БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Кафедра информатики

Факультет ИНО

Специальность ИиТП

Практическая работа № 1

по дисциплине «Методы защиты информации»

Выполнил студент: Дегтярев А.А.

группа 393551

Зачетная книжка № 902021-26

Минск 2018

**ИПР №1**

#### Часть 1 Шифрование файлов

**1. Введение**

**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.

**2. Схема алгоритма**



**3. Скриншоты ввода данных и результатов выполнения программы**

Порядок использования программы:



Необходимо указать файл для чтения с помощью флага **–i**, выходной файл указывать необязательно, программа автоматически создаст его, но если это необходимо, можно указать после флага **–o**. По умолчанию программа работает в режиме шифрования, для дешифрования необходима указать флаг **–d**

**Использовать флаг CAESAR(сaesar) для указания алгоритма**

Алгоритм использует простой сдвиг для каждого байта данных на заданное число. Для использование алгоритма представлено простое API:

**void** caesar\_process\_block(uint8\_t\* block, uint8\_t shift,**bool** encrypt);

В качестве аргументов передается (*указатель на блок данных*, *смещение*, *флаг шифрование/расшифровка*)

Содержимое тестового файла:  


Пример использования:

****

В результате был создан новый файл test\_encrypted:



Легко заметить что смещение = 4. Шифр является легко взламываемым, и ненадежным.  
  
Попробуем расшифровать сообщение, добавим флаг –d и укажем файл test\_encrypted



В результате получим исходный файл:  


**4. Исходные файлы:**

Caesar.h

#ifndef MZI\_CAESAR\_H  
#define MZI\_CAESAR\_H  
#include <cstdint>  
#include <cstdio>  
**void** caesar\_process\_block(uint8\_t\* block, uint8\_t shift,**bool** encrypt);  
#endif //MZI\_CAESAR\_H

Caesar.cpp

#include "caesar.h"  
**void** caesar\_process\_block(uint8\_t\* block, uint8\_t shift,**bool** encrypt) {  
 uint16\_t tempblock = \*block;  
 **if**(encrypt) {  
 \*block = **static\_cast**<uint8\_t>((tempblock + shift) % UINT8\_MAX);  
 } **else**{  
 \*block = **static\_cast**<uint8\_t>((tempblock - shift) % UINT8\_MAX);  
 }  
}

Часть кода вызова метода из Main.cpp

}**else if**(config.type == *CAESAR*){  
 printf("%s %s\n", "caesar", config.encrypt ? "encrypt" : "decrypt");  
 uint8\_t buf8 = 0;  
 uint8\_t shift = 4;  
 **while** (fread(&buf8, **sizeof**(buf8),1,inputFile) == 1){  
 caesar\_process\_block(&buf8,shift,config.encrypt);  
 fwrite(&buf8, **sizeof**(buf8),1,outputFile);  
 }

**5. Вывод:**

Шифр Цезаря один из самых простых и наиболее широко известных методов шифрования. Шифр Цезаря может быть легко взломан даже в случае, когда взломщик знает только зашифрованный текст.