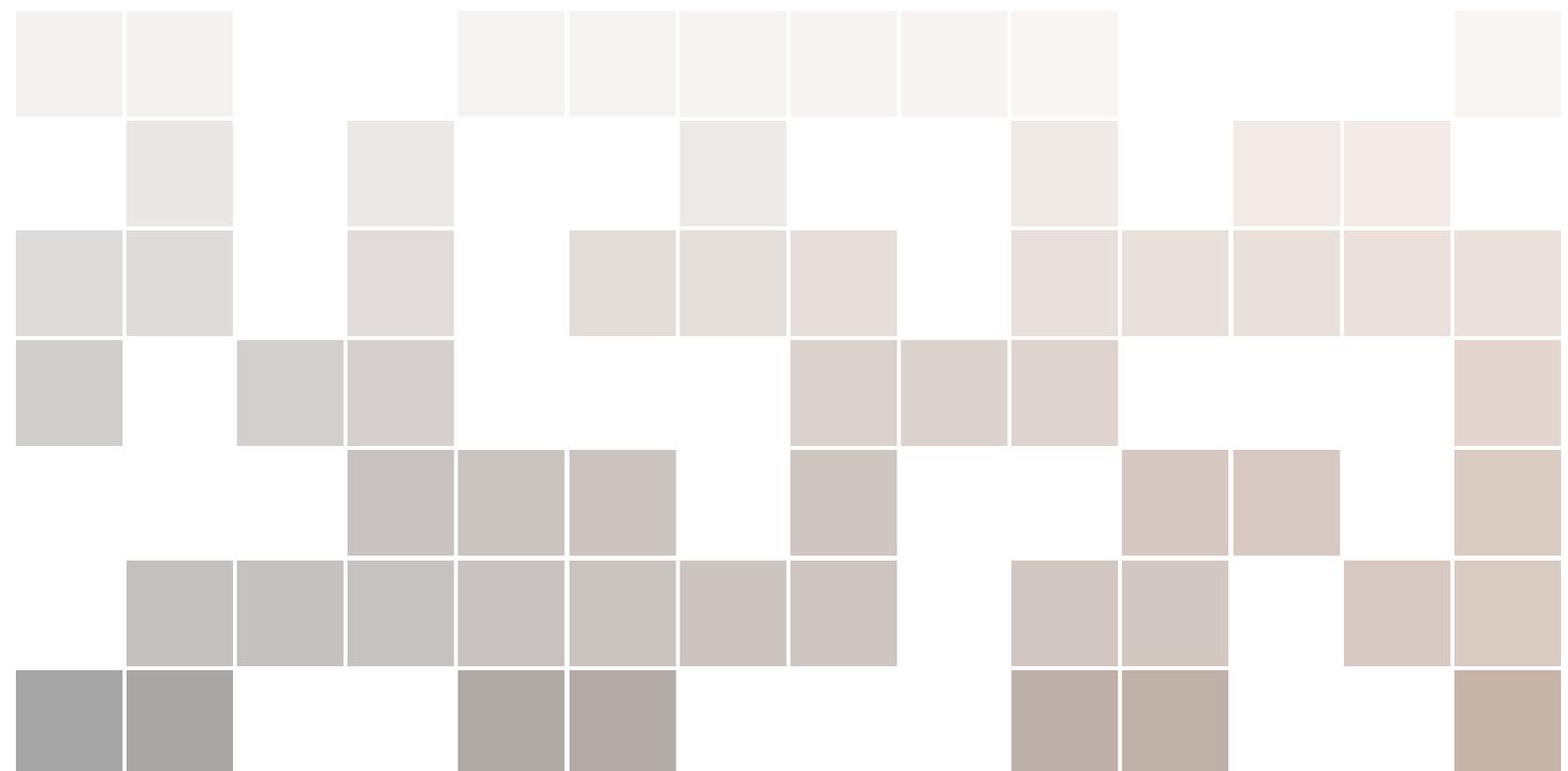


GostCrypt User Guide

Laboratoire de Cryptologie et de
Virologie Opérationnelles - France



Copyright © 2014 Laboratoire de Cryptologie et de Virologie Opératoinnelles - France

GOSTCRYPT.ORG



Contents

| | | |
|----------|--------------------------------------|-----------|
| 1 | Introduction | 5 |
| 2 | Using GostCrypt Volumes | 7 |
| 2.1 | File container encryption | 7 |
| 2.2 | Encrypted Partition / Drive | 13 |
| 2.3 | Hidden Volumes | 13 |
| 3 | Favorites | 15 |
| 3.1 | Favorite Volumes | 15 |
| 3.2 | System Favorite Volumes | 15 |
| 4 | Main Program Window | 17 |
| 5 | Keyfiles | 23 |
| 6 | Encryption Algorithms | 25 |
| 6.1 | GOST 28147-89 | 25 |
| 7 | Hash Algorithms | 27 |
| 7.1 | GOST R 34.11-2012 | 27 |
| 7.2 | GOST R 34.11-94 | 27 |
| 7.3 | Whirlpool | 27 |

| | | |
|------------|---------------------------------|-----------|
| 8 | Command Line Usage | 29 |
| 8.1 | GostCrypt.exe | 29 |
| 8.2 | GostCrypt Format.exe | 30 |
| 9 | Encryption Scheme | 31 |



1. Introduction

The Gostcrypt project has been launched at the end of 2013 as fork of the (late) Truecrypt project. Snowden's leaks have made clear more than ever that the massive use of encryption by citizens must become a reality. This is possible only if there is a vast, rich offer of trusted, open source products like Truecrypt, with the strong support of the hacker community. However, at that time we did not foresee the unprecedented upheaval of terrible shock with the recent Truecrypt disappearance. More than ever we all need more and more projects to replace it. Gostcrypt is one among (we hope) many others. The variety and richness of encryption solutions is THE solution.



2. Using GostCrypt Volumes

2.1 File container encryption

Creating an encrypted file container is the easiest way to encrypt data in GostCrypt. In this process, you will create an encrypted file of a size you specify. Once this file has been created, you can open it as a storage device in which you can store your sensitive data.

Creating the volume

In order to encrypt data on your system, you will first need to create a new GostCrypt volume. To open the GostCrypt Volume Creation Wizard, click on the “Create Volume” button on the main screen of GostCrypt (as seen in figure 2.1).

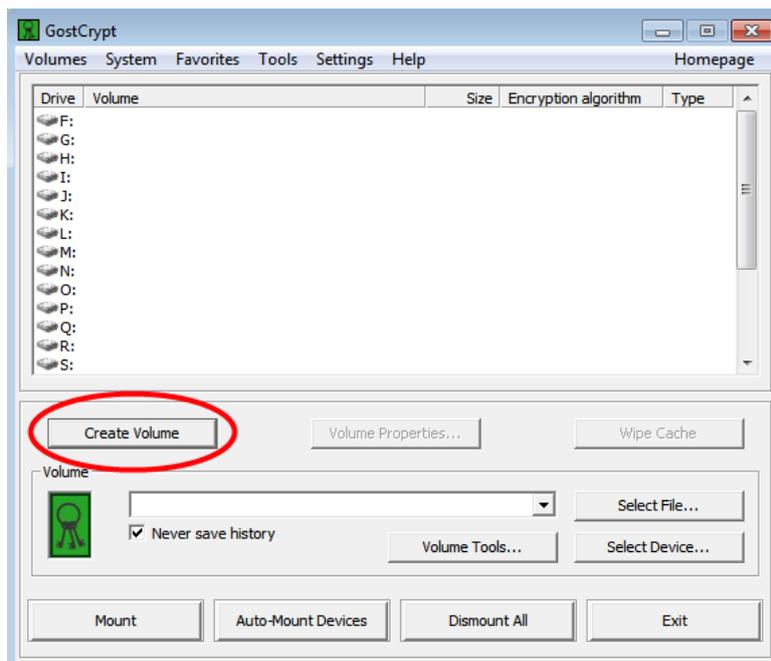


Figure 2.1: GostCrypt main window

In the GostCrypt Volume Creation Wizard, select the “Create an encrypted file container” option and click next.

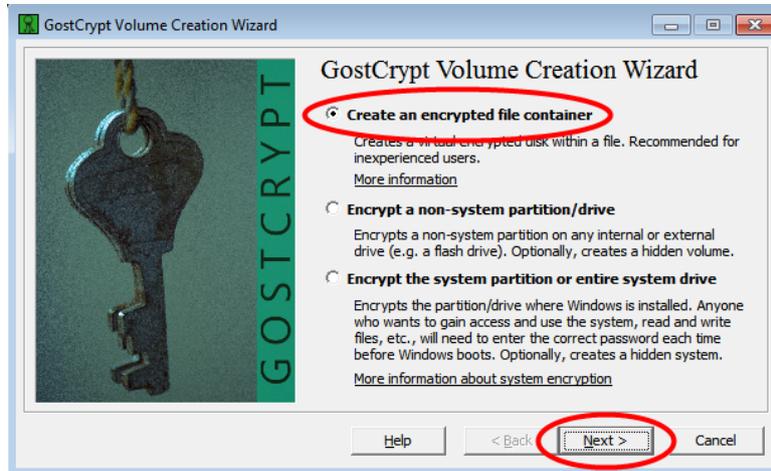


Figure 2.2: Select encrypted file container

In the next screen, you are asked to choose between the creation of a standard GostCrypt volume and a hidden GostCrypt volume. For this exercise, select “Standard GostCrypt volume”. For hidden volumes, see chapter 2.3.

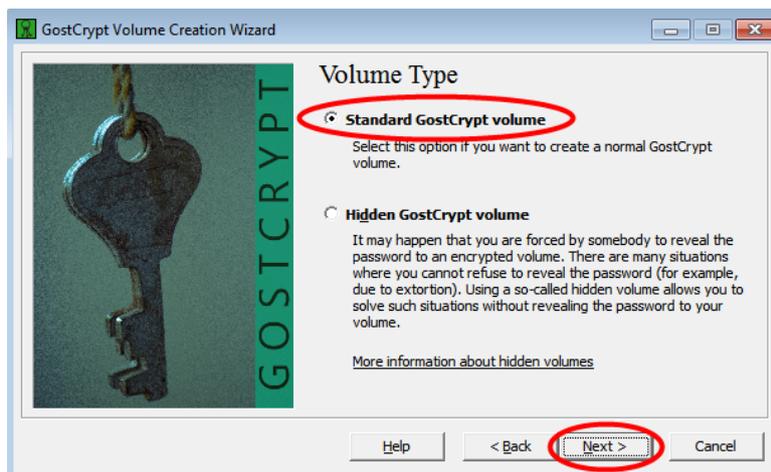


Figure 2.3: Select standard GostCrypt volume

In the next dialog, provide GostCrypt with the location where you want the file container to be created.



Figure 2.4: Provide GostCrypt with a file location

By clicking the “Select File...” button, you can specify where you want to save your file container in an easy manner.

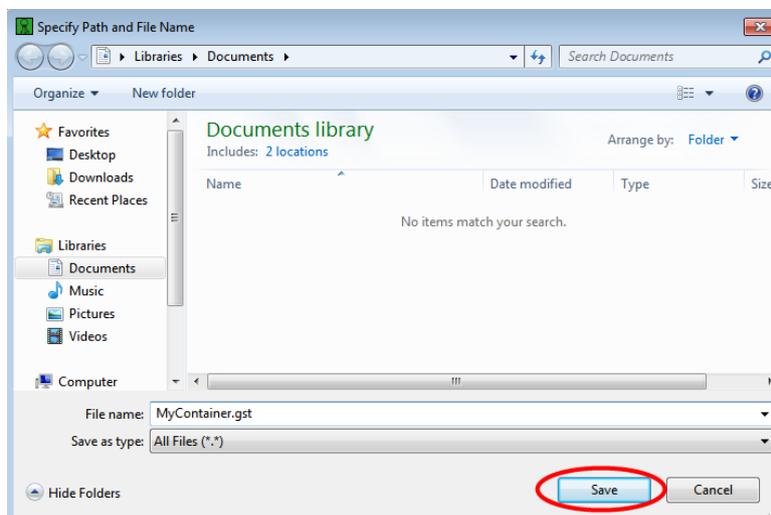


Figure 2.5: Use the “Save file” dialog for easy navigation

In the next dialog, the encryption algorithm and hash algorithm used to encrypt the file container can be chosen. This dialog also allows you to navigate to the “Test vector” dialog and “Benchmark” dialog. If you are unsure of the differences in the available algorithms, you can leave them as is and proceed to the next dialog.

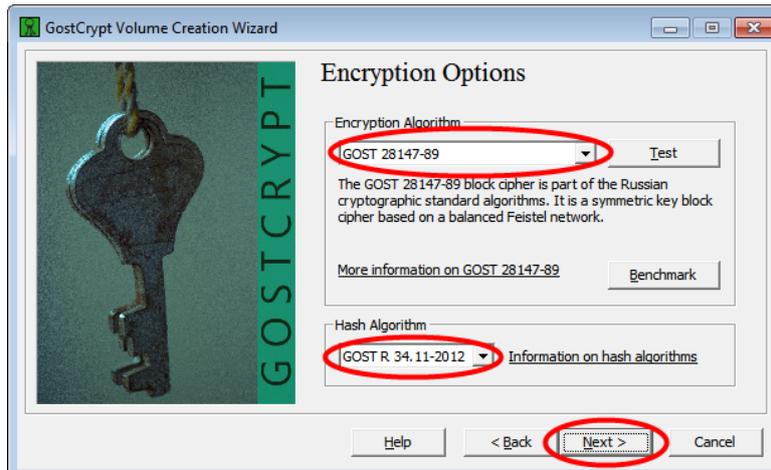


Figure 2.6: Select the preferred algorithms

You can now specify the size you want the file container to be. Specify a size in KB, MB or GB and click Next.

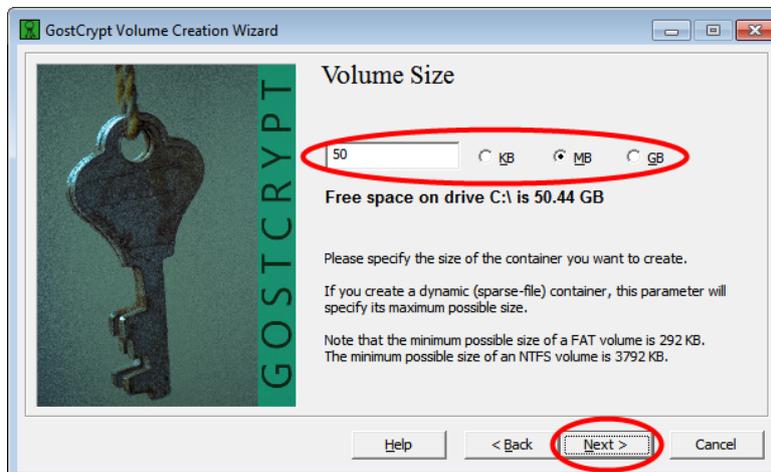


Figure 2.7: Specify the file container size

In the next dialog, you will be asked to enter the volume password. This is the password that will be used to calculate the volume header key. Make sure to follow the instructions this dialog provides on choosing a good password. You can also specify a keyfile here. For more information on keyfiles, see chapter 5.



Figure 2.8: Volume password

The Volume Format dialog is the final step in creating an encrypted file container. Here, you can specify the filesystem you want to use, as well as the cluster size. If you saved the file container on an NTFS filesystem, you also have the option to make the file container “dynamic”. Using this mode, the file container will not take up much disk space at first. Instead, it will grow as you write more data to it. Note that this mode makes the resulting GostCrypt volume slower in operation. It also allows adversaries to see how much data is in your GostCrypt volume, as it grows when data is added. If you are unsure about which options to choose here, the default settings will suffice for most use cases.

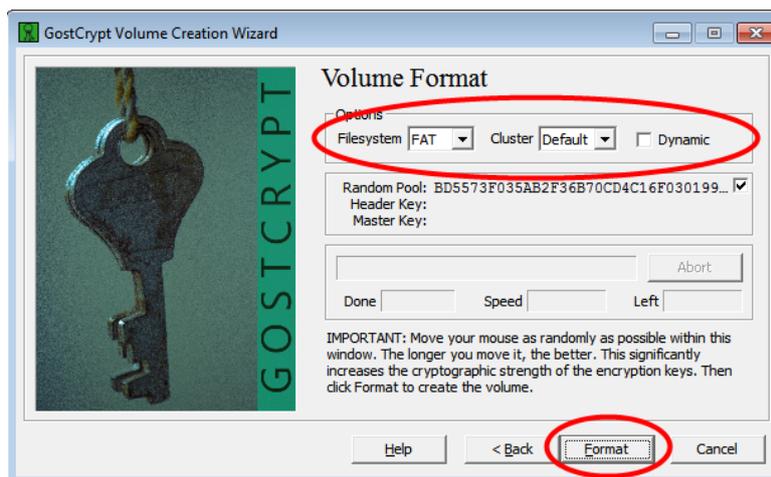


Figure 2.9: Volume format

The encrypted file container has now been created and you can exit out of the GostCrypt Volume Creation Wizard.



Figure 2.10: Volume created

Volume mounting

In order to start using the encrypted file container, go back to the starting window of GostCrypt. Here, you can select a free drive letter that GostCrypt will use for this file container. Next, click the “Select File” button and open the file container. Finally, click the “Mount” button.

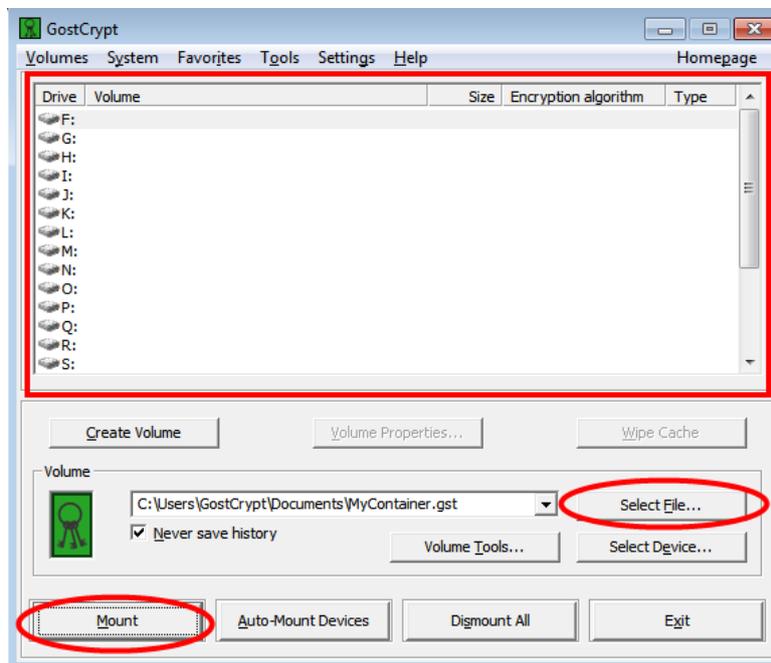


Figure 2.11: Mounting an encrypted file container

A dialog pops up which asks for the user password associated with the volume. Enter your previously specified password here. You can click “OK” to mount the volume.

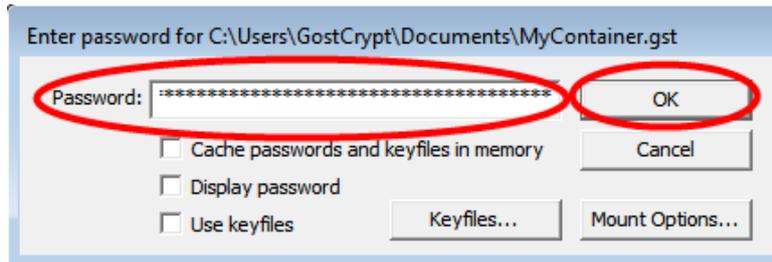


Figure 2.12: Volume mounting password dialog

The encrypted file container can now be accessed like a normal partition.

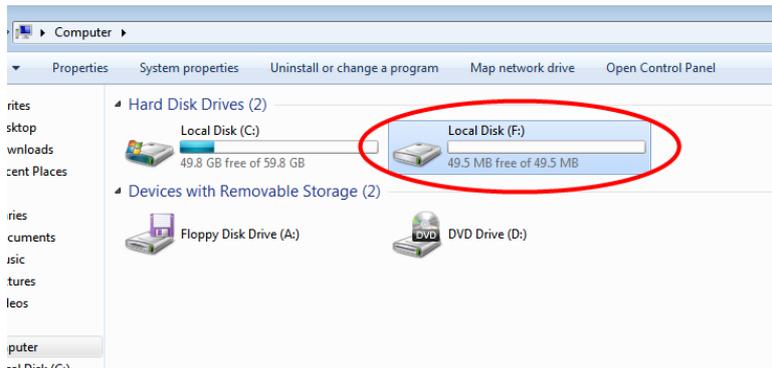


Figure 2.13: Encrypted file container mounted

2.2 Encrypted Partition / Drive

GostCrypt allows you to encrypt disk partitions and entire disk drives. The creation and mounting of partitions or drives follows the same rules associated with the creation of encrypted file containers. Follow the steps from the previous sections, but select the second or third option at the beginning of the *GostCrypt Volume Creation Wizard* and follow the instructions in the wizard.

GostCrypt also allows you to encrypt the partition on which Windows is installed, or even the entire drive from which Windows boots. Without encrypting the Windows partition, sensitive data about encrypted volumes might still be leaked by the Windows operating system (such as information about recently used files or even entire plaintext files that reside on an encrypted volume). Therefore, encrypting the Windows partition or entire Windows boot drive provides the highest level of security GostCrypt has to offer.

2.3 Hidden Volumes

Hidden volumes allows for plausible deniability in GostCrypt volumes. When you are forced to disclose your GostCrypt volume password, you can give the password to the overarching outer volume. Within this outer volume, a hidden volume is stored that is indistinguishable from the rest of the encrypted data in the outer volume. Only when you try to mount the volume with the password of the hidden volume, will GostCrypt recognize the presence of the hidden volume and mount it.

Creating a hidden volume in GostCrypt can be done using your preferred method of encryption using the *GostCrypt Volume Creation Wizard*. During this wizard, GostCrypt will ask if you want to create a hidden volume. Note that after the hidden volume has been created, writing data

to the outer volume might corrupt the underlying hidden volume. If you want to write data to the outer volume, make sure to mount it with the mount option *Protect hidden volume against damage caused by writing to outer volume* enabled and by providing the correct password for the hidden volume. This causes GostCrypt to mount the outer volume while also monitoring the area where the hidden volume resides, blocking any data being written to the hidden volume area.



3. Favorites

Favorite (system) volumes provides a mechanism of storing the location and mounting options of volumes, making it easier to mount them in the future. GostCrypt has two types of favorite volumes: regular favorite volumes and system regular volumes.

3.1 Favorite Volumes

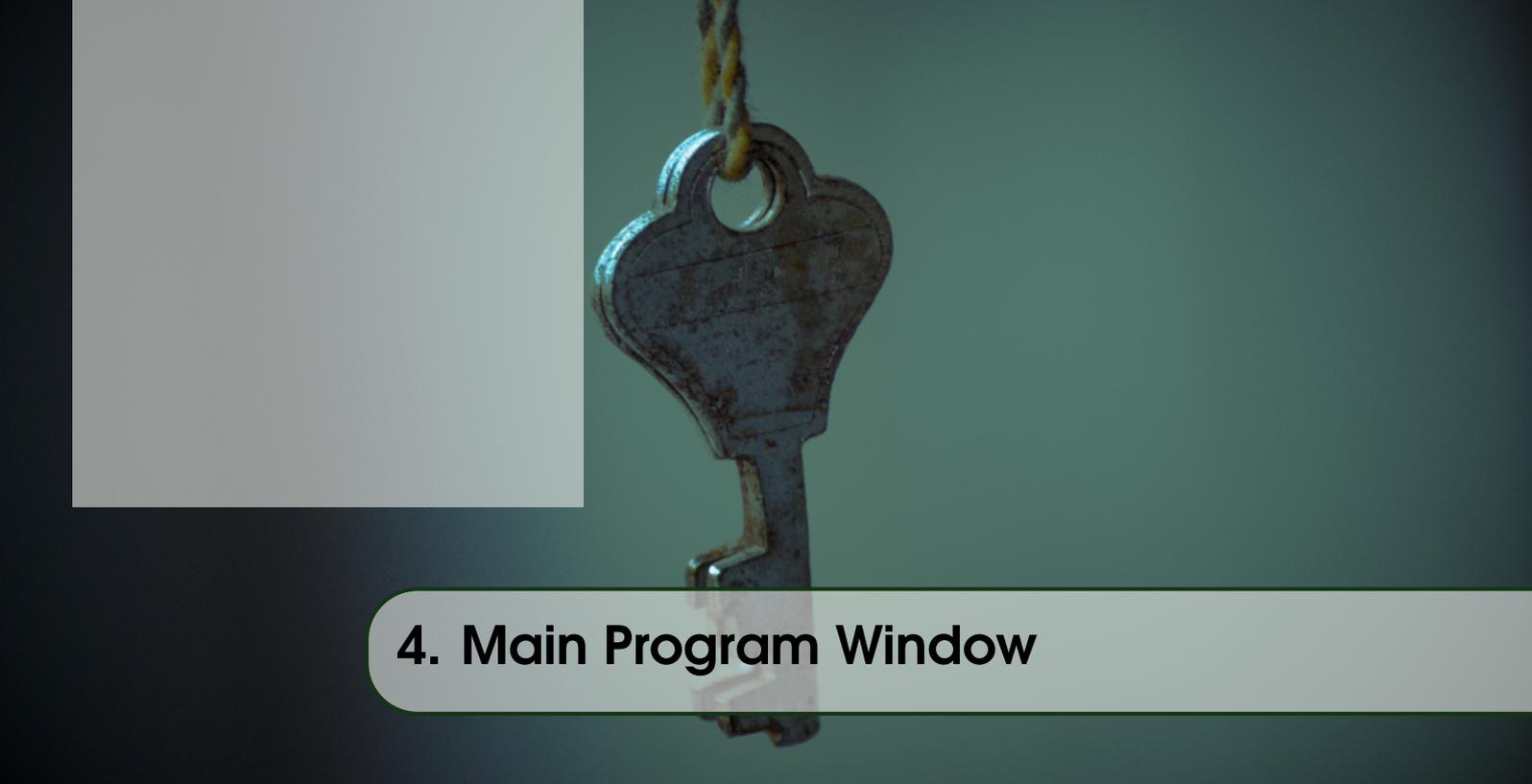
Favorite volumes are GostCrypt volumes that you want GostCrypt to remember. Favorite volumes can be mounted by pressing the *Mount Favorite Volumes* menu item or the menu item of your favorite volume in the *Favorites* menu of the main GostCrypt window.

Adding a GostCrypt volume to the list of favorite volumes can be done by selecting the volume from the list of mounted volume in the main GostCrypt window, right-clicking it and selecting the *Add to Favorites* menu item. In the *Favorite Volumes* menu, you can select mount options for the favorite volumes and give the volume a label. Note that this label is only used within GostCrypt to identify the favorite for the user.

3.2 System Favorite Volumes

System favorite volumes work in a similar fashion to regular favorite volumes, but they are mounted before the applications and services of the operating system load. This can be useful in scenarios where applications or services rely on a certain volume being available at launch. System favorite volumes can only be selected when system encryption is currently active and if the volume share a password with the pre-boot authentication password.

Adding a GostCrypt volume to the list of system favorite volumes can be done by selecting the volume from the list of mounted volumes in the main GostCrypt window, right-clicking it and selecting the *Add to System Favorites* menu item. In the resulting menu, you can select mount options and even forbid non-administrator users from dismounting or modifying the volume.



4. Main Program Window

Volumes

Select File

Allows the user to select a GostCrypt encrypted file container.

Select Device

Allows the user to select a GostCrypt encrypted partition or drive.

Create New Volume

Opens the *GostCrypt Volume Creation Wizard* that allows the creation of new GostCrypt volumes.

Resume Interrupted Process

Opens a previously interrupted process. For example, when in the process of performing full disk encryption, you can interrupt this process and resume it on a later date.

Mount Volume

Attempt to mount the selected partition, device or file container by asking for the user's password.

Mount Volume with Options

Attempt to mount the selected partition, device or file container by displaying mount options and asking for the user's password.

Auto-Mount All Device-Hosted Volumes

GostCrypt scans all available drives and partitions and attempts to mount them using the user supplied password or keyfile. As GostCrypt has to attempt all possible mounting configurations for each partition and drive, this process can take a long time on slow computers.

Dismount Volume

Dismounts the currently selected GostCrypt volume.

Dismount All Mounted Volumes

Dismounts all currently mounted GostCrypt volumes.

Change Volume Password

Enables the user to change the password used to derive the selected volume's header key and change the pseudo-random function used in the key derivation process. Note that for this process, the selected volume must be dismounted.

Add/Remove Keyfiles to/from Volume

Allows the addition or removal of keyfiles to the key used to decrypt the volume header of the GostCrypt volume.

Remove All Keyfiles from Volume

Allows the removal of all keyfiles currently used to decrypt the volume header of the GostCrypt volume.

Volume Properties

Shows the properties of the currently selected mounted GostCrypt volume. This view includes information about the size and location of the volume, as well as information about the used cryptographic algorithms.

System**Encrypt System Partition/Drive**

Starts the volume creation wizard for the encryption of the partition or drive on which Windows is currently running.

Permanently Decrypt System Partition/Drive

Decrypts the entire encrypted partition or drive on which Windows is currently running.

Resume Interrupted Process

Resumes a previously interrupted system encryption or decryption process.

Create Hidden Operating System

Starts the process of creating a hidden operating system within the encrypted area of another GostCrypt protected operating system. This feature provides plausible deniability. In situations in which the user is forced to disclose his or her GostCrypt volume password, the password of the non-hidden operating system can be given.

Create Rescue Disk

Starts the process of creating a new GostCrypt Rescue Disk for the currently encrypted Windows partition or drive.

Verify Rescue Disk

Verifies an already created GostCrypt Rescue Disk.

Mount Without Pre-Boot Authentication

Mounts the selected device that is part of the system encryption scheme of another operating system. The selected device is mounted as a regular GostCrypt volume.

Change Password

Changes the password of the current system encryption GostCrypt Volume Header.

Set Header Key Derivation Algorithm

Changes the header key derivation algorithm used for the currently mounted system encryption device.

Properties

Displays the GostCrypt volume properties of the current system encryption scope. The window includes information about the size of the device, as well as information about the used cryptographic algorithms.

Settings

Allows the user to change settings related to system encryption, such as enabling the caching of the pre-boot password or changing the message displayed during pre-boot authentication.

Favorites

Add Mounted Volume to Favorites

Adds the currently selected mounted GostCrypt volume to the list of favorite volumes. Favorite volumes can be mounted all at once, they remember their assigned drive letter and have remember several mount options.

Add Mounted Volume to System Favorites

Adds the currently selected mounted GostCrypt volume to the list of system favorite volumes. System favorite volumes are auto-mounted before Windows applications and services are starting during the boot process. The password for system favorite volumes must be the same as the pre-boot authentication password used for system encryption.

Organize Favorite Volumes

Displays the list of all favorite volumes and allows the modification of favorite volume related settings.

Organize System Favorite Volumes

Displays the list of all system favorite volumes and allows the modification of favorite volume related settings.

Mount Favorite Volumes

Mounts all favorite volumes by asking the user for the volume passwords or keyfiles.

Tools

Benchmark

Test the speed of the available encryption algorithms using a buffer of variable size to be encrypted.

Test Vectors

Manually test the output of the available block ciphers by providing all input parameters and validating the output.

Traveler Disk Setup

Copies the files necessary to run GostCrypt in portable mode to the destination (usually an USB key or CD / DVD).

Volume Creation Wizard

Opens the GostCrypt Volume Creation Wizard, which allows the creation of new GostCrypt volumes.

Keyfile Generator

Opens a wizard used to generate cryptographically strong pseudo-random keyfiles that can be used to protect GostCrypt volumes.

Manage Security Token Keyfiles

Manage the collection of available security token keyfiles. A security token keyfile can be supplied by a smart card or similar devices, using a PKCS#11 library from the device's vendor.

Close All Security Token Sessions

All currently used security token sessions are terminated.

Backup Volume Header

Creates a backup of the currently selected GostCrypt volume. Keep in mind that this backup will still work with the password used at the time the backup is created, even if you change the password of the GostCrypt volume at a later date.

Restore Volume Header

Allows the recovery of a GostCrypt volume using a backup header file that was created on an earlier date.

Refresh Drive Letters

Obtains an up-to-date list of the currently available drive letters on the system.

Clear Volume History

If GostCrypt was configured to remember previously used volumes, this option clears the volume history.

Wipe Cached Passwords

If GostCrypt was configured to cache used passwords, this option clears the password cache.

Settings**Language**

Brings up the language selection screen. If language packs are installed (by copying language packs into the GostCrypt install directory), other languages can be selected from this menu.

Hot Keys

Allows the user to designate key combinations to trigger certain actions within GostCrypt.

System Encryption

Allows the user to change settings related to system encryption.

System Favorite Volumes

Allows settings related to favorite volumes to be changed.

Performance

Allows for the modification of the amount of CPU cores to be used by GostCrypt for encryption and decryption.

Default Keyfiles

Shows the list with currently remembered keyfiles used for mounting GostCrypt volumes.

Security Tokens

Shows the settings related to security tokens, such as the location of the security token library to use.

Preferences

General preferences of GostCrypt. The user can select GostCrypt-wide mount options, windows behavior and cache management.



5. Keyfiles

Keyfiles are additions or replacements for the regular passwords used to mount GostCrypt volumes. Keyfiles are often a lot larger than regular passwords and contain a higher level of randomness. Keyfiles can be stored on an external device, like a USB key or smart card. It is strongly advised not to store keyfiles on the same medium as the GostCrypt volume, as this will allow potential attackers to trivially decrypt the GostCrypt volume.

Generating keyfiles can be done using GostCrypt, by going to the *Tools* menu in the main GostCrypt window and selecting the *Keyfile generator* menu item. After moving your mouse in order to increase the cryptographic strength of the resulting keyfile, press the *Generate and Save Keyfile* button and store the resulting keyfile to a safe location.

When creating a new GostCrypt volume or changing the password on an existing one, check the *Use keyfiles* checkbox and click the *Keyfiles* button in order to add one or more keyfiles to the password.



6. Encryption Algorithms

| Encryption Algorithm | Key size (bits) | Block size (bits) |
|----------------------|-----------------|-------------------|
| GOST 28147-89 | 256 | 64 |

Table 6.1: Encryption Algorithms in GostCrypt

6.1 GOST 28147-89

The GOST 28147-89 block cipher is part of the Russian cryptographic standard algorithms. The block cipher was standardized as a *Gosudarstvennyi Standart (GOST)* in 1989 and was declassified and made public in 1994. It was developed to be an alternative to the U.S. Data Encryption Standard (DES) and shares properties with this algorithm.

GOST 28147-89 is, like DES, a symmetric key block cipher based on a balanced Feistel network. The block size of the algorithm is 64 bits and it uses a 256 bit key, which is split into eight 32 bit subkeys.



7. Hash Algorithms

| Hash Algorithm | Digest size (bits) | Block size (bits) |
|-------------------|--------------------|-------------------|
| GOST R 34.11-2012 | 512 | 512 |
| GOST R 34.11-94 | 256 | 256 |
| Whirlpool | 512 | 512 |

Table 7.1: Hash Algorithms in GostCrypt

7.1 GOST R 34.11-2012

The GOST R 34.11-2012 hash function is part of the Russian cryptographic standard algorithms. It is the official successor of the GOST R 34.11-94 algorithm and was implemented on 1 January 2013. The standard uses the “Stribog” hash function, developed by the *Federal Security Service* (FSB) and InfoTeKS. While the structure of Stribog is very similar to the GOST R 34.11-94 hash function, its compression function is very different. The compression function in a hash algorithm is the function that mixes potentially large amounts of data into a single, small digest (hash output). Stribog uses an algorithm that is similar to Rijndael in its compression function, which is the block cipher used in AES. The GOST R 34.11-94 hash function uses GOST 28147-89 as its block cipher for its compression function.

7.2 GOST R 34.11-94

The GOST R 34.11-94 hash function is part of the Russian cryptographic standard algorithms. It was standardized as a *Gosudarstvennyi Standart* (GOST) in 1994.

The GOST R 34.11-94 hash function makes extensive use of the GOST 28147-89 block cipher as part of its compression function.

7.3 Whirlpool

Whirlpool is a hash function designed by Vincent Rijmen and Paulo S. L. M. Barreto in 2000. It was identified as a recommended hash function by the NESSIE, a research project funded by the European Union between 2000 and 2003. It has since been standardized by ISO and IEC as the ISO/IEC 10118-3 international standard.

The Whirlpool hash function is a Merkle-Damgård construction based on AES. It uses an internal block size of 512 bits and produces a 512 bit digest.



8. Command Line Usage

This section covers the available command line flags that can be used with the Windows application `GostCrypt.exe` and `GostCrypt Format.exe`.

8.1 GostCrypt.exe

/help or */?* Display command line help.

/volume or */v* File and path name of a GostCrypt volume to mount (do not use when dismounting). To mount a partition/device-hosted volume, use, for example, */v \Device\Harddisk1\Partition3* (to determine the path to a partition/device, run `GostCrypt` and click *Select Device*). You can also mount a partition or dynamic volume using its volume name (for example, */v \\?\Volume{5cceb196-48bf-46ab-ad00-70965512253a}*). To determine the volume name use e.g. `mountvol.exe`. Also note that device paths are case-sensitive.

/letter or */l* Drive letter to mount the volume as. When */l* is omitted and when */a* is used, the first free drive letter is used.

/explore or */e* Open an Explorer window after a volume has been mounted.

/beep or */b* Beep after a volume has been successfully mounted or dismounted.

/auto or */a* If no parameter is specified, automatically mount the volume. If *devicesc* is specified as the parameter (e.g., */a devicesc*), auto-mount all currently accessible device/partition-hosted GostCrypt volumes. If *favorites* is specified as the parameter, auto-mount favorite volumes. Note that */auto* is implicit if */quit* and */volume* are specified. If you need to prevent the application window from appearing, use */quit*.

/dismount or */d* Dismount volume specified by drive letter (e.g., */d x*). When no drive letter is specified, dismounts all currently mounted GostCrypt volumes.

/force or */f* Forces dismount (if the volume to be dismounted contains files being used by the system or an application) and forces mounting in shared mode (i.e., without exclusive access).

/keyfile or */k* Specifies a keyfile or a keyfile search path. For multiple keyfiles, specify e.g.: */k c:\keyfile1.dat /k d:\KeyfileFolder /k c:\kf2*. To specify a keyfile stored on a security token or smart card, use the following syntax: *token://slot/SLOT_NUMBER/file/FILE_NAME*.

/tokenlib Use the specified PKCS #11 library for security tokens and smart cards.

- /cache* or */c y* or no parameter: enable password cache; *n*: disable password cache (e.g., */c n*). Note that turning the password cache off will not clear it (use */w* to clear the password cache).
- /history* or */h y* or no parameter: enable saving history of mounted volumes; *n*: disables saving history of mounted volumes (e.g., */h n*).
- /wipecache* or */w* Wipes any passwords cached in the driver memory.
- /password* or */p* The volume password. If the password contains spaces, it must be enclosed in quotation marks (e.g., */p 'My Password'*). Use */p ''* to specify an empty password. *Warning: This method of entering a volume password may be insecure, for example, when an unencrypted command prompt history log is being saved to unencrypted disk.*
- /quit* or */q* Automatically perform requested actions and exit (main GostCrypt window will not be displayed). If *preferences* is specified as the parameter (e.g., */q preferences*), then program settings are loaded/saved and they override settings specified on the command line. */q background* launches the GostCrypt Background Task (tray icon) unless it is disabled in the Preferences.
- /silent* or */s* If */q* is specified, suppresses interaction with the user (prompts, error messages, warnings, etc.). If */q* is not specified, this option has no effect.
- /mountoption* or */m ro* or *readonly*: Mount volume as read-only. *rm* or *removable*: Mount volume as removable medium. *ts* or *timestamp*: Do not preserve container modification timestamp. *sm* or *system*: Without pre-boot authentication, mount a partition that is within the key scope of system encryption (for example, a partition located on the encrypted system drive of another operating system that is not running). Useful e.g. for backup or repair operations. Note: If you supply a password as parameter of */p*, make sure that the password has been typed using the standard US keyboard layout (in contrast, the GUI ensures this automatically). This is required due to the fact that the password needs to be typed in the pre-boot environment (before Windows starts) where non-US Windows keyboard layouts are not available. *bk* or *headerbak*: Mount volume using embedded backup header. Note: All volumes created by GostCrypt contain an embedded backup header (located near the end of the volume). *recovery*: Do not verify any checksums stored in the volume header. This option should be used only when the volume header is damaged and the volume cannot be mounted even with the mount option *headerbak*. Example: */m ro*. To specify multiple mount options, use e.g.: */m rm /m ts*.

8.2 GostCrypt Format.exe

- /noisochek* or */n* Do not verify that GostCrypt Rescue Disks are correctly burned. **WARNING:** *Never attempt to use this option to facilitate the reuse of a previously created GostCrypt Rescue Disk.* Note that every time you encrypt a system partition/drive, you must create a new GostCrypt Rescue Disk even if you use the same password. A previously created GostCrypt Rescue Disk cannot be used as it was created for a different master key.



9. Encryption Scheme

When GostCrypt tries to mount a volume using the user supplied password, the following steps are performed:

1. The GostCrypt Volume Header (the first 512 bytes of the volume) are read into RAM. For system encryption, the last 512 bytes of the first logical drive track are read into RAM instead, as this area contains the GostCrypt Volume Header when using system encryption.
2. From byte 65536 for regular volumes or 65536 for system encryption, 512 bytes are read into RAM. This is the location where the GostCrypt Volume Header resides if the volume contains a hidden volume.
3. GostCrypt cannot derive which encryption algorithm, mode of operation or pseudo-random function (PRF, used in the header derivation function) was used to encrypt the volume. Therefore, all possible combinations are attempted until a combination of encryption algorithm, mode of operation and PRF results in a decrypted GostCrypt Volume Header. This process is first attempted on the data read in step (1).
4. If step (3) fails, it is repeated, but using the volume header area obtained in step (2) instead.
5. Given that one of the two GostCrypt Volume Headers was decrypted, the primary master key (and secondary master key, in the case of the XTS mode of operation) is extracted from the header. These keys are used for encryption and decryption of the data that is protected by the GostCrypt Volume. The cryptographic data used to decrypt the GostCrypt volume header is removed from RAM, the primary master key (and secondary master key) are kept in kernel memory and the volume is mounted.

