Лабораторная работа № 3

Тема: исследование гаммирования при шифровании.

Цель: изучить теоретические основы генерации псевдослучайных последовательностей и гаммирования при шифровании данных. Составить программу, позволяющую закодировать текст и выполнить обратное преобразование.

1 Теоретический вопрос

Алгоритм RC4, как и любой потоковый шифр, строится на основе генератора псевдослучайных битов. На вход генератора записывается ключ, а на выходе читаются псевдослучайные биты. Длина ключа может составлять от 40 до 2048 бит. Генерируемые биты имеют равномерное распределение.

Основные преимущества шифра:

* высокая скорость работы;
* переменный размер ключа.

RC4 довольно уязвим, если:

* используются не случайные или связанные ключи;
* один ключевой поток используется дважды.

RC4 — фактически класс алгоритмов, определяемых размером блока (в дальнейшем S-блока). Параметр n является размером слова для алгоритма и определяет длину S-блока. Обычно, n = 8, но в целях анализа можно уменьшить его. Однако для повышения безопасности необходимо увеличить эту величину. В алгоритме нет противоречий на увеличение размера S-блока . При увеличении n, допустим, до 16 бит, элементов в S-блоке становится 65 536 и соответственно время начальной итерации будет увеличено. Однако, скорость шифрования возрастёт.

Внутреннее состояние RC4 представляется в виде массива размером 2n и двух счётчиков. Массив известен как S-блок, и далее будет обозначаться как S. Он всегда содержит перестановку 2n возможных значений слова.

Генератор ключевого потока RC4 переставляет значения, хранящиеся в S. В одном цикле RC4 определяется одно n-битное слово K из ключевого потока. В дальнейшем ключевое слово будет сложено по модулю два с исходным текстом, которое пользователь хочет зашифровать, и получен зашифрованный текст.

2 Выполнение шифрования и дешифрования методом сложения по модулю N

В следующих таблицах продемонстрирован процесс шифрования с N = 44

Таблица 1 – Шифрование фразы 1

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **T** | Х | А | С | А | Н | \_ | 2 | 5 | 0 | 0 | 0 | \_ | Т | О | Н | Н |
| **G** | А | Л | Е | К | С | Е | Й | А | Л | Е | К | С | Е | Й | А | Л |
| **T** | 23 | 1 | 19 | 1 | 15 | 34 | 36 | 39 | 44 | 44 | 44 | 34 | 20 | 16 | 15 | 15 |
| **G** | 1 | 13 | 6 | 12 | 19 | 6 | 11 | 1 | 13 | 6 | 12 | 19 | 6 | 11 | 1 | 13 |
| **T+G** | 24 | 14 | 25 | 13 | 34 | 40 | 47 | 40 | 57 | 50 | 56 | 53 | 26 | 27 | 16 | 28 |
| **mod N** | 24 | 14 | 25 | 13 | 34 | 40 | 3 | 40 | 13 | 6 | 12 | 9 | 26 | 27 | 16 | 28 |
| **C** | Ц | М | Ч | Л | \_ | 6 | В | 6 | Л | Е | К | 3 | Ш | Щ | О | Ъ |

Таблица 2 – Шифрование фразы 2

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **T** | Х | А | Л | К | И | Н | Г | О | Л | \_ | 1 | 9 | 3 | 9 | \_ | Г |
| **G** | Е | М | Е | Л | Ь | Я | Н | Е | М | Е | Л | Ь | Я | Н | Е | М |
| **T** | 23 | 1 | 13 | 12 | 10 | 15 | 4 | 16 | 13 | 34 | 35 | 43 | 37 | 43 | 34 | 4 |
| **G** | 6 | 14 | 6 | 13 | 30 | 33 | 15 | 6 | 14 | 6 | 13 | 30 | 33 | 15 | 6 | 14 |
| **T+G** | 29 | 15 | 19 | 25 | 40 | 48 | 19 | 22 | 27 | 40 | 48 | 73 | 70 | 58 | 40 | 18 |
| **mod N** | 29 | 15 | 19 | 25 | 40 | 4 | 19 | 22 | 27 | 40 | 4 | 29 | 26 | 14 | 40 | 18 |
| **C** | Ы | Н | С | Ч | 6 | Г | С | Ф | Щ | 6 | Г | Ы | Ш | М | 6 | Р |

Таблица 3 – Шифрование фразы 3

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **T** | Х | А | Б | А | Р | О | В | С | К | \_ | 6 | 8 | 0 | 0 | 6 | 3 |
| **G** | Т | И | М | О | Ф | Е | Й | Т | И | М | О | Ф | Е | Й | Т | И |
| **T** | 23 | 1 | 2 | 1 | 18 | 16 | 3 | 19 | 12 | 34 | 40 | 42 | 44 | 44 | 40 | 37 |
| **G** | 20 | 10 | 14 | 16 | 22 | 6 | 11 | 20 | 10 | 14 | 16 | 22 | 6 | 11 | 20 | 10 |
| **T+G** | 43 | 11 | 16 | 17 | 40 | 22 | 14 | 39 | 22 | 48 | 56 | 64 | 50 | 55 | 60 | 47 |
| **mod N** | 43 | 11 | 16 | 17 | 40 | 22 | 14 | 39 | 22 | 4 | 12 | 20 | 6 | 11 | 16 | 3 |
| **C** | 9 | Й | О | П | 6 | Ф | М | 5 | Ф | Г | К | Т | Е | Й | О | В |

Таблица 4 – Шифрование фразы 4

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **T** | Н | Е | Р | Ю | Н | Г | Р | И | \_ | 2 | 3 | 0 | \_ | К | М |
| **G** | М | А | Р | Ь | Я | Н | А | М | А | Р | Ь | Я | Н | А | М |
| **T** | 15 | 6 | 18 | 32 | 15 | 4 | 18 | 10 | 34 | 36 | 37 | 44 | 34 | 12 | 14 |
| **G** | 14 | 1 | 18 | 30 | 33 | 15 | 1 | 14 | 1 | 18 | 30 | 33 | 15 | 1 | 14 |
| **T+G** | 29 | 7 | 36 | 62 | 48 | 19 | 19 | 24 | 35 | 54 | 67 | 77 | 49 | 13 | 28 |
| **mod N** | 29 | 7 | 36 | 18 | 4 | 19 | 19 | 24 | 35 | 10 | 23 | 33 | 5 | 13 | 28 |
| **C** | Ы | Ё | 2 | Р | Г | С | С | Ц | 1 | И | Х | Я | Д | Л | Ъ |

Таблица 5 – Шифрование фразы 5

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **T** | А | М | У | Р | З | Е | Т | \_ | 3 | 5 | 0 | 0 | 0 | \_ | Ш | Т |
| **G** | В | А | Р | В | А | Р | А | В | А | Р | В | А | Р | А | В | А |
| **T** | 1 | 14 | 21 | 18 | 9 | 6 | 20 | 34 | 37 | 39 | 44 | 44 | 44 | 34 | 26 | 20 |
| **G** | 3 | 1 | 18 | 3 | 1 | 18 | 1 | 3 | 1 | 18 | 3 | 1 | 18 | 1 | 3 | 1 |
| **T+G** | 3 | 15 | 39 | 21 | 10 | 24 | 21 | 37 | 38 | 57 | 47 | 45 | 62 | 35 | 29 | 21 |
| **mod N** | 3 | 15 | 39 | 21 | 10 | 24 | 21 | 37 | 38 | 13 | 3 | 1 | 18 | 35 | 29 | 21 |
| **C** | В | Н | 5 | У | И | Ц | У | 3 | 4 | Л | В | А | Р | 1 | Ы | У |

Таблица 6 – Шифрование фразы 6

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **T** | З | Е | Й | С | К | А | Я | \_ | 2 | 5 | 0 | 0 | \_ | Т | О | Н | Н |
| **G** | В | И | Т | А | Л | И | Й | В | И | Т | А | Л | И | Й | В | И | Т |
| **T** | 9 | 6 | 11 | 19 | 12 | 1 | 33 | 34 | 36 | 39 | 44 | 44 | 34 | 20 | 16 | 15 | 15 |
| **G** | 3 | 10 | 20 | 1 | 13 | 10 | 11 | 3 | 10 | 20 | 1 | 13 | 10 | 11 | 3 | 10 | 20 |
| **T+G** | 12 | 16 | 31 | 20 | 25 | 11 | 44 | 37 | 46 | 59 | 45 | 57 | 44 | 31 | 19 | 25 | 35 |
| **mod N** | 12 | 16 | 31 | 20 | 25 | 11 | 44 | 37 | 2 | 15 | 1 | 13 | 44 | 31 | 19 | 25 | 35 |
| **C** | К | О | Э | Т | Ч | Й | 0 | 3 | Б | Н | А | Л | 0 | Э | С | Ч | 1 |

В следующих таблицах продемонстрирован процесс дешифрования с N = 44

Таблица 7 – Дешифрование фразы 7

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **C** | Й | Ё | Ё | Л | Щ | Д | 2 | 8 | З | Б | Д | Е | Я | Ш | С |
| **G** | Б | Е | Р | И | Н | Г | Б | Е | Р | И | Н | Г | Б | Е | Р |
| **C** | 11 | 7 | 7 | 13 | 27 | 5 | 36 | 42 | 9 | 2 | 5 | 6 | 33 | 26 | 19 |
| **G** | 2 | 6 | 18 | 10 | 15 | 4 | 2 | 6 | 18 | 10 | 15 | 4 | 2 | 6 | 18 |
| **C-G** | 9 | 1 | -11 | 3 | 12 | 1 | 34 | 36 | -9 | -8 | -10 | 2 | 31 | 20 | 1 |
| **+44** | 53 | 45 | 33 | 47 | 56 | 45 | 78 | 80 | 35 | 36 | 34 | 46 | 75 | 64 | 45 |
| **modN** | 9 | 1 | 33 | 3 | 12 | 1 | 34 | 36 | 35 | 36 | 34 | 2 | 31 | 20 | 1 |
| **О.Т.** | З | А | Я | В | К | А | \_ | 2 | 1 | 2 | \_ | Б | Э | Т | А |

Таблица 8 – Дешифрование фразы 8

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **C** | 8 | О | Я | М | \_ | Д | Н | Н | Р | 3 | А | Н | Ф | А | Е | 5 |
| **G** | Х | И | Н | Г | А | Н | Х | И | Н | Г | А | Н | Х | И | Н | Г |
| **C** | 42 | 16 | 33 | 14 | 34 | 5 | 15 | 15 | 18 | 37 | 1 | 15 | 22 | 1 | 6 | 39 |
| **G** | 23 | 10 | 15 | 4 | 1 | 15 | 23 | 10 | 15 | 4 | 1 | 15 | 23 | 10 | 15 | 4 |
| **C-G** | 19 | 6 | 18 | 10 | 33 | -10 | -8 | 5 | 3 | 33 | 0 | 0 | -1 | -9 | -9 | 35 |
| **+44** | 63 | 50 | 62 | 54 | 77 | 34 | 36 | 49 | 47 | 77 | 44 | 44 | 43 | 35 | 35 | 79 |
| **modN** | 19 | 6 | 18 | 10 | 33 | 34 | 36 | 5 | 3 | 33 | 0 | 0 | 43 | 35 | 35 | 35 |
| **О.Т.** | С | Е | Р | И | Я | \_ | 2 | Д | В | Я | 0 | 0 | 9 | 1 | 1 | 1 |

Таблица 9 – Дешифрование фразы 9

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **C** | И | Г | Я | Ё | Щ | Т | 6 | А | В | \_ | Ю | Г | Й | М | Б |
| **G** | Д | А | Л | Я | Н | Ь | Д | А | Л | Я | Н | Ь | Д | А | Л |
| **C** | 10 | 4 | 33 | 7 | 27 | 20 | 40 | 1 | 3 | 34 | 32 | 4 | 11 | 14 | 2 |
| **G** | 5 | 1 | 13 | 33 | 15 | 30 | 5 | 1 | 13 | 33 | 15 | 30 | 5 | 1 | 13 |
| **C-G** | 5 | 3 | 20 | -26 | 12 | -10 | 35 | 0 | -10 | 1 | 17 | -26 | 6 | 13 | -11 |
| **+44** | 49 | 47 | 64 | 18 | 56 | 34 | 79 | 44 | 34 | 45 | 61 | 18 | 50 | 57 | 33 |
| **modN** | 5 | 3 | 20 | 18 | 12 | 34 | 35 | 0 | 34 | 1 | 17 | 18 | 6 | 13 | 33 |
| **044** | 5 | 3 | 20 | 18 | 12 | 34 | 35 | 44 | 34 | 1 | 17 | 18 | 6 | 13 | 33 |
| **О.Т.** | Д | В | Т | Р | К | \_ | 1 | 0 | \_ | А | П | Р | Е | Л | Я |

Таблица 10 – Дешифрование фразы 10

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **C** | Э | Ф | Э | Д | Ц | Х | Ф | Ъ | М | Д | Г | 2 | К | Ё | Г | У |
| **G** | К | О | Л | Ы | М | А | К | О | Л | Ы | М | А | К | О | Л | Ы |
| **C** | 31 | 22 | 31 | 5 | 24 | 23 | 22 | 28 | 14 | 5 | 4 | 36 | 12 | 7 | 4 | 21 |
| **G** | 12 | 16 | 13 | 29 | 14 | 1 | 12 | 16 | 13 | 29 | 14 | 1 | 12 | 16 | 13 | 29 |
| **C-G** | 19 | 6 | 18 | -24 | 10 | 22 | 10 | 12 | 1 | -24 | -10 | 35 | 0 | -9 | -9 | -8 |
| **+44** | 63 | 50 | 62 | 20 | 54 | 66 | 54 | 56 | 45 | 20 | 34 | 79 | 44 | 35 | 35 | 36 |
| **modN** | 19 | 6 | 18 | 20 | 10 | 22 | 10 | 12 | 1 | 20 | 34 | 35 | 0 | 35 | 35 | 36 |
| **044** | 19 | 6 | 18 | 20 | 10 | 22 | 10 | 12 | 1 | 20 | 34 | 35 | 44 | 35 | 35 | 36 |
| **О.Т.** | С | Е | Р | Т | И | Ф | И | К | А | Т | \_ | 1 | 0 | 1 | 1 | 2 |

Таблица 11 – Дешифрование фразы 11

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **C** | Я | 6 | Ш | Ю | Т | У | Е | Н | Й | Й | К | Д | Ё | М | О |
| **G** | О | Х | О | Т | С | К | О | Х | О | Т | С | К | О | Х | О |
| **C** | 33 | 40 | 26 | 32 | 20 | 21 | 6 | 15 | 11 | 11 | 12 | 5 | 7 | 14 | 16 |
| **G** | 16 | 23 | 16 | 20 | 19 | 12 | 16 | 23 | 16 | 20 | 19 | 12 | 16 | 23 | 16 |
| **C-G** | 17 | 17 | 10 | 12 | 1 | 9 | -10 | -8 | 5 | -9 | -7 | -7 | -9 | -9 | 0 |
| **44** | 61 | 61 | 54 | 56 | 45 | 53 | 34 | 36 | 49 | 35 | 37 | 37 | 35 | 35 | 44 |
| **modN** | 17 | 17 | 10 | 12 | 1 | 9 | 34 | 36 | 5 | 35 | 37 | 37 | 35 | 35 | 0 |
| **044** | 17 | 17 | 10 | 12 | 1 | 9 | 34 | 36 | 5 | 35 | 37 | 37 | 35 | 35 | 44 |
| **О.Т.** | П | П | И | К | А | З | \_ | 2 | Д | 1 | 3 | 3 | 1 | 1 | 0 |

Таблица 12 – Дешифрование фразы 12

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **C** | С | В | И | Ь | Ё | 6 | Ё | П | Й | Р | 0 | З | 1 | 2 | 2 | М |
| **G** | А | Б | А | К | А | Н | А | Б | А | К | А | Н | А | Б | А | К |
| **C** | 19 | 3 | 10 | 30 | 7 | 40 | 7 | 17 | 11 | 18 | 44 | 9 | 35 | 36 | 36 | 14 |
| **G** | 1 | 2 | 1 | 12 | 1 | 15 | 1 | 2 | 1 | 12 | 1 | 15 | 1 | 2 | 1 | 12 |
| **C-G** | 18 | 1 | 9 | 18 | 6 | 25 | 6 | 15 | 10 | 6 | 43 | -6 | 34 | 34 | 35 | 2 |
| **44** | 62 | 45 | 53 | 62 | 50 | 69 | 50 | 59 | 54 | 50 | 87 | 38 | 78 | 78 | 79 | 46 |
| **modN** | 18 | 1 | 9 | 18 | 6 | 25 | 6 | 15 | 10 | 6 | 43 | 38 | 34 | 34 | 35 | 2 |
| **О.Т.** | Р | А | З | Р | Е | Ч | Е | Н | И | Е | 9 | 4 | \_ | \_ | 1 | Б |

3 Блок схемы

На рисунке 1 представлена блок схема шифрования и дешифрования сообщения.



Рисунок 1 – Блок схемы шифрования и дешифрования методом сложения по модулю N

На рисунке 2 представлена блок схема ГПСП.



Рисунок 2 – Блок схема ГПСП

4 Описание работы программы

Ключ применяется для генерации гаммы и может быть любой последовательностью символов ASCII. Текст в зависимости от направления алгоритма необходимо заполнять в ASCII для шифрования и шестнадцатеричном формате для дешифрования. Необходимость задания разных форм обусловлена наличием в зашифрованной строке непечатных символов, что затрудняет их запись и воспроизведение.

На рисунке 3 представлен скриншот интерфейса разработанной программы.

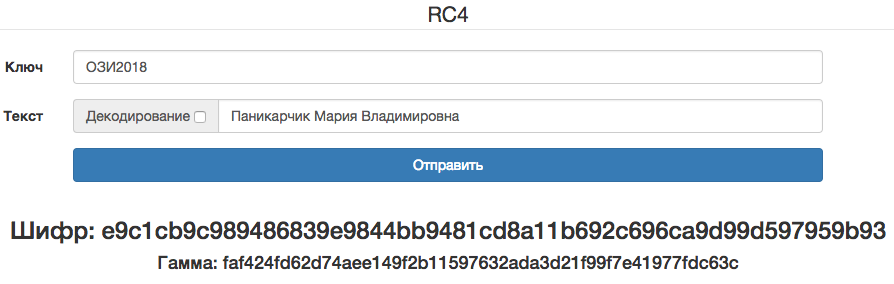


Рисунок 3 – Интерфейс программы

5 Текст программы

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | 1 | <?php | | 2 |  | | 3 | *function* rc4( *$key\_str*, *$len* ) { | | 4 | $key = []; | | 5 | for ( $i = 0; $i < strlen($key\_str); $i += 2 ) { | | 6 | $key[] = hexdec($key\_str[$i].$key\_str[$i+1]); | | 7 | } | | 8 | $state = [ 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15, | | 9 | 16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31, | | 10 | 32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47, | | 11 | 48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63, | | 12 | 64,65,66,67,68,69,70,71,72,73,74,75,76,77,78,79, | | 13 | 80,81,82,83,84,85,86,87,88,89,90,91,92,93,94,95, | | 14 | 96,97,98,99,100,101,102,103,104,105,106,107,108,109,110,111, | | 15 | 112,113,114,115,116,117,118,119,120,121,122,123,124,125,126,127, | | 16 | 128,129,130,131,132,133,134,135,136,137,138,139,140,141,142,143, | | 17 | 144,145,146,147,148,149,150,151,152,153,154,155,156,157,158,159, | | 18 | 160,161,162,163,164,165,166,167,168,169,170,171,172,173,174,175, | | 19 | 176,177,178,179,180,181,182,183,184,185,186,187,188,189,190,191, | | 20 | 192,193,194,195,196,197,198,199,200,201,202,203,204,205,206,207, | | 21 | 208,209,210,211,212,213,214,215,216,217,218,219,220,221,222,223, | | 22 | 224,225,226,227,228,229,230,231,232,233,234,235,236,237,238,239, | | 23 | 240,241,242,243,244,245,246,247,248,249,250,251,252,253,254,255 ]; | | 24 | $index1 = $index2 = 0; | | 25 | for( $counter = 0; $counter < 256; $counter++ ){ | | 26 | $index2  = ( $key[$index1] + $state[$counter] + $index2 ) % 256; | | 27 | $tmp = $state[$counter]; | | 28 | $state[$counter] = $state[$index2]; | | 29 | $state[$index2] = $tmp; | | 30 | $index1 = ($index1 + 1) % count($key); | | 31 | } | | 32 | $result = ''; | | 33 | $x = $y = 0; | | 34 | for ($counter = 0; $counter < $len; $counter++) { | | 35 | $x = ($x + 1) % 256; | | 36 | $y = ($state[$x] + $y) % 256; | | 37 | $tmp = $state[$x]; | | 38 | $state[$x] = $state[$y]; | | 39 | $state[$y] = $tmp; | | 40 | $result .= dechex($state[($state[$x] + $state[$y]) % 256]); | | 41 | } | | 42 |  | | 43 | return $result; | | 44 | } | | 45 |  | | 46 | *function* gamma(*$gamma*, *$text*) { | | 47 | $result = ''; | | 48 | for($i=0;$i<strlen($text);$i++) { | | 49 | $result .= dechex(ord($gamma[$i]) ^ ord($text[$i])); | | 50 | } | | 51 | return $result; | | 52 | } | | 53 |  | | 54 | $result = false; | | 55 | $gamma = false; | | 56 | if(isset($\_REQUEST['key']) && isset($\_REQUEST['text'])) { | | 57 | $key = iconv("UTF-8", "CP866", $\_REQUEST['key']); | | 58 | $hex\_mode = isset($\_REQUEST['text\_hex']) && $\_REQUEST['text\_hex'] == '1'; | | 59 | if($hex\_mode) { | | 60 | $text = ''; | | 61 | $tmp = $\_REQUEST['text']; | | 62 | for($i=0;$i<strlen($tmp)-1;$i+=2) { | | 63 | $text .= chr(hexdec($tmp[$i].$tmp[$i+1])); | | 64 | } | | 65 | } else { | | 66 | $text = iconv("UTF-8", "CP866", $\_REQUEST['text']); | | 67 | } | | 68 | $gamma = rc4($key, strlen($text)); | | 69 | $gammed = gamma($gamma, $text); | | 70 | if($hex\_mode) { | | 71 | $result = ''; | | 72 | for($i=0;$i<strlen($gammed)-1;$i+=2) { | | 73 | $result .= chr(hexdec($gammed[$i].$gammed[$i+1])); | | 74 | } | | 75 | } else { | | 76 | $result = $gammed; | | 77 | } | | 78 | $result = iconv("CP866", "UTF-8", $result); | | 79 | } | | 80 | ?> | | 81 |  | | 82 | <html> | | 83 | <head> | | 84 | <title>Gamma RC4</title> | | 85 | <link rel="stylesheet" type="text/css" href="assets/css/bootstrap.min.css"> | | 86 | <link rel="stylesheet" type="text/css" href="assets/css/main.css"> | | 87 | <meta charset="utf-8"> | | 88 | </head> | | 89 | <body> | | 90 | <div class="container"> | | 91 | <form class="form-horizontal text-center"> | | 92 | <fieldset> | | 93 |  | | 94 | <!-- Form Name --> | | 95 | <legend>RC4</legend> | | 96 |  | | 97 | <!-- Text input--> | | 98 | <div class="form-group"> | | 99 | <label class="col-md-2 control-label" for="key">Ключ</label> | | 100 | <div class="col-md-8"> | | 101 | <input id="key" name="key" type="text" placeholder="" class="form-control input-md" required=""> | | 102 | </div> | | 103 | </div> | | 104 |  | | 105 | <!-- Prepended checkbox --> | | 106 | <div class="form-group"> | | 107 | <label class="col-md-2 control-label" for="text">Текст</label> | | 108 | <div class="col-md-8"> | | 109 | <div class="input-group"> | | 110 | <label class="input-group-addon"> Декодирование | | 111 | <input type="checkbox" name="text\_hex" value="1"> | | 112 | </label> | | 113 | <input id="text" name="text" class="form-control" type="text" placeholder=""> | | 114 | </div> | | 115 | </div> | | 116 | </div> | | 117 |  | | 118 | <!-- Button --> | | 119 | <div class="form-group"> | | 120 | <div class="col-md-8 col-md-offset-2"> | | 121 | <button type="submit" class="btn btn-primary btn-block">Отправить</button> | | 122 | </div> | | 123 | </div> | | 124 | </fieldset> | | 125 | </form> | | 126 | <div class="text-center"> | | 127 | <?php if($result !== false): ?> | | 128 | <h3>Шифр: <?= $result ?></h3> | | 129 | <h4>Гамма: <?= $gamma ?></h4> | | 130 | <?php endif ?> | | 131 | </div> | | 132 | </div> | | 133 | <script src="assets/js/jquery-3.3.1.min.js"></script> | | 134 | <script src="assets/js/bootstrap.min.js"></script> | | 135 | <script src="assets/js/main.js"></script> | | 136 | </body> | | 137 | </html> | |  |

Вывод

В ходе выполнения лабораторной работы были изучены теоретические основы генерации псевдослучайных последовательностей и гаммирования при шифровании данных. Составлена программа, позволяющая закодировать текст и выполнить обратное преобразование с использованием ГПСП RC4.