#### Министерство науки и высшего образования Российской Федерации

#### Федеральное государственное бюджетное образовательное учреждение науки и высшего образования

#### «Владимирский государственный университет

#### имени Александра Григорьевича и Николая Григорьевича Столетовых»

**(ВлГУ)**

**Кафедра информационных систем и программной инженерии**

Лабораторная работа № 05

по дисциплине

"Администрирование и безопасность программно-информационных систем"

Тема: "Шифрование методом перестановки"

Выполнил:

ст. гр. ПРИ-117

В.Г. Хлызова

Принял:

И.В. Спирин

Владимир, 2020 г.

## ЦЕЛЬ РАБОТЫ

Выполнить шифрование заданного сообщения простейшим шифром перестановок и выполнить проверку правильности шифрования.

ХОД РАБОТЫ

Зашифровать следующий текст: Двадцать первое. Ночь. Понедельник. Очертанья столицы во мгле. Сочинил же какой-то бездельник, что бывает любовь на земле. И от лености или от скуки все поверили, так и живут: ждут свиданий, боятся разлуки и любовные песни поют.

(1 вариант – “головоломка”)

<?php

// удаляем все пробелы и символы и переводим в нижний регистр

function conversion($line){

    $line=mb\_strtolower($line);

    $array\_of\_characters = array(' ', ".", ",", "-", ":");

    foreach($array\_of\_characters as $character)

        $line=str\_replace($character, '',$line);

    return $line;

}

// каждой букве ключа присваиваем номер

function selecting\_a\_number($key, $alphabet){

    $key = preg\_split("//u", $key, -1, PREG\_SPLIT\_NO\_EMPTY);

    $alphabet = preg\_split("//u", $alphabet, -1, PREG\_SPLIT\_NO\_EMPTY);

    $array\_key=array();

    array\_push($array\_key,$key);

    $array\_number=array\_fill(0, count($key), 0);

    $i=0;

    foreach($alphabet as $a)

        foreach($key as $c=>$k)

            if($k==$a) {

                $array\_number[$c]=++$i;

            }

    array\_push($array\_key,$array\_number);

    return  $array\_key;

}

// в массив с ключем добавляется текст для шифрования

function add\_line($line, $array\_key){

    $array\_for\_encryption=array();

    $array\_for\_encryption=array\_merge($array\_for\_encryption, $array\_key);

    $line = preg\_split("//u", $line, -1, PREG\_SPLIT\_NO\_EMPTY);

    $array\_symbols=array();

    $i=0;

    foreach($line as $l){

        if ($i<count($array\_key[0])){

            $array\_symbols[$i] = $l;

            $i++;

        }else{

            array\_push($array\_for\_encryption, $array\_symbols);

            $array\_symbols=array();

            $array\_symbols[0]=$l;

            $i=1;

        }

    }

    $c=count($array\_symbols);

    for ($i=$c; $i<=count($array\_key[0]); $i++){

        $array\_symbols[$i]='';

    }

    array\_push($array\_for\_encryption, $array\_symbols);

    return $array\_for\_encryption;

}

// из массива записываем в строку столбики в соответствии с номерами букв ключа

function returning\_an\_encrypted\_line($array\_for\_encryption){

    $line="";

    for ($i = 1; $i <= count($array\_for\_encryption[0]); $i++){

        $key = array\_search($i, $array\_for\_encryption[1]);

        for($n=2; $n<count($array\_for\_encryption);$n++){

        $line=$line.$array\_for\_encryption[$n][$key];

        }

    $line=$line." ";

    }

    return $line;

}

// возвращаем из зашифрованной строки массив символов

function return\_an\_array\_of\_symbol($line){

    $line = explode(" ", $line);

    $array\_of\_symbol=array();

    $max=0;

    foreach($line as $l){

        $l=preg\_split("//u", $l, -1, PREG\_SPLIT\_NO\_EMPTY);

        array\_push($array\_of\_symbol, $l);

        if($max<count($l)) $max=count($l);

    }

    foreach($array\_of\_symbol as $key=>$symbol){

        if (count($symbol)<$max) $array\_of\_symbol[$key][$max-1]='';

    }

    return $array\_of\_symbol;

}

// в массив с ключем добавляем текст для расшифровки

function return\_array\_for\_decode($array\_of\_symbol, $array\_key){

    for($j=0; $j<count($array\_of\_symbol[0]); $j++){

        $i=0;

        $array\_for\_decode=array();

        foreach($array\_key[1] as $numb){

            $array\_for\_decode[$i]=$array\_of\_symbol[$numb-1][$j];

            $i++;

        }

        array\_push($array\_key, $array\_for\_decode);

    }

    return $array\_key;

}

//\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*ИСХОДНЫЕ ДАННЫЕ\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

$alphabet='абвгдеёжзийклмнопрстуфхцчшщъыьэюя';

$line=readline("Введите исходный текст: ");

$key=readline("Введите ключ: ");

echo "\n\n";

$action=readline("1-зашифровать, 2-расшифровать: ");

switch ($action){

//\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*ШИФРОВАНИЯ\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

    case (string)1:

        //переводим строку в нижний регистр, удаляем пробелы и знаки препинания

        $line=conversion($line);

        echo "Преобразуем строку: \n$line\n\n";

        //каждой букве ключа задаём номер

        echo "  Каждой букве ключа присваиваем номер: \n";

        $array\_key=selecting\_a\_number($key, $alphabet);

        foreach ($array\_key as $k=>$a){

            foreach ($a as $i){

                if((gettype($i)=="integer")&(strlen("$i")==2)) echo " $i ";

                else echo "  $i ";

            }

            echo "\n";

        }

        echo "\n\n";

        //добавляем в массив текст

        $array\_for\_encryption=add\_line($line, $array\_key);

        echo " Записываем весь текст в массив: \n";

        foreach ($array\_for\_encryption as $k=>$a){

            foreach ($a as $i){

                if((gettype($i)=="integer")&(strlen("$i")==2)) echo " $i ";

                else echo "  $i ";

            }

            echo "\n";

        }

        echo "\n\n";

        //возвращаем зашифрованный текст обратно в строку

        echo "Зашифрованное сообщение: \n";

        $line=returning\_an\_encrypted\_line($array\_for\_encryption);

        echo "$line\n\n";

        break;

//\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*РАСШИФРОВКА\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

    case (string)2:

        //Вовзвращаем массив символов из строки

        $array\_of\_symbol=return\_an\_array\_of\_symbol($line);

        foreach($array\_of\_symbol as $arr){

            foreach($arr as $a){

                echo $a;

            }

            echo "\n";

        }

        echo "\n\n";

        //каждой букве ключа задаём номер

        echo "  Каждой букве ключа присваиваем номер: \n";

        $array\_key=selecting\_a\_number($key, $alphabet);

        foreach ($array\_key as $k=>$a){

            foreach ($a as $i){

                if((gettype($i)=="integer")&(strlen("$i")==2)) echo " $i ";

                else echo "  $i ";

            }

            echo "\n";

        }

        echo "\n\n";

        //собираем масив для дешифрования

         $array\_for\_decode=return\_array\_for\_decode($array\_of\_symbol, $array\_key);

         foreach ($array\_for\_decode as $k=>$a){

            foreach ($a as $i){

                if((gettype($i)=="integer")&(strlen("$i")==2)) echo " $i ";

                else echo "  $i ";

            }

            echo "\n";

        }

        echo "\n\n";

        break;

    default: echo "Был введен неверный символ(";

}

?>

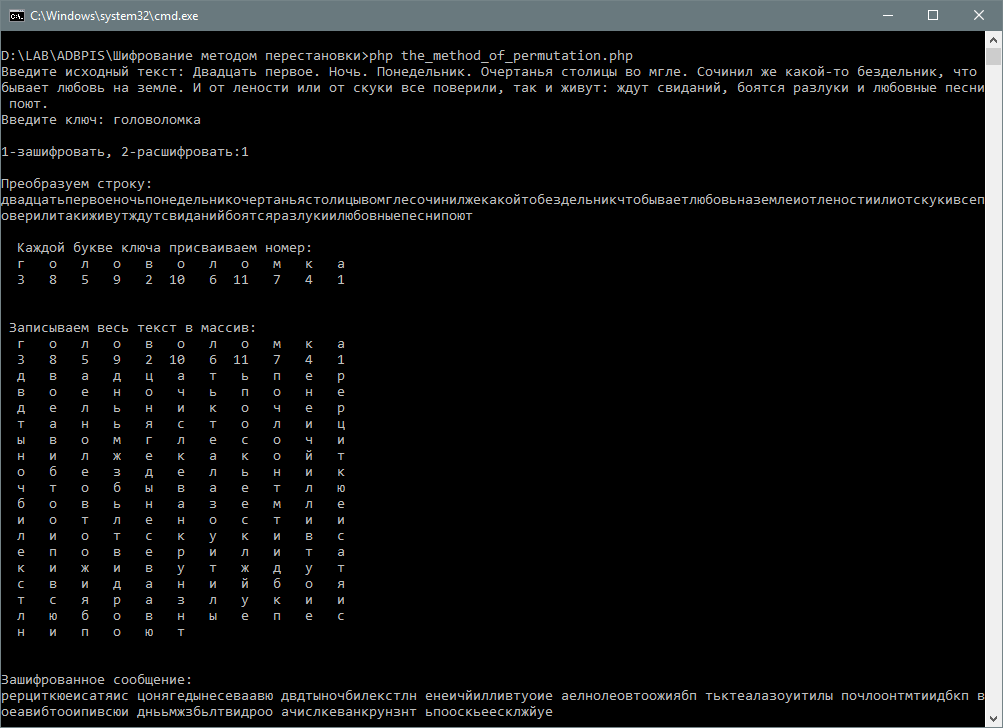


Рисунок 1. Выполняем шифрование.

Зашифрованное сообщение: рерциткюеисатяис цонягедынесеваавю двдтыночбилекстлн енеичйилливтуоие аелнолеовтоожиябп тьктеалазоуитилы почлоонтмтиидбкп воеавибтооипивсюи днььмжзбьлтвидроо ачислкеванкрунзнт ьпооскьеесклжйуе.

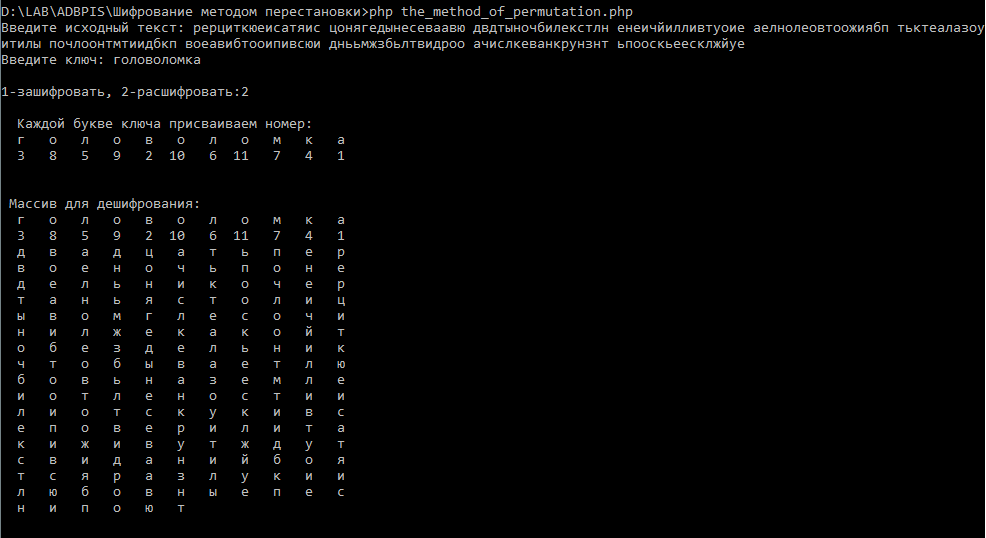


Рисунок 2. Расшифровка полученного сообщения.

ВЫВОД

В ходе лабораторной работы было выполнено шифрование заданного сообщения простейшим шифром перестановок и выполнена проверка правильности шифрования.