Transport Encoding/Decoding and Cryptographic Protection of Computer Storage

Introduction

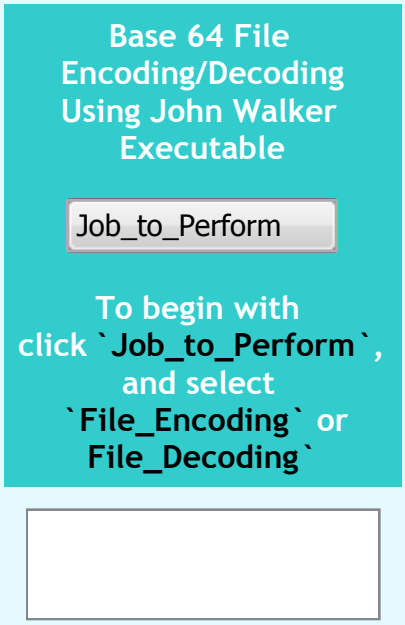
The presented Maple worksheet contains two user-friendly useful applications. Running them requires the use of the left mouse button only. The first application performs `**Base 64 File Encoding/Decoding**`. The `**Base 64**` format is useful for encoding arbitrary binary information, such as, for example, *.exe files, encrypted messages, cryptographic keys and audio and image files, for transmission by electronic mail. The application is contained in the section `**Base 64 File Encoding/Decoding**`. It relies on the freeware executable published by John Walker ((https://www.fourmilab.ch/webtools/base64/) and it enables the user to encode/decode an arbitrary file. A file encoded to the `base 64` format has its original file name with a `b64` extension added. While performing encoding/decoding the input file has been removed.

The second application, named `**Strong Computer Storage Cryptographic Protection**`, is mainly a proposition for non-computer science specialists (linguists, economists, clergymen, etc.) who store secret data on their computers. It performs the following tasks: `**Folder_Encryption**`, `**Folder_Decryption**`, `**Name_Decryption**` or `**Secret_Key**`. The plain-text files to be cryptographically protected should be stored in the folder having no sub-folders. The user can also determine the folder without sub-folders where the encrypted files will be saved. It should be noted that the folder for encrypted files must not be the same as the one for plain-text files. The application encrypts the names of the plain-text files (thus the format of the plain-text file is hidden) and their contents as well. The cryptographic key of the application is made of the `**AE**` and

`**AD**` Arrays, the list of integers `key` and the integer `**sd**`. Obviously, the user should substitute these variables by his own data calculated using the `**Secret_Key**` option. The key space for the procedures `**encdir**` and `**decdir**` (which use a quasigroup-based stream cipher) is very large (about 5000 bits), and, therefore, the encrypted contents of the file is unbreakable in practice. The task `**Folder_Decryption**` executes the decryption of all files stored in the folder. The option `**Name_Decryption**` deciphers the encrypted file names stored in the selected folder. It is also possible to decrypt one file or several files. Since this application contains a secret key, it should be copied to the carefully minded USB flash drive, whereas the encrypted folder can be stored anywhere (hard disk, pen drive, Microsoft `OneDrive`, etc.).

To run the application the user should open the section `**Base 64 File Encoding/Decoding**` or `**Computer Storage Cryptographic Protection**`. While opening the sections the user can see easy-to-use GUI`s. The applications must have permission to save files in the selected folders and the processed files must not be `read only`.

Base 64 File Encoding/Decoding



Computer Storage Cryptographic

Protection

Computer Storage Cryptographic Protection

Job_to_Perform

To begin with click `Job_to_Perform`, and select `Folder_Encryption`, Folder_Decryption`, `Name_Decryption` or `Secret_Key`

References

Acknowledgement

Notice