

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
АДЫГЕЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Инженерно-физический факультет
Кафедра автоматизированных систем обработки информации и
управления

ОТЧЕТ ПО ПРАКТИКЕ

Программная реализация шифрования и
дешифрования. *Шифрование и дешифрование
текста шифром Цезаря.*

2 курс, группа 2ИВТ2(2)

Выполнила:

_____ М. В. Белуха
«___» _____ 2024 г.

Руководитель:

_____ С. В. Теплоухов
«___» _____ 2024 г.

Майкоп, 2024 г.

1. Введение.

- 1) Теория о шифре Цезаря.
- 2) Пример кода, решающего данную задачу.
- 3) Скриншоты примеров работы программы.

2. Ход работы

2.1. Теория о шифре Цезаря.

В криптографии при шифровании по методу Цезаря, также известном как шифр Цезаря, используется один из самых простых и широко известных методов шифрования. Шифр Цезаря назван в честь римского полководца Гая Юлия Цезаря, использовавшего его для шифрования текстов при переписке со своими военачальниками. Шифрование шифром Цезаря часто является промежуточным шагом при шифровании более сложными шифрами, например, шифром Виженера. С точки зрения математики шифр Цезаря является частным случаем аффинного шифра.

Шифр Цезаря - это разновидность шифра замены, при которой каждая буква в открытом тексте (В криптографии, обычно означает незашифрованную информацию, ожидающую ввода в криптографические алгоритмы, обычно в алгоритмы шифрования.) заменяется буквой, стоящей на некотором фиксированном расстоянии в алфавите.

Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование и дешифрование можно выразить формулами модульной арифметики. где: x -символ открытого текста, y -символ шифрованного текста, n -мощность алфавита, а k -ключ (сдвиг).

Формула шифрования символа: $y = (x + k) \bmod n$

Формула дешифрования символа: $x = (y - k) \bmod n$

Например, при сдвиге на 3: А заменяется на D, В становится Е и так далее. Пример сдвига (рис. 1).

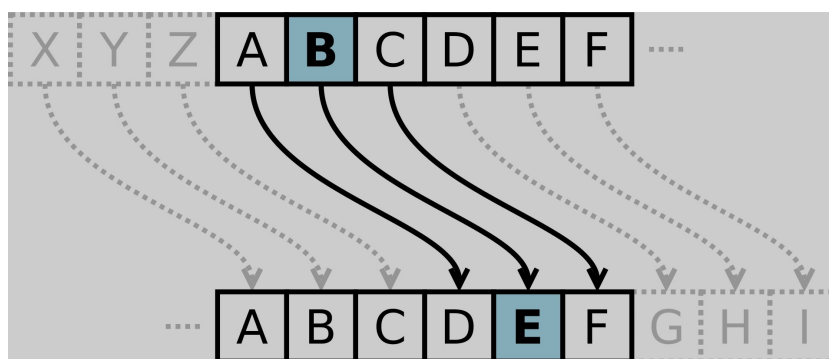


Рис. 1. Шифр Цезаря со сдвигом 3.

Как и все шифры с однобуквенной заменой, шифр Цезаря легко взломать, и в современной практике он практически не обеспечивает безопасность связи.

2.2. Пример кода, решающего данную задачу.

Далее представлен мой вариант функции на C/C++ шифрования и дешифрования текста на английском шифром Цезаря. В этом варианте используется кодировка ASCII просчитанная вручную для этих двух функций. Это рабочий способ но с Русским текстом так же сделать сложно из-за самой кодировки ASCII так как между частями алфавита (если смотреть по возрастанию десятичных кодов) есть другие символы.

```
void EinHE(string& str, int shift)
{
    cout << shift;
    int ind;
    for (int i = 0; i <= str.size(); i++)
    {
        ind = int(str[i]);
        if (((ind >= 65) and (ind <= (90 - shift))) or ((ind >= 97) and
(ind <= (122 - shift)))) str[i] = char(ind + shift);
        else if (((ind > (90 - shift)) and (ind <= 90)) or
((ind > (122 - shift)) and (ind <= 122))) str[i] = char(ind - 26 + shift);
    }
}
void HEinE(string& str, int shift)
{
    int ind;
    for (int i = 0; i <= str.size(); i++)
    {
        ind = int(str[i]);
        if (((ind >= (65 + shift)) and (ind <= 90)) or
((ind >= (97 + shift)) and (ind <= 122))) str[i] = char(ind - shift);
        else if (((ind >= 65) and (ind < (65 + shift))) or
((ind >= 97) and (ind < (97 + shift)))) str[i] = char(ind+26-shift);
    }
}
```

Далее мой вариант кода на C/C++ шифрования и дешифрования текста на английском и русском шифром Цезаря. Код работает с текстом без разделения на абзацы, с пробелами, другими символами кроме букв (без шифрования и дешифрования), буквами Русского и Английского алфавита. Есть возможность выбрать сдвиг, ввести новый текст или оставить прежний после операций. Программа закончит свою работу только после выбора выхода, который можно совершить при предоставлении любого выбора. Есть также текст и сдвиг заданные по умолчанию.

```

#include <iostream>
#include <string>
using namespace std;

const char lowRch[] = {'a','б','в','г','д','е','ё','ж','з','и','й','к',
'л','м','н','о','п','р','с','т','у','ф','х','ц','ч','ш','щ','ъ','ы',
'ь','э','ю','я'}; //массив строчных Русского алфавита
const char highRch[] = {'А','Б','В','Г','Д','Е','Ё','Ж','З','И','Й','К',
'Л','М','Н','О','П','Р','С','Т','У','Ф','Х','Ц','Ч','Ш','Щ','Ъ','Ы','Ь',
'Э','Ю','Я'}; //массив заглавных Русского алфавита
const char lowEch[] = {'a','b','c','d','e','f','g','h','i','j','k','l',
'm','n','o','p','q','r','s','t','u','v','w','x','y','z' };
//массив строчных букв Английского алфавита
const char highEch[] = {'A','B','C','D','E','F','G','H','I','J','K','L',
'M','N','O','P','Q','R','S','T','U','V','W','X','Y','Z'};
//массив заглавных букв Английского алфавита

void correct(int& j, string& str, string ch, int shift, int i, int ABC)
{ //функция для шифрования/дешифрования символа со сдвигом
  j += shift; //введённый сдвиг индекса буквы по алфавиту
  if (j >= ABC) j -= ABC;
  //корректировка при необходимости символа в диапазон алфавита
  else if (j < 0) j += ABC;
  str[i] = ch[j]; //замена символа на зашифрованный
}

void NH(string& str, int shift, int coise)
{ //функция для определения символа и его шифрования/дешифрования
  int ABCe = 26; //количество букв Английского алфавита
  int ABCr = 33; //количество букв Русского алфавита
  if (coise == 2) shift = -shift; //корректировка вида операции
  for (unsigned i = 0; i < str.size(); i++)
  { //цикл для всех символов строки
    for (int j = 0; j < 33; j++)
    { //перебор всех буквы обоих алфавитов для поиска соответствия
      if (str[i] == lowEch[j] and j < 26)
      { //сравнение с строчной английской буквой
        correct(j, str, lowEch, shift, i, ABCe);
        break;
      }
      else if (str[i] == highEch[j] and j < 26)
      { //сравнение с заглавной английской буквой
        correct(j, str, highEch, shift, i, ABCe);
        break;
      }
    }
  }
}

```

```

    }
    else if (str[i] == lowRch[j])
    { //сравнение с строчной русской буквой
        correct(j, str, lowRch, shift, i, ABCr);
        break;
    }
    else if (str[i] == highRch[j])
    { //сравнение с заглавной русской буквой
        correct(j, str, highRch, shift, i, ABCr);
        break;
    }
}
}
if (coise == 2) shift = -shift;
//корректировка сдвига для следующий операций без его изменения
}

```

```

void correctcin(int& choice)
{ //функция для ввода выбора и его проверки на корректность
    cin >> choice; //ввод выбора
    if (choice == 3) exit(0); //выбор выйти
    if (choice != 1 and choice != 2)
    { //проверка корректности и при некорректности повторный ввод
        cout << "\nВвод некорректный, попробуйте снова. ->";
        cin >> choice;
        if (choice == 3) exit(0);
    }
}

```

```

int main()
{
    setlocale(LC_ALL, "Russian"); //задаёт русский текст
    system("chcp 1251");

    string str="АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ
абвгдеёжзийклмнопрстуфхцчшщъыьэюя
ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz";
    cout << "\nВведите '3' для выхода при любом вводе выбора.";

    int choice=1, shift=3;

    cout << "\n Текст по умолчанию: ";
    cout << str;
}

```

```

cout << "\n Сдвиг по умолчанию: ";
cout << shift;

for ( ; choice!=3; )//цикл с выходом только при условии выбора выхода
{
    cout << "\nВыберите текст";
    cout << "('1'-оставить прошлый, '2'-ввести новый). ->";
    correctcin(choice);
    if (choice == 2)
        //в случае выбора введения нового текста его ввод
        //(ввод без разделения абзацев)
        {
            cout << "\n";
            cin.ignore();
            getline(cin, str);
            cout << "\n";
        }

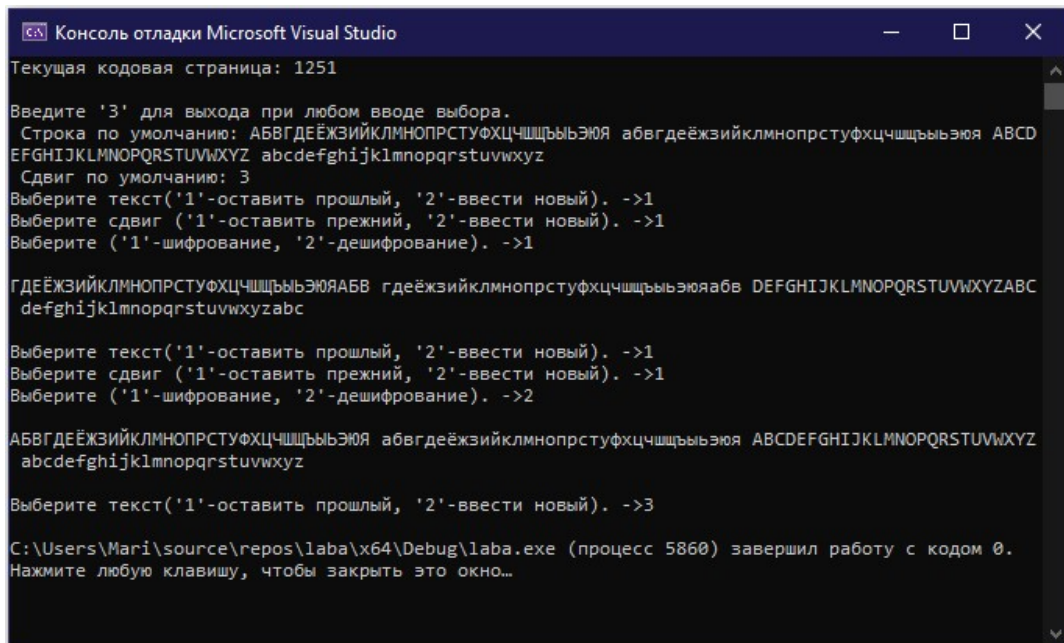
    cout << "Выберите сдвиг ";
    cout << "('1'-оставить прежний, '2'-ввести новый). ->";
    correctcin(choice);
    if (choice == 2) cin >> shift;
    //в случае выбора введения нового сдвига его ввод

    cout << "Выберите ('1'-шифрование, '2'-дешифрование). ->";
    correctcin(choice);
    NH(str, shift, choice);
    cout << "\n" << str << "\n";//вывод текста после операции
}
return 0;
}

```

Примеры работы программы приведены в пункте 2.3 на стр. 7 на рис. 2, 3.

2.3. Скриншоты примеров работы программы.



```
Консоль отладки Microsoft Visual Studio
Текущая кодовая страница: 1251

Введите '3' для выхода при любом вводе выбора.
Строка по умолчанию: АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ абвгдеёжзийклмнопрстуфхцчшщъыьэюя ABCD
EFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz
Сдвиг по умолчанию: 3
Выберите текст ('1'-оставить прошлый, '2'-ввести новый). ->1
Выберите сдвиг ('1'-оставить прежний, '2'-ввести новый). ->1
Выберите ('1'-шифрование, '2'-дешифрование). ->1

ГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВ гдеёжзийклмнопрстуфхцчшщъыьэюяабв DEFGHIJKLMNOPQRSTUVWXYZABC
defghijklmnopqrstuvwxyzabc

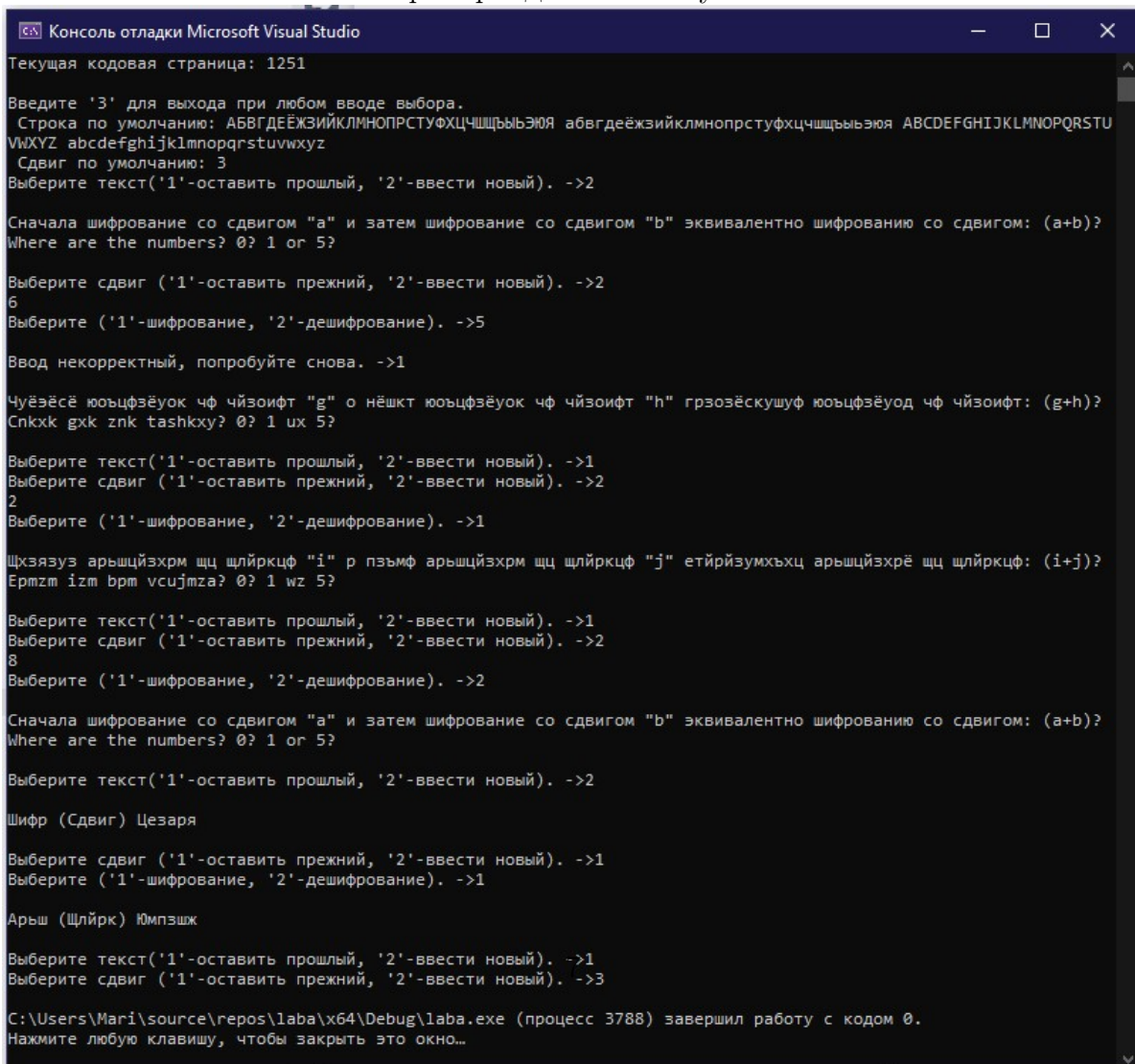
Выберите текст ('1'-оставить прошлый, '2'-ввести новый). ->1
Выберите сдвиг ('1'-оставить прежний, '2'-ввести новый). ->1
Выберите ('1'-шифрование, '2'-дешифрование). ->2

АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ абвгдеёжзийклмнопрстуфхцчшщъыьэюя ABCDEFGHIJKLMNOPQRSTUVWXYZ
abcdefghijklmnopqrstuvwxyz

Выберите текст ('1'-оставить прошлый, '2'-ввести новый). ->3

C:\Users\Mari\source\repos\laba\64\Debug\laba.exe (процесс 5860) завершил работу с кодом 0.
Нажмите любую клавишу, чтобы закрыть это окно...
```

Рис. 2. Пример с данными по умолчанию.



```
Консоль отладки Microsoft Visual Studio
Текущая кодовая страница: 1251

Введите '3' для выхода при любом вводе выбора.
Строка по умолчанию: АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ абвгдеёжзийклмнопрстуфхцчшщъыьэюя ABCDEFGHIJKLMNOPQRSTU
VWXYZ abcdefghijklmnopqrstuvwxyz
Сдвиг по умолчанию: 3
Выберите текст ('1'-оставить прошлый, '2'-ввести новый). ->2

Сначала шифрование со сдвигом "a" и затем шифрование со сдвигом "b" эквивалентно шифрованию со сдвигом: (a+b)?
Where are the numbers? 0? 1 or 5?

Выберите сдвиг ('1'-оставить прежний, '2'-ввести новый). ->2
6
Выберите ('1'-шифрование, '2'-дешифрование). ->5

Ввод некорректный, попробуйте снова. ->1

Чуёэёсё юьцфзёук чф чйзоифт "g" о нёшт юьцфзёук чф чйзоифт "h" грзозёскушф юьцфзёуод чф чйзоифт: (g+h)?
Cпkxk gxxk znk tashkxy? 0? 1 ux 5?

Выберите текст ('1'-оставить прошлый, '2'-ввести новый). ->1
Выберите сдвиг ('1'-оставить прежний, '2'-ввести новый). ->2
2
Выберите ('1'-шифрование, '2'-дешифрование). ->1

Щхзязуэ арьщйзхрм щц шйрkcф "i" р пзъмф арьщйзхрм щц шйрkcф "j" етйрйзумхъхц арьщйзхрё щц шйрkcф: (i+j)?
Ертzm izm brm vcujmza? 0? 1 wz 5?

Выберите текст ('1'-оставить прошлый, '2'-ввести новый). ->1
Выберите сдвиг ('1'-оставить прежний, '2'-ввести новый). ->2
8
Выберите ('1'-шифрование, '2'-дешифрование). ->2

Сначала шифрование со сдвигом "a" и затем шифрование со сдвигом "b" эквивалентно шифрованию со сдвигом: (a+b)?
Where are the numbers? 0? 1 or 5?

Выберите текст ('1'-оставить прошлый, '2'-ввести новый). ->2

Шифр (Сдвиг) Цезаря

Выберите сдвиг ('1'-оставить прежний, '2'-ввести новый). ->1
Выберите ('1'-шифрование, '2'-дешифрование). ->1

Арьш (Щйрк) Юмпзшж

Выберите текст ('1'-оставить прошлый, '2'-ввести новый). ->1
Выберите сдвиг ('1'-оставить прежний, '2'-ввести новый). ->3

C:\Users\Mari\source\repos\laba\64\Debug\laba.exe (процесс 3788) завершил работу с кодом 0.
Нажмите любую клавишу, чтобы закрыть это окно...
```

Рис. 3. Пример с введенными с клавиатуры текстом и сдвигом.

3. Источники информации.

Список литературы

- [1] [https://dwwweb.ru/page/css/fonts/007 skopirovat russkiy alfavit.html](https://dwwweb.ru/page/css/fonts/007_skopirovat_russkiy_alfavit.html) (Сайт для копирования Русского алфавита.)
- [2] [https://dwwweb.ru/page/css/fonts/004 skopirovat angliyskiy alfavit.html](https://dwwweb.ru/page/css/fonts/004_skopirovat_angliyskiy_alfavit.html) (Сайт для копирования Английского алфавита.)
- [3] <https://poformule.ru/text/shifr-cezarya> (Сайт онлайн шифрования и дешифрования текста шифром Цезаря для проверки работы программы.)
- [4] <https://studfile.net/preview/712575/> (Таблица ASCII.)
- [5] https://translated.turbopages.org/proxy_u/en-ru.ru.16d9700b-665a6738-35ed5a8b-74722d776562/https/en.wikipedia.org/wiki/Plaintext (О шифре Цезаря.)
- [6] <https://worldofhistory.ru/kak-skryvali-informatsiyu-istoriya-shifrov/> (О шифровании.)