УДК 004

RapidKey (программный продукт)

Дорощук И.Р. (ГБНОУ СПбГЦДТТ)
Научный руководитель – педагог дополнительного образования, Преображенская В.О.
(Государственное бюджетное нетиповое образовательное учреждение
Санкт-Петербургский городской центр детского технического творчества)

Введение. Сегодня все больше организаций оцифровываются, то есть начинают работать онлайн. Теперь мы можем записаться к врачу или оплатить штраф за превышение скорости не выходя из дома. Но сама система подачи документов пока что не поменялась, поэтому требуется хранить гораздо больше личной информации на своем компьютере и в сети. Это делает нас более уязвимыми к потере персональных данных, поэтому требуются новые и надежные методы защиты информации.

Основная часть. В качестве своего проекта я разработал программное обеспечение, которое позволяет оборудовать любой флеш-накопитель (флешку) ключом безопасности. Это позволяет сделать мой новый алгоритм шифрования паролей.

Программное обеспечение представляет собой консольное приложение, написанное на языке Python (в дальнейшем планируется разработать визуальный интерфейс). Код разделяется на четыре основные функции:

- *Взаимодействие с пользователем*
- *Добавление нового флеш-носителя*
- *Кодирование пароля и создание ключа (наиболее важная!)*
- *Использование ключа (Дешифрование цепи)*

Как работает мой программный продукт, и как с ней взаимодействует пользователь?
Пользователь запускает программу

1. Далее пользователю нужно добавить любой флеш-накопитель в систему. Для этого ему требуется выбрать опцию из меню «Добавить новый флеш-носитель», после чего программа будет ожидать подключение нового USB-устройства в течение минуты. Если устройство обнаружено, то на него сохраняется структура папок для дальнейшей работы и файл с уникальным кодом для предотвращения копирования с одного устройства на другое.
2. После добавления флеш-накопителя в систему, на него можно сохранять ключ безопасности. Пользователю предлагается ввести название для ключа (мой программный продукт позволяет хранить несколько ключей на одном флеш-носителе), а затем пароль для данного ключа. Этот пароль и шифруется с помощью моего алгоритма шифрования. *Кратко об алгоритме:* Итак, введенный пользователем пароль записывается в файл, для которого генерируется случайное имя. Затем этот файл шифруется с уникальным ключом, который также генерируется. Этот ключ и имя предыдущего файла сохраняется в следующий файл, который также шифруется с уникальным ключом. Такой цикл проходит несколько раз, пока не будет создано случайное количество файлов, которые я называю блоками, а все файлы цепью. Цепь, потому что каждый последующий блок связан с предыдущим через его уникальное имя. На выходе получается «хэш», который можно декодировать, но только при помощи всех блоков. Его можно свободно хранить, ведь без полной цепи он не имеет никакой ценности. Блоки сохраняются случайным образом или на компьютер, или на флеш-носитель. То есть на флешке храниться только некоторая часть цепи, при этом несвязанные между собой блоки. Это позволяет обесценить информацию, которая хранится на флеш-накопителе. (Алгоритм дешифрования секретен)
3. *Как пользоваться данным ключом?* По задумке ключ используется как мера дополнительной защиты для важных аккаунтов (банковских аккаунтов, брокерских

счетов). Сайт, использующий мою систему, будет запрашивать вставить ключ (в виде USB-флеш-накопителя), затем ввести название ключа и пароль от него.

Выводы. Разработано программное обеспечение, позволяющее создать ключ безопасности из обычной флэшки, которое имеет ряд плюсов, например, алгоритм шифрования, который способен при шифровании одного и того же набора символов выдать разный хэш, но при этом однозначно дешифровать. У данного программного обеспечения есть широкая область возможного применения.

Список использованных источников:

1. Ключ (криптография) — Текст: электронный // Википедия: свободная энциклопедия. - URL: https://ru.wikipedia.org (дата обращения: 16.12.2022)
2. Как создать USB-ключ безопасности в Windows 10 - Текст: электронный // Школа Windows: все о работе с компьютерной системой - URL: https://windows-school.ru/ (дата обращения: 03.01.23)
3. 5 Common Encryption Algorithms and the Unbreakables of the Future - Текст: электронный // Arcserve: официальный сайт - URL: www.arcserve.com/ (дата обращения: 15.01.23)

Дорощук И.Р. (автор) Подпись

Преображенская В.О (научный руководитель) Подпись