

# [File vaults](https://assignbuster.com/file-vaults/)

File Vault Help   
Parisien Research Corporation   
Copyright (C) 1996 Harvey Parisien   
Email: emailprotected   
This software is free to use.

In a recent article in Defense News (Vol 12 No 31) Aug 4-10, 1997   
William Crowell, National Security Agency deputy director said " If   
a product of 64-bit strength were used by a military org... it   
would take 6, 000 to 7, 000 years to recover just one message."   
1. File Vault - 64-bit (8 bytes) block encryption algorithm   
variable length key up to 448 bits   
File Vault - Places a number of user selected files in a single   
self extracting / self decrypting executable file called a File   
Vault. A File Vault can be sent easily to anyone over the   
internet and only accessed with your password. The recipient of a   
File Vault does not have to have any special software installed to   
decrypt or access a file vault. Each File Vault is totally self   
contained. This makes for easy attaching, receiving and general   
use.

File Vault allows you to open the vault, access the files, then   
close the vault which performs a secure wipe of the files from the   
disk surface. In an encrypted file vault, filename information is   
encrypted too, so if someone examines the vault with a disk   
editor, no information on contents is available other than the   
optional description line entered during creation. Great for " Your   
Eyes Only" files...

The encryption algorithm is the highly regarded BLOWFISH by Bruce   
Schneier, world renowned Cryptographer. See VGP information below   
for more detail.

File Vault is available at... www. alcuf. ca/fv   
- - - -   
A word on compression: When you use Winzip or other compression   
utilities from Windows, they often will create temporary files   
that can reside on the users system which are complete duplicate   
files, or parts of files that you would rather be fully secured.

Therefore, rather than zipping files and containing them in a   
vault, build a vault first which securly containes your files, and   
then create the zip (or other archive) file. That way any   
temporary stuff created by the archiver will be encrypted and   
remain secure.

- - - -   
2. Other free utilities included with File Vault   
---------------------------------------------   
The following utilities are stand alone utilities that reside   
on your File Vault directory. These can be moved or deleted as   
you wish.

DISKWIPE. EXE (and diskinfo. dll) - this utility is used to   
securly remove deleted information from a hard drive to prevent   
undeleting. Let's say you have a bunch of stuff you just   
deleted, and need to make sure nothing that was on the system   
can be undeleted and accessed again. This utility creates a   
file the size of the free remaining space on your drive and   
fills it with space, then deletes it. This means that any   
files recovered (by modifying your fat table) will only contain   
space.

FILEWIPE. EXE - this utility is used to securly remove a file.

It opens the file, writes it full of space, then closes it and   
deletes it. This way any attempt to recover the file will   
prove rather uninteresting.

3. Information on VGP the Encryption Editor   
----------------------------------------   
VGPWIN Encryption Editor   
VGPWIN is a simple WINDOWS editor for text files, much like   
NOTEPAD, but offers an optional encryption feature. VGP also uses   
clipboard features that allow you to swap text to/from another   
application with ease. VGPWIN will also encrypt and decrypt disk   
files using the same powerful encryption routines.

The Encryption Method   
The Encryption Engine is a multi-pass system by Parisien Research   
Corporation. VGP gives you a high level of data protection since   
one pass is the highly regarded BLOWFISH algorithm by Bruce   
Schneier, world renowned Cryptographer. Because of the   
implementation of the Blowfish algorithm, the encryption produced   
is several orders of magnitude stronger than DES (Digital   
Encryption Standard). Blowfish is a 64-bit (8 bytes) block   
encryption algorithm. It uses a variable length key. The key   
length can be up to 448 bits. It is extremely fast and is so   
secure that it can not be sold outside the U. S. due to federal   
export restrictions ITAR.

VGP and File Vault are free to use.

---   
How to use File Vault:   
1. Select files to place in a vault   
2. Describe your vault (optional)   
3. Define location (default is last location)   
4. Define autoexec command. This is OPTIONAL. If you want the user   
to receive 1 or more files and then be forced to run a specific   
file (executable or otherwise) you can place that command here.

For example, let's say I create a vault containing a file called   
beach. bmp. If I define the optional autoexec