Ivory Tower
Software

Documentation for shareware **Private Cryptographer™** version 1.21
Updated March 17, 1994

Private Cryptographer

"Cryptography" means literally "secret writing." Now any Windows user can safeguard sensitive information. You probably are aware that a network system administrator can examine any of your network files at any time, but did you know that your employer can legally snoop on your hard drive at work any time he wants to? In safeguarding their employer's interests, employee's files can be encrypted to protect company proprietary material and trade secrets too.

Private Cryptographer can ensure privacy. Privacy and secrecy are two sides of the same coin. Some other available encryption programs use the Data Encryption Standard (DES) encryption algorithm. Many computer scientists have pointed out two significant weaknesses with DES: the key limitation of 56 bits is not strong enough, and the S-functions have built-in trap doors (which are classified SECRET by the Department of Defense) which only the US Government knows how to operate. *Private Cryptographer* has absolutely no trap doors. If you forget a password, there is no way for you to recover your encrypted data.

Installation

Copy the ENCRYP.EXE, GRPMGR.MDB, KEYMGR.MDB, and SAMPLEn.TXT files to a directory on your hard drive. Copy the CMDIALOG.VBX and COMMDLG.DLL files to your Windows SYSTEM directory. The dynamic link library VBRUN300.DLL should also be in your Windows SYSTEM directory. You may obtain VBRUN300.DLL from the CompuServe WINSHARE forum library as VBRUN3.ZIP.

If your system supports Windows sound, also copy the two .WAV files to your *Private Cryptographer* directory. Those two sounds are used to notify you when

the encryption/decryption of a large file is complete.

To use the Password Manager feature you will need the Microsoft Access VB dynamic link libraries in your Windows SYSTEM directory. You can download MSAJT110.DLL, MSAES110.DLL, and VBDB300.DLL as MSA11.ZIP from the WinShare forum. The Password Manager and File Group Manager databases also require SHARE.EXE to be installed (SHARE.EXE is part of DOS). Note: *Private Crytographer* will work just fine without the Password Manager and File Group Manager features, except that password length will be more limited and you won't be able to manage groups of files for encryption and decryption. We recommend that you download MSA11.ZIP and use the Password Manager.

(The MSA11.ZIP file contains the Microsoft Access version 1.1 dynamic link library files and the Visual Basic database dynamic link library. These files may be distributed freely by Visual Basic programmers for use with their applications. Private cryptographer uses the Microsoft Access database engine for the Password Manager database and the File Group Manager database. Using the Microsoft Access database features allows programming with structured query language (SQL) to create and maintain a relational database. Using the relational model allows future implementation of new features with a minimum of design breakage.)

You may install *Private Cryptographer* as an icon in your Program Manager in the usual manner.

Using Private Cryptographer

There are three ways to use *Private Cryptographer*. First, you can encrypt and decrypt text in the Windows clipboard directly (from the "Encryption" menu). Second, you can use the editor window to type or paste text or open a text file, and encrypt the text in the window (again, from the "Encryption" menu). Or third, you can encrypt or decrypt files directly from the "File" menu. To encrypt text, simply choose the appropriate "encrypt" command and enter a password when prompted to do so. To decrypt the text, choose the appropriate "decrypt" command, and enter the password **exactly** as it was entered for the "encrypt" command.

Private Cryptographer passwords can contain mixed case, numbers, spaces, and punctuation. If you share secret data, it is a good idea to have a different password for each partner you share with, and to change passwords periodically. The Password Manager window (from the "Passwords, Password Manager..." menu) provides a convenient database for your passwords. To use the Password Manager as the source for your encryption passwords, check the "Options, Use Password Manager" menu option. Access to the Password Manager is protected with its own password.

Private Cryptographer works well with word processing, graphics, and even executable files, using the "File, Encrypt File" menu option. To encrypt your e-mail messages, copy your message to the Windows clipboard, encrypt it directly using the "Encryption, Encrypt Clipboard Text" menu command, and paste it back into your e-mail program. The recipient can decrypt the message in a similar manner.

Note: some e-mail systems (such as Internet Mail) cannot accept the 8-bit characters that Private Cryptographer generates. To allow 7-bit output text for e-mail, use the "ASCII En/Decrypt" option from the "Options" menu. This affects both the text window encryption as well as the clipboard text. However, files encrypted from the "File" menu will always be encrypted and decrypted as 8-bit binary.

Caution: If you attempt to decrypt an encrypted file using the wrong password, the target file will not be recoverable. Similarly, if you attempt to decrypt a file that has not been encrypted, there will be warning, but the file will not be recoverable.

The File Group Manager

Access the File Group Manager from the "Encryption" menu to encrypt and decrypt groups of files on your hard disk. The File Group Manager always uses binary encryption. Set the "Use Password Manager" option from the "Options" menu for convenient password operation.

Directory Encryption

From the File Group Manager the "Directory..." button will lead you to a modal dialog box that allows you to encrypt and decrypt entire directories. Needless to say, encrypting directories, like encrypting other groups of files, is potentially hazardous. I suggest that you create a subdirectory specifically for that purpose. The directory encryption window tests the status of the indicated directory by either "Plain" or "Cipher" using the name of the path leaf. Two different directories with the same leaf name will give confusing results. The root directory cannot (and should never) be encrypted--don't try it.

Encryption Strength

As it says in the "disclaimer" below, the only provably secure encryption system is the "one time pad." However, when used with long passwords (keys) as described in the Password Manager Help, I believe *Private Cryptographer* is quite secure from even the most resourceful of attacks. If you should have reason to suspect otherwise, please let me know of your concern. Accompanying your message with the plaintext contents of "Test Two" in the "Options" menu will serve to bolster your claim. To date, no one has done this.

While the security of the algorithm does not depend on its secrecy, the exact implementation is proprietary information and is not normally disclosed. The program uses polyalphabetic substitution with a special approach to foil a Kerchoffs attack.

Attempting to decrypt with an incorrect password will destroy the message beyond recovery. Because communications are (should be) always backed up, this characteristic is actually a privacy enhancement.

To get the benefits of completely secure communication, use of the Password Manager and long "keys" is essential. Any clear text document can be used as an excellent key, and use of the Password Manager by both the sender and recipeint ensures that proper decryption will occur.

When sending encrypted messages and files, your recipient needs the program and the password (preferably a very long key for absolute security). Communicating the key securely is the traditional weak point of private key systems. Physical transfer is usually necessary. However, once this transfer has been accomplished, new keys can be sent in an encrypted message. Keys should be changed on a regular basis.

Shareware

Private Cryptographer is shareware. That means that you can evaluate this program to see if it meets your needs before you purchase a license. You may also copy the evaluation version for distribution to others for their evaluations. To keep using *Private Cryptographer* after your evaluation is complete you must purchase a user license. For a copy of the latest version and a single license to use the software on any machine, send $50 to **Ivory Tower Software** at the address below.

If there are any features you would like to see in future versions of this software,

or if you find a bug or have any other comment, please contact me at the following address:

Ivory Tower Software
Richard Wagner
4319 W. 180th St.
Torrance, CA 90504

You may also send me a message via **CompuServe** (76427,2611). If you are reporting a bug, please mention the version number.

History

Vers.	Date	Description
1.00	24-May-93	The program which had been developed by **Ivory Tower Software** for inclusion in the popular *Network Email* system was adapted for publication as a stand-alone shareware program.
1.01	27-May-93	This version fixes a very minor bug which unnecessarily appended an extra *crlf* character pair to saved files. It also enhances some of the Edit menu commands and adds the Options for Test.
1.02	29-May-93	This version allows encryption and decryption of all files, even executables. Random password generation and high priority multitasking are now options accessed from the "Options" menu. Files and messages encrypted with previous versions should be decrypted with the older version and then re-encrypted with this version.
1.03	19-July-93	This version is compiled with Visual Basic 3.0 and fixes bugs which caused some spurious error messages with two of the text file commands.
1.04	28-July-93	Fixes some very minor window caption bugs.
1.10	9-Aug-93	The encipher and decipher algorithms have been made more resistant to a Kerchoffs attack. Files and texts encrypted with previous versions should be decrypted with the old version and re-encrypted with the new version.
1.11	16-Aug-93	The Password Manager database has been added.

1.12	21-Aug-93	This version adds wave file sound support.
1.13	2-Sep-93	Incorporates password protection for the Password Manager, by user request.
1.14	3-Sep-93	Adds the "ASCII" option for 7-bit input and output. Slipstream bug fix for clipboard encryption incompatibility.
1.15	6-Sep-93	Adds the File Group Manager.
1.16	12-Sep-93	Adds directory encryption and fixes a bug which prevented file specification deletion in the File Group Manager.
1.17	19-Dec-93	The delete key in the main editing window will now delete the next character if no text is highlighted.
1.18	25-Dec-93	Fixes an ASCII encryption bug: null characters are not handled well by some devices so the ASCII 0 character is now not used in encrypted text with the ASCII option.
1.19	27-Jan-94	Adds the startup warning about decrypting with the wrong password. This warning (and the exit nag) is not displayed to registered users.
1.20	27-Jan-94	Minor cosmetic changes in some dialog boxes.