

10 July 2007

By: Ionut Ilascu, Editor, Software Reviews



Kruptos 2 splash screen

## [Blowfish All Your Files for Free](#)

### *File and folder encryption, and secure shredding*

Keeping your files safe seems to no longer be an issue in Windows environment. The various encryption algorithms have penetrated the digital world at a large scale. The myriad of applications able to encrypt your data has truly flooded the market. Encrypted messages can also be sent without prying eyes spying on your conversation. Despite the abundance of encryption tools on the market, finding a free application to provide this service is quite a task. However, with the migration of GPG on Windows protecting your files and sending encrypted messages has taken an awesome turn. You can now strongly secure the sensitive data in just a few mouse clicks. Another application with the same protection attributes has been developed for quite a while by Steve Becket. It is also free, but if you experience an urge of donating something in order to feed the project, there is no obstacle as the developer accepts donations. Its name is Kruptos 2 and already reached version 3. The interface is quite plain and simple, but supplies all the **functionality** you need. If you are looking for bells and whistles in an encryption software, then Kruptos is the last place where you should seek. The most used options are located in the toolbar and if you want some more alternatives and choices, expand the menus above. The main area is dedicated to the files and folders you want to crypt. As soon as you add an item the application will show info on the file. Only the **significant details** are available, like the size of the file, its attribute and the path to its location. Once all the files you want to process are added in the window, either by drag and drop or by browsing for them, Kruptos makes available three options: encrypt/decrypt, shredding and create a **self-extracting** file (executable). The encryption algorithm used for almost all of these options is Blowfish 128-bit. This algorithm is not easily crackable and few will be attempting to break it, but most of the attackers will speculate the weakness of your password, so that should be a strong one. The files will be encrypted automatically and no additional file will be created. Also, you can choose to protect the files inside entire folders and even all the contents of a drive (**USB flash drives** included). For protection purposes, you can enable **obfuscate file names** from the Configuration, under the Options menu. This will disguise the newly encrypted file's name. Kruptos 2 takes all the precautions necessary and only the names of the files will be changed, leaving the name of the folder containing them intact. This way you can find your name to the files and decrypt them. An additional option to quickly find the desired files is to **search** them. The application can search a certain folder or partition for encrypted files and add them automatically in the window. It'll even find the files that have been sent to Recycle Bin. If you want only certain files to be encrypted, you can create **project files**. Simply add the files from different locations in the application, encrypt them and instead of exiting, press the diskette in the toolbar to save the project. Now every time you need those certain files, just load the project file and decrypt them. By creating a self-extracting archive you can avoid launching the application in order to gain access to the file. However, in this case, your file will be protected only by your password and it'll not be encrypted. In this case, the original file will not be automatically converted and the resulting executable can have any location you wish. But Kruptos is ahead of things and provides the option of automatically deleting the original once the archiving is complete. Configuring the software to work in your interest is even easier than encrypting the files. All you need to do is enable the option and you are done. The alternatives in the menu are Obfuscate Filenames (disguise the names of the files), Show summary after operation (a log will be displayed at the end of the task), show message when the operation completed properly, ask for confirmation before the operation starts and show a warning when a file is removed from the project. One would think that the

options for **shredding** the files would be a bit more complicated. But ease of use is Kruptos' main attribute so all there is to the task is dragging a slider in order to choose the security level (from 1 to sixteen, 1 being the fastest and less secure and 16 the most secure and the longest to complete). Some of you may think that all this configuration and encryption of the files is way too complicated and you may want all these in one mouse click. Kruptos seems to get along with Windows quite well (even with Vista) so by enabling **Windows integration** a command for the application will be created in the context menu. The dynamic command contains all the variables available in the interfaced version. Even the options menu will be present and you will be able to encrypt, decrypt, create self-extracting files and shred the selected file. The only thing you will be deprived of will be the search tool. **The Good** Kruptos 2 has all the functionality and ease of use any user needs: un-complicated options, perfect Windows integration, strong encryption algorithm and also provides the possibility of securing the files on an entire drive, be it fixed or portable USB flash drive. **The Bad** Almost every encryption application provides protection only against prying eyes. It is OK that you can protect your data this way, but what if the prying eyes, tired of attempting to open the file, turn into a Shift+Delete machine and wipe the files from your computer. And what if that it's done by using the very software that has encrypted the files? **The Truth** Save the mischief presented above, the application is 100% rock solid. However, keep in mind that once the files are encrypted, the only way to decode them is by using the correct key. So your password takes all responsibility if your files are viewed by unauthorized persons. *Here are some snapshots of the application in action:*