VMPCrypt

www.vmpcrypt.com

User's manual

Table of content

1. Introduction

VMPCrypt works under Microsoft Windows 98/ME/2000/XP/2003/Vista/7 operating systems. It was carefully designed to provide the highest level of cryptographic security of the encrypted data. In particular the application is useful for:

- Encryption of files/folders on local or network drives. Encrypted data is saved in archive files or an encrypted copy of each file can be created separately.
- Encryption of text messages and emails – edited in a built-in text editor. The messages can be sent directly as email with the default email client, saved in a text file or in an encrypted book.
- Generation of high quality cryptographic keys from entropy derived from random mouse moves – from mouse cursor position and time spaces between mouse moves measured to one thousandth of a second.
- Secure unrecoverable wiping of files from disk with pseudorandom data overwriting existing files from 1 to 99 times.

2. Installation of VMPCrypt

After inserting the installation CD to the drive an application-opening window is launched (start.exe). From this level you can run the application directly from the CD or install it on your computer.

After selecting to install the application the installation guide will open (setup.exe). You will be asked to confirm the folder in which the application will be installed and whether to create desktop shortcuts and a folder in the system menu Start → Programs.

After selecting to run the application directly from the CD the application will be launched without the need to install it (vmpcrypt.exe). You can also copy this file to any other media, e.g. USB memory, and run it from there – having the application always with you.

3. General idea of cryptography and critical role of key

A fundamental component of an encryption process is the cryptographic key (further referred to as a key or a password). The key is a parameter of the encryption process. Once we know the value of the key, decryption of a message can be run as fast as encryption. The strength of an encryption algorithm lies in the complexity of decrypting the message without knowing the key.

From the current state of the knowledge, breaking the VMPC encryption technology, used in VMPCrypt, requires an average computational effort of about 2^{900} operations. Even if each atom in the Universe performed a billion operations per second for a billion years – executing 2^{900} operations would be by far unreachable.
The application is supplied with an additional security layer – a specially designed key initialization algorithm (VMPC-KSA3). Even if hypothetically the VMPC cipher was broken, construction of the VMPC-KSA3 algorithm makes that decrypting any other message, even encrypted with the same key as the broken one, is impossible. To break the encryption technology applied in application it is necessary not only to break the VMPC stream cipher, but also to invert (break) the VMPC-KSA3 function, which is computationally even more complex.

Fundamental conditions for achieving real security of encryption are:

- Keeping the key secret
- Using keys of sufficient length and of high quality

Using short keys (e.g. "hdp") or regular keys (e.g. "aB2aB2aB2a") creates only an illusionary security. For example breaking a 6-character small-letters-only password on a home computer with a 3,2 GHz processor requires LESS THAN HALF AN HOUR of work.

Regularities in passwords can also be a serious threat to security because an attacker, knowing that a human being made up the password, can test the regular passwords before turning to the more random-looking ones.

The VMPCrypt application offers an advanced module for generating high quality keys of user-selected length. To derive entropy (randomness) for the generation of keys, the application uses temporary mouse cursor position during user's random mouse moves. The application additionally measures and uses time spaces between the mouse moves measured to one thousandth of a second. Recreating a series of random mouse moves by an attacker is practically impossible. The application transforms the information derived from the random mouse moves and generates a string of characters, which is undistinguishable from a truly random data-stream. Thanks to this algorithm the generated keys are of highest quality and they can be comfortably used to secure even the most confidential data.

4. Encryption of files and folders

VMPCrypt stores encrypted files and folders in an archive file (**encrypt to archive**) or an encrypted copy of each file can be created separately (**encrypt separately**).

One archive file can contain an unlimited number of encrypted files/folders. Archive files are fully encrypted – there is no plain (unencrypted) data (e.g. like unencrypted headers) in the files. This ensures the highest level of security of stored data – the structure of the archive files cannot be distinguished from a file containing truly random data.

Critically important components of the archive files (archive header and file-name-block) are stored in the archive in two copies (each time encrypted with a different value of the initialization vector, therefore both copies have randomly different structure) in case of local damages of the archive files (e.g. as a result of disk errors). Such situations are incredibly rare but if they occur, VMPCrypt will attempt to read the second copy of the block, which might enable to open the archive and decrypt data even in the event of archive local damage.

Archive files can be saved as self-decrypting archives. Such archive is an EXE file (an application) which can be open and decrypted without the VMPCrypt application.

Archives can be automatically split archives into files of selected maximum size so that it is easy e.g. to copy them on CDs.

The application also offers very flexible tools for detailed selection of files/folders to be encrypted (or decrypted, wiped or updated in the archive).

For files encrypted separately an encrypted copy of each file, e.g. data.txt, will be created. Its file name will have an additional .vmpc extension (e.g. "data.txt.vmpc"). The encrypted files will remain in their original folders or will be saved in a new user-selected folder.

4.1. How to select files/folders for encryption (or wiping)

Selecting files or folders for encryption (or wiping), is enabled by a file-browsing window, which can be open by pressing the "**Select files**" button found on the left side of the application's main screen.

4.1.1. The "Selection of Files / Folders" window

After pressing the "**Select files**" button a file-browsing window is open in which we can select those files/folders which are to be encrypted or wiped. Selecting the file or folder, which is highlighted by the cursor, is possible with the "**Select**" button. The "Select" button can also be accessed by pressing Space on the keyboard or by pressing right mouse button and selecting "**Select**". The selected file(s)/folder(s) will be added to the list in the application's main window. To highlight more than one file/folder, hold the Ctrl or Shift key and press left mouse button or the up-arrow/down-arrow key.

To change location of the browsed files, the "**Browse**" button or the Insert key can be used. The new location can be a local or a network drive. The new location can also be entered manually in the edit window at the top of the file browsing window. The recently selected location can be saved using the "**Save**" button. When the program is run again, the file-browsing window will be open in this folder.

If we are interested only in files of given type (e.g. only applications – files with EXE extension, e.g. App1.exe), we can use the filter at the bottom of the window. It is enough to enter the desired template (e.g. *.EXE filter displays only files with EXE extension (only applications). KEY*.TX? displays only files which name begins with KEY (e.g. KEY1, KEYBACKUP) and extension begins with TX and consists of exactly 3 characters (e.g. TXT, TX1 but not TXABC). *.* displays all files. Character case is ignored (*.EXE is equivalent to *.exe) and after pressing Enter or Tab key, only the files matching the selected filter will be displayed (when the box is checked) or names not satisfying the filter (when the box is not checked).

The **„vmpc"** button sets the filter to vmpc-type files (encrypted separately, see sect. 4.6). Using this button is comfortable if we want to select these files for decryption. After selecting them the "Decrypt separately" button can be used (see sect. 6).

The **„not vmpc"** button sets the filter to other files than vmpc-type (not encrypted separately).

The **„all"** button sets the filter to display all files.

To Select all files and folders currently displayed in the window – the button "**All**" can be used. It can be also accessed by pressing Ctrl + Space.

The "**Default**" button adds default decryption folder (see sect. 7.3) and leaves it e.g. ready for wiping. It can be defined during archive decryption.

Once we have selected all files/folders we wish to encrypt or wipe – we can press the "**Close**" button or Escape key or right mouse button → "Close".

4.1.2. Further file/folder selection options

When the selected files/folders are already in the main window's list – we can specify in more detail which of the selected files/folders or what parts of the content of the selected folders we want to encrypt or wipe. This is enabled by the four buttons found under the list.

"**Unselect**" button qualifies selected files/folders for ignoring. During encryption or wiping they will not be encrypted/wiped.

"**Select**" button qualifies selected files/folders back for encryption (or wiping).

"**Unselect All**" button qualifies all visible files/folders selected on the list for ignoring. During encryption or wiping they will not be encrypted/wiped.

"**Select All**" button qualifies all visible files/folders selected on the list for encryption (or wiping).

To select more than one file/folder, hold the Ctrl or Shift key and press left mouse button or the up-arrow/down-arrow key.

These four buttons are also available from the context menu visible after pressing right mouse button on the selected file(s)/folders(s).

The "**Clear**" button, on the left side of the window, clears the list of selected files/folders. If there are unselected files/folders on the list (qualified for ignoring with "Unselect" button), only the unselected files/folders are removed from the list. Otherwise all files/folders are removed from the list. No operation is performed on the files – their names are only removed from the list.

4.2. Preparing encryption options for encryption to archive

Before starting encryption we can specify whether files will be compressed before encryption and whether they will be wiped from disk after encryption.

4.2.1. "Compress" option

The "**Compress**" option can be checked in the bottom part of the application's main window. This option selects, whether files will be compressed before encryption. Compression decreases archive size but is slow and when encrypting big files it can be irritating. We recommend to use compression only when obtaining small archive size is necessary, e.g. when the encrypted archive is to be sent through the Internet.

4.2.2. "Wipe" option

The "**Wipe**" option can be checked in the bottom part of the application's main window.

Selects, whether files/folders will be wiped from disk after encryption. We recommend to wipe files/folders always after encryption. We should however be careful and keep in mind that if after encryption and wiping we lost the key, which was sufficiently long, recovering the encrypted data would not be possible in any way.

After encryption original files should be wiped from disk. Removing files from Windows recycle bin is reversible with specialized software. Wiping files is done by writing new (pseudorandom) data into the original file and only after this - logical removing of (wiped) files from disk. After unerasing a wiped file the attacker will only see pseudorandom data. If we assume risk that our disks will be analysed in specialized labs, we should consider that magnetic structure of disk surface is - to some extent - dependent on data that was stored on disk before. Only multiple wiping of file content blurs original magnetic structure extensively enough that recovering original content is impossible. For maximum security level we recommend 10-round wiping (although it is a time-consuming operation and in most practical applications 1-round wiping is sufficient). According to some sources (e.g. the Gutmann method) as much as 35-round wiping is recommended. The number of rounds of wiping can be specified in the "**Wipe rounds**" field found in the bottom part of the window in range from 0 to 99. 0 means that the files will only be logically deleted (not wiped).

VMPCrypt wipes only those files which were successfully encrypted and starts the wiping procedure only after the archive, storing the encrypted files/folders, has been completely and successfully created. This way e.g. in case of a disk read error – the files which had this error will not be wiped.

4.3. Starting encryption – specifying the key

After the files/folders for are selected, encryption can be started by pressing the "**Encrypt to archive**" button (this button can have additional information on it – "Compress" and/or "Wipe" – according the user's choice or "**Encrypt separately**".

After the button is pressed, a key-input window is open. A key (password) can be entered there from keyboard. After the key is entered, press "**OK**". The buttons of this window are described in sect. 7.1.1.

The "**Create random key**" button in the key-input window allows to generate a key from random mouse moves. After pressing it the Key Generation Module will be open, described in detail in sect. 11.

After entering the key the key-input window will re-appear for verification of the key. If you are completely sure that the entered key is correct, you can press "**Don't verify**" to cancel the key verification.

The "**Remember key**" option sets that the once entered key is remembered and it is possible to encrypt and decrypt data without entering the key each time. The key can be wiped from memory at any moment with the "**Remove key**" button in the application's main window.

4.4. Specifying parameters of the created archive

Archives created by VMPCrypt are encrypted in 100% - they contain no unencrypted data like e.g. headers. The archive file is undistinguishable from a file containing random numbers.

After inputting the key, a "**Save archive**" window will be open. In this window we can specify the archive file and a number of other options of the created archive.

Once these options are specified, the "**Encrypt**" button can be pressed to start encryption using all the selected options. After the encryption the created archive will be test-opened and once this operation is successful, a window summarizing the information about the archive will be displayed. If the files were to be wiped after encryption, the wiping will start only after all files are encrypted and after the test-open of the archive is successful. Moreover only those files which caused no problems (e.g. disk read errors) will be wiped.

4.4.1. File selection buttons

The "**Select file**" button Opens file browsing window to select location and name of the created archive.

The "**Other folder**" button proposes another folder to save the archive in. The folders are proposed from the list of files for encryption.

The "**Name + date**" button adds current date and time to the proposed archive's file name.

4.4.2. "Split archive into files of size" option

Specifies maximum size of a single file of the archive. This function allows to split archives into files of selected maximum size so that it was easy e.g. to copy them on CDs. If the archive is multifile (selected maximum size of a single file of the archive is lower than the total size of the archive), the consecutive files will be created according to a scheme ARCH1.VMPAx, where x=1,2,3,... When opening the archive ("Open archive" button in the application's main window) all files of a multifile archive (e.g. main file ARCH1.VMPA and remaining files ARCH1.VMPA1, ARCH1.VMPA2) must be in the same folder.

4.4.3. "self-decrypting archive (exe)" option

Specifies whether a self-decrypting archive is created. Such archive is an EXE file (an application) which can be open and decrypted without the VMPCrypt application. A self-decrypting archive can also be decrypted and updated using the VMPCrypt application - just as a standard archive - after opening the archive with the "Open archive" button in the application's main window. A standard archive can be transformed into a self-decrypting one and vice versa by using the "Open for update" button when opening the archive and then pressing the "Update" button.

Self-decrypting archives are comfortable to store data independently of the VMPCrypt application or for transmitting the archives, e.g. through the Internet. Decryption of such archives is possible after running the archive as a standard Windows application and inputting the correct key.

4.4.4. "Save original locations of files" option

Specifies whether the original locatios of encrypted files/folders will be saved in the archive. With this option on - it will be possible to automatically decrypt files to their original locations.

4.4.5. "Comment" window

Enables to input a text comment to the archive. In the comment any additional information about the archive can be saved. The comment can be read after opening the archive ("Open archive" button in the application's main window) and then using the "Archive info" button (see sect. 7.1). The comment can be empty. The comment is stored in archive fully encrypted.

4.5. Sending created archive through email

After creating the archive it can be easily transmitted through the Internet via email. It is enough to press the "Open archive" button in the application's main window, find the archive file on the file list, highlight the file and press right mouse button to display the context menu. From that menu we can select "Send to" → "Email recipient". An email message with the archive file attached will be created.

If the archive is multifile, then all the files of the archive must be attached (e.g. for a 3-file archive, files: ARCH1.VMPA and ARCH1.VMPA 1, ARCH1.VMPA2,…). In such situation change the file mask at the bottom of the file browsing window to "All files" and select all the files of the archive.

4.5.1. Blocking of exe email attachments in Windows

Some email clients block executable (EXE) attachments. This may disturb sending self-decrypting archives via email. An easy way to avoid this problem is to manually change the archive's filename e.g. from arch.exe to arch.exe1. An exe1 file should not be blocked. After receiving the file its name should be changed back to arch.exe.

4.6. Encryption of files separately

After selecting the files to encrypt (using the "**Select files**" button, sect. 4.1) press the "**Encrypt separately**" button. A key-input window will appear (see sect. 4.3). All files will be encrypted with the same key. Then (if we checked the "**to other folder**" option) a window for selecting a new folder for the encrypted files will be open. If we want to leave the encrypted files in the same folders where the source files are, press Cancel in the folder selection window or uncheck the "to other folder" option.

For each file, e.g. data.txt, its encrypted copy will be saved in a file with an additional .vmpc extension (data.txt.vmpc).

4.7. Evaluating the checksum of files

To evaluate the checksum of the files on the list use the "**Checksum**" button. The sequence of files is irrelevant. If any bit of any file changes the checksum will be completely different. This function enables to check whether the files were not damaged. The checksum is a "fingerprint" (a hash function) of the selected files computed with the VMPC-MAC algorithm.

5. Wiping files/folders

VMPCrypt can also be used only for unrecoverable wiping files from disk. This function is enabled by the "**Wipe**" button on the application's main window.

To select files/folders which are to be wiped, the „**Select files**" button can be used, which opens a file browsing window and which is described in detail sect. 4.1.1 and 4.1.2.

After selecting files/folders, the number of rounds of wiping can be selected (how many times the original content of the files will be overwritten by pseudorandom data) in the "**Wipe rounds**" field. More information about selecting the number of wipe rounds can be found in sect. 4.2.2.

6. Decryption of files separately

To select files for decryption use the "**Select files**" button, sect. 4.1). Then press the "**Decrypt separately**" button. A key-input window will appear (see sect. 4.3). Then (if we checked the "**to other folder**" option) a window for selecting a new folder for the decrypted files will be open. If we want to leave the decrypted files in the same folders where the encrypted files are, press Cancel in the folder selection window or uncheck the "to other folder" option in the key-input window.

For each encrypted file, e.g. data.txt.vmpc, its decrypted copy will be saved in a file without the .vmpc extension (data.txt).

For each file its MAC checksum is computed. If even one byte was changed in the file (e.g. due to transmission errors or deliberate action), the MAC checksum will detect the change and an error message will be displayed. This way if after decryption no error messages occurred, we can be sure that files after decryption contain exactly the same data as files before encryption.

7. Decryption of files/folders stored in archive

To decrypt selected files/folders stored in the archive, the archive should be open (this is possible only after inputting the correct key), select the files/folders we wish to decrypt and start decryption by pressing the "**Decrypt**" button.

7.1. Opening the archive

The archive can be open using the "**Open archive**" button on the left side of the application's main screen. This button opens a file browsing window in which we can find the archive we would like to open (it can be either a standard or a self-decrypting archive). After selecting the archive, a key input window will be open.

7.1.1. "Key input" window

In the upper side of the window a key edit field can be found, where the key can be entered from keyboard. Below there is a button "**Load key**" which enables to load key from a file. A key can be saved to a file using the "**Save key**" button in this window or in the Key Generation Module, as described in sect. 11.6.

After inputting the key we can make sure that the key was input correctly by pressing the "**Zoom key**" button, which displays the key enlarged in graphic format.

If more than one key was used to encrypt the files in the archive, then the "**Next key**" button should be used after inputting each key, in any sequence. If multiple keys were used and even one key is missing, decrypting the ciphertext is not possible. In such situation breaking the ciphertext using all the remaining keys is as complex as breaking the missing key. If data was encrypted after using the "Join keys" function in the Key Generation Module, here only the resulting accumulated key should be input.

The "**Clear**" key clears the key currently input in the key edit field.

The "**Show key**" option specify, whether the key is visible in the key edit window. Unchecking the "Show key" option allows to achieve better secrecy - the key will never appear on the screen.

The "**Cancel**" button closes the key input window and clears all key-related data in RAM memory. Decryption will be aborted.

The "**Remember key**" option sets that the once entered key is remembered and it is possible to encrypt and decrypt data without entering the key each time. The key can be wiped from memory at any moment with the 'Remove key' button in the application's main window.

After the key has been input we can press the "**Open for decryption**" button. It will open the archive in decryption mode and enable to decrypt selected files/folders stored in the archive.

When opening the archive always both copies of the header and the file-name-block are read and their MAC checksums are verified. If an error is encountered in any of the copies, a message is displayed with a recommendation to update the archive. Storing two copies of the critical blocks secures the archive against local damages – the archive may be possible to be open even in case of local damage, e.g. caused by disk read errors.

7.2. Selecting files/folders for decryption

After opening the archive, as described in sect. 7.1, names of all files and folders encrypted and stored in the archive will be displayed on the list in the application's main window. By double clicking on folder names we can browse the structure of the folders stored in the archive. The left arrow goes a level back in folder structure.

7.2.1. Further options of selecting files/folders for decryption

Once the content of the archive is displayed in the main window, we can specify which files and/or folders we wish to decrypt. VMPCrypt offers flexible selection functions, realized by the four buttons found below the list. To highlight more than one file/folder, hold the Ctrl or Shift key and press left mouse button or the up-arrow/down-arrow key.

The "**Select**" button qualifies highlighted files/folders for decryption.

The "**Select All**" button qualifies all files/folders in the open archive for decryption.

The "**Unselect**" button cancels qualifying highlighted files/folders for decryption.

The "**Unselect All**" button cancels qualifying all files/folders in the open archive for decryption.

The above four buttons are also available in the context menu after pressing right mouse button on the list.

7.3. Selecting location for decrypted files/folders

After selecting the files/folders for decryption and pressing the „**Decrypt**" button, a window "**Choose location for decrypted files**" will be automatically open.

Option "**Decrypt to original folders**" specifies that all decrypted files/folders will be saved in exactly the same locations (disks and folders) from which they were encrypted. This option is available only when the "Save original locations of files" option was selected during encryption (see sect. 4.4.4).

Option "**Decrypt to folder:**" specifies that all decrypted files/folders will be saved in a selected location. Structure of subfolders will be reconstructed as for the original encrypted files and the selected location will be a mother folder to the decrypted files/folders. By default a subfolder "**Decrypt**" of the folder in which the archive file is stored is proposed.

The new location can be either typed in the edit window or selected using the "**Choose folder**" button.

If the selected destination folder does not exist, it will be automatically created.

We can also use the "**To default folder**" option, which selects that all decrypted files/folders will be saved in the default decryption folder. To define it use the '**Save default**' button.

The "**Open folder after decryption**" option selects that after decryption the folder where the decrypted files/folders were saved will be automatically open.

Once the location has been selected, the decryption process can be started by pressing the "**Decrypt**" button.

When after decryption a message "MAC: OK…" is displayed, we can be sure that all the selected files/folders were decrypted correctly.

7.4. Displaying information about the open archive

When an archive is open, a detailed information about its size and other parameters can be displayed by pressing the "**Archive info**" button.

7.5. Closing the open archive

The open archive can be closed at any moment by pressing the "**Close**" button on the left side of the application's main window. All data, including file names and key, will be wiped from memory.

8. Updating archive content and key change

VMPCrypt offers flexible functions for updating content of the archives – adding and removing files/folders, overwriting the ones already stored in the archive and changing archive's encryption key.

To start archive update, the archive should be first open – using the "**Open archive**" button in the application's main window, then inputting the correct key and pressing the "**Open for update**" button. Opening archives is described in more detail in sect. 7.1.

After opening the archive, all files and folders stored in the archive will be displayed on the list in the application's main window.

To add new files/folders to the open archive, the "**Select files**" button can be used (see sect. 4.1.1. for more details on selecting and adding files/folders).

Using four buttons below the list we can specify what operations we would like to perform on the selected files/folders. To highlight more than one file/folder, hold the Ctrl or Shift key and press left mouse button or the up-arrow/down-arrow key.

The "**Overwrite**" button qualifies selected files/folders for overwriting with new files/folders, with the same names and locations, read from disk.

This option is available only when the "Save original locations of files" option was selected during encryption (see sect. 4.4.4).

The "**Remove**" button qualifies selected files/folders for removing from archive. If those files/folders have just been added with " Select files" button – they will be qualified for ignoring (whey will not be added to archive or wiped after pressing "Update" button).

The "**Clear**" button cancels qualifying selected files/folders for overwriting, removing or ignoring the newly added ones

The "**Clear All**" button cancels qualifying all visible files/folders on the list for overwriting, removing or ignoring the newly added ones

The above four buttons are also available in the context menu after pressing right mouse button on the list.

By checking the "**Wipe**" option in the bottom part of the application's main window we can specify whether the files/folders added to the archive and overwritten in the archive will be wiped after the archive has been successfully updated. A detailed description of the wiping option can be found in sect. 4.2.2.

To change the archive's encryption key, check the "**Change key**" option situated next to the "Update" button.

Once the updating options are set, we can press the "**Update**" button. The "Save archive" window, described in detail in sect. 4.4, will appear. There we can optionally change the archive's name, change the maximum size of a single file of the archive, change the archive type (into self-decrypting or standard one) or add/change the comment.

After specifying these parameters (or leaving them unchanged) we can press the "**Update**" button and all the selected changes to the archive will be applied.

8.1. Mechanism of updating archive

Archive update is a sensitive operation because it operates on the content of archives, which by nature can be valuable and unique. VMPCrypt has mechanisms which secure the content of the updated archive in case of events like power failure, where the computer stops operating in an unpredictable moment.

If archive name is not changed, the update procedure creates new temporary archive ~~ARCH.VMPA (where ARCH.VMPA is the original archive name) and copies the content of the original archive to the temporary one along with performing all selected modifications. After the update is finished successfully, the original archive is renamed to ~ARCH.VMPA and upon user's confirmation is removed from disk. The temporary archive (~~ARCH.VMPA) is renamed into the original one (ARCH.VMPA). This mechanism secures archive content in case of power failure or other unexpected events which could terminate the update in undefined moment. If such event occurs - at any moment the original archive will still be on disk.

If the "Wipe" option was checked only the files correctly written to the archive will be wiped.

8.2. Deleting the archive

To delete the open archive, we can press the "**Delete**" button in the bottom part of the application's main screen. The user will be asked for additional confirmation, information about the archive will be displayed and upon confirmation it will be deleted. Note that wiping archives is not necessary because they contain only encrypted data. If however we are afraid that the encryption key might have leaked it is better to wipe the archive instead of simple deletion of it.

9. Encryption of texts

To switch to text encryption mode, the "**Text Mode**" button in the application's main window can be pressed. A secure text editor will appear (not creating temporary files and storing the edited text only in RAM memory).

By pressing the "**File Mode**" button we can switch back to file/folder encryption mode at any moment.

9.1. Sending encrypted email

To send encrypted email it is enough to type the text of the message in the text edit window and press the "**Email**" and then "**Encrypt**" button. The key-input window is open (see sect. 4.3) and then all text in the text edit window is encrypted using the input key. The encrypted text is automatically transformed into Base64 system which uses only characters (A..Z, a..z, 0..9, +/=)

to represent binary data. This enables easy transfer of the encrypted text using email. The encrypted message is automatically copied to clipboard and the default email client is run. When editing the email message the encrypted text can be pasted into the message using keys Ctrl + V or using menu option Edit → Paste.

9.2. Decrypting email

Before decrypting the message, in the email client the encrypted message should be copied to the clipboard using keys Ctrl + A (=select all) and then Ctrl + C (=copy) or using menu options Edit → Select All and then Edit → Copy.

Then it is enough to press the "**Email**" and "**Decrypt**" button. The encrypted message will be pasted into the text edit window and the "Key input" window will be open (see sect. 7.1.1). After inputting the key, the message will be decrypted and the MAC checksum of the message will be computed. If the message arrived correctly in 100% and a correct key was used, a "MAC: OK…" message will be displayed.

Otherwise a message "MAC: Error…" will be displayed. In such situation: if the message looks like random data, then most likely an incorrect key was used; if the message looks correctly, then most likely some minor corruptions happened to the content of the message and the message we see after decryption is not exactly the same message which was encrypted. In such situation – if the message is precise – we might want to ask the sender to transmit the message again. We don't know whether the changes were caused by transmission errors or by an adversary. Only the "MAC: OK…" message after decryption gives us a practical guarantee that the message was not corrupted and was decrypted correctly.

9.3. Encrypted chat mode

The encrypted chat mode is comfortable if we want to send encrypted messages on a chat or through a text online communicator. The mode can be turned on by pressing the "**Chat**" button. In this mode the once input key is remembered and it is possible to encrypt and decrypt texts using one click of a button (Encrypt / Decrypt) without the need to input the key each time. After finishing the chat session use the "Remove key" button to wipe the key from memory.

9.4. Additional text edit and encryption functions

9.4.1. Encryption of text

We can encrypt the text from the text edit window without sending it via email by pressing the "**Encrypt**" button. It opens the key-input window and encrypts all text in the text edit window using the input key. The encrypted text is automatically transformed into Base64 system which uses only characters (A..Z, a..z, 0..9, +/=) to represent binary data.

9.4.2. Decryption of text

To decrypt text from the text edit window we can press the "Decrypt" button. It asks for the key (see sect. 7.1.1) and decrypts all text in the text edit window using the input key. If a message "MAC: OK…" is displayed, then we can be sure the message was decrypted correctly. Otherwise (a "MAC: Error…" message), either we used an incorrect key or the message was corrupted.

9.4.3. The "Send" button

Copies the content of text edit window into clipboard and runs the default email client. When editing the email message the text can be pasted into the message using keys Ctrl + V or using menu option Edit → Paste.

9.4.4. Other text edit functions

The "**Search**" button searches for a given phrase in the text.

The "**Copy**" button copies the content of the text edit window into clipboard. The content of clipboard can be pasted using any text-edit application (e.g. an email client), using keys Ctrl + V or using menu option Edit → Paste.

The "**Paste**" button clears the text edit window and pastes the content of clipboard.

The "**Clear**" button clears the text edit window.

The "**Save to file**" button saves the content of the text edit window in a text file.

The "**Open file**" button loads the content of a text file into the text edit window. Previous content of the window is cleared.

The "**Font size**" option changes font size in the text edit window.

The "**File**" button switches to text-file encryption mode. In this mode text is automatically saved to a selected file after pressing "Encrypt" and is automatically loaded from a file before pressing "Decrypt". After decryption key is remembered. It can be removed from memory at any time with the "Remove key" button.

The "**Email**" button switches to email encryption mode. In this mode encrypted text is automatically copied to clipboard and a default email client is open. The encrypted text can be pasted into the message using Ctrl + V keys or using menu option Edit → Paste.

The "**Chat**" button switches to encrypted chat mode. In this mode the once input key is remembered and it is possible to encrypt and decrypt texts using one click of a button (Encrypt / Decrypt) without the need to input the key each time. After finishing the chat session use the "Remove key" button to wipe the key from memory.

The "**Text**" button switches to basic text encryption mode.

The "**Copy**" option selects whether encrypted text is automatically copied to clipboard.

The "**Send**" option selects whether encrypted text is automatically copied to clipboard and a default email client is open. The encrypted text can be pasted into the message using Ctrl + V keys or using menu option Edit → Paste.

The "**Save**" option selects whether encrypted text is automatically saved to a file.

The "**Paste**" option sets that after pressing the "Decrypt" button encrypted text will be first pasted from clipboard and then decrypted.

The "**Open**" option selects whether after pressing the "Decrypt" button text is automatically loaded from a file before decryption.

The "**Remember key**" option sets that the once input key is remembered and it is possible to encrypt and decrypt texts using one click of a button (Encrypt / Decrypt) without the need to input the key each time. The key can be later wiped from memory using the "Remove key" button.

10. Encrypted book

In the text encryption mode (after pressing the "Text Mode" button) an option of an encrypted book is available. It works as an encrypted database of text documents. It is comfortable for secure storage of passwords, contacts, clients' data or chapters of a book. The text documents saved in the book are referred to as **documents** and they can be edited in the built-in text editor.

Documents can be comfortably organized in folders. Each folder can also contain subfolders for more flexibility. It is possible to copy and move documents between folders.

Each encrypted book is saved in a single file (filename with .VMPB extension). This file – like the archive file – is encrypted in 100%, i.e. each byte of the file is encrypted and the file contains no unencrypted data like e.g. headers. The file is undistinguishable from a random data stream.

The book's header and the list of documents – being vital for the book to work properly – are saved in the book file in **two copies** for better security in case of disk damage. Both copies are encrypted with a different initialization vector, which means that after encryption they look completely different.

All operations on the book are secured against system failure (e.g. power failure). During any operation on the book (like encryption or removing a document) the whole book is copied to a temporary book together with applying the desired modifications. The temporary book filename has a "~" prefix added to the original book filename. Only after the operation is finished successfully the original book file is removed and the name of the temporary book file is changed to the original filename.

Thanks to this mechanism even when system failure takes place during an operation on the book only the temporary book will be lost (the writing to it will be terminated in an undefined position) and the book file from before the changes will still be on disk intact.

10.1. Creating a new book

To create a new book we can press the „**Book**" button. The book navigation window appears. We can type the document's title, press "**Open**" and the new document will be in the edit window.

10.2. Encrypting document

After typing the document's content we can press the "**Encrypt document**" button. The whole content of the edit window will be encrypted and saved in the book's file. If we were editing a newly created book, we will be also asked to enter the book's filename and the encryption key.

10.3. Opening an existing book

We can open an existing book using the "**Open book**" button. After pressing it the book's encryption key will need to be entered.

10.4. Closing a book

At any time the open book can be closed using the "**Close**" button. The application will return to standard text encryption mode.

10.5. Navigating the book

After pressing the "**Book**" button when a book is open the book navigation window appears. It allows to perform several operations on the book's content.

Some buttons adjust their function depending on whether the documents' or the folders' list is active. The lists' **sizes** can be changed by moving the line separating them with the mouse. **Changing** the active list is possible either by clicking the mouse on the desired list or by using the left/right **arrows** on the keyboard.

The "**Open**" button opens selected document (or documents – when the "**marked**" option next to the button is checked) or folder.

The "**Close**" button closes the encrypted book.

The "**New**" button creates a new document or folder.

The "**Change**" button changes document's title or folder's name.

The "**Delete**" button deletes the marked documents.

The "**Mark**" and "**Unmark**" buttons mark or unmark selected documents. Then it is possible to delete the marked ones or to export them to the edit window. We can export the marked documents by checking the "**marked**" option and pressing the "**Open**" button.

The "Mark" and "Unmark" buttons are also available in the context menu open after pressing right mouse button on the documents' list. A context menu is also available on the folders' list.

The "**Clear**" button unmarks all documents and folders.

The "**Search**" button searches for documents or folders containing a given phrase in title or - if the "**inside documents**" option is checked - in documents' content.

The "**Sort**" button changes sorting method – the marked documents and folders are displayed at the top of the lists. To sort the documents by name or by number click the appropriate column header.

10.6. Copying and moving documents between folders

The copy/move options are available in the context menu (appearing after pressing right mouse button on the documents' list) and in the book's main menu in the "**Edit**" option.

The "**Copy marked here**" option copies all marked documents to the current folder. The marked documents are decrypted, then re-encrypted and the newly encrypted copy is saved in the current folder. The original encrypted document stays in its original location. A new initialization vector is used to re-encrypt the document thanks to which the form of the newly copied document after encryption is completely different from the form of the original document after encryption. This way even after multiple copying the same document each copy will have a completely different form after encryption.

The "**Move marked here**" option moves all marked documents from its original folder to the current folder. The documents disappear from their original folders and appear only in the current folder.

10.7. Book's menu options

At the top of the book navigation window the following options can be found:

"**File**" – "**Encrypt document**" – encrypts the edit window content and saves it to the book's file

"**File**" – "**Change key**" – changes book's encryption key

"**File**" – "**Save as**" – saves the book to another file

"**File**" – "**New book**" – creates a new book

"**Close document**" – closes the current document. The edit window switches to standard text encryption mode but the book remains open.

"**Close book**" – closes the open book

"**Close window**" – closes the book navigation window.

Functions in the "**Edit**" menu are described in section 10.6.

The "**Delete folder**" option in the "Edit" menu deletes the selected folder.

When a document is open then in the application's main window new buttons "**Copy row 1, 2, 3**' appear. They make it easier to copy specified blocks of text. They can be useful when we keep e.g. passwords on specified positions in the documents, e.g. always in the first row. The "**Copy cursor**" button copies the row in which the cursor currently is to clipboard.

11. Key Generation Module

The Key Generation Module can be run after starting encryption by pressing the "**Create random key**" button in the key-input window. The Module can also be open by pressing the "**Create key**" button or Ctrl + K in the program's main window, e.g. to create a key that will be used in the future.

11.1. Selecting key size

In the upper-left part of the Key Generation Module's window in the "Key generation" tag a field "**Key size in bytes (1..64)**" can be found. It allows to set the length of the key generated from random mouse moves. As default a size of 256 bits is chosen (which is equivalent to 45-character password made of small and capital letters and digits.

The choice of the key length is up to the user. To help decide what length to use, the application automatically assesses and displays how much time it would take to break a key of given length by two kinds of supercomputers. To achieve high security level we recommend to use 256-bit or longer keys.

11.2. The "Use" field – choice of character-set to represent the key

In the upper-left part of the Key Generation Module's window in the „Key generation" tag a field "**Use**" can be found. This field allows to choose from what characters the key generated from random mouse moves will be built. Small letters (a..z), capital letters (A..Z) and digits (0..9) can be chosen and any combination is possible. To avoid possible misunderstandings, the following letters are never used in the generated keys: I i (as "idea"); L l (as "land"); O o (as "oak").

The "**Show key**" option specifies if the key is visible on the screen. Unchecking the "Show key" option (as by default) allows to achieve better security.

11.3. The "Generate key" button

Starts generating key from random mouse moves. After pressing the button the mouse cursor should be moved as irregularly as possible – in the "**Mouse position capture area**". A key of selected length is generated from temporary position of mouse cursor and also from time intervals between mouse moves measured to a millisecond (1/1000 s). Keys derived from random mouse moves are practically indistinguishable from truly random data streams. Such keys are hardest to break.

11.4. The "Enter key" button

Enables to input key from keyboard (a password). We recommend to use keys generated from random mouse moves. To ensure that a key (password) entered from keyboard is as secure as it can be – we recommend to use as many characters as possible (small and capital letters, digits, special characters, like @$#[* etc.).

According to the length of the typed password and characters used in it the length of equivalent binary key (in bits) is assessed. We recommend to use long passwords, such that their binary equivalent length is at least 128 bits. Entering keys shorter than 8 characters raises a real risk of breaking the key even using a home computer.

We recommend to use the information about the estimated time required to break the password, displayed on the right side of the window, to help to select the sufficient length for the key.

11.5. "Load key" button

Enables to load key from file. Any key can be saved to a file using "Save key" button in the "Save key" tab (see sect. 11.6).

11.6. "Save key" button

In the upper-left part of the Key Generation Module's window in the "Save key" tag a button "**Save key**" can be found. It allows to select a text file to which key will be saved. Key is saved at the beginning of the file in pure text format. The key ends with an additional character "<" (ASCII code 60 [hex:3C]). Keys shorter than 155 characters are additionally filled with characters "-" (minus, ASCII code 45 [hex:2D]) up to length of 156 bytes. Then the key is additionally filled with the "-" characters up to 1024 characters of length so that the copies of the key are written in the file in certain distance to better insure against local disk damage.

Such prepared key is saved to the file in **three copies** written one after another for additional security in case of a possible disk failure.

At the end of the file a characteristic constant string is added which may help find the key on a damaged disk. The string is:

uvdrakbcrhytckbsvsqeysnzzvampahwkhnmxkeawapswjdbtexwnaswe

Saving keys to files can be comfortable e.g. if we use long and high quality keys generated from random mouse moves. We recommend to save the keys on removable disks (like CD/DVD, Pen-Drives, etc.). Saving keys on hard disks should be treated as a temporary operation, which will be followed by copying the keys onto removable disks. After this the keys should be wiped from the hard disks for security reasons.

The "**Zoom key**" function can also be used for non-standard methods of storing the key, e.g. by taking a photograph of the screen while the zoom of the key is displayed.

The above rule has smaller effect if we consider our computer safe and encrypt the data only to transmit it, e.g. through the Internet.

11.7. The "Next key" button

Allows to generate the next key. Using multiple keys to one encryption can be useful e.g. when data should be accessed (decrypted) only by a **full group of users**. Each user owns his own key and successful decryption is possible only when all keys are input. This function can also be used to increase security level by a single user by using multiple keys. One key can for example be a 256-bit key generated from random mouse moves and stored on a CD, floppy or Pen-Drive and another key, e.g. input from keyboard, cold further increase the security level. Number of keys possible to input is unlimited. Sequence of inputting the keys is irrelevant. If even one key is missing, breaking the ciphertext using all the remaining keys is as complex as breaking the missing key

11.8. "Join keys" button

Joins all the input keys into one accumulated key. To decrypt data only the resulting accumulated key should be input. This function can be useful in a multi-channel key agreement protocol, where parties exchange many keys using different channels (e.g. telephone, SMS, fax, Internet, personally, with traditional mail, PKI or other) and then join the keys into a single accumulated key, which will be used for encryption and decryption. The purpose of such solution is minimizing the risk that ALL the transmitted keys will be intercepted by hostile parties. A given set of keys always generates the same accumulated key, regardless of the sequence of inputting the keys. If even one key is missing, breaking the ciphertext or finding the accumulated key using all the remaining keys is as complex as breaking the missing key.

11.9. General functions of the Key Generation Module

“**Cancel**” and “**OK**” buttons wipe the key data from memory and closes the Key Generation Module.

The “**Reset**” button resets the Key Generation Module to its initial state. The generated key (or keys) is wiped from memory and the Module is ready to generate the first key.

11.10. Key management

Key management routines depend directly on the individual requirements of the user. The application offers flexible functions of generating keys and storing them on any kind of disks, in standard text files. The key management should comply the fundamental rules that the key should be kept secret and should be stored safely. If e.g. a CD with the key is lost, then decrypting the data is impossible. There is probably an unlimited number of key management procedures based on the key-related functions offered by the application. Choosing or defining the right one depends on the particular situation and the security requirements of a particular user.

12. Additional functions of the application

12.1. Remembering the key

The once input key can be remembered so that it is possible to encrypt / decrypt more data using the same key without the need to input the key each time. The “**Remember key**” option in the key input window (see sect. 7.1.1) enables this. The remembered key can be wiped from memory at any moment with the “**Remove key**” button in the application's main window.

12.2. Encryption in private mode

This option is available only for owners of licensed copies of the application (the free trial version available in the Internet does not support it). Data encrypted in private mode can be decrypted only using a **licensed** copy of the application (after entering the correct key). Entering the correct key in the free version will not decrypt the data.

Switching to the private mode is accomplished by a special key input procedure: as the first key enter ‘**.**’ (**full stop / period**). After entering it the private mode will be switched on and then the proper encryption key (or keys) can be entered.

Encryption technology and security levels in the private mode and in standard mode are **identical**. Technically: the only difference in the two modes comes in different initial values of the internal permutation in the Key Initialization Algorithm. Using the private mode instead of the standard mode to improve security is pointless.

The private mode can be used e.g. by our company to publish information **exclusively** to our clients.

12.3. Encryption with a constant key

If no key was input when encrypting files to archive, data will be encrypted with a **constant key**. Encrypting with a constant key gives no cryptographic security. It can however be useful if we would only like to compress the files or store many files/folders or text documents in a single file.

12.4. Searching for files and folders

When working with files to encrypt or with an open archive it is possible to search for files and folders on the list. The "**Search**" button searches for files and folders containing a given phrase.

12.5. Setup

After pressing the "**Setup**" button (of F1 key) a window is open in which we can configure many of the application's parameters.

12.6. Drag-and-drop of files

To make it easier to find the desired files it is possible to drag-and-drop them from the Windows explorer (press left mouse button on the file, move the cursor to the application's window and release the mouse button). The applications recognizes archive files (VMPA), files encrypted separately (VMPC), encrypted book files (VMPB) and text files if we are in text encryption mode.

12.7. Current help system

VMPCrypt has a system of current help – pressing right mouse button on each function-button or any other object in the application displays a detailed information about how it works.

12.8. System of hotkeys

The application enables to access all buttons from keyboard. The hotkey combination is displayed on most of the buttons and can be viewed in detail after moving mouse cursor over the button and holding it there for a while.

12.9. System of self-control

VMPCrypt has a system of self-control. Each time the application is run, a MAC checksum of the EXE file containing the application is computed. This way if even one byte of the application was changed or was added to the application's EXE file (e.g. by a virus), it will be detected at application's startup. In such situation an information about the corruption of the application's file will be displayed but the application will keep running.

12.10. Running from command-line

The application can be run from **command-line** (this mode is useful e.g. for automatic file archiving with commands written it a BAT file). The following functions are available: separate encryption / decryption of a single file or the whole folder (see chapter 4.6), wiping a file (also wiping without previous encryption) and reading the key either from the command-line or from a file. The application accepts the following parameters:

Running the application from command-line. Parameter list:

/k=... Key. E.g. "/k=abc"
/kf=... Key file. E.g. "/kf=c:\vmpck1.txt"
If none of the /k or /kf parameters is given,
files are encrypted/decrypted with a CONSTANT KEY

/src=... Source file or folder. E.g. "/src=c:\file.txt" "/src=c:\my private folder"

/dst=... Destination folder. E.g. "/dst=c:\my folder"
The /dst parameter is optional. If it is not given,
the output files are stored in the same folders as the input files

/e Encrypt
/d Decrypt
/x Only wipe the given file or the contents of the given folder

/w... Specify the number of wiping rounds. E.g. "/w0" "/w1" "/w25"
/w0 is equivalent to only logical deleting of files (0 wiping rounds)

The /w parameter is used along with the /e, /d, /x parameters.
E.g. /e /w2 wipes the files using 2 rounds after encryption.
E.g. /d /w0 logically deletes the files (0 wiping rounds) after decryption

/i Automatically overwrite existing files

/v Automatically add the "vmpc" extension to the decrypted file name
E.g. "/src=c:\file.txt" /d /v decrypts the c:\file.txt.vmpc file

------ DEFAULT VALUES: ------

When wiping files (/x) and no /w parameter is given,
then 1 wiping round is assumed (equivalent to /x /w1).

When encrypting (/e) or decrypting (/d) files and no /w parameter is given,
then the input files will NOT BE WIPED OR DELETED.

When encrypting (/e) or wiping files (/x) and only "/w" parameter is given (not e.g. "/w3"),
then 1 wiping round is assumed.

When decrypting (/d) and only "/w" parameter is given (not e.g. "/w3"),
then only logical deleting of files (0 wiping rounds) is assumed.

------ ADDITIONAL REMARKS: ------

For the /kf /src /dst parameters:
If the file name contains spaces then
the whole parameter must be given in QUOTATION MARKS "...", e.g. "/src=my file.txt".
To avoid the risk of a mistake we recommend to always give the
"/kf=..." "/src=..." "/dst=..." parameters in quotation marks.

The sequence of the parameters is irrelevant but due to security reasons
the KEY (/k or /kf) must be given as the FIRST parameter.

12.11. Working without installation

This application can work also without installation. The application's file – vmpcrypt.exe – can be copied anywhere (e.g. to a CD or USB memory) and run from there. This enables to have the application **always with you**.

The vmpcrypt.exe file can be found on the application's installation CD. If the application was delivered only in electronic form then it should be installed on a computer first. Then you can find the vmpcrypt.exe file in the folder where the application was installed and you can copy it from there.