Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет непрерывного и дистанционного обучения

Кафедра информатики

**Индивидуальная практическая работа №1**

по дисциплине

" Методы защиты информации. Часть 2"

Выполнил студент гр. 493551 Авхимович Алексей Валерьевич

E-mail: [droon2112@gmail.com](mailto:droon2112@gmail.com)

Минск 2018

**Часть 1.1 Шифрование файлов**

**Изучите теоретические сведения**

**Цель:**Реализуйте программное средство шифрования и дешифрования текстовых файлов при помощи Шифра Цезаря, (шифра сдвига, кода Цезаря).

**Результат:** Программа шифрования, осуществляющая криптографическое преобразование введенного текста с помощью Шифра Цезаря, (шифра сдвига, кода Цезаря).

**Общая постановка задачи:**  Создать программу, читающую данные из файла и шифрующие (дешифрующие) их с помощью с помощью Шифра Цезаря.

Введение

Крайне простой пример симметричного шифрования — этоподстановочный шифр. Подстановочный шифр заменяет каждую часть информации другой информацией. Чаще всего это достигается смещением букв алфавита. Пара примеров — это Секретное кольцо-декодер капитана Миднайта, которое могло быть у вас в детстве, и шифр Юлия Цезаря. В обоих случаях алгоритм состоит в том, чтобы сдвинуть алфавит, а ключ — это число букв, на которое произведено смещение.

Допустим, если мы решим зашифровать слово «SECRET», используя ключ Цезаря, равный 3, то сдвинем латинский алфавит так, чтобы он начинался с третьей буквы (D).

Итак, беря исходный вариант

ABCDEFGHIJKLMNOPQRSTUVWXYZ,

и смещая всё на 3, получаем

DEFGHIJKLMNOPQRSTUVWXYZABC,

где D=A, E=B, F=Cи т. д.

Используя эту схему, открытый текст «SECRET» превращается в «VHFUHW». Чтобы кто-то мог восстановить исходный текст, вы сообщаете ему, что ключ — 3.

Очевидно, что по сегодняшним меркам это чрезвычайно слабый алгоритм, тем не менее, даже он помогал Цезарю! И прекрасно демонстрирует, как действует симметричное шифрование.

Блок – схему алгоритма.

Распечатку скриншотов результатов ввода данных и исполнения программы.

Распечатку программного кода.

Вывод.

**ЛИТЕРАТУРА**

1. Концепция государственной политики в области информатизации. В ред. указа Президента Республики Беларусь от 07.08.2002 N 433
2. Концепция развития банковской системы Республики Беларусь на 2001 – 2010 годы. Зарегистрировано в Национальном реестре правовых актов Республики Беларусь 29 мая 2002 г. № 1/3717.
3. Концепция развития национальной платежной системы Республики Беларусь до 2010 года с учетом мировых тенденций. Утверждена Постановлением Правления Национального банка Республики Беларусь от 26.05.2004 № 84.
4. Инструкция по организации функционирования автоматизированной системы межбанковских расчетов Республики Беларусь. Зарегистрирована в Национальном реестре правовых актов Республики Беларусь 5 января 2001 г. N 8/4715
5. Гайкович В., Першин А. Безопасность электронных банковских систем. М.: Единая Европа, 1994.