Руководство пользователя

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ

1.2 Область применения

Компьютерное приложение «CRYPTOGRAPHER» может применяться малыми организациями и частными лицами для защиты конфиденциальных данных и позволяет решать следующие задачи:

- шифрование файлов пользователя с предоставлением ключа шифрования,
- расшифровка зашифрованных фалов с помощью ранее предоставленного ключа шифрования.

1.2 Краткое описание возможностей

Компьютерное приложение «CRYPTOGRAPHER» обеспечивает защиту конфиденциальной информации пользователей, в том числе при хранении её на внешних носителях, используя, предоставленные приложением, алгоритмы шифрования.

1.3 Уровень подготовки пользователя

Для успешного использования системы пользователи должны иметь навыки работы на персональных компьютерах с различными операционными системами, а также с любой интегрированной средой разработки Python.

1.4 Перечень эксплуатационной документации

Руководство пользователя компьютерного приложения для шифрования и расшифровки данных «CRYPTOGRAPHER».

2 НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ

2.1 Виды деятельности, функции

Компьютерное приложение «CRYPTOGRAPHER» позволяет пользователю зашифровывать и расшифровывать файлы с помощью алгоритмов шифрования Triple DES, AES, RSA.

2.2 Условия применения

Для обеспечения нормального функционирования компьютерного приложения «CRYPTOGRAPHER» рекомендуется следующая конфигурация системы:

- 2 Gb оперативной памяти,
- 1 Gb свободного дискового пространства.

3 ПОДГОТОВКА К РАБОТЕ

3.1 Состав и содержание носителя данных

Компьютерное приложение «CRYPTOGRAPHER» поставляется на любом электронном носителе или скачивается с указанного репозитория в GitHub в виде программного кода на языке программирования Python.

3.2 Порядок загрузки программ и данных

Для работы приложения на компьютере пользователя необходимо установить следующее программное обеспечение:

- Python 3 версии 3.10 или выше,
- дополнительные библиотеки Python 3: PyQt5, pyperclip, cryptography,
- интегрированную среду разработки Python, например, PyCharm.

3.3 Порядок проверки работоспособности

Для проверки работоспособности компьютерного приложения «CRYPTOGRAPHER» необходимо запустить предоставленный программный код в интегрированной среде разработки Python.

В случае если приложение работоспособно, на этом шаге будет открыто стартовое окно, показанное на рисунке 1.

4 ОПИСАНИЕ ОПЕРАЦИЙ

4.1 Запуск (открытие) приложения

Запустить предоставленный программный код в интегрированной среде разработки Python. После этого откроется стартовое окно приложения, показанное на рисунке 1.

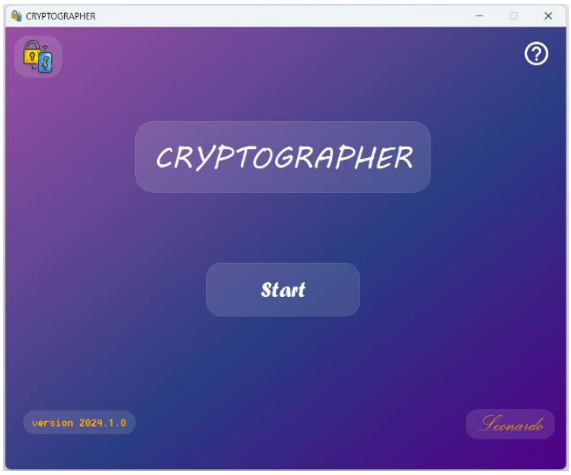


Рисунок 1 – стартовое окно приложения

В стартовом окне пользователь видит:

- название приложения «CRYPTOGRAPHER»,
- в левом нижнем углу – версию приложения,
- в правом нижнем углу – логотип разработчика.

Так же данное окно имеет две функциональные кнопки:

- в правом верхнем углу кнопка справочной информации,
- по центру кнопка «START», позволяющая перейти к следующему окну.

4.2 Выбор алгоритма шифрования и операции, которую необходимо выполнить с файлом

После того как пользователь нажмёт кнопку «START» на стартовом окне, он попадает в следующее окно «Intermediate», показанное на рисунке 2.

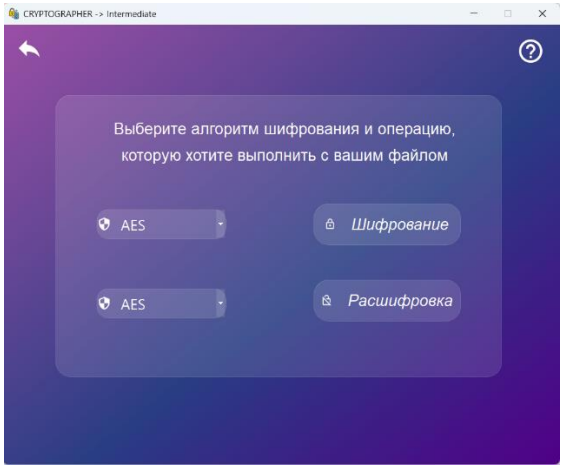


Рисунок 2 – окно «Intermediate»

В окне «Intermediate» пользователь видит краткое описание действий.

Так же данное окно имеет следующие функциональные кнопки:

- в правом верхнем углу кнопка справочной информации,
- в левом верхнем углу кнопка возвращения к предыдущему окну,
- по центру два выпадающих списка с возможностью выбрать алгоритм шифрования,
- справа от выпадающих списков находятся кнопки выбора операции «Шифрование» и «Расшифровка».

Сначала пользователь из выпадающего списка выбирает необходимый алгоритм шифрования, который будет использоваться при шифровании или расшифровки файла. Затем нажимает кнопку «Шифрование», если выбирал алгоритм шифрования в верхнем выпадающем списке или кнопку «Расшифровка», если выбирал алгоритм шифрования в нижнем выпадающем списке.

4.3 Операция шифрования с помощью алгоритма Triple DES, AES, RSA

Если пользователь в окне «Intermediate» выбрал алгоритм шифрования и нажал кнопку «Шифрование», то он в зависимости от выбранного алгоритма попадёт в одно из ниже представленных окон:

- окно «DES_Encryption», показанное на рисунке 3,
- окно «AES_Encryption», показанное на рисунке 4,
- окно «RSA_Encryption», показанное на рисунке 5.

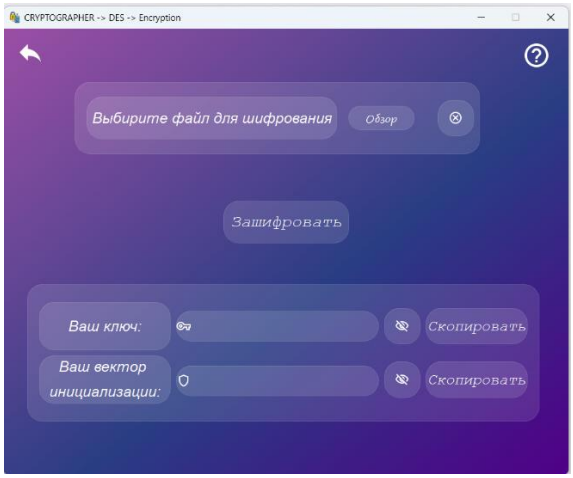


Рисунок 3 – окно «DES_Encryption»

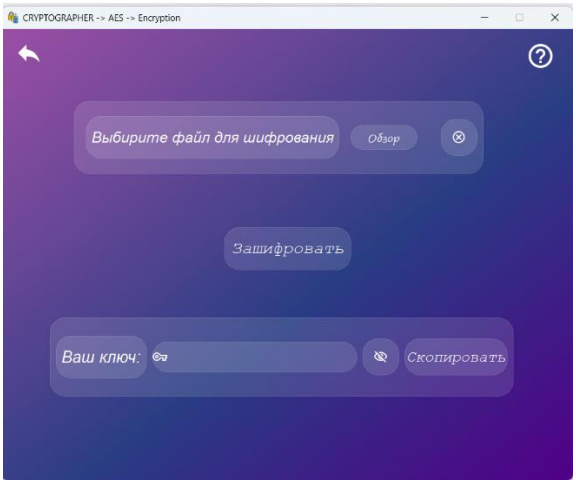


Рисунок 4 – окно «AES_Encryption»

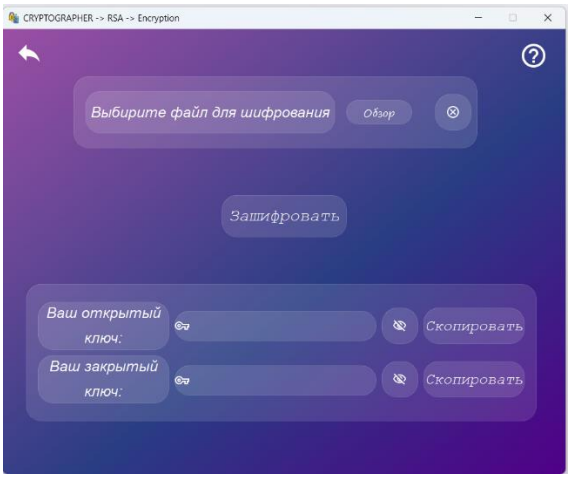


Рисунок 5 – окно «RSA_Encryption»

Выше указанные три окна имеют следующие функциональные кнопки:

- в правом верхнем углу кнопка справочной информации,
- в левом верхнем углу кнопка возвращения к предыдущему окну,
- вверху кнопка «Обзор»,

- справа от кнопки «Обзор» находится меняющийся индикатор, показывающий выбрал пользователь, или еще нет, файл для шифрования,
- по центру кнопка «Зашифровать»,
- внизу текстовые поля, для показа ключа и вектора инициализации для алгоритма Triple DES; ключа для алгоритма AES; открытого и закрытого ключей для алгоритма RSA,
- справа от каждого текстового поля находятся кнопка скрытия и открытия для чтения текста в данном поле и кнопка «Скопировать».

Сначала пользователю необходимо нажать кнопку «Обзор», после чего появится стандартное окно проводника операционной системы. После выбора файла и нажатия кнопки «Открыть» пользователь опять возвращается в соответствующее окно шифрования.

Затем пользователь нажимает кнопку «Зашифровать». Сразу появляется всплывающее окно «Choicesafe», где пользователю надо будет выбрать вид операции с файлом. Окно «Choicesafe» представлено на рисунке 6.

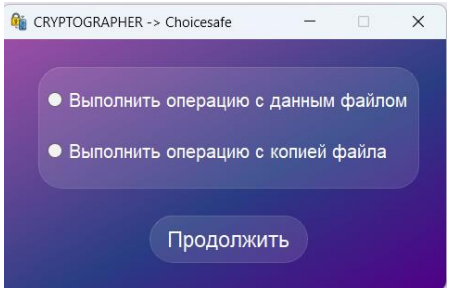


Рисунок 6 – окно «Choicesafe»

Если пользователь выберет «Выполнить операцию с данным файлом», то начнётся процесс шифрования, сопровождающийся всплывающим окном прогресс-бара, которое после окончания шифрования заменится всплывающим окном информирующем об успешном окончании шифрования файла.

Если пользователь выберет «Выполнить операцию с копией файла», то сначала откроется стандартное окно проводника операционной системы, где пользователю необходимо указать имя копии файла, его расширение и место сохранения. После нажатия кнопки «Открыть» начнётся процесс шифрования, сопровождающийся всплывающим окном прогресс-бара, которое после окончания шифрования заменится всплывающим окном информирующем об успешном окончании шифрования файла.

Окно прогресс-бара и окно окончания шифрования показаны на рисунке 7 и на рисунке 8, соответственно.

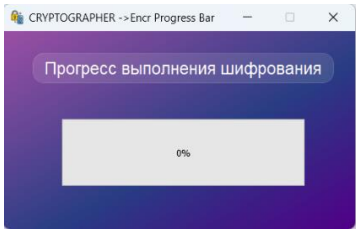


Рисунок 7 – окно «Encr Progress Bar»

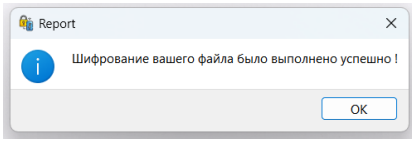


Рисунок 8 – окно, информирующее об успешном окончании шифрования

В сплывающем окне, информирующем об успешном окончании шифрования пользователь нажимает кнопку «ОК» и в основном окне шифрования он может посмотреть созданные алгоритмом ключи и вектор инициализации, в зависимости от выбранного алгоритма шифрования.

ВАЖНО! Созданные ключи, вектор инициализации необходимо скопировать, нажав кнопку «Скопировать» и сохранить в заранее созданном текстовом документе любого текстового редактора, например, «Блокнот».

После этого пользователь может закончить работу и закрыть приложение или может с помощью кнопки возврата перейти в предыдущее окно продолжить работу с приложением.

4.4 Операция расшифровки с помощью алгоритма Triple DES, AES, RSA

Если пользователь в окне «Intermediate» выбрал алгоритм шифрования и нажал кнопку «Расшифровка», то он в зависимости от выбранного алгоритма попадёт в одно из ниже представленных окон:

- окно «DES_Decryption», показанное на рисунке 9,
- окно «AES_Decryption», показанное на рисунке 10,
- окно «RSA_Decryption», показанное на рисунке 11.

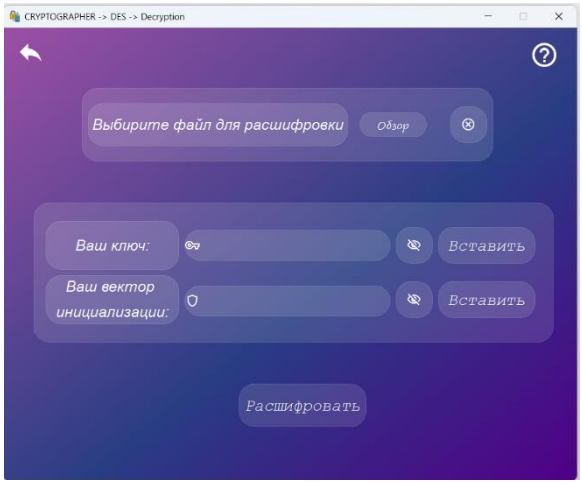


Рисунок 9 – окно «DES_Decryption»

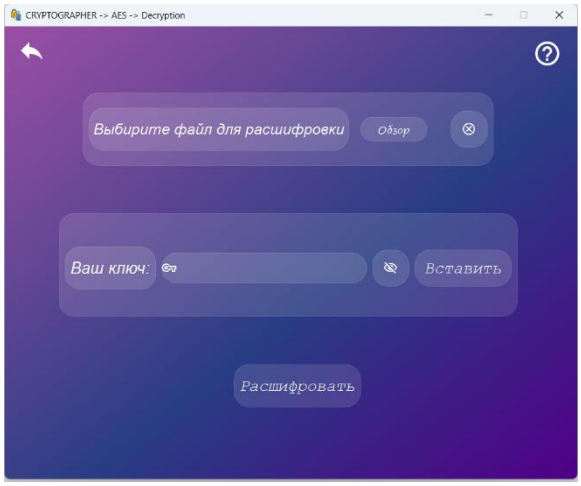


Рисунок 10 – окно «AES_Decryption»

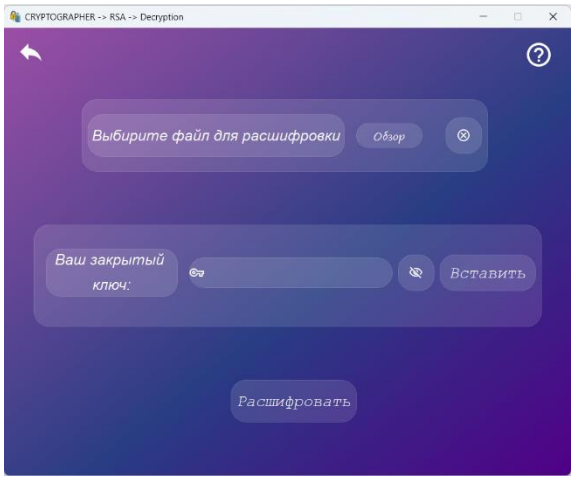


Рисунок 11 – окно «RSA_Decryption»

Выше указанные три окна имеют следующие функциональные кнопки:

- в правом верхнем углу кнопка справочной информации,
- в левом верхнем углу кнопка возвращения к предыдущему окну,
- вверху кнопка «Обзор»,
- справа от кнопки «Обзор» находится меняющийся индикатор, показывающий выбрал пользователь, или еще нет, файл для шифрования,
- по центру текстовые поля, для показа ключа и вектора инициализации для алгоритма Triple DES; ключа для алгоритма AES; закрытого ключа для алгоритма RSA,
- справа от каждого текстового поля находятся кнопка скрытия и открытия для чтения текста в данном поле и кнопка «Вставить».
- внизу кнопка «Расшифровать».

Сначала пользователю необходимо нажать кнопку «Обзор», после чего появится стандартное окно проводника операционной системы. После выбора файла, который требуется расшифровать, и нажатия кнопки «Открыть» пользователь опять возвращается в соответствующее окно расшифровки.

Затем пользователь копирует в соответствии с выбранным алгоритмом шифрования ранее сохранённые ключ, вектор инициализации, закрытый ключ требующиеся для расшифровки выбранного файла, и нажимает кнопку «Вставить» напротив

соответствующего текстового поля, в котором сразу появляется скопированные данные.

Далее пользователь нажимает кнопку «Расшифровать». Сразу появляется всплывающее окно «Choicesafe» (описанное выше), где пользователю надо будет выбрать вид операции с файлом.

Если пользователь выберет «Выполнить операцию с данным файлом», то начнётся процесс расшифровки, сопровождающийся всплывающим окном прогресс-бара, которое после окончания расшифровки заменится всплывающим окном информирующем об успешном окончании расшифровки файла.

Если пользователь выберет «Выполнить операцию с копией файла», то сначала откроется стандартное окно проводника операционной системы, где пользователю необходимо указать имя копии файла, его расширение и место сохранения. После нажатия кнопки «Открыть» начнётся процесс расшифровки, сопровождающийся всплывающим окном прогресс-бара, которое после окончания расшифровки заменится всплывающим окном информирующем об успешном окончании расшифровки файла.

Окно прогресс-бара и окно окончания расшифровки показаны на рисунке 12 и на рисунке 13, соответственно.

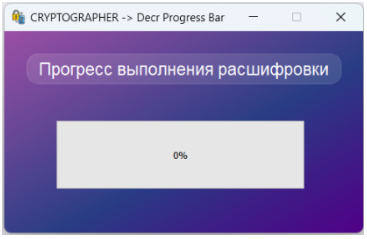


Рисунок 12 – окно «Decr Progress Bar»

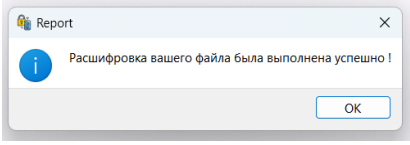


Рисунок 13 – окно, информирующее об успешном окончании расшифровки

В сплывающем окне, информирующем об успешном окончании расшифровки пользователь нажимает кнопку «ОК», после чего он может закончить работу и закрыть приложение или может с помощью кнопки возврата перейти в предыдущее окно продолжить работу с приложением.

5 АВАРИЙНЫЕ СИТУАЦИИ

Если пользователь при работе с интерфейсом приложения нарушает последовательность правильной работы алгоритма программы, то приложение будет информировать его об этом с помощью всплывающих окон ошибок. В приложении предусмотрены следующие варианты ошибочных действий пользователя:

- при выполнении операции шифрования:

1) не выбран файл для шифрования и нажата кнопка «Зашифровать», окно ошибки показано на рисунке 14;

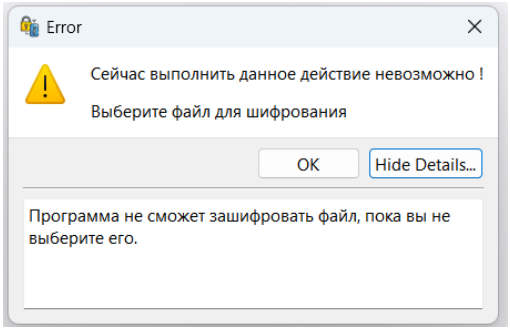


Рисунок 14 – окно ошибки, если не выбран файл шифрования

2) в окне «Choicesafe» не выбран вариант сохранения файла и нажата кнопка «Продолжить», окно ошибки показано на рисунке 15;

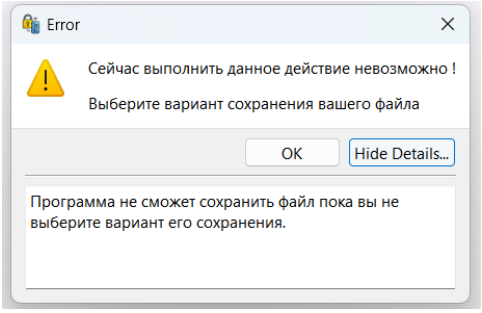


Рисунок 15 – окно ошибки, если не выбран вариант сохранения файла

3) при пустом поле ввода ключа (вектора инициализации, открытого ключа, закрытого ключа) нажата кнопка «Скопировать», окна ошибок показаны на рисунке 16;

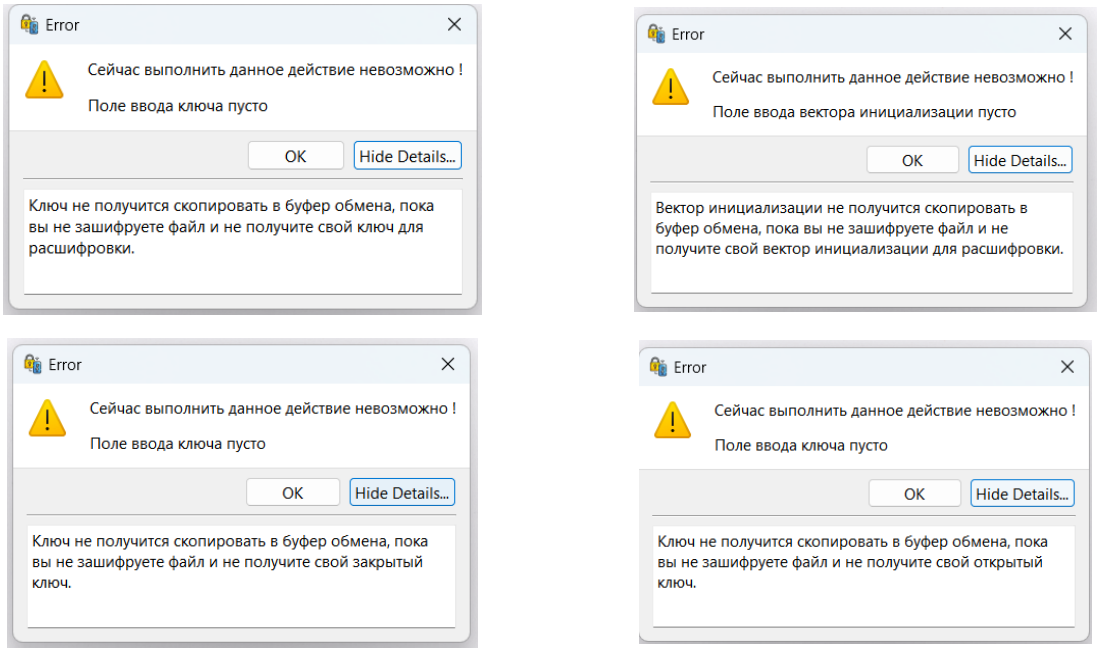


Рисунок 16 – окна ошибок, если поле ввода ключа (вектора инициализации, открытого ключа, закрытого ключа) пусто

4) при работе с алгоритмом RSA был выбран файл не являющимся текстовым или длина текста превышает 190 символов, окно ошибки показано на рисунке 17;

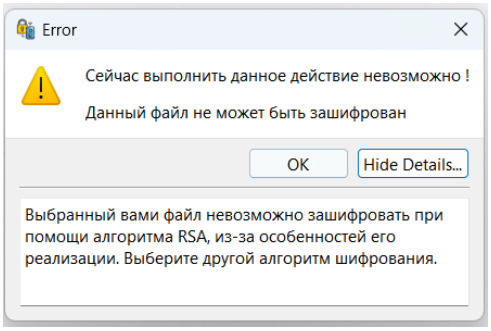
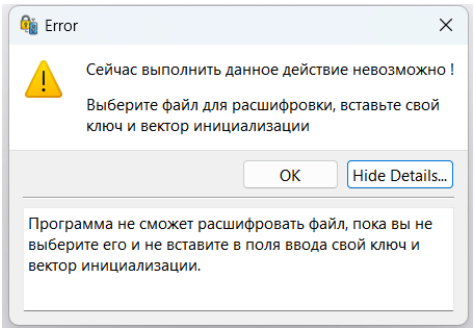
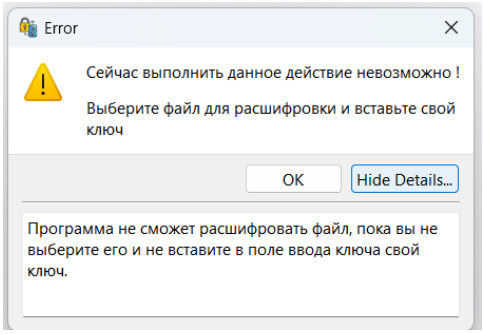


Рисунок 17 – окно ошибки, если выбранный файл, не поддерживается при работе с алгоритмом шифрования RSA

- при выполнении операции расшифровка:

1) нажата кнопка «Расшифровать» без выбора файла для расшифровки и при пустом поле ввода ключа (вектора инициализации, закрытого ключа), окна ошибок показаны на рисунке 18;





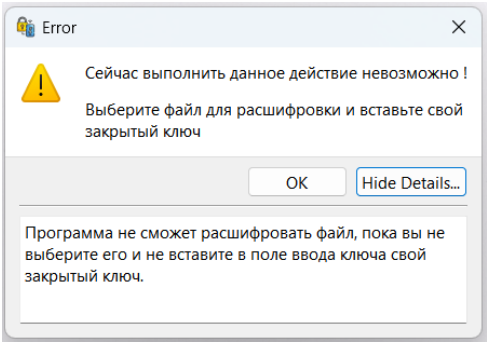


Рисунок 18 – окна ошибок, если не выбран файл для расшифровки и поля для ввода ключа (вектора инициализации, закрытого ключа) пусты

2) не выбран файл для расшифровки и нажата кнопка «Расшифровать», окно ошибки показано на рисунке 19;

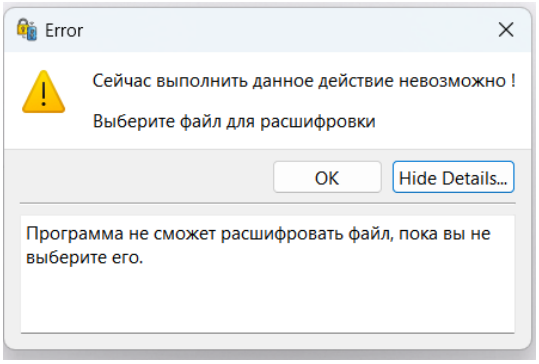
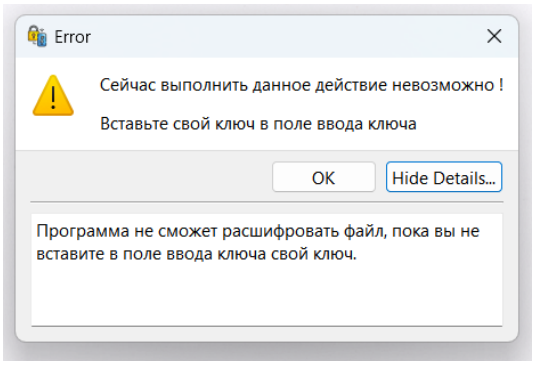
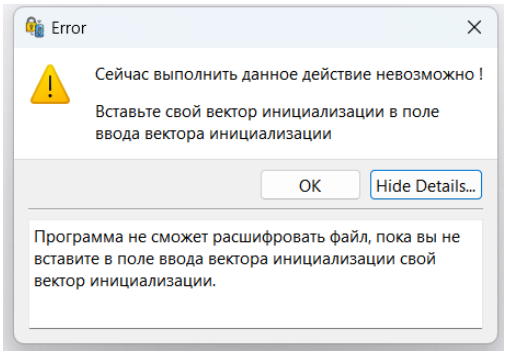


Рисунок 19 – окно ошибки, если не выбран файл для расшифровки

3) при пустом поле ввода ключа (вектора инициализации, закрытого ключа) нажата кнопка «Расшифровать», окна ошибок показаны на рисунке 20;





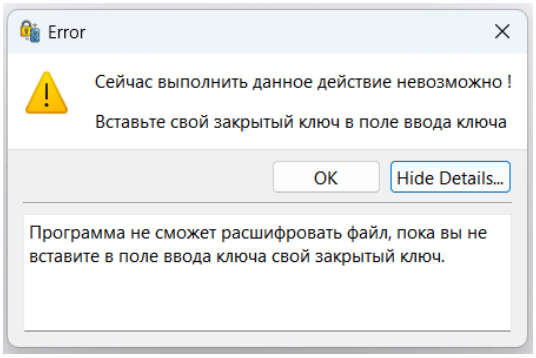


Рисунок 20 – окна ошибок, если поля для ввода ключа (вектора инициализации, закрытого ключа) пусты

4) если нажать кнопку «Вставить» не скопировав предварительно в буфер обмена ключ (вектор инициализации, закрытый ключ), окна ошибок показаны на рисунке 21;

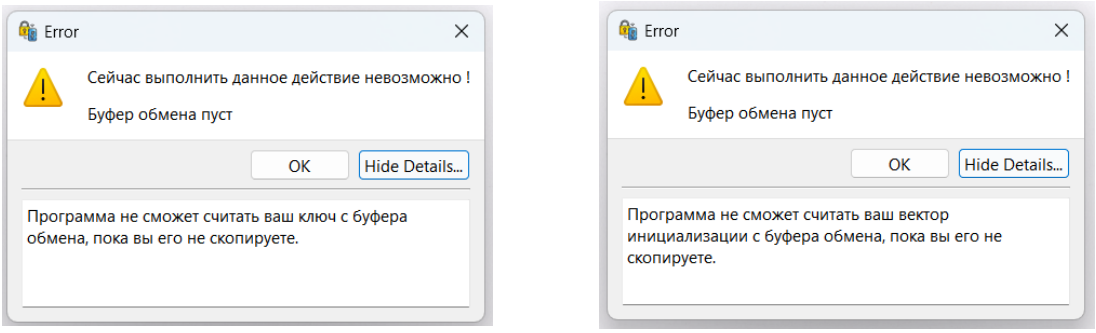


Рисунок 21 – окна ошибок, если при вставке ключа (вектора инициализации, закрытого ключа) буфер обмена пуст

5) если выбранный алгоритм или ключ (вектор инициализации) не подходит для расшифровки выбранного файла, окно ошибки показано на рисунке 22;

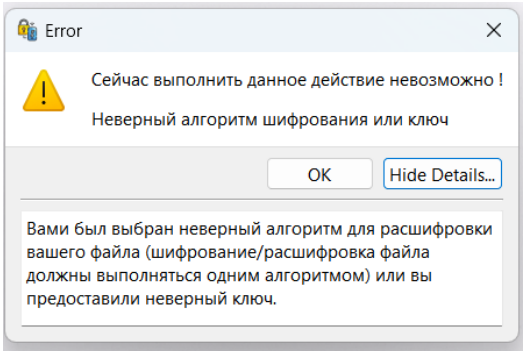


Рисунок 22 – окно ошибки, если выбранный алгоритм или ключ (вектор инициализации) не подходит для расшифровки выбранного файла

6) в окне «Choicesafe» не выбран вариант сохранения файла и нажата кнопка «Продолжить», окно ошибки показано на рисунке 15.

Любое окно ошибки имеет две функциональные кнопки:

- кнопка «OK»,
- кнопка «Show Details…».

Если при работе приложение выдаёт всплывающее окно ошибки, пользователь может нажать кнопку «Show Details…», после чего откроется текстовое поле с краткой инструкцией для пользователя по его дальнейшим действиям, при этом название кнопки изменится на «Hide Details…». Если нажать на кнопку «Hide Details…», то скроется текстовое поле с краткой инструкцией. Для закрытия окна ошибки и выхода в основное окно приложения пользователю необходимо нажать кнопку «OK».

6 РЕКОМЕНДАЦИИ ПО ОСВОЕНИЮ

Для успешного освоения приложения необходимо иметь навыки работы с ПК, с интегрированной средой разработки Python, а также изучить настоящее руководство пользователя.