#### 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 № 06

по дисциплине

"Администрирование и безопасность программно-информационных систем"

Тема: "Использование гаммирования при шифровании"

Выполнил:

ст. гр. ПРИ-117

В.Г. Хлызова

Принял:

И.В. Спирин

Владимир, 2020 г.

## ЦЕЛЬ РАБОТЫ

Освоить на практике применение алгоритма шифрования методом гаммирования.

ОПИСАНИЕ АЛГОРИТМА

Для примера зашифруем слово “гаммирование”, используя знаки гаммы: 1 9 2 8 3.

1. Представим символы исходного слова в виде двоичного кода. Представление букв в двоичной системе берем из таблицы в методических указаниях к лабораторной работе.

Таблица 1. Таблица для шифрования.





1. Знаки гаммы так же представляем в виде двоичного кода.



1. Применяем любую логическую операцию (например, сложение по модулю два) посимвольно к двоичному представлению шифруемого текста и знакам гаммы. Так как знаков гаммы меньше чем букв в шифруемом слове, знаки гаммы будут повторятся циклически.



Суть такого метода шифрования заключается в наложение символов гаммы на сообщение. Для расшифровки с помощью гаммы мы получаем из зашифрованного текста двоичные символы исходного текста, отталкиваясь от законов используемой логической операции.

Например, если зашифрованный символ имеет код 001010, знак гаммы – 000001, то исходный символ – 001011. Таким образом получаем все символы зашифрованного сообщения в двоичном коде и по таблице 1 возвращаем букву по её двоичному представлению.

ЗАДАНИЕ

Зашифруйте следующее предложение методом гаммирования. «Помехоустойчивое кодирование – это кодирование с возможностью восстановления потерянных или ошибочно принятых данных.»

Знаки гаммы: 2 3 10 4 1 5 6 7 8 11 15 14 12 13 9 0.

Шифрование происходит в цикле (знак гаммы повторяется циклически).

<?php

    function mod\_add($binone, $bintwo){

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

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

        $result="";

        for($i=0; $i<count($binone); $i++){

            $result.=($binone[$i]+$bintwo[$i])%2;

        }

        return $result;

    }

    function decrypt\_mod\_add($binone, $bintwo){

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

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

        $result="";

        for($i=0; $i<count($binone); $i++){

            if($binone[$i]==$bintwo[$i]){

                $result.="0";

            } else $result.="1";

        }

        return $result;

    }

   $alphabet = ["а"=>"000001", "б"=>"001001", "в"=>"001010",

                "г"=>"001011", "д"=>"001100", "е"=>"000010",

                "ж"=>"001101", "з"=>"001110", "и"=>"000011",

                "й"=>"011111", "к"=>"001111", "л"=>"010000",

                "м"=>"010001", "н"=>"010010", "о"=>"000100",

                "п"=>"010011", "р"=>"010100", "с"=>"010101",

                "т"=>"010110", "у"=>"000101", "ф"=>"010111",

                "х"=>"011000", "ц"=>"011001", "ч"=>"011010",

                "ш"=>"011011", "щ"=>"011100", "ъ"=>"100000",

                "ы"=>"011101", "ь"=>"011110", "э"=>"000110",

                "ю"=>"000111", "я"=>"001000", " "=>"100001"];

    $gammy\_signs = [2, 3, 10, 4, 1, 5, 6, 7, 8, 11, 15, 14, 12, 13, 9, 0];

    $gammy\_signs\_binary = [];

    $msg=readline(" введите сообщение: ");

    //Двоичное представление знаков гаммы

    foreach ($gammy\_signs as $sign){

        $s=decbin($sign);

        $len=strlen($s);

        for ($i=0; $i<6-$len; $i++){

            $s="0".$s;

        }

        array\_push($gammy\_signs\_binary, $s);

    }

    echo "\nЗнаки гаммы: \n";

    for($i=0; $i<count($gammy\_signs); $i++){

        if(strlen($gammy\_signs[$i])==2)

            echo "  ".$gammy\_signs[$i]." -> ".$gammy\_signs\_binary[$i]."\n";

        else echo "  ".$gammy\_signs[$i]."  -> ".$gammy\_signs\_binary[$i]."\n";

    }

    echo "\n выберите действия\n   1: зашифровать сообщение\n   2: расшифровать сообщение\n";

    $action=readline();

    switch ($action){

        case 1:

            echo "\n зашифровываем сообщение\n\n";

            //удаляем пробелы и знаки препинания из сообщения

            $msg=mb\_strtolower($msg);

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

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

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

            //делаем массив из строки

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

            //каждой букве сообщения присваиваем двоичный код из алфавита

            $msg\_binary=[];

            foreach($msg as $ms){

                array\_push($msg\_binary, $alphabet[$ms]);

            }

            $j=1;

            for($i=0; $i<count($msg); $i++){

                echo "  ".$msg[$i]." -> ".$msg\_binary[$i]."  ";

                if (($j++)%7==0) echo "\n";

            }

            //сложение по модулю 2

            $j=0; $result="";

            for($i=0; $i<count($msg\_binary); $i++){

                if ($j<count($gammy\_signs\_binary)){

                    $result.=mod\_add($msg\_binary[$i], $gammy\_signs\_binary[$j])." ";

                    $j++;

                }

                else{

                    $result.=mod\_add($msg\_binary[$i], $gammy\_signs\_binary[0])." ";

                    $j=1;

                }

            }

            echo "\n\n зашифрованное сообщение: \n  ".$result."\n";

            break;

        case 2:

            echo "\n расшифровываем сообщение\n\n";

            //делаем массив из строки

            $msg=str\_replace(' ', '', $msg);

            $msg=str\_split($msg, 6);

            //получаем массив букв в двоичном виде

            $j=0; $result=[];

            for($i=0; $i<count($msg); $i++){

                if ($j<count($gammy\_signs\_binary)){

                    array\_push($result, decrypt\_mod\_add($msg[$i], $gammy\_signs\_binary[$j]));

                    $j++;

                }

                else{

                    array\_push($result, decrypt\_mod\_add($msg[$i], $gammy\_signs\_binary[0]));

                    $j=1;

                }

            }

            echo " массив букв в двоичном виде: \n";

            $j=1;

            for($i=0; $i<count($result); $i++){

                echo "  ".$result[$i]."  ";

                if (($j++)%7==0) echo "\n";

            }

            //возвращаем буквы

            $finally\_line="";

            foreach($result as $r){

                $finally\_line.=array\_search($r, $alphabet);

            }

            echo "\n\n расшифрованное сообщение: \n  ".$finally\_line."\n";

            break;

        default:

            echo "\n был введен не верный символ";

    }

?>

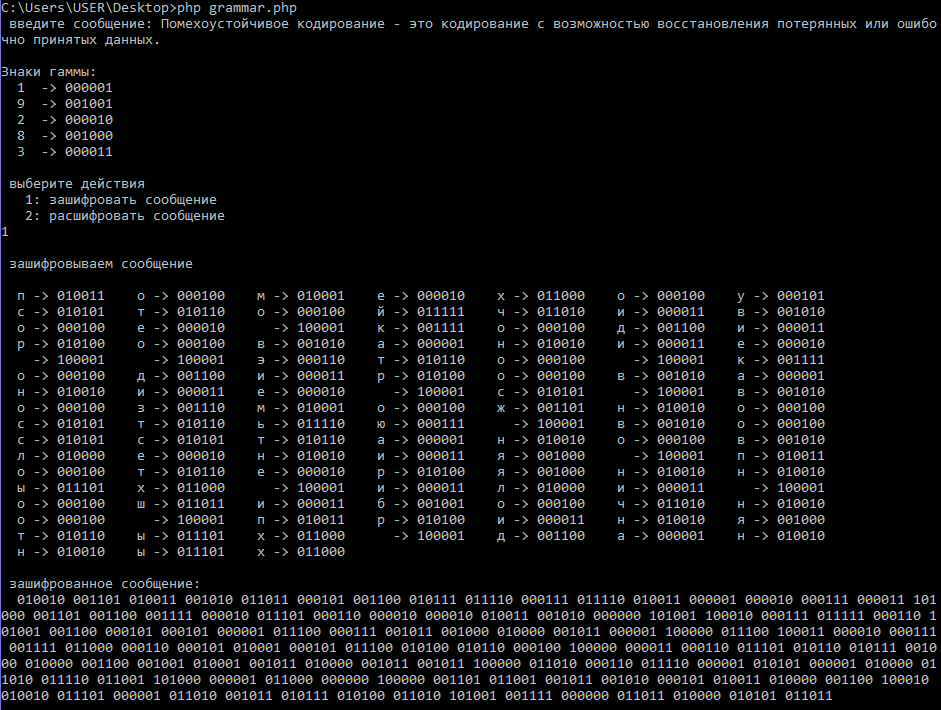


Рисунок 1. Зашифровываем сообщение.

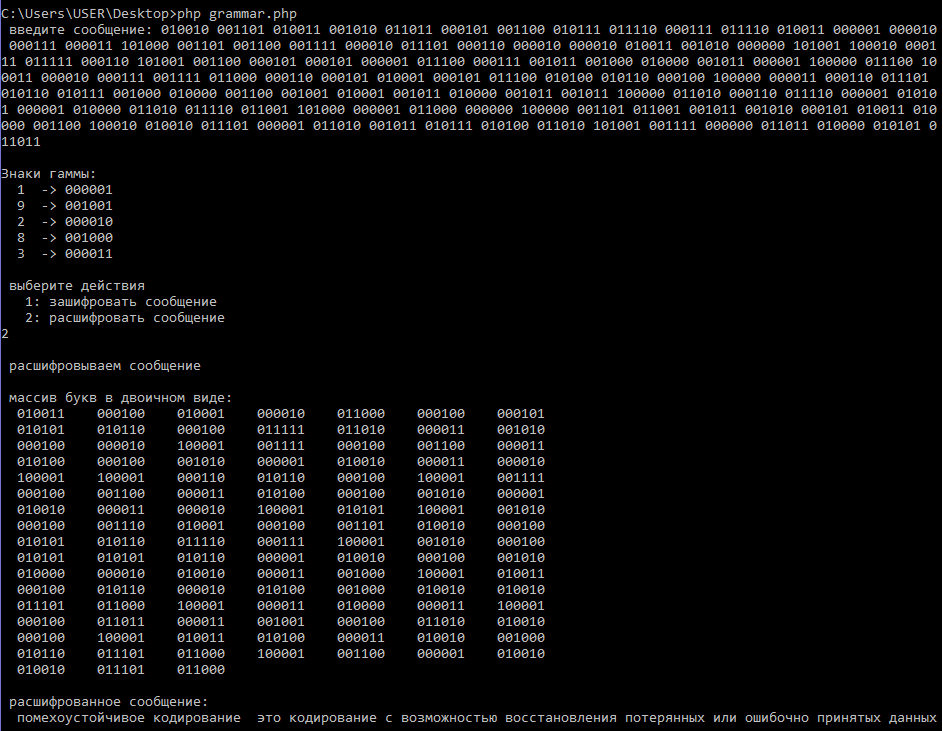


Рисунок 2. Расшифровываем сообщение.

ВЫВОД

В ходе лабораторной работы было выполнено шифрования методом гаммирования.