

Министерство образования Республики Беларусь
Учреждение образования «Белорусский государственный университет
информатики и радиоэлектроники»

Факультет компьютерных систем и сетей

Кафедра информатики

Дисциплина: Информационные сети. Основы безопасности

ОТЧЁТ
к лабораторной работе №2
на тему

ЭЛЕМЕНТЫ КРИПТОГРАФИИ

Выполнил: студент гр.253504 Лавренова А.С.
Проверил: ассистент кафедры информатики
Герчик А.В.

Минск 2025

СОДЕРЖАНИЕ

Введение.....	3
1 Теоретические сведения	4
1.1 Шифр Цезаря	4
1.2 Шифр Виженера	4
2 Пример выполнения программного средства	5
2.1 Запуск программы и выбор режима шифрования	5
2.2 Пример выполнения шифра Цезаря	5
2.3 Пример выполнения шифра Виженера	6
Заключение	8
Список использованных источников	9
Приложение А (обязательное)	10

ВВЕДЕНИЕ

В современном мире информационная безопасность становится одной из важнейших задач, стоящих перед разработчиками программного обеспечения и специалистами в области криптографии. Одним из основных методов обеспечения конфиденциальности данных является шифрование, которое позволяет защитить информацию от несанкционированного доступа. В данной лабораторной работе рассматриваются классические алгоритмы симметричного шифрования – шифр Цезаря и шифр Виженера.

В этой лабораторной работе будет реализована разработка программных средств для шифрования и дешифрования текста с использованием указанных алгоритмов. При этом особое внимание уделяется корректной обработке различных типов символов, включая латинские и кириллические буквы, а также цифровые символы, что демонстрирует универсальность подхода.

Актуальность данной работы обусловлена тем, что классические шифры, несмотря на свою простоту, служат отправной точкой для понимания более сложных криптографических систем. Реализация этих алгоритмов на практике позволяет наглядно увидеть принципы симметричного шифрования, а также осознать, как даже элементарные преобразования могут существенно усложнить задачу несанкционированного доступа к информации.

Таким образом, выполнение данной лабораторной работы позволит получить практические навыки реализации криптографических алгоритмов, а также углубит понимание основ информационной безопасности и методов защиты данных.

1 ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

В данном разделе изложены основные теоретические аспекты, лежащие в основе реализованных алгоритмов шифрования – шифра Цезаря и шифра Виженера.

Шифрование, как процесс, представляет собой преобразование исходного (открытого) текста в зашифрованный (шифротекст) с использованием определенного алгоритма и ключа. Дешифрование, в свою очередь, является обратным процессом, при котором зашифрованный текст преобразуется обратно в исходный текст с применением соответствующего ключа. Ключ, таким образом, выступает в роли параметра (или набора параметров), который определяет конкретное преобразование символов в процессе шифрования и дешифрования. [1]

1.1 Шифр Цезаря

Шифр Цезаря — один из древнейших методов симметричного шифрования, названный в честь римского императора Юлия Цезаря, который использовал его для защиты своих сообщений. Основной принцип шифра заключается в циклическом сдвиге букв алфавита на фиксированное количество позиций. Например, при сдвиге на 3 символ 'А' преобразуется в 'Г', а 'Б' — в 'Д'.

Ключевыми особенностями шифра являются:

- простота реализации;
- ограниченная криптостойкость.

1.1 Шифр Виженера

Шифр Виженера является развитием идеи шифра Цезаря и относится к методам многоалфавитной подстановки. Его суть заключается в использовании повторяющегося ключа для определения величины сдвига каждой буквы в исходном тексте. Таким образом, каждый символ шифруется индивидуально, что значительно усложняет задачу для потенциального злоумышленника. [2]

Особенности шифра Виженера:

1. Использование нескольких алфавитов делает криптоанализ более сложным по сравнению с одноалфавитным шифром Цезаря.
2. Чем длиннее и сложнее ключ, тем выше стойкость шифра. Однако, при повторении ключа возможно применение статистических методов для восстановления исходного текста.

Таким образом, теоретическая база, представленная в данном разделе, служит фундаментом для дальнейшей реализации практических алгоритмов шифрования и дешифрования текста, демонстрируя их возможности и ограничения.

2 ПРИМЕР ВЫПОЛНЕНИЯ ПРОГРАММНОГО СРЕДСТВА

В данном разделе приведены примеры работы разработанной программы, демонстрирующие этапы шифрования и дешифрования текста с использованием алгоритмов шифра Цезаря и шифра Виженера. Примеры выполнены на языке программирования C++ и показывают корректность работы реализованных алгоритмов.

2.1 Запуск программы и выбор режима шифрования

При запуске программы пользователь видит главное меню (рисунок 2.1), в котором предлагается выбрать режим шифрования:

- для работы с шифром Цезаря;
- для работы с шифром Виженера.

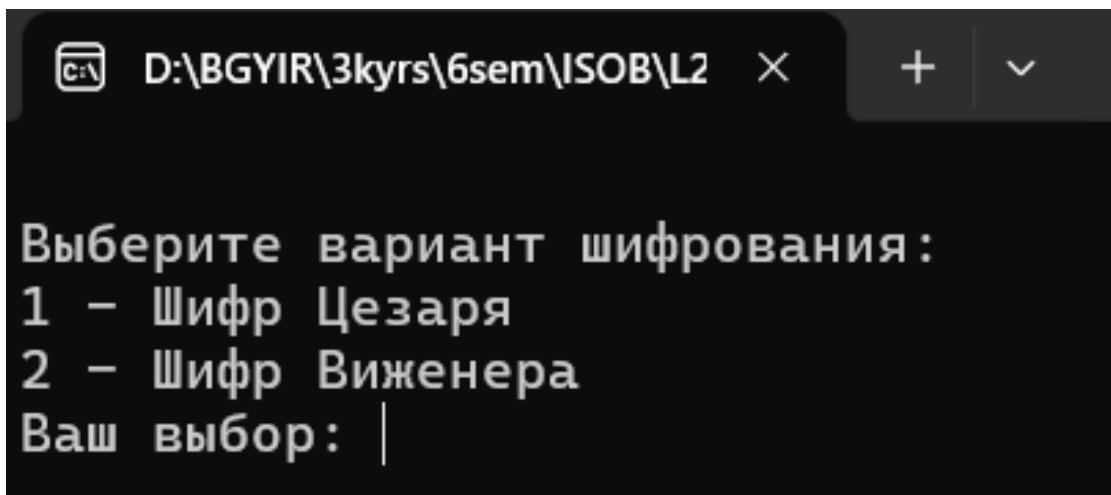


Рисунок 2.1 – Запуск программы

На данном рисунке показано основное меню программы, где пользователь может выбрать нужный режим шифрования. Это обеспечивает интуитивно понятный интерфейс для дальнейшей работы.

2.2. Пример выполнения шифра Цезаря

После выбора режима шифра Цезаря программа запрашивает:

- ввод исходного текста;
- ввод ключа (сдвига) для шифрования.

После ввода данных программа выводит зашифрованный текст. Затем, при вводе ключа для дешифрования, отображается восстановленный исходный текст (рисунок 2.2).

```
Выберите вариант шифрования:  
1 – Шифр Цезаря  
2 – Шифр Виженера  
Ваш выбор: 1  
Введите текст для шифрования: абвгд 111ABCD///  
Введите ключ (сдвиг): 2  
Зашифрованный текст: вгдеж 333CDEF///  
Введите ключ для дешифрования: 2  
Расшифрованный текст: абвгд 111ABCD///  
  
Хотите выполнить операцию ещё раз? (Y/N): |
```

Рисунок 2.2 – Работа шифра Цезаря

Данный рисунок демонстрирует этап ввода исходного текста и ключа для шифрования с помощью шифра Цезаря, а также отображение зашифрованного текста. Видно, как программа преобразует текст согласно заданному сдвигу. Также продемонстрирован процесс ввода ключа для дешифрования, после чего программа успешно восстанавливает исходный текст. Это подтверждает корректность реализации алгоритма обратного преобразования.

2.3. Пример выполнения шифра Виженера

При выборе режима шифра Виженера пользователь вводит:

- исходный текст для шифрования;
- ключ для шифрования.

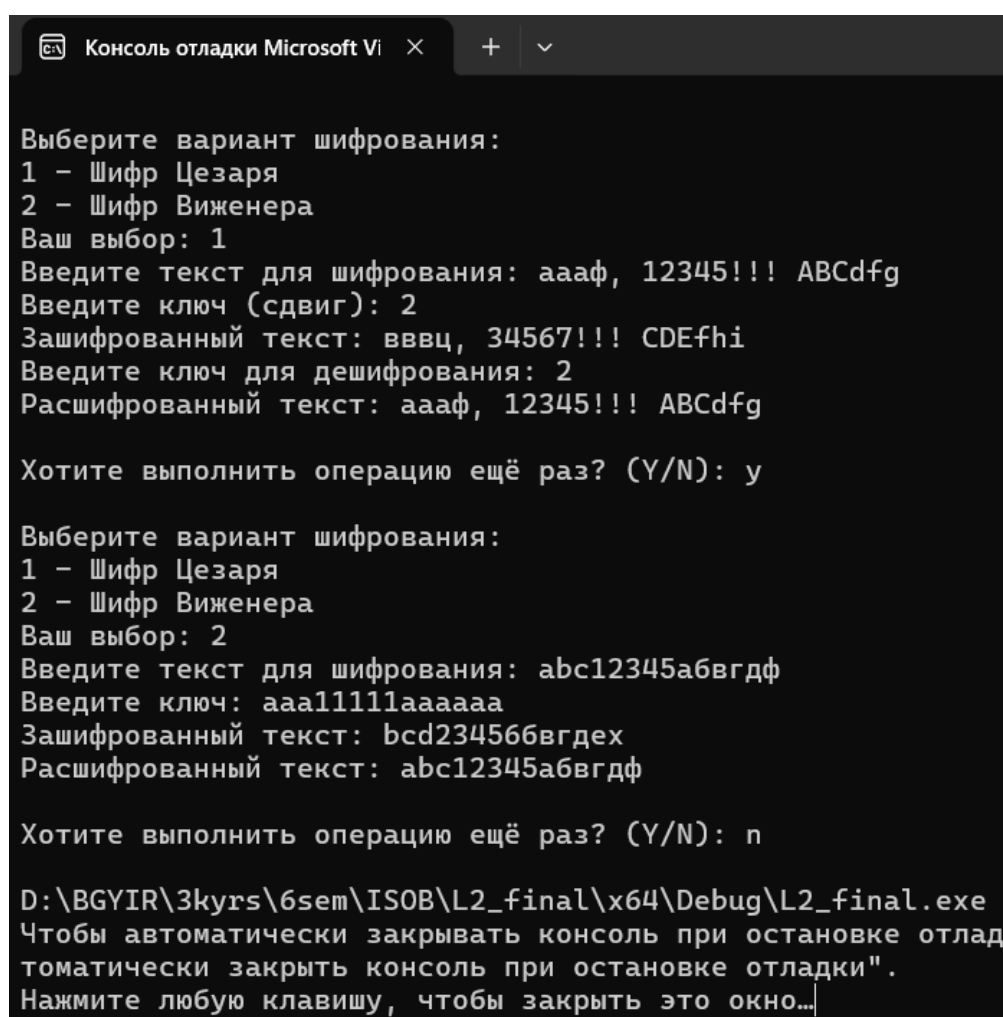
После ввода данных программа выполняет шифрование, выводя зашифрованный текст. Аналогичным образом происходит дешифрование, после чего программа выводит восстановленный исходный текст (рисунок 2.3).

```
Хотите выполнить операцию ещё раз? (Y/N): у  
  
Выберите вариант шифрования:  
1 – Шифр Цезаря  
2 – Шифр Виженера  
Ваш выбор: 2  
Введите текст для шифрования: abc12345абвгдф  
Введите ключ: aaa11111aaaaaa  
Зашифрованный текст: bcd234566вгдех  
Расшифрованный текст: abc12345абвгдф
```

Рисунок 2.3 – Работа шифра Виженера

На этом рисунке видно, как пользователь вводит исходный текст и ключ для шифрования с использованием шифра Виженера. Результат шифрования демонстрирует работу многоалфавитного метода, который усложняет процесс криптоанализа. Также виден процесс дешифрования, где программа успешно восстанавливает исходный текст, подтверждая правильность реализации алгоритма Виженера.

Показанные примеры демонстрируют, что реализованные алгоритмы шифрования и дешифрования корректно работают с различными типами данных (латинские и кириллические символы, цифры). Программа, написанная на языке C++, позволяет не только зашифровать текст, но и восстановить его исходное состояние при использовании соответствующих ключей. Это подтверждает эффективность и практическую применимость разработанного программного средства (рисунок 2.4).



```
Консоль отладки Microsoft Vi x + v

Выберите вариант шифрования:
1 - Шифр Цезаря
2 - Шифр Виженера
Ваш выбор: 1
Введите текст для шифрования: аааф, 12345!!! ABCdfg
Введите ключ (сдвиг): 2
Зашифрованный текст: вввц, 34567!!! CDEfhi
Введите ключ для дешифрования: 2
Расшифрованный текст: аааф, 12345!!! ABCdfg

Хотите выполнить операцию ещё раз? (Y/N): y

Выберите вариант шифрования:
1 - Шифр Цезаря
2 - Шифр Виженера
Ваш выбор: 2
Введите текст для шифрования: abc12345абвгдф
Введите ключ: ааа11111аааааа
Зашифрованный текст: bcd23456бвгдех
Расшифрованный текст: abc12345абвгдф

Хотите выполнить операцию ещё раз? (Y/N): n

D:\BGYIR\3kysr\6sem\ISOB\L2_final\x64\Debug\L2_final.exe (
Чтобы автоматически закрывать консоль при остановке отладки,
автоматически закрыть консоль при остановке отладки".
Нажмите любую клавишу, чтобы закрыть это окно...
```

Рисунок 2.4 – Работа программного средства

Данный рисунок демонстрирует полный процесс работы программы от выбора режима до завершения операций шифрования и дешифрования, что подтверждает стабильность и правильность функционирования разработанного решения.

ЗАКЛЮЧЕНИЕ

В ходе выполнения данной лабораторной работы была реализована программа для шифрования и дешифрования текста с использованием классических криптографических алгоритмов – шифра Цезаря и шифра Виженера. Программа, написанная на языке программирования C++, демонстрирует принципы симметричного шифрования и предоставляет практическое применение теоретических знаний, полученных в ходе изучения криптографии.

Реализация алгоритмов на C++ позволила эффективно работать с различными алфавитами (латиницей и кириллицей), а также с цифровыми символами, что является важным аспектом при разработке универсальных средств защиты информации. В процессе работы было изучено, как простые алгоритмы шифрования могут обеспечить базовую защиту данных и какие ограничения связаны с их криптостойкостью.

Таким образом, выполненная лабораторная работа не только способствовала закреплению теоретических знаний в области криптографии, но и дала возможность получить практические навыки реализации алгоритмов шифрования и дешифрования на языке C++. Это является хорошей базой для дальнейшего изучения более сложных методов защиты информации.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

[1] Алгоритмы шифрования. Специальный справочник. С. Панченко. – [Электронный ресурс]. – Режим доступа: <https://www.litres.ru/book/sergey-panchenko/algorithmy-shifrovaniya-specialnyy-spravochnik-991711/?ysclid=m79bb3uvu1735966776>.

[2] Прикладная криптография: протоколы, алгоритмы и исходный код на С. – [Электронный ресурс]. – Режим доступа: https://library.bsuir.by/m/12_101945_1_141673.pdf.

ПРИЛОЖЕНИЕ А

(обязательное)

Исходный код

```
#include <iostream>
#include <string>
#include <clocale>
#include <windows.h>
using namespace std;
// Шифр Цезаря
wchar_t caesarEncryptChar(wchar_t ch, int key) {
    if (ch >= L'A' && ch <= L'Z') {
        return (ch - L'A' + key + 26) % 26 + L'A';
    }
    else if (ch >= L'a' && ch <= L'z') {
        return (ch - L'a' + key + 26) % 26 + L'a';
    }
    else if (ch >= L'A' && ch <= L'Я') {
        return (ch - L'A' + key + 32) % 32 + L'A';
    }
    else if (ch >= L'a' && ch <= L'я') {
        return (ch - L'a' + key + 32) % 32 + L'a';
    }
    else if (ch == L'Ё') {
        return L'Ё';
    }
    else if (ch == L'ё') {
        return L'ё';
    }
    else if (ch >= L'0' && ch <= L'9') {
        return (ch - L'0' + key + 10) % 10 + L'0';
    }
    return ch;
}
// Функция для шифрования текста шифром Цезаря
wstring caesarCipherEncrypt(const wstring& text, int key) {
    wstring encryptedText;
    for (wchar_t ch : text) {
        encryptedText += caesarEncryptChar(ch, key);
    }
    return encryptedText;
}
// Функция для дешифрования текста шифром Цезаря
wstring caesarCipherDecrypt(const wstring& text, int key) {
    return caesarCipherEncrypt(text, -key);
}
// Шифр Виженера
wchar_t vigenereEncryptChar(wchar_t ch, wchar_t keyChar, bool
decrypt = false) {
    int shift = decrypt ? -1 : 1; // Если дешифруем, сдвиг в
    обратную сторону

    if (ch >= L'A' && ch <= L'Z') {
        return (ch - L'A' + shift * (keyChar - L'A') + 26) % 26 +
L'A';
    }
    else if (ch >= L'a' && ch <= L'z') {
```

```

        return (ch - L'a' + shift * (keyChar - L'a') + 26) % 26 +
L'a';
    }
    else if (ch >= L'A' && ch <= L'Я') {
        return (ch - L'A' + shift * (keyChar - L'A') + 32) % 32 +
L'A';
    }
    else if (ch >= L'a' && ch <= L'я') {
        return (ch - L'a' + shift * (keyChar - L'a') + 32) % 32 +
L'a';
    }
    else if (ch == L'Ё') {
        return ch;
    }
    else if (ch == L'ё') {
        return ch;
    }
    else if (ch >= L'0' && ch <= L'9' && decrypt == false) { //
при шифровании
        return (ch - L'0' + shift * (keyChar - L'0') + 10) % 10 +
L'0' - 1;
    }
    else if (ch >= L'0' && ch <= L'9' && decrypt == true) { // при
дешифровании
        return (ch - L'0' + shift * (keyChar - L'0') + 10) % 10 +
L'0' + 1;
    }
    return ch;
}
// Функция для шифрования текста шифром Виженера
wstring vigenereEncrypt(const wstring& text, const wstring& key) {
    wstring encryptedText;
    int keyIndex = 0;
    for (wchar_t ch : text) {
        encryptedText += vigenereEncryptChar(ch, key[keyIndex],
false) + 1;
        keyIndex = (keyIndex + 1) % key.length();
    }
    return encryptedText;
}
// Функция для дешифрования текста шифром Виженера
wstring vigenereDecrypt(const wstring& text, const wstring& key) {
    wstring decryptedText;
    int keyIndex = 0;
    for (wchar_t ch : text) {
        decryptedText += vigenereEncryptChar(ch, key[keyIndex],
true) - 1;
        keyIndex = (keyIndex + 1) % key.length();
    }
    return decryptedText;
}
int main() {
    setlocale(LC_ALL, "ru_RU.UTF-8");
    SetConsoleOutputCP(65001);
    SetConsoleCP(65001);
    bool repeat = true;
    while (repeat) {

```

```

int choice;
wcout << L"\nВыберите вариант шифрования:\n";
wcout << L"1 - Шифр Цезаря\n";
wcout << L"2 - Шифр Виженера\n";
wcout << L"Ваш выбор: ";
wcin >> choice;
wcin.ignore(); // удаляем символ новой строки из буфера
if (choice == 1) {
    // Режим шифрования Цезаря
    wstring text;
    int key;
    wcout << L"Введите текст для шифрования: ";
    getline(wcin, text);
    wcout << L"Введите ключ (сдвиг): ";
    wcin >> key;
    wcin.ignore();
    wstring encryptedText = caesarCipherEncrypt(text,
key);
    wcout << L"Зашифрованный текст: " << encryptedText <<
endl;

    int decryptKey;
    wcout << L"Введите ключ для дешифрования: ";
    wcin >> decryptKey;
    wcin.ignore();
    wstring decryptedText =
caesarCipherDecrypt(encryptedText, decryptKey);
    wcout << L"Расшифрованный текст: " << decryptedText <<
endl;
}
else if (choice == 2) {
    // Режим шифрования Виженера
    wstring text, key;
    wcout << L"Введите текст для шифрования: ";
    getline(wcin, text);
    wcout << L"Введите ключ: ";
    getline(wcin, key);
    wstring encryptedText = vigenereEncrypt(text, key);
    wcout << L"Зашифрованный текст: " << encryptedText <<
endl;

    wstring decryptedText = vigenereDecrypt(encryptedText,
key);
    wcout << L"Расшифрованный текст: " << decryptedText <<
endl;
}
else {
    wcout << L"Неверный выбор!" << endl;
}
wcout << L"\nХотите выполнить операцию ещё раз? (Y/N): ";
wchar_t answer;
wcin >> answer;
wcin.ignore();
if (answer == L'N' || answer == L'n') {
    repeat = false;
}
}
return 0;
}

```