Пояснительная записка

Приложение “Cryptography”

Иванов Герман

Лицей Академии Яндекса

08.10.2021

Описание 3

Функции 3

Поддерживаемые алгоритмы 3

Интерфейс 4

Используемые библиотеки 4

Системные требования 5

# Описание

Программа “Cryptography” — простой набор инструментов для шифрования и хеширования. Она предназначена в первую очередь для тех, кто плохо знаком с криптографией и хочет использовать алгоритмы, представленные в этой программе. Присутствуют описания каждого из алгоритмов и примеры их применения.

# Функции

* Шифрование и дешифрование (где возможно) текста
* Хеширование текста
* Описание каждого алгоритма с целями его применения
* Возможность проверки хеш-суммы файлов
* Поддержка сохранения ключей шифрования
* Поддержка импорта и экспорта ключей в виде CSV файла
* Наличие диалогов для подтверждения действий и оповещениях об ошибках
* Возможность сравнения хешей
* Удобные кнопки для копирования/вставки текста в поля
* Поддержка английского и русского языков.

# Поддерживаемые алгоритмы

* Fernet (реализация AES)
* SHA-1
* Семейство алгоритмов SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512)
* Семейство алгоритмов SHA-3 (SHA3-224, SHA3-256, SHA3-384, SHA3-512)

# Интерфейс

Для реализации интерфейса использовался PyQt5. В главном окне содержатся 5 вкладок (шифрование и расшифровка Fernet, хеширование SHA и MD5, сравнение). В верхнем меню есть выбор языка программы, а также доступ к просмотру и очистке базы данных с ключами Fernet. Чтобы добавлять ключи в эту базу данных, можно воспользоваться кнопкой “Сохранить” в первых 2 вкладках программы.

В каждой из вкладок находятся кнопки “Копировать” и “Вставить” рядом с соответствующими полями. В нижней части окна есть кнопка для открытия помощи с описанием алгоритма и подсказками по использованию программы.

Всего в программе 2 окна. Все элементы окон выровнены с помощью средств, предоставляемых Qt5 (QFormLayout, QVerticalLayout, QHorizontalLayout и QGridLayout). Оба окна могут быть растянуты.

# Используемые библиотеки

* PyQt5 >= 5.14.2
* Cryptography >= 35.0.0
* Pyperclip >= 1.8.1

И также версия Python >= 3.7.0 со следующими встроенными библиотеками:

* Hashlib
* Locale
* sys
* os
* csv

# Системные требования

Все системы, которые поддерживают необходимую версию Python 3. Работоспособность проверялась только на macOS 12.0.1 и Windows 11 (build 22499, ARMx64). Рекомендуется минимум двухъядерный процессор. Поддержка 32-битных архитектур не гарантируется. Релизы предоставляются для macOS (10.9 и выше), Windows (7 и выше) и GNU/Linux.