

Home > Encryption Software > Advanced Encryption Package

## File Encryption Software Features

### Strong and proven encryption algorithms to protect your confidential documents

To secure sensitive data AEP PRO file encryption software uses 20 proven and strong encryption algorithms including AES, Blowfish, Twofish, GOST, Serpent and others.

### Easy to use for novices. Integration with Windows context menu.



Encryption technology is a difficult thing, especially if you are not technically savvy. How is an older family member supposed to figure out how to create a self-decrypting file, securely delete a file, or use Public Key Infrastructure to receive mails securely?

This file encryption software is made easy for novices. It integrates nicely with Windows Explorer, allowing you to use Explorer's context menus for file encryption/decryption/secure deletion directly from well known Windows Explorer.

AEP file encryption software can encrypt a single file, multiple files at once or even whole Windows folder(s).

See [Screenshots: How to encrypt and decrypt files from context menu of Windows Explorer](#)

### Using USB sticks to store encryption / decryption keys



It is possible to store all your encryption passwords on a USB Flash Drive. You just need to remember a single Master Password for the password vault on the USB memory stick. There is no need to keep 20 passwords in mind when you can store these encryption keys on flash memory in an encrypted form and remember just one password.

It might sound simplistic, but strong passwords are a must for good security. A good password is a combination of several words that aren't themselves a word interspersed with special characters (e.g., l4scOrE&sDayNYeaRs\_ag0).

What is the real difference between a weak password and strong randomly generated password?

AEP file encryption software can generate a really strong encryption key (a real example is "(+3!';0.;4{M>tMpRnK7&\*u'F7)SYu2Q)"). The ability to remember such strong passwords (with the help of a USB memory stick of course) is the key to using modern encryption algorithms 100% effectively.

See [Screenshots: How to use AEP to keep encryption & decryption keys on USB memory stick](#)

### Securely delete source files after encryption. Never delete confidential files using Windows Explorer!



It is a common misconception of PC users that once they have dropped a file into the recycle bin and emptied it that, there is nothing left to do and that the file is gone for good.

All that happens when you erase a file by either deleting it or putting it into the trash is that Windows has been told to not recognize the file so that you do not see it when you open a folder or your desktop. In fact, it is not erased at all, the data is still there on your hard drive and it will remain there until the information is overwritten by some other file or data.

We know all about this, as we have developed special [software to recover accidentally deleted files](#) and we also know all about the file systems used in Windows 7, Vista, XP and 2003/2000.

AEP file encryption software can **wipe** the contents of the original pre-encrypted file beyond recovery **to make sure** that not even a trace remains after shredding. AEP PRO matching and exceeding the specifications of the U.S. Department of Defense to stop software and hardware recovery tools.

AEP supports about 20 ways to securely delete file: *Peter Gutmann algorithm, U.S. DoD 5200.28, VSITR, German Standard, Bruce Schneier algorithm, NATO Data Destruction Standard, GOST P50739-95 Russian Standard, The National Computer Security Center Standard, Canadian Standard, NAVSO P-5239-26, US Navy Standard, AFSSI-5020, US Air-Force Standard, AR380-19, US Army Standard and simple Quick Wipe algorithm.*

See [Screenshots: How to sanitize files using AEP PRO](#)

Encryption Software

Advanced Encryption Package

Crypt4Free

Screenshots / How to

News & Updates

Downloads

Complete protection offer

Self Defence Package

3 product bundle (CD Encryption + USB Encryption + File Encryption + Drive Encryption) at a special price

Read More

Newsletter

Subscribe to our Newsletter.

Get notified about new products releases, new significant updates of existing products. Be first to know about short season's discounts and special offers.

Subscribe

Spotlight

AEP PRO 5.66 - Enhancements in the documentation and gui

August 28, 2012

Minor enhancements in the gui and documentation..

AEP PRO 5.65 - Enhancements in gui and documentations.

July 18, 2012

Minor enhancements in the gui and documentation..

AEP PRO 5.64 - Fixed bug in the gui

June 15, 2012

Fixed bug in gui - the password used for blowfish encryption & decryption was truncated to 32 characters..

News archive...

Compatilbe with Windows 7

## Symmetric and asymmetric encryption (support for PKI)



AEP PRO file encryption software supports symmetric and asymmetric encryption.

In the first mode (symmetric), you just use the same password and for encryption and for decryption using one of ~20 available **symmetric** encryption algorithms (AES, Blowfish, Serpent etc).

In the second mode (asymmetric), you create (using AEP PRO) a pair of keys: the public key and the private key. You publish the public key file on a web site (or send it to any person via e-mail). This key is used to encrypt a file and send it back to you. Once encrypted, the file cannot be decrypted using this public key file. You receive the file and use the private key file - i.e. your secret key file to decrypt document.

- AEP PRO includes the PKI keys manager and the key generator tool. It generates a pair of public/private keys with the strength: 512, 768, 1024 or 2048 bit.
- RSA encryption is used with strong symmetric encryption algorithms together. The public key is used to encrypt a randomly generated password. This password is used to encrypt whole file.
- AEP PRO can protect a private key file by way of a password. Therefore, you can store your decryption keys in an open form on USB sticks, windows folders, etc. It can be stolen but cannot be used.

See Screenshots: [Public-Key cryptography in Advanced Encryption Package Pro](#)

## Bonus! Command line utility to automate file encryption and decryption tasks



In a program folder you will find a separate command line utility (aepcmd.exe). It supports all program operations: encryption and decryption with a password, PKI encryption and decryption, secure file deletion, and the generation of PKI keys. This utility understands file masks, can process windows folders recursively, can fetch file/folder list from text file, or can be set in a command line.

This command line utility can easily be integrated with your batch script because this console utility returns status codes on every operation (errorlevel, that can be analyzed in your script). All command line keys and switches and status codes are fully documented in the help file.

AEPAMD can be configured to securely delete file(s) after encryption and you can use it to encrypt all new files in a folder and its subfolders on a scheduled basis (the encryption console utility will recognize and skip already encrypted files).

See [Screenshots: How to automate file encryption tasks](#)

## Easily share confidential documents / safely transfer data via the Internet. No need to have AEP on the other side.



Once encrypted, the document/file can safely be uploaded to your web site, sent as an attachment in an email, sent on a compact disc via postal mail, etc. Your email/compact disc with important documents can be intercepted by a third party. But nobody can read these documents without the password and there is absolutely no way to break this password.

When you burn encrypted files to compact disc, simply burn our [free decryption utility](#) Crypt4Free to this CD as well. Your recipient can use this utility to decrypt the files on your compact disc. This utility can also be downloaded from our web site absolutely free by everyone.

Alternatively, you can create **self-decrypting** versions of your encrypted files. A self-decrypting file is just the **usual executable file** with an encrypted file inside. The recipient of this secure document simply launches this executable file and will then see a text field in order to enter the decryption password and then click the "decrypt" button. Therefore, the recipient of your files has no need to purchase an AEP program to decrypt your files.

See [Screenshots: Self-extracting encrypted file](#)

Additionally, in a situation when both the sender and recipient have AEP PRO file encryption software, they can use **Public Key Infrastructure to exchange files**. You just generate a **public/private key pair** and send the public key to your recipient. The recipient uses your **public key file to encrypt** a confidential file and then sends it back to you in an encrypted form. You **decrypt** it using **another** key - **private key file**. In this situation you will never need to reveal the decryption password via telephone to your friends/colleagues and it cannot be heard/recorded by a third party.

In addition, AEP PRO **compresses** the file before encryption to reduce its size significantly.

## Scrambling text messages

AEP includes a special utility: Clipboard Encryptor. Its icon is located in the tray notification area and it monitors the Windows Clipboard.

By pressing the special global hot key, the text in the clipboard can be scrambled and then you can paste it into your email message.

See [Screenshots: How to scramble text messages](#)

## "Compatible with Windows® 7" software



**Advanced Encryption Package Pro** has been tested to meet all of the technical requirements to be Compatible with Windows® 7. ...>

## Reviews

### Great tool to help make things just a little easier

*Advanced Encryption Package Professional is a tool that can ease some of the pain of working with encrypted messages and files.*



## Awards



SnapFiles has awarded AEP PRO by VERY GOOD award!

### **AEP prevents the use of 'weak' passwords and enhances total security**

AEP file encryption software controls entered encryption password in different ways. On the one hand it has a special **password quality** indicator. It turns red for weak passwords (short passwords, passwords consisting of characters only or digits only, etc.). On the other hand, AEP maintains an internal dictionary of 45,000 common English words and recognizes these words in the password and warns you when you use a weak dictionary password to prevent a well known dictionary attack.

Copyright (c) 2010-1998 InterCrypto Ltd. All Rights Reserved.