (eg: PCPLUS.EXE /B).

Option I (Path for utilities) is the path for the compression/decompression programs that work in conjunction with CODER.

Option J specifies how many times the file wipe facility (Alt F3) overwrites a file before deleting it. If a number greater than 1 is specified each wipe will be with a different character value. Filenames are also removed so that an attempted undelete will reveal nothing.

Option K is the extension that will be given to enciphered files.

Option L specifies the encryption key that will be used with the secure file storage facility (Alt F6 and Alt F7). This key is stored securely in the configuration file (TECOD.CNF) so is not available to anyone who does not know the password to access CODER. Certain keys are not suitable for the storage facility but the program will inform you when you have chosen one of these.

Saving the settings: When you have made all the changes, press 'S' to save the settings. This will update the configuration file TECOD.CNF.

Once your system is configured there is usually no need to change it. You would only do this if you change the name of your editor or comms program, one of the directories or the storage key.

Note: The path to your word processor and communications programs, as well as the names of these programs only have relevance if the programs you are calling are DOS programs. If you are running CODER under Windows you cannot call Windows programs from CODER. You must switch out of CODER and open these programs in the normal way by clicking on their icons.

F9: Terminal

Pressing F9 takes you to your communications program (if it is a DOS program). When you exit from the communications program you will find yourself back in 'F5 - Decipher Files' irrespective of which module you were in when you pressed F9. This will display any received files and allow you to decipher them immediately

F10: Quit

Press F10 to quit CODER and return to the level from which you launched the program (DOS, Windows etc). CODER will always exit back to the drive/directory from which it was called.

Alt F1: Merge files

Use Alt F1 to merge (join) separate files into one single file. Do not merge wordprocessor files as the wordprocessing package will have problems dealing such files. This facility is primarily intended for merging text files although it will join any files whatever their type.

A file or files to be joined can be joined to an existing file or to a new file specified in the 'Join to:' box.

Alt F2: Wipe disk

This facility allows you to wipe the free space on any floppy disk. It writes characters

over the free space of the disk eliminating all traces of what might have been stored on this area.

On pressing Alt F2 the program will default to the drive set in option C (Path for data/message disk) of the configuration (F8). This is the same drive as used for the Data Disk.

Use wipe disk when you wish to prevent the unerasure of files that have been deleted with a program other than CODER. The use of wipe disk is not necessary if all files have been deleted with CODER's delete and wipe facilities (F3 and Alt F3).

Alt F3: Wipe files

This facility works in the same way as F3 except that it overwrites files more thoroughly. The number of times files are overwritten before being deleted is set in the configuration (F8). This number should be set to at least 3. If it is set to 1 it will be the same as F3 and offer no advantage. Each wipe is with a different character value.

The original filename is also deleted so that an attempted unerasure will lead to nothing.

Alt F4: Compress files

This facility allows you to compress one or more files into a single file for sending with your communications program.

Compressing single files: To compress a single file highlight it and press Enter. To create a compressed file with the same name as the original, only the output path needs to be specified. If you want the compressed file to have a new name then specify a name. A path and name can be specified to send the compressed file to a new location with a new name.

Compressing multiple files: To compress more than one file into a single file tag the files to be compressed with the space bar. To compress them press CTRL Enter and give a path (and/or name) for the output file.

Encryption: It is possible to compress files with encryption. To turn encryption on press ALT E. The header in the bottom window will then say 'COMPRESS FILES (Alt E: Encryption ON)'. After specifying a name (and/or path) for the compressed file you will be asked for a key. Enter a key. This key has to be one that is shared with the other side.

Alt F5: Decompress files

This is the reverse of Alt F4. To decompress a file simply highlight it and press Enter. Give a path for the output file(s). Usually this is the same path as the compressed

file.

To decompress more than one compressed file tag the files to be decompressed and press CTRL Enter. Give a path for the output files.

Encryption: Files that have been compressed with encryption ON have to be decompressed with encryption ON, otherwise nothing will happen. To turn encryption on press ALT E. The header in the bottom screen will then say 'DECOMPRESS FILES (Alt E: Encryption ON)'. After specifying a name (and/or path) for the decompressed file(s) you will be asked for a key. Enter a key. This key has to be one that is shared with the other side.

Alt F6: Store files

This facility allows you to store your sensitive files in compressed form with encryption. Many separate files can be stored securely in a single compressed archive file.

To store a single file highlight it and press Enter; to store multiple files tag them and press CTRL Enter. The cursor will then jump to the 'Add to:' box where you specify the file to which you wish to add the file(s). If the file does not exist you will be prompted by the computer to create it; if it already exists the file(s) will be added.

The output files of Alt F6 always have a '.SAV' extension. Even if another extension is specified in the 'Add to:' box it will be removed and replaced with '.SAV'. This allows you to recognise encrypted storage files.

Any number of files may be added to a storage file but the file will become somewhat cumbersome if too many files are added to it. It is recommended that a new storage file be created every week or month depending on how much is added to it.

Alt F7: Retrieve stored files

Alt F7 allows you to retrieve files previously stored with Alt F6.

On pressing Alt F7 only files with a '.SAV' extension (files created with Alt F6) will be shown in the directory listing of the current drive/directory.

To view the contents of a storage file (file with '.SAV' extension) highlight the file and press CTRL F. This will list all the separate files inside the storage file. Take note of the file(s) that you wish to retrieve and press a key to return to the Alt F7 screen.

To extract a file or files from a '.SAV' file highlight the file and press Enter. In the 'Get file:' box type in the name of the file you wish to extract or, if you wish to extract all files, type '*.*'. Other normal DOS wildcards can also be used.

Note: when you have extracted files they will not immediately show on screen as Alt F7 only shows files with a '.SAV' extension. Press any of the other function keys to see the file names.

Alt F8: Configure

See F8 above.

Alt F9: Run a program

Pressing this key allows you to run another program out of CODER. Simply highlight the program you wish to run and press Enter. You will be asked if you wish to specify any switches. Type them in or just press Enter. The program will run. When you exit from the program you will be brought back to CODER.

Alt F10 : Shell to DOS

If you press ALT F10 the program will shell to DOS. To return to CODER from DOS type 'EXIT' at the DOS prompt.