МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Белорусский Государственный Технологический Университет

**РЕФЕРАТ**

по дисциплине: «Основы Алгоритмизации и Программирования»

на тему: «Функции шифрования и дешифрования»

Выполнил студент группы

ФИТ, ПИ, 8 группы

Лужецкий Владислав Константинович

г.Минск

Оглавление

[История и предназначение: 3](#_Toc151033177)

[Что такое шифрование: 3](#_Toc151033178)

[Что такое расшифрование и дешифрование. Их отличия: 4](#_Toc151033179)

[Виды шифрования: 5](#_Toc151033180)

[Задача: 6](#_Toc151033181)

[Структура и пояснение к задаче: 9](#_Toc151033182)

# История и предназначение:

**Криптография** – это метод защиты информации путем использования закодированных алгоритмов, хэшей и подписей

Криптография как техника защиты текста возникла вместе с письменностью. В древнеиндийских текстах среди 64 искусств названы способы изменения текста, некоторые из них можно отнести к криптографическим. В дальнейшем встречаются различные упоминания об использовании криптографии, большая часть относится к использованию в военном деле.

Другой пример древнего шифра — семитский атбаш. Это классический моноалфавитный шифр, в котором шифрование осуществляется путем подмены в словах букв еврейского алфавита по формуле n — i +1, где i — номер заменяемой буквы, а n — число букв в алфавите. По такому же принципу работал и «шифр Цезаря», используемый в Древнем Риме.

Криптография из разрозненных практик начала оформляться в полноценную дисциплину. **Расширилась и сфера ее применения**. Стали применять в гражданской сфере, **прежде всего в торговле и в банковском деле для защиты коммерческой информации**.

Одним из первых зафиксированных шифров является шифр Цезаря (около 100 г. до н.э.). Его принцип был прост: каждая буква исходного текста заменялась на другую, отстоящую от нее по алфавиту на определенное число позиций. Зная это число, можно был разгадать шифр.

# Что такое шифрование:

**Шифрование —** это математический процесс, используемый для превращения информации в нечитаемый (зашифрованный) вид. При этом восстановление первоначального вида информации (расшифровывание) возможно лишь с помощью специальных знаний. **В процессе шифрования используются шифр и ключ.**

**Ключом является инструкция для шифра**: как именно нужно шифровать и расшифровывать данные. Ключи являются одной из наиболее важных составляющих в шифровании.

|  |  |
| --- | --- |
| **Открытый ключ** | **Закрытый ключ** |
| Можно свободно распространять | Должен быть в тайне от всех |
| Отправителю необходим открытый ключ | Используется для расшифровывания  Сообщений с помощью откр. Ключа. |
| Можно использовать для аутентификации | Используется для цифровых подписей, можно проверить личность отправителя |
| При желании может быть размещён в постоянных общедоступных базах данных |  |

# Что такое расшифрование и дешифрование. Их отличия:

**Расшифрование иногда путают с дешифрованием**. Отличие в том, что **первое — легитимная процедура, быстро выполняемая с помощью известного ключа, а второе — попытка «взломать шифр», то есть восстановить без знания ключа открытый текст зашифрованного сообщения.**

**Процедура расшифрования может выполняться незаметно для пользователя. С ней регулярно сталкивается каждый из нас, разблокировав смартфон, или оплачивая покупки картой. Дешифрование — сложный процесс, требующий специальных познаний в криптографии.**

**Дешифрование является одной из задач криптографического анализа**. В рамках последнего также рассматривается более общая задача — восстановление ключа по шифр-текстам. Решение данной задачи позволяет быстро прочитать все перехваченные сообщения, зашифрованные тем же ключом, по сути, сводя дешифрование к расшифрованию.

# Виды шифрования:

Сегодня используются **два** основных **вида шифрования**:

**Симметричное**. В нем для шифровки и дешифровки сообщения **используется один и тот же ключ**. Этот ключ должен быть секретным, но известным как отправителю, так и получателю сообщения.

**Асимметричное**. В таком шифровании для шифровки и дешифровки сообщения **используются два разных ключа, математически связанные друг с другом**. При этом первый ключ может быть открытым, но второй обязательно делается секретным.

|  |  |
| --- | --- |
| Симметричное шифрование | **Асимметричное шифрование** |
| быстрое | медленное |
| Не требует больших вычисл. мощностей | Требует больших вычисл. мощностей |
| Используется для больших и маленьких сообщений | Только для небольших сообщений |
| Необходим обмен ключами для шифрования и расшифрования | Нельзя делиться ключом |
| Не используется аутентификация | Может использоваться аутентификация |

**Шифр Цезаря**: Простой вид шифрования, при котором каждая буква заменяется другой с фиксированным сдвигом.(*Симметричное шифрование*)

**Моноалфавитные шифры**: каждая буква заменяется другой буквой, сохраняя постоянное соответствии.(*Симметричное шифрование*)

**Полиалфавитные шифры**: используют несколько шифров, что делает их более сложными для взлома.(*Симметричное шифрование*)

**Шифрование с открытым ключом:** Использует два ключа: открытый и закрытый, обеспечивая безопасный обмен данными. (*Асимметричное шифрование*)

Для примера рассмотрим один из самых простых алгоритмов шифрования:

Шифр цезаря(см. выше)

# Задача:

#include <iostream>

#include <fstream>

#include <string>

using namespace std;

// Функция для шифрования символа(цезарь)

char encrypt(char c, int shift) {

if (isalpha(c)) {

char base = isupper(c) ? 'A' : 'a';

return (c - base + shift) % 26 + base; // Шифрование символа и возврат результата

}

return c; // Возврат неизмененного символа, если он не является буквой

}

// Функция для дешифрования символа

char decrypt(char c, int shift) {

if (isalpha(c)) {

char base = isupper(c) ? 'A' : 'a';

return (c - base - shift + 26) % 26 + base;

}

return c;

}

int main() {

setlocale(0,"");

// Открытие файла для чтения (входной файл)

ifstream inputFile("A.txt");

if (!inputFile.is\_open()) {

cout << "Не удалось открыть файл A.txt" << endl;

return 0;

}

int shift;

cout << "Введите сдвиг для шифрования (целое положительное число): ";

cin >> shift;

// Открытие файла для записи

ofstream encryptedFile("B.txt");

if (!encryptedFile.is\_open()) {

cout << "Не удалось открыть файл B.txt" << endl;

return 0;

}

char c;

// Цикл шифрования и записи в файл

while (inputFile.get(c)) {

char encryptedChar = encrypt(c, shift);

encryptedFile << encryptedChar;

cout << encryptedChar;

}

inputFile.close();

encryptedFile.close();

cout << "\nТекст успешно зашифрован и сохранен в файл B.txt" << endl;

// Открытие файла для чтения

ifstream encryptedInput("B.txt");

if (!encryptedInput.is\_open()) {

cout << "Не удалось открыть файл B.txt для чтения" << endl;

return 0;

}

// Открытие файла для записи

ofstream decryptedFile("C.txt");

if (!decryptedFile.is\_open()) {

cout << "Не удалось открыть файл C.txt" << endl;

return 0;

}

cout << "\nДешифрованный текст:\n";

// Цикл дешифрования и записи в файл

while (encryptedInput.get(c)) {

char decryptedChar = decrypt(c, shift);

decryptedFile << decryptedChar;

// Вывод дешифрованных символов на экран

cout << decryptedChar;

}

// Закрытие файлов для дешифрования

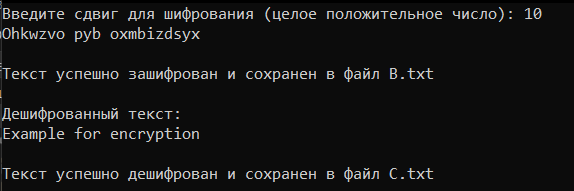
encryptedInput.close();

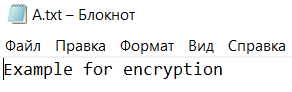
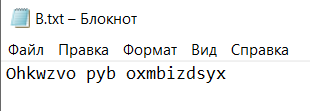
decryptedFile.close();

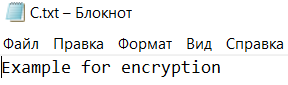
cout << "\nТекст успешно дешифрован и сохранен в файл C.txt" << endl;

return 0;

}





# Структура и пояснение к задаче:

В этом коде я использовал шифр цезаря. Изначально у нас есть исходный файл A.txt, в котором содержится текст для шифрования. Дальше функция encrypt шифрует текст исходного файла и записывает его в текстовый файл B.txt. После чего, с помощью дешифратора мы расшифровываем зашифрованное сообщение из B.txt и сохраняем его в C.txt.

*Примечание* : для корректной работы программы необходим исходный файл A.txt, в ходе работы, программа сама создаст необходимые файлы для хранение зашифрованной и дешифрованной информации(B.txt, C.txt)