

Математические основы защиты информации и информационной безопасности. Отчет по лабораторной работе № 3

шифрование гаммированием

Мохамед Либан Абдуллахи

Содержание

Цель работы	1
Задание	1
Выполнение Работы	1
Исходный код	2
Результат Работы	5
Выводы	5
Список литературы	5

Цель работы

Освоить на практике применение алгоритма шифрования методом гаммирования.

Задание

Реализовать алгоритм шифрования гаммированием.

Выполнение Работы

Для выполнения работы была написана программа с помощью языка программирования PHP. Зашифруем 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).

Исходный код

```
<?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 = ["a"=>"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 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";

?>

```

Результать Работы

```
Windows PowerShell
PS C:\apache\localhost\www\encrption> php Gamma.php
введите сообщение: Помехоустойчивое кодирование - это кодирование с возможностью восстановления потерянных или ошибочно принятых данных
ых

Знаки гаммы:
2 -> 000010
3 -> 000011
10 -> 001010
4 -> 000100
1 -> 000001
5 -> 000101
6 -> 000110
7 -> 000111
8 -> 001000
11 -> 001011
15 -> 001111
14 -> 001110
12 -> 001100
13 -> 001101
9 -> 001001
0 -> 000000

Зашифровываем сообщение

п -> 010011   о -> 000100   м -> 010001   е -> 000010   х -> 011000   о -> 000100   у -> 000101
с -> 010101   т -> 010110   о -> 000100   й -> 011111   ч -> 011010   и -> 000011   в -> 001010
о -> 000100   е -> 000010   -> 100001   к -> 001111   о -> 000100   д -> 001100   и -> 000011
р -> 010100   о -> 000100   в -> 001010   а -> 000001   н -> 010010   и -> 000011   е -> 000010
-> 100001   -> 100001   э -> 000110   т -> 010110   о -> 000100   -> 100001   к -> 001111
о -> 000100   д -> 001100   и -> 000011   р -> 010100   о -> 000100   в -> 001010   а -> 000001
н -> 010010   и -> 000011   е -> 000010   -> 100001   с -> 010101   -> 100001   в -> 001010
о -> 000100   э -> 001110   м -> 010001   о -> 000100   ж -> 001101   н -> 010010   о -> 000100
с -> 010101   т -> 010110   ь -> 011110   ю -> 000111   -> 100001   в -> 001010   о -> 000100
с -> 010101   с -> 010101   т -> 010110   а -> 000001   н -> 010010   о -> 000100   в -> 001010
л -> 010000   е -> 000010   н -> 010010   и -> 000011   я -> 001000   -> 100001   п -> 010011
о -> 000100   т -> 010110   е -> 000010   р -> 010100   я -> 001000   н -> 010010   н -> 010010
ы -> 011101   х -> 011000   -> 100001   и -> 000011   л -> 010000   и -> 000011   -> 100001
о -> 000100   ш -> 011011   и -> 000011   б -> 001001   о -> 000100   ч -> 011010   н -> 010010
о -> 000100   -> 100001   п -> 010011   р -> 010100   и -> 000011   н -> 010010   я -> 001000
т -> 010110   ы -> 011101   х -> 011000   -> 100001   д -> 001100   а -> 000001   н -> 010010
н -> 010010   ы -> 011101   х -> 011000

зашифрованное сообщение:
010001 000111 011011 000110 011001 000001 000011 010010 011110 001111 010000 010100 001111 000111 001101 000010 100011 001100 001110
001000 000010 010001 000010 001101 001001 011001 001100 001100 101101 101100 001111 010110 000110 100010 000101 000000 001101 000110
010010 000011 000010 001010 011101 001101 001110 101100 011100 100001 001000 000111 000100 010101 000101 001000 010100 000011 011101 0
11101 010001 001001 101101 000111 001101 010101 010111 010101 010110 000101 001111 010110 000101 011010 001000 000111 101111 01
1111 001001 011111 000010 010110 001011 011000 010110 011100 011101 100111 000100 011000 001000 101110 001010 010111 001110 000000 000
100 011000 010001 001110 100101 010010 010001 000101 010101 000000 011101 010010 010110 101101 000001 001000 010010 010000 011110 0100
10

PS C:\apache\localhost\www\encrption>
```

Выводы

Освоено на практике применение алгоритма шифрования методом гаммирования.

Список литературы

1. Методические материалы курса