My goal for this application is for it to be as user-friendly as possible, but also feature-rich and robust enough for use by professional cryptographers.

En/decryptor

IT PAT PHASE 1  
**GR.11 2021**

Waldo Lemmer

**Submission date on/before 30 JULY 2021**

Contents

[Task description 2](#_Toc71629600)

[User requirements 3](#_Toc71629601)

[Flow diagram 4](#_Toc71629602)

[Database design (Optional) 4](#_Toc71629603)

[Graphical User Interface (GUI) 5](#_Toc71629604)

[Data Dictionary 6](#_Toc71629605)

[Input, Processing and Output (IPO) 7](#_Toc71629606)

[**Annexure B** 8](#_Toc71629607)

[**Learner declaration – Phase \_\_\_\_** 8](#_Toc71629608)

[**Annexure A: Assessment Tools** 0](#_Toc71629609)

## Task description

I was given the task to develop a program that encrypts messages using a cipher and decrypts messages using the same cipher. For example, if someone sends an encrypted message to another person, that person must be able to use the program to decrypt the message.

The program supports 5 different ciphers with varying levels of security and efficiency. The program uses these ciphers to encrypt/decrypt a message. Some ciphers allow the use of a custom key or offset which increases security even further when used correctly (and responsibly). The ciphers are:

* ROT-13
  + Very fast
  + Very insecure
* Caesar cipher
  + Fast
  + Insecure
  + Optional offset improves security
* Waldo’s shuffling cipher
  + Medium speed
  + Secure
  + Optional numerical “seed” improves security
* Simple substitution cipher
  + Slow
  + Very secure
  + Optional 95-character alphanumeric key improves security
* One-time pad
  + Very slow
  + Virtually uncrackable
  + Alphanumeric secure key (“OTP”) required

The program will provide various methods of entering and retrieving text:

* Text boxes
* Copy/Paste buttons
* Importing/exporting text files

## User requirements

|  |  |
| --- | --- |
| User 1 | |
| Who is the user? | Message sender/receiver |
| Role of user: | Writes/reads messages |
| Activities of user: | Uses the program to encrypt a message before sending or decrypt a message after receiving |
| Limitation of user: | Not very experienced with ciphers and computing. A user-friendly GUI is a must. |

|  |  |
| --- | --- |
| User 2 | |
| Who is the user? | Cryptographer |
| Role of user: | Enjoys cracking and/or examining ciphers |
| Activities of user: | Examines the program’s output, tries cracking encrypted text. |
| Limitation of user: | Requires a vast feature set with great customisability |

## Flow diagram

## Graphical User Interface (GUI)

## Data Dictionary

Explain the working of the database (optional), text files (must use at least 1 file), Classes and objects (must contain at least 1 class) and other data structures (such as arrays).

Text file

Database (Optional)

Array(s)

## Input, Processing and Output (IPO)

Use IPO tables of at least two forms to explain the Input, processing and output of the specific form.  
Include data validation and error messages. See rubric for specific instructions.

|  |  |  |
| --- | --- | --- |
| Input | Processing | Output |
|  |  |  |
|  |  |  |

**Annexure B**

**Learner declaration – Phase \_\_\_\_**

I understand that work submitted for assessment must be my own.

Have you received help/information from anyone to produce this work?

□No □Yes (provide details below)

|  |  |
| --- | --- |
| Help/information received from (person): | Nature of the help/information (provide evidence): |
|  |  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_ / \_\_\_ / 2021  Signature of Learner Date | |

**Annexure A: Assessment Tools**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Phase 1: Name of learner:** | | | | | | | |
| **Scenario/Scope**  **(± 200 words)** | **4** | **3** | **2** | **1** | **0** |  |  |
| **Scenario and Scope**   * Topic is clearly stated. * Thorough description of what the problem/task involves (purpose). * Describe a possible solution for the problem/task. * Brief description of the scope. | An excellent presentation of all FOUR points listed | All FOUR points were presented with short comings  OR  A good presentation of THREE points | THREE points were presented with short comings  OR  A good presentation of TWO points | TWO points were presented with short comings  OR  A good attempt to present ONE of the points | Totally inadequate or not applicable  Poor or no coverage of aspects.  No scope or extremely vague and unclear | **4** |  |
| **User Requirements** | **4** | **3** | **2** | **1** | **0** |  |  |
| State WHO the users are.  Role, activity and  limitations of the users  (In table format or a use case diagram) | * Role, activity and limitations of at least TWO different types of users of the system discussed. * Well documented, neat and to the point. | * Minor shortcomings in discussion of role, activity and limitations of at least TWO different types of users of the system. * Documented well but can improve slightly. | * Shortcomings in discussion of role, activity and limitations of users, for example sections left out. * Only ONE user of the system discussed. * Not well documented but still acceptable. | * Major shortcomings in discussion of role, activity and limitations of users. * Only ONE user of the system discussed. * Poorly documented – not acceptable. | * Not done or incorrect or irrelevant. | **4** |  |
| **Navigation/Description of flow diagram** | **4** | **3** | **2** | **1** | **0** |  |  |
| **A diagrammatical representation of the design and flow of events when the program is used** | An excellent attempt to show the sequence of all steps and flow of events when the program is executed with no shortcomings. | A good attempt to show the sequence of all steps and flow of events when the program is executed with minor shortcomings. | A satisfactory attempt to show the sequence of steps and flow of events when the program is executed with significant shortcomings. | A poor attempt to show the sequence of steps and flow of events when the program is executed with major shortcomings. | No diagram OR incorrect, irrelevant or unsuitable for the application. | **4** |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **DATA STRUCTURES** | **4** | **3** | **2** | **1** | | | **0** |  |  |
| **Database design (optional)**   * All fields are relevant * Type and size of fields well-chosen   (Makes total 48 or 44 without) | All database design requirements met. A well designed database. | Good database design with minor shortcomings. | Average design with several shortcomings | Database design done, but with limited value. | | | No database or incorrect or irrelevant. | **4** |  |
| **Text files(s)** | Excellent and relevant description of use of a text file(s). | Good description of use of a text file | Relevant description of use of a text file with some shortcomings | An attempt to describe the use of a text file with many shortcomings. | | | Not done or incorrect or irrelevant. | **4** |  |
| **Array/(s)** | Excellent and relevant description of use of an array. | Good description of use of an array. | Relevant description of use of an array | An attempt to describe the use of an array with shortcomings. | | | Not done or incorrect or irrelevant. | **4** |  |
| **GUI Design** | **4** | **3** | **2** | **1** | | | **0** |  |  |
| * Design fits to program's intended use * Appropriate components * Ease of use, logical flow * Clearly marked navigation * Friendly dialogue/Help | Good GUI design, all of the listed principles applied throughout the system e.g. with data capturing, output, navigation, etc. | Satisfactory GUI design, most (at least 4) of the principles applied throughout the system e.g. with data capturing, output, navigation, etc. | Limited GUI design, most (at least 3) of the principles applied throughout the system e.g. with data capturing, output, navigation, etc. | | Poor GUI design applied less than 50% (less than 3) of the principles. | GUI design is not functional or does not support the intended use at all. | | **4** |  |
| **Data Input** | **4** | **3** | **2** | | **1** | **0** | |  |  |
| **Input interfaces (at least TWO)**   * Source of input, such as from the keyboard, text file, array or the database. * Data type * Format of the input for example date, gender (M/F). * GUI component used. | Clearly describes all inputs according to all FOUR points listed | Minor shortcomings in describing all inputs according to all FOUR points listed | Clear description according to THREE points listed  OR  Major shortcomings in describing all inputs according to all FOUR points listed | | Poor attempt to describe input values | No inputs described  OR  Incorrect | | **4** |  |
| **Input Validation**   * At least THREE different data types validated * At least THREE inputs validated including: * Validate for NULL/empty field AND * Test if value was selected in a selection component * Associated error messages | Clearly describes all points listed | Clearly describes TWO points listed  OR  Minor shortcomings in describing all points listed | Clearly describes ONE points listed  OR  Major shortcomings in describing all points listed | | Poor attempt to describe validation | No validation described  OR  Incorrect | | **4** |  |
| **Data Processing** | **4** | **3** | **2** | | **1** | **0** | |  |  |
| **WHAT** processing will need to be done | Clearly lists at least SIX processes to be done. | One or two processes not listed. | About 50% of the processes listed. | | Only one or two processes listed. | No processes listed | | **4** |  |
| **How** Processing Will Be Done – Supply Algorithms, Formulas, Etc. | Clearly describes how at least FOUR processes will be done. | Clearly describes how THREE processes will be done | Clearly describes how TWO processes will be done.  OR  An attempt to describe how FOUR processes will be done. | | Clearly describes how ONE process will be done.  OR  A poor attempt to describe TWO or THREE processes. | Processes not described/ incorrect or irrelevant | | **4** |  |
| **Data Output** | **4** | **3** | **2** | | **1** | **0** | |  |  |
| **Output interfaces (at least TWO)**   * Data to output * Format of the output, for example currency, date. * Output component, such as dbGrid, rich edit, label, etc. | Clearly describes all outputs by addressing all THREE points listed | Minor shortcomings in describing all outputs by addressing all THREE points listed | Clear description of all outputs by addressing TWO points listed  OR  Limited outputs described | | Poor attempt to describe outputs | No output described  OR  Incorrect | | **4** |  |
| **TOTAL** | | | | | | | | **48 or 44** |  |

|  |
| --- |
| **Comments/feedback:**      **Teacher name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Teacher signature: :\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |

