муниципальное общеобразовательное учреждение «Лицей №86»

Проектная работа на тему:

**Разработка программы для шифрования файлов с использованием смартфона в качестве электронного ключа**

**Выполнил:**

Тампио Илья

Ученик 10 «Б» класса, лицея №86, г. Ярославль

**Научный руководитель:**

Вахромеева Наталья Александровна учитель

информатики, лицей №86, г. Ярославль

Ярославль

2019г.

**Введение**

В настоящее время при хранении и передаче данных на электронных носителях должны соблюдаться конфиденциальность информации и ее целостность. Для этого в настоящее время используется шифрование. Шифрование - обратимое преобразование информации с помощью ключа в целях сокрытия от [неавторизованных](https://ru.wikipedia.org/wiki/%D0%90%D0%B2%D1%82%D0%BE%D1%80%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F" \o "Авторизация) лиц, с предоставлением, в это же время, [авторизованным](https://ru.wikipedia.org/wiki/%D0%90%D0%B2%D1%82%D0%BE%D1%80%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F" \o "Авторизация) пользователям доступа к ней.

Допустим, у нас есть база данных учетных записей пользователей почтового сервиса, которую нам надо загрузить из одного сервера в другой таким образом, чтобы никто, кроме нас не мог узнать ее содержимое. Для этого база данных шифруется определенным ключом, который на данный момент чаще всего является паролем, вводимым человеком, после чего отправляется по сети или переносится на съемном носителе на другой сервер.

Подобное шифрование является надёжным, при условии что сложность и длина пароля высоки. Большинство людей в настоящее время не задумываются об этих качествах ключа, используя простые пароли длиной до 16 символов, из-за чего появляется риск нарушения конфиденциальности информации посредством нахождения пароля злоумышленником методом полного перебора.

Если использовать вместо пароля связку пароля, телеметрии телефона и автоматически генерируемого пароля, хранимого в файле, в свою очередь хранимым в памяти телефона, в качестве ключа для шифрования данных, риск нарушения конфиденциальности информации резко уменьшается, из-за увеличения длины и сложности ключа. Также, шифрование и дешифрование файла можно будет произвести только при наличии смартфона, с помощью которого шифровалась информация, то есть из-за того, что большинство людей носят свои смартфоны при себе, без участия владельца процесс дешифрования будет невозможен, что обеспечивает гарантию целостности и конфиденциальности информации, позволяя пользователю полностью контролировать доступ к ней.

**Цель проекта:** разработать программу для шифрования и дешифрования файлов с помощью ключа, являющимся связкой пароля, телеметрии смартфона и автоматически генерируемого программой файла, хранимым в его памяти.

**Задачи проекта:** разработать и реализовать алгоритм шифрования файла посредством разработки программного обеспечения с графическим интерфейсом для шифрования файлов данным алгоритмом, провести криптоанализ разработанного шифрования для выявления возможных уязвимостей алгоритма.

**Разбор аналогов**

**WinRAR и 7-Zip**

WinRARи 7-Zip – это программы-архиваторы, основной задачей которых является слияние нескольких файлов в один для их сжатия и удобства передачи с одного устройства на другое. Тем не менее, в них есть возможность защиты архива паролем, что позволяет использовать даннное программное обеспечение для обеспечения криптографической безопасности данных. Для шифрования архивов WinRAR и 7-Zip используют алгоритм шифрования AES с ключом 256 бит, однако 7-Zip позволяет так же защитить архив с помощью менее надёжного алгоритма ZipCrypto. Криптостойкость зашифрованного таким способом криптоконтейнера зависит только от сложности пароля.

**VeraCrypt**

VeraCrypt – это программное обеспечение для создания стойких криптоконтейнеров, разработанное на основе ныне устаревшего и признанного небезопасным TrueCrypt. Основной задачей подобных программ является обеспечение безопасности данных, а потому они зачастую реализуют несколько различных алгоритмов шифрования. Так, VeraCrypt позволяет создать криптоконтейнеры используя следующие алгоритмы шифрования: AES, Serpent, Twofish, Camellia, Кузнечик – а так же их комбинации. Стоит отметить, что VeraCrypt поддерживает возможность отрицаемого шифрования, позволяя создавать внутри зашифрованного контейнера, ещё один «скрытый том». Также, данная программа позволяет использовать в качестве цифрового ключа файл, что значительно усиливает безопасность криптоконтейнера.

**Вывод**

Большинство аналогов имеют недостаток в виде пароля или файла-ключа для шифрования, которые могут быть легко забыты или потеряны пользователем. Моё инновационное решение призвано исправить этот недостаток, используя лучшие стороны аналогичных программ, а именно использовать телефон в качестве электронного ключа в связке с общепризнанными методами шифрования для обеспечения конфиденциальности и безопасности данных.