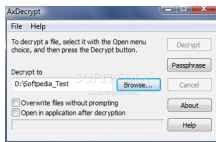


9 October 2007

By: Ionut Ilascu, Editor, Software Reviews



AxCrypt

[Windows Explorer's File Encryption Menu](#)

Free encryption for sensitive data

There are never enough solutions for protecting your data. At least there never seem to be. Anti-spywares and anti viruses do a great job, but what if the digital thief is right in front of your computer, or you lose your laptop? All your files will be protected only by a user account password (if you have any) which can be easily overridden in some cases. So the only chance seems to be in the hands of data encryption software. At this time, the only operating system that comes with this kind of feature is Vista Ultimate Edition. Its BitLocker component is able to encrypt the entire computer, thus keeping all the files for the eyes of the owner. However, if you do not want to shell out the money for buying Microsoft's OS there are far cheaper software solutions. It is true that there isn't any that can encrypt an entire drive without risks, but for file encryption they do a hell of a job. [TrueCrypt](#) is a great way to secure important files without much of an effort. It comes complete with all necessary options, minus one: protection against deletion, but this can very well be fixed by using the "hidden drive" feature) Another application worth mentioning is [Kruptos 2](#) which comes with a more limited set of options but it can do a very good job as well. Besides encrypting [Kruptos 2](#) is also perfectly capable of secure deletion of the data by shredding it to pieces. AxCrypt is yet another component of the freeware family of data encrypting software. It may not look much, in fact there is little interface available but it can help you with protecting sensitive files from prying eyes. Although it has not been updated for a long time it can very well function under Vista. It integrates perfectly in Explorer menu and can be used for any file on your computer regardless of its nature. All you need to start the encryption process is a right click on the desired file and from there access AxCrypt extended menu. Unlike other file encrypting applications, besides protecting the encryption with a user-defined password, AxCrypt also allows the user to create a key-file which is a text document containing a random string of characters that can be used for both securing the file and decrypting it. The application uses AES 128-bit algorithm which is a bit behind the time, but still a very strong one. You have to know that if you are only using a passphrase, AxCrypt will protect the data within its limits. In order to benefit from the application's full protection, it is recommended to use a key-file. This way, you no longer have to memorize passwords but only the location for the file-key. There are three options for file encryption. AxCrypt permits creating a copy of the file and encrypting it, creating a self-extracting file or just encrypt the original without creating any copy. The self-extracting option is extremely handy for those users trying to open the original but do not have AxCrypt installed. This will permit simply typing in the password and the file will be automatically decrypted in the same location. For using key-files you will have to create them first. There is no option for this in the interface and Explorer context menu is again the only way to create it. It is saved as a TXT file and can be saved anywhere on the computer. Once the key-file is available, you can use it for encrypting and decrypting documents. The great thing about AxCrypt is that you do not have to go through right click menu in order to open an encrypted file. All you need to do is open the file normally and enter the requested password and the document will automatically open in the associated program. Another method which avoids entering the password completely is enabling "Remember this for decryption". This will skip password verification and automatically open the file. However, care should be taken when enabling this option as leaving your computer unattended will allow anyone to mess with your documents. In case you are worried about forgetting to disable this option each time you finish the work with the encrypted files, don't. The option will de-activate at your next logon. AxCrypt is tailored to make the encryption process as

comfortable as possible and comes with an option that allows users to use a default password and key-file for each encryption. It is not recommended to keep them long periods of time as making a change once in a while diminishes the chances for third parties to learn them. If there are few means of getting around AxCrypt encryption (copies of the documents may be left in temporary files folders and your computer may be bugged with a keylogger), not the same thing can be said about file shredding (or secure deletion). Unfortunately, during our testing, we managed to recover some shredded files with no effort at all. But this happened only once. However, in all tests, filenames were perfectly visible. I had expected them to be overwritten as well as the data. For a freeware, AxCrypt behaves very well although it does not come with a complete set of options. There is little user input as all you can do is enter password and add the key-file. **The Good** AxCrypt is a freebie designed to encrypt your sensitive data. It integrates perfectly in Explorer menu and provides an easy way to secure important files. Batch encryption is supported, in which case all the files are encrypted with the same key. You can create self extracting files which do not require installation of AxCrypt in order to be decrypted. **The Bad** will not say a thing about the encryption algorithm, but I will say something about the file shredding feature. Users have no option in this sense and there is no information on how the process takes place. Drive encryption is not supported. **The Truth** The application is reliable as long as you learn how to use it in your own interest. I wish there were more choices for data encryption, but I guess AES 128-bit will do till next version. There is no setting for secure deleting data and an average file recovery software will have no problem showing the name of the file. *Here are some snapshots of the application in action:*