МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ

УНИВЕРСИТЕТ им. Р.Е.АЛЕКСЕЕВА

Институт радиоэлектроники и информационных технологий

ОТЧЕТ

по лабораторной работе №1

«Шифры замены»

по дисциплине

«Методы и средства защиты информации»

РУКОВОДИТЕЛЬ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_ Капранов С. Н.\_\_

(подпись) (фамилия, и.,о.)

СТУДЕНТ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Сухоруков В.А.\_\_\_

(подпись) (фамилия, и.,о.)

\_\_\_\_\_\_19-ВМ\_\_\_\_\_\_\_\_

(шифр группы)

Работа защищена «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_

С оценкой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

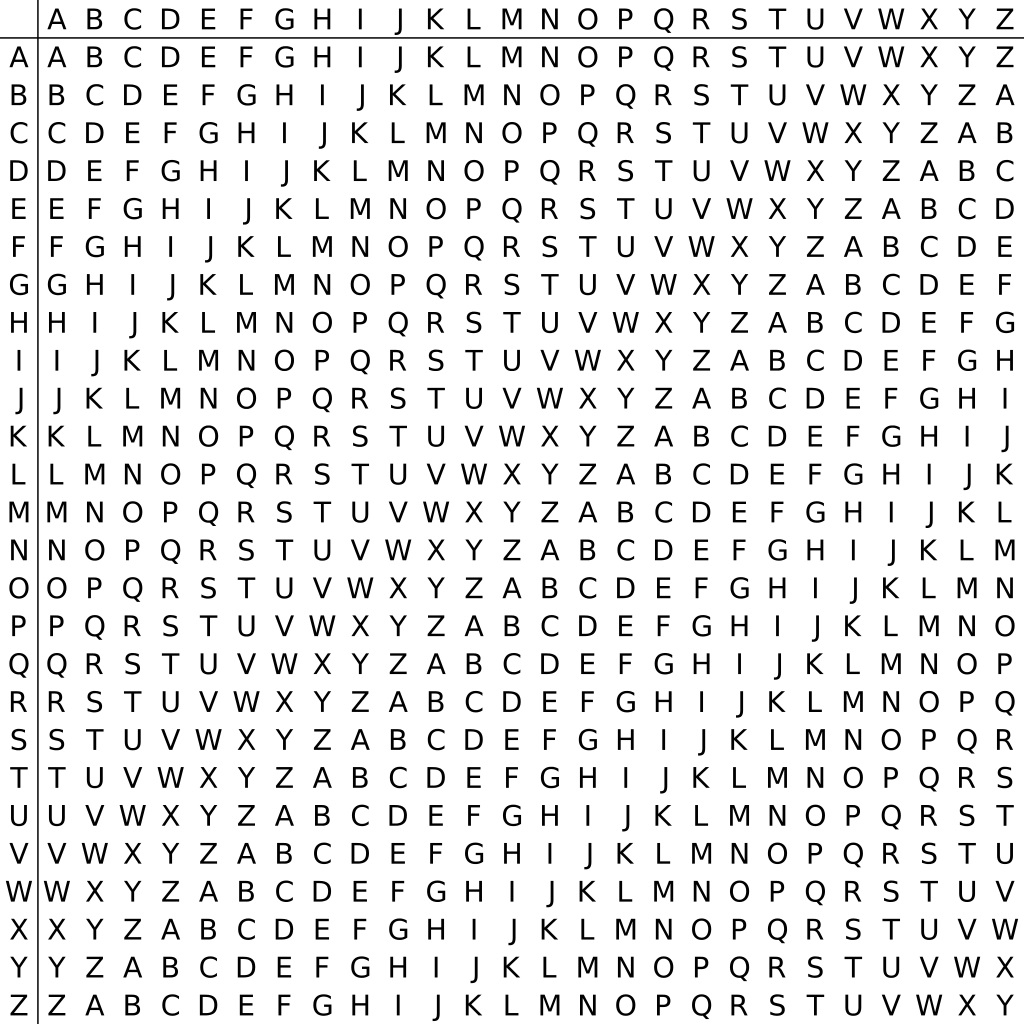
Нижний Новгород 2022

# Задание №1.6

Реализовать алгоритм шифрования данных «Шифр Вижинера»

# Описание алгоритма.

Шифр Виженера состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига. Для зашифровывания может использоваться таблица алфавитов, называемая квадрат Виженера. Применительно к латинскому алфавиту таблица Виженера составляется из строк по 26 символов, причём каждая следующая строка сдвигается на несколько позиций. Таким образом, в таблице получается 26 различных шифров Цезаря. На каждом этапе шифрования используются различные алфавиты, выбираемые в зависимости от символа ключевого слова.



Например, предположим, что исходный текст имеет такой вид:

ATTACKATDAWN

Человек, посылающий сообщение, записывает ключевое слово («LEMON») циклически до тех пор, пока его длина не будет соответствовать длине исходного текста:

LEMONLEMONLE

Первый символ исходного текста («A») зашифрован последовательностью L, которая является первым символом ключа. Первый символ зашифрованного текста («L») находится на пересечении строки L и столбца A в таблице Виженера. Точно так же для второго символа исходного текста используется второй символ ключа; то есть второй символ зашифрованного текста («X») получается на пересечении строки E и столбца T. Остальная часть исходного текста шифруется подобным способом.

Исходный текст: ATTACKATDAWN

Ключ: LEMONLEMONLE

Зашифрованный текст: LXFOPVEFRNHR

Расшифровывание производится следующим образом: находим в таблице Виженера строку, соответствующую первому символу ключевого слова; в данной строке находим первый символ зашифрованного текста. Столбец, в котором находится данный символ, соответствует первому символу исходного текста. Следующие символы зашифрованного текста расшифровываются подобным образом.

# Алгебраическое описание

Если N - количество букв в алфавите, mi - номер буквы открытого текста, ki - номер буквы ключа в алфавите, то шифрование Виженера можно записать следующим образом:

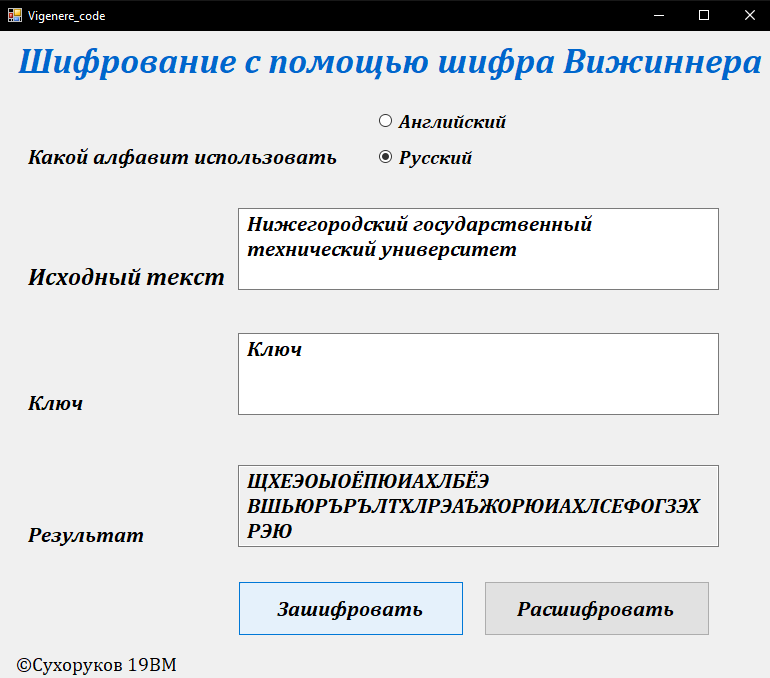
***Ci = (Mi+Ki) mod N***

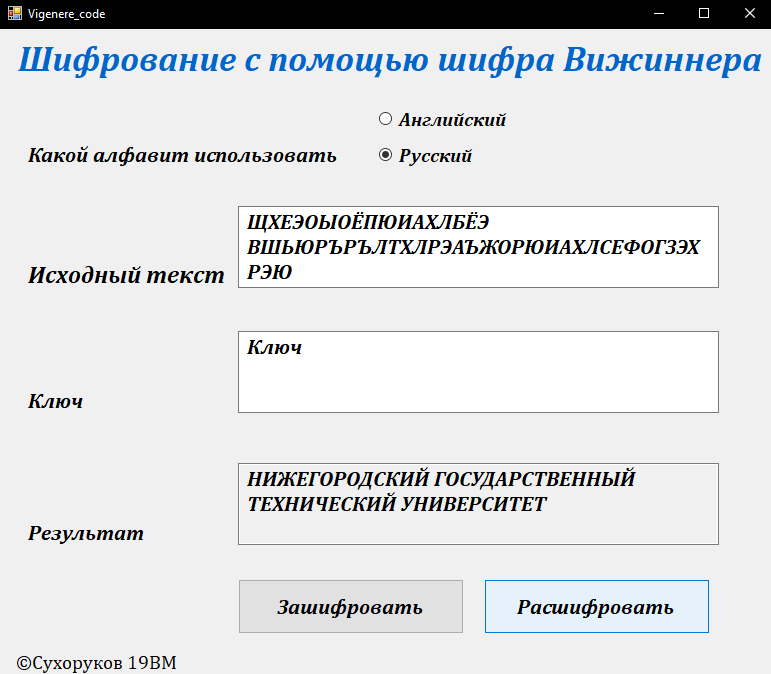
И расшифровывание:

***Mi = (Ci-Ki+N) mod N***

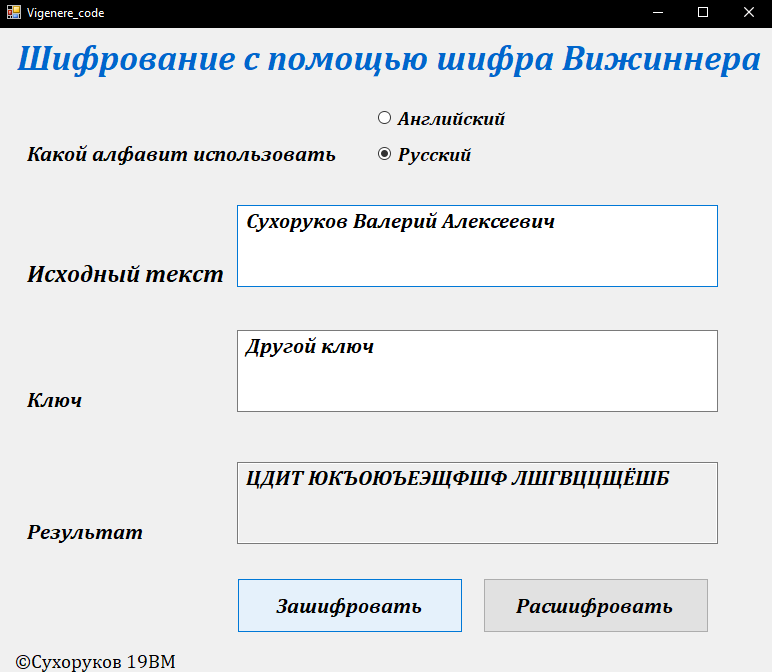
# Примеры шифрования и расшифровывания

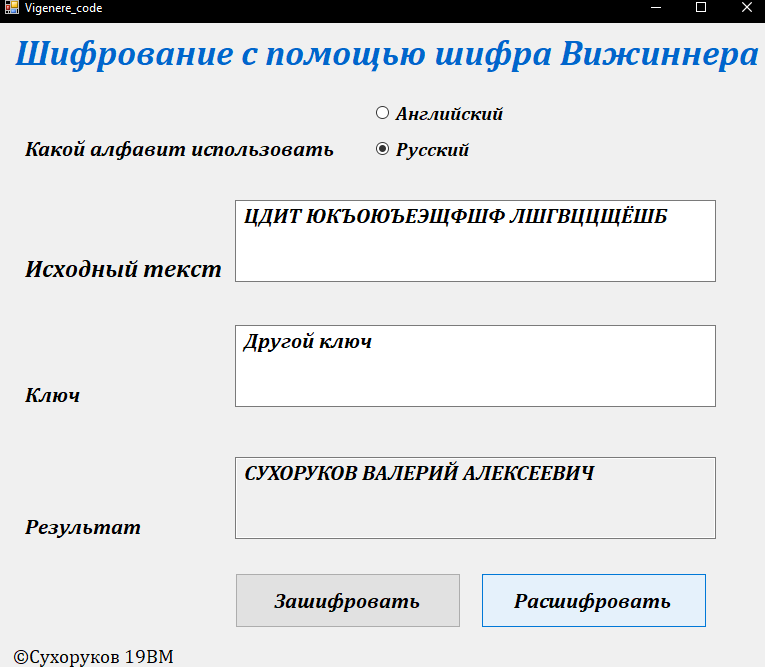
* Нижегородский государственный технический университет





* Сухоруков Валерий Алексеевич





# Текст программы

* Функция зашифровки текста

//Зашифровать

String^ Encode(String^ input\_string, String^ key, string language) {

String^ characters(L"");

//Выбор языка алфавита

if (language == "en") {

characters = " ABCDEFGHIJKLMNOPQRSTUVWXYZ";

}

if (language == "rus") {

characters = " АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ";

}

size\_t N = characters->Length;

String^ res="";

size\_t key\_index = 0,c=0,c1=0,c2=0;

//Приведение букв открытого текста и ключа

//к верхнему регистру

key = key->ToUpper();

input\_string = input\_string->ToUpper();

for (size\_t i = 0; i < input\_string->Length; i++) {

//Поиск в алфавите текущей буквы открытого текста

//И запоминание её номера

c = characters->IndexOf(input\_string[i]);

// Поиск в алфавите текущей буквы ключа

//И запоминание её номера

c1= characters->IndexOf(key[key\_index]);

//Расчет номера буквы закрытого текста

c2 = (c1 + c) % N;

//Добавление буквы в зашифрованный текст

res = res + characters[c2];

key\_index++;

//Если индекс буквы ключа равен длине ключа,

//То повторяем ключ

if (key\_index == key->Length) { key\_index = 0; }

}

return res;

}

* Функция расшифровки текста

//Расшифровать

String^ Decode(String^ input\_string, String^ key,string language) {

String^ characters(L"");

//Выбор языка алфавита

if (language == "en") {

characters = " ABCDEFGHIJKLMNOPQRSTUVWXYZ";

}

if (language == "rus") {

characters = " АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ";

}

size\_t N = characters->Length;

String^ res = "";

size\_t key\_index = 0, c = 0, c1 = 0, c2 = 0;

//Приведение букв закрытого текста и ключа

//к верхнему регистру

key = key->ToUpper();

input\_string = input\_string->ToUpper();

for (size\_t i = 0; i < input\_string->Length; i++) {

//Поиск в алфавите текущей буквы закрытого текста

//И запоминание её номера

c = characters->IndexOf(input\_string[i]);

//Поиск в алфавите текущей буквы ключа

//И запоминание её номера

c1 = characters->IndexOf(key[key\_index]);

//Расчет номера буквы открытого текста

c2 = (c - c1 + N) % N;

//Добавление буквы в расшифрованный текст

res = res + characters[c2];

key\_index++;

//Если индекс буквы ключа равен длине ключа,

//То повторяем ключ

if (key\_index == key->Length) { key\_index = 0; }

}

return res;

}