USER MANUAL

VIA CRYPTOGRAPHY COURSE WORK

v.1.0

12.12.2022

TABLE OF CONTENTS

1. INTRODUCTION

As a part of the Introduction to Cryptography course at Vidzeme University of Applied Sciences, third course students developed an encryption/decryption program to learn AES and DES encryption standards.

AES stands for Advanced Encryption Standard. DES stands for Data Encryption Standard. Both DES and AES are symmetric-key block ciphers that are used in encryption where just one key (the secret key) is utilized to encode and decode electronic data.

1.1. BENEFACTORS

- Students interested in encryption standards
- Cybersecurity enthusiasts
- Cryptography enthusiasts

1.2. KEY FEATURES

- User friendly graphical interface (GUI)
- Fast encryption/decryption
- Open-source code
- No fees are associated with using this program

2. REQUIREMENTS

2.1. MINIMUM PC REQUIREMENTS

The minimum requirements for running the software are listed below:

- Operating System:
    - Windows 7/10
    - Mac OS X 10.11 or higher, 64-bit
    - Linux RHEL 6/7, 64-bit
- x86 64-bit CPU (Intel / AMD architecture)
- 4 GB RAM
- 10 MB free disk space
- Python support*

2.2. PYTHON

Python is an interpreted, object-oriented, high-level programming language with dynamic semantics. Its high-level built-in data structures, combined with dynamic typing and dynamic binding, make it attractive for Rapid Application Development, as well as for use as a scripting or glue language to connect existing components together. Python's simple, easy to learn syntax emphasizes readability and therefore reduces the cost of program maintenance. Python supports modules and packages, which encourages program modularity and code reuse. The Python interpreter and the extensive standard library are available in source or binary form without charge for all major platforms and can be freely distributed.

Download Python from the official website: https://www.python.org/downloads/

3. GETTING STARTED

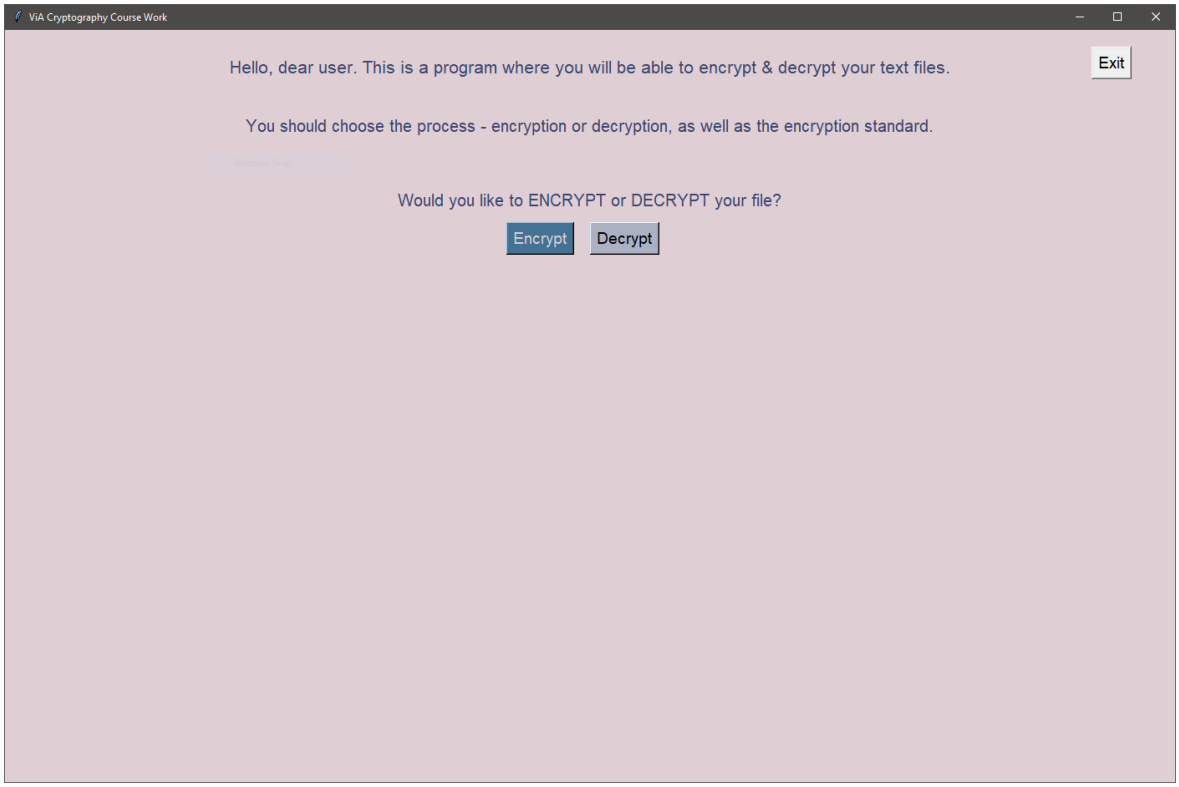
3.1. DOWNLOAD THE SOFTWARE

The program is hosted on https://www.github.com/ - an Internet hosting service for software development and version control using Git. It provides the distributed version control of Git plus access control, bug tracking, software feature requests, task management, continuous integration, and wikis for every project.

1. Navigate to *releases* page of projects GitHub website at https://github.com/EgijaG/ViACryptographyCourseWork
2. Ensure that the system requirements of the computer or laptop in use, meet those listed on the page.
3. Click on the relevant download icon.
4. If anti-virus software is installed on the computer, it may ask for confirmation that the download is allowed.
5. Once the file is downloaded, start the program by running the *UserInterface.py*.

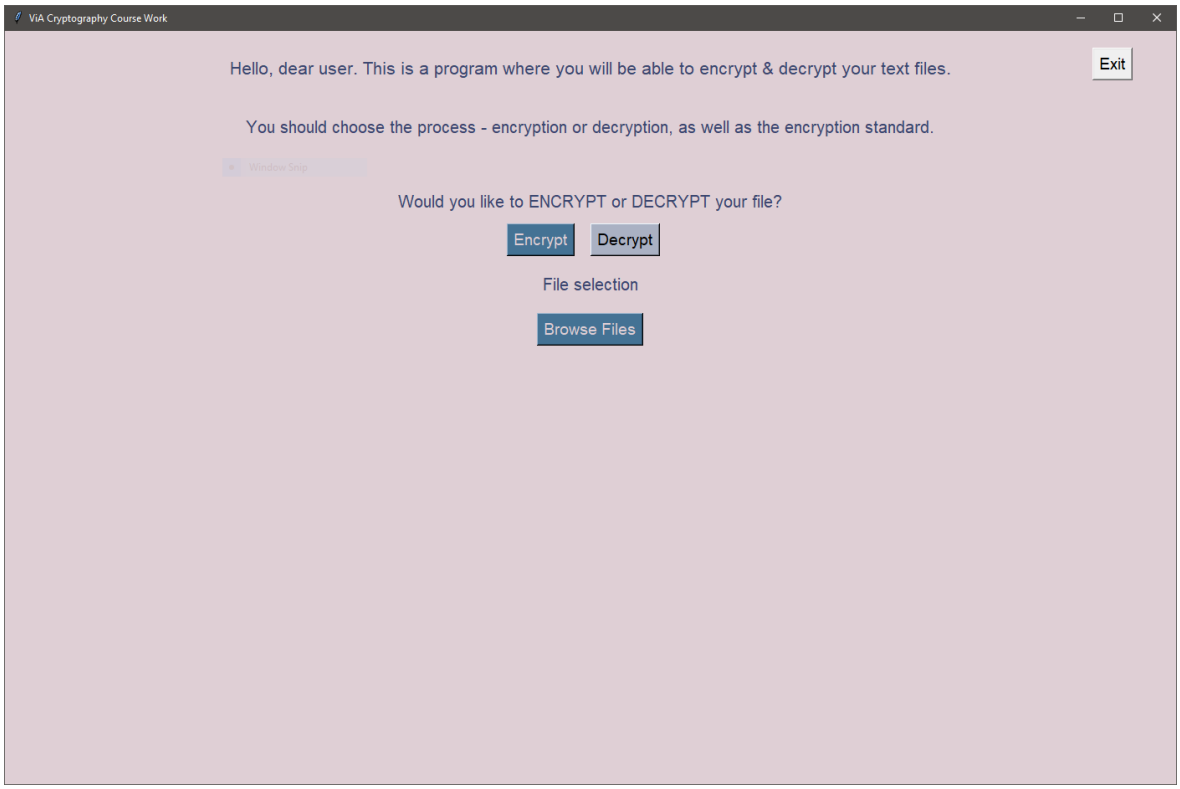
3.2. USING THE SOFTWARE

1. After launching the program from *UserInterface.py* you will see starting screen. Follow the on-screen prompt to either choose encryption or decryption mode.



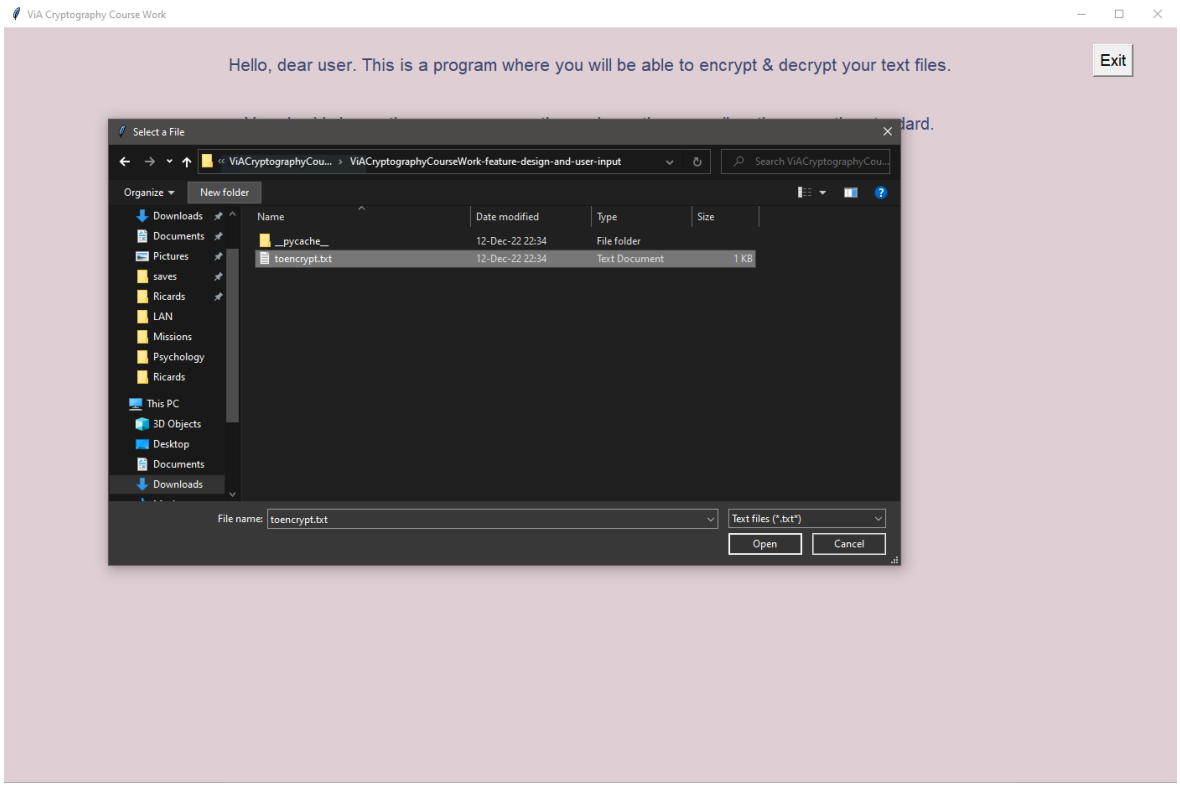
Picture 1Main Screen

2. A button “Browse Files” will appear. Click it to open File explorer.



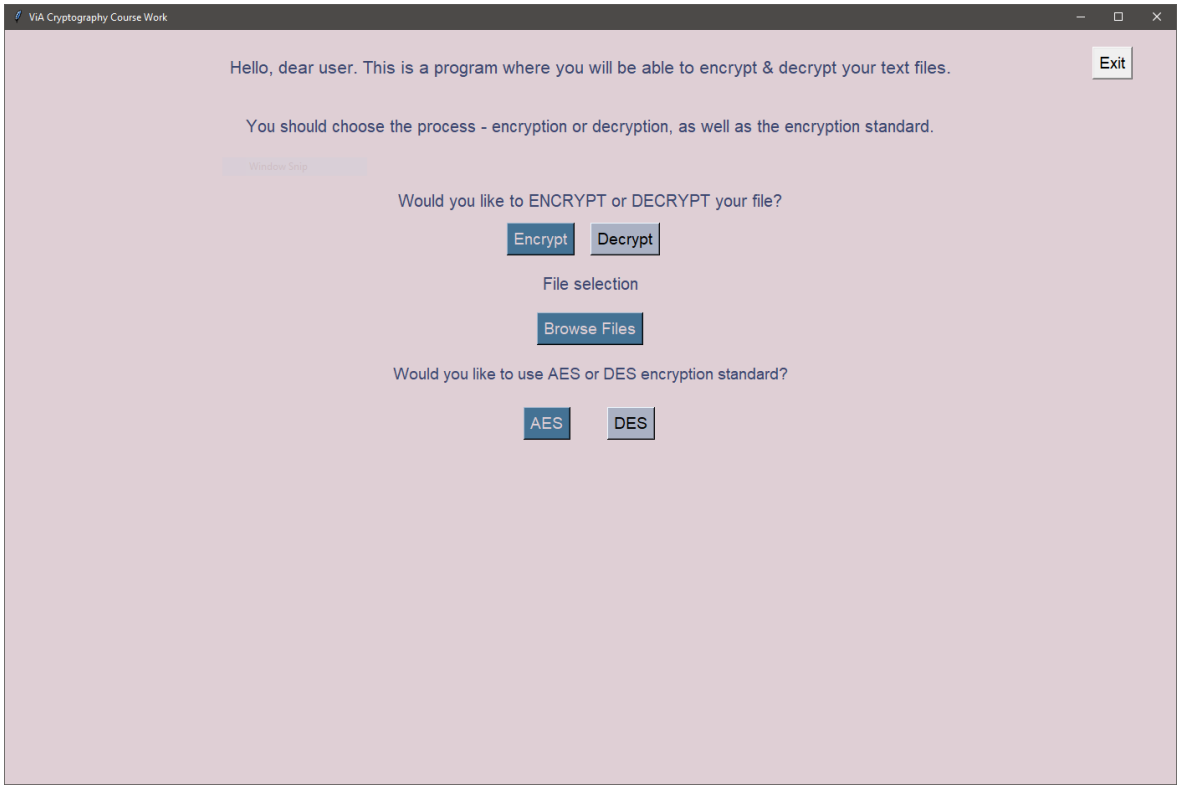
Picture 2 Browse Files button

3. Use the File explorer to choose the file you wish to either encrypt or decrypt.



Picture 3 File exlorer screen

4. After choosing the file, a prompt will show asking to choose between AES or DES encryption standards. Use the button to encrypt or decrypt the chosen file.



Picture 4 Encryption standart prompt

4. RECOMMENDATIONS

1. Check the aforementioned *releases* page regularly to download most up to date software version.
2. After using the program, delete unnecessary files.
3. Don’t use this software for actual security-related tasks, as it is in early development stage and might be susceptible to bugs and errors.

5. SUPPORT

The support page can be viewed on the program's website hosted at https://github.com/EgijaG/ViACryptographyCourseWork/ under the Issues menu.

All bugs, issues and unexpected issues can be reported there using built-in report page.

APPENDIX A: RECORD OF CHANGES

Table 1. – Record of changes.

Version number	Date	Author/Owner	Desc. of change
v.1.0	12.12.2022	ViA IT3	Initial release

APPENDIX B: GLOSSARY

Table 1. – Glossary.

Term	Acronym	Definition
Advanced Encryption Standard	AES	Specification for the encryption of electronic data
Central processing unit	CPU	Electronic machinery that carries out instructions from programs that allows a computer or other device to perform its tasks
Data Encryption Standard	DES	Symmetric-key algorithm for the encryption of digital data
Git	Git	Distributed version control system: tracking changes in any set of files, usually used for coordinating work among programmers collaboratively developing source code during software development
Graphical user interface	GUI	Form of user interface that allows users to interact with electronic devices through graphical icons and audio indicator such as primary notation, instead of text-based UIs, typed command labels or text navigation
Megabyte	MB	Multiple of the unit byte for digital information
Random-access memory	RAM	Form of computer memory that can be read and changed in any order, typically used to store working data and machine code
Vidzemes Augstskola	VIA	Vidzeme University of Applied Sciences