

# Picofactory

For all your free portable software needs ... NO INSTALLATION. NO HASSLE. IT JUST WORKS.

[Home](#) [Download](#) [Software](#) [Contact](#) [About](#)

[Home](#) » [Free Software](#) » Encryption Software

## Portable Encryption Software

### Description

It is a small and extremely fast encryption utility that uses **Blowfish** encryption algorithm in CBC mode. It is easy to use and support multiple files drag-and-drop. In addition, it is portable, you can put it on your USB memory stick and run it anywhere you go! Very useful for users who want to keep their document secure on their computer or transfer over Internet using unsecure channel.

It uses a 128-bits key that is the **MD5** message-digest of user password.

### Download Now!

0.1.1 for Windows, English 13KB

### Details

**File size:** 13KB

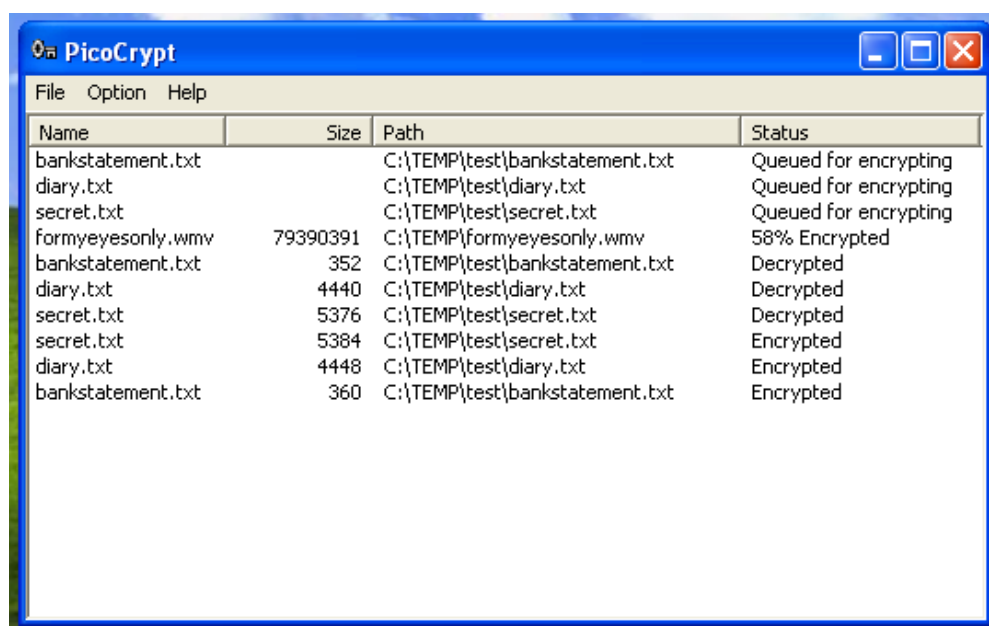
**Date updated:** Aug 29, 2005

**Platform Available:** Windows 95/98/Me/2000/XP

**Platform Tested:** Windows 95/2000/XP

**License:** Free

### Screen shot



### Instructions

#### Installation

No installation is needed. Just download and saves the executable file into your desktop or any other directories of your choice. You can even run it on your USB memory stick!

#### Running the utility

#### Our Software

Encryption Software  
Unit Converter  
Currency Converter  
Sticky Note  
PC XT Emulator  
Weather Monitoring  
Stock Charting WIP!  
Stock Trading Simulator WIP!  
Duplicate File Finder WIP!  
File Comparison WIP!  
File Splitter & Merger WIP!  
Secure File Eraser WIP!

#### WIP Software

Help Desk Software  
CRM Software  
Backup Software  
Management Software  
Marketing Software  
Trading Software  
Monitoring Software  
Tracking Software  
Scheduling Software  
Control Software  
Calculators

When you first run the utility, it will ask you for a default password. This default password will be later use for encrypting and decrypting all the files. If you want to use a different password for each file, then click "CANCEL" when prompted. You can set the default password later. **Note: The default password and other passwords that you have entered, are not saved on any files on your computer system. They are immediately hash using MD5 hashing algorithm.**

### Encrypting a file

To encrypt a file, you can drag and drop the specify file icon on to the utility windows and click "Encrypt" when prompt for the required operation. Alternatively, you can click menu "File"->"Encrypt ..." to open a file dialog box for you to choose the file you want to encrypt.

If the encryption is successful, the status will show "Encrypted" text.

### Decrypting a file

To decrypt a file, you can drag and drop the specify file icon on to the utility windows and click "Decrypt" when prompt for the required operation. Alternatively, you can click menu "File"->"Decrypt ..." to open a file dialog box for you to choose the file you want to decrypt.

If the decryption is successful, the status will show "Decrypted" text.

---

## Important Notes

The utility will encrypt the file you specified. The file will be replaced with the encrypted version and no backup copy will be made. As such, please ensure that you have key in your intended password correctly, else the file will be lost forever.

---

## Implementation Notes

For implementors wishing to write software compatible with this utility, the following notes are provided.

In the Blowfish CBC mode, plain text is encrypted in units of 64 bits (8 bytes, also called a block). To ensure that the plain text file is encrypted correctly, the utility will (internally) append from 1 to 8 bytes, the last byte containing an integer stating how many bytes of that final block are from the plain text file, and encrypt the resulting block. Hence, when decrypting, the last block may contain from 0 to 7 characters present in the plain text file, and the last byte tells how many. Note that if during decryption the last byte of the file does not contain an integer between 0 and 7, either the file has been corrupted or an incorrect key has been given.

This implementation uses a 128-bits key that are computed from the MD5 message-digest of the password entered by the user. In addition, it always uses an initialization vector of 0 (that is, all zeroes).