Министерство образования и науки Российской Федерации

Севастопольский государственный университет

Кафедра ИС

Отчёт

по лабораторной работе № 4

Аналитическое моделирование дискретных систем

Выполнил: Ст. Гр. ИС/б-42-о

Лисянский А.И.

Проверил:

Маслова М.А.

Севастополь

2015

Цель работы

Исследование простых шифров

Вариант задания 92

Поменьше говори -больше услышишь

Ход работы

1.Зашифровать сообщение методом Виженера

При шифровании считаем, что алфавит не содержит буквы ё.

Таблица 1

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| а | б | в | г | д | е | ж | з | и | й | к | л | м | н | о | п | р | с |
| т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я | \_ | . | - | ! |

Ключевое слово: зил

Таблица 2 – Шифрование методом Виженера

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| исходная | п | о | м | е | н | ь | ш | е |  | г | о | в | о | р | и | - | б | о |
| сдвиг | 7 | 8 | 11 | 7 | 8 | 11 | 7 | 8 | 11 | 7 | 8 | 11 | 7 | 8 | 11 | 7 | 8 | 11 |
| зашифр. | ц | ц | ч | м | х | г | я | н | з | к | ц | н | х | ш | у | е | й | щ |
| исходная | л | ь | ш | е |  | у | с | л | ы | ш | и | ш | ь |  |  |  |  |  |
| сдвиг | 7 | 8 | 11 | 7 | 8 | 11 | 7 | 8 | 11 | 7 | 8 | 11 | 7 |  |  |  |  |  |
| зашифр. | т | а | ! | м | д | ю | ш | у | в | я | р | ! | ! |  |  |  |  |  |

2.Зашифровать сообщение методом квадрат Полибия

Таблица 3 – Квадрат Полибия

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | А | Б | В | Г | Д | Е |
| 2 | Ж | З | И | Й | К | Л |
| 3 | М | Н | О | П | Р | С |
| 4 | Т | У | Ф | Х | Ц | Ч |
| 5 | Ш | Щ | Ъ | Ы | Ь | Э |
| 6 | Ю | Я | \_ | . | - | ! |

Поменьше говори - больше услышишь

Зашифрованное сообщение : 34 33 31 16 32 55 51 16 63 14 33 13 33 35 23 65 12 33 26 55 51 16 63 42 36 26 54 51 23 51 55

3.Зашифровать методом Цезаря

При шифровании считаем, что алфавит не содержит буквы ё.

Смещение 3.

Таблица 4 – Алфавит по которому было выполнено шифрование

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| А | Б | В | Г | Д | Е | Ж | З | И | Й | К | Л | М | Н | О | . | Р | С |
| т | у | ф | Х | ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | \_ | П | - | ! |

Таблица 5 – Шифрование методом Цезаря

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Исходная | п | о | м | е | н | ь | ш | е |  | г | о | в | о | р | и | - | б | о |
| Сдвиг | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 |
| Зашифр. | т | с | . | и | р | я | ы | и | ! | ж | с | е | с | у | л | б | д | с |
| Исходная | л | ь | ш | е |  | у | с | л | ы | ш | и | ш | ь | ! |  |  |  |  |
| Сдвиг | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 |
| Зашифр. | о | я | ы | и | ! | ц | ф | о | ю | ы | л | ы | о | в |  |  |  |  |

4.Зашифровать сообщение методом колонной (строчной) замены

Поменьше говори -больше услышишь

Ключевое слово: пирог.

Запишем исходное сообщение в таблицу, в которой 13 строк и 5 столбцов. Первая строка – это ключевое слово, а вторая строка – номер следования столбца при шифровании. Зашифруем сообщение с помощью ключевого слово: пирог. Буквы ключевого слова пишутся над столбцами и указывают порядок этих столбцов (по возрастанию номеров букв в алфавите).

Таблица 6 – Шифрование методом колонной (строчной) замены

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| П | И | Р | О | Г |
| 4 | 2 | 5 | 3 | 1 |
| П | о | м | е | н |
| ь | ш | е |  | г |
| о | в | о | р | и |
| - | б | о | л | ь |
| ш | е |  | у | с |
| л | ы | ш | и | ш |
| ь |  |  |  |  |

Чтобы получить зашифрованный текст, надо выписывать буквы по столбцам с учетом их нумерации.

Зашифрованное сообщение: нгиьсшошвбеые рлуипьо-шльмеоо ш

1. Зашифровать сообщение методом Вернама

Таблица 7 – Алфавит, составленный с помощью двоичного безизбыточного кода

|  |  |  |  |
| --- | --- | --- | --- |
| Символ | Код | Символ | Код |
| П | 00000 | Р | 01010 |
| О | 00001 | И | 01011 |
| М | 00010 | Г | 01000 |
| Е | 00011 | - | 01100 |
| Н | 00100 | Б | 01101 |
| Ь | 00101 | Л | 01110 |
| Ш | 00110 | У | 01111 |
| \_ | 00111 | С | 10000 |
| Г | 01000 | Ы | 10001 |
| В | 01001 |  |  |

Поменьше говори-больше услышишь

Шифрование с ключом: 11010. Для того чтобы выполнить шифрование исходное сообщение необходимо объединить операцией «[исключающее ИЛИ](https://ru.wikipedia.org/wiki/%D0%98%D1%81%D0%BA%D0%BB%D1%8E%D1%87%D0%B0%D1%8E%D1%89%D0%B5%D0%B5_%D0%98%D0%9B%D0%98)» с секретным [ключом](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D1%8E%D1%87_(%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F)).

Таблица 8 – Шифрование методом Вернама

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Буква | П | о | м | е | н | ь | ш | е |
| Исходная | 00000 | 00001 | 00010 | 00011 | 00010 | 00100 | 00110 | 00011 |
| Ключ | 11010 | 11010 | 11010 | 11010 | 11010 | 11010 | 11010 | 11010 |
| Зашифр. | 11010 | 11011 | 11000 | 11001 | 11000 | 11110 | 11100 | 11001 |
| Буква | \_ | г | о | в | о | р | и | \_ |
| Исходная | 00111 | 01000 | 00001 | 01001 | 00001 | 01010 | 01011 | 00111 |
| Ключ | 11010 | 11010 | 11010 | 11010 | 11010 | 11010 | 11010 | 11010 |
| Зашифр. | 11101 | 10010 | 11011 | 10011 | 11011 | 10000 | 10001 | 11101 |
| Буква | - | б | о | л | ь | ш | е | \_ |
| Исходная | 01100 | 01101 | 00001 | 01110 | 00100 | 00110 | 00011 | 00111 |
| Ключ | 11010 | 11010 | 11010 | 11010 | 11010 | 11010 | 11010 | 11010 |
| Зашифр. | 10110 | 10111 | 11011 | 10100 | 11110 | 11100 | 11001 | 11101 |
| Буква | у | с | л | ы | ш | и | ш | ь |
| Исходная | 01111 | 10000 | 01110 | 10001 | 00110 | 01011 | 00110 | 00100 |
| Ключ | 11010 | 11010 | 11010 | 11010 | 11010 | 11010 | 11010 | 11010 |
| Зашифр. | 10101 | 01010 | 10100 | 01011 | 11100 | 10001 | 11100 | 11110 |

Вывод

В ходе выполнения лабораторной работы было выполнено шифрование сообщение методом Виженера, методом квадрата Полибия, методом Цезаря, методом колонной (строчной) замены, методом Вернама.