# VGP v3.01
## Encryption System

**http://www.alcuf.ca/vgp.htm**

Parisien Research Corporation
Copyright (C) 1996 Harvey Parisien
Email: parisien@alcuf.ca
FidoNet: 1:249/114

This software is free to use.

**NOTE: Versions older than v3.00 are beta versions, and should be upgraded to v3.00 or newer.**

## 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].

## General Use

VGP allows simple implementation with most email processors, and simple password management by the users. When you VGP Encrypt a file with any password, it simply needs that password to Decrypt it using VGP. Simply decide on a mutual password with a friend, and that's it, no creating keys, and reading a large book to make it work.

When opening a text file to edit, VGP will detect a previously VGP encrypted file, and prompt you to decrypt it. If it was not encrypted, or it is a new file, it will prompt you on exit to optionally encrypt it.

VGP can be used with email systems, PIM's, database systems, or for any text editing where encryption is required.

If you have an email system that allows you to define an editor of choice, define VGPWIN.EXE and the encryption process will be transparent. If you can not define VGPWIN as an editor in your application, then use the Clipboard features to collect and process text.

VGP in Windows makes interfacing with EMAIL simple.

### How to use VGPWIN in Windows with EMAIL systems...

Here is a typical CLIPBOARD session with Eudora on the Internet:

1. Encrypted mail is received using Eudora.
2. To read it, reply to the message, and place the cursor at the beginning of the message body...
   a) press Ctrl+a Ctrl+x to "select all" then "cut" it to the clipboard (removing the message body from the reply).
   or b) using the pulldown menus under edit, select all, and cut.
3. Switch to VGP, and press Ctrl+R to replace/paste the message to VGP, or use the pulldown File menu to do the same.
4. Press Ctrl+D to Decrypt message, or use the menus.
5. Read the message, and reply...
6. Press Ctrl+E to Encrypt message, or use the menus.
7. Press Ctrl+F to feed the Encrypted message back to Eudora.
8. Then press the Send button.

When using different email systems there may be different key sequences, but the menus will have the same features.

Test it using a dummy paragraph of text in NOTEPAD, and pretend it is your email reader.

## Password Picklist

VGP has a password picklist which is like an address book with names and passwords in it. This file is encrypted on your hard drive and only accessible by entering a password. When prompted for a password, you have an option to select a picklist. The picklist requires a password to activate it. Once this password is entered (*only required once during each VGP session)* your picklist allows you to select passwords by names *(or any other identification you defined)* rather than remembering them. First time using it, you will be prompted to add at least one entry. This way you only have to remember one password, the one that unlocks your picklist. This can be a very powerful password, so don't forget it. It is impossible to recover a picklist without the password because it is VGP encrypted.

Resellers: VGP can be bundled with other software or services. This is conditional upon either; a) the entire contents being contained in the archive or on the distribution disk unmodified, or if b) VGPWIN.exe VGPWIN.dll VGPWIN.doc vbrun300.dll and cmdialog.vbx are contained on your distribution disk in such a way that it gets properly installed. Drop us a note for clarification.

Note*: A stand alone VGPFILE is available. It contains only the encrypt / decrypt routines for Clipboard or File use. This was created since it may be easier to control from other programs.*

Special thanks to the following people for helping with the project;
Bruce Schneier, Scott Dudley, Chris Carter, Bruce Baugh and Alan Olsen.

parisien@alcuf ca
**http://www.alcuf.ca/vgp.htm**