Министерство образования и науки РФ

Севастопольский государственный университет

Институт информационных технологий и управления в технических системах

Лабораторная работа №4

«Исследование простых шифров»

Выполнил:

ст.гр. ИСб-22д

Воронин И.Ю.

Проверил:

Маслова М.А

Севастополь

2015

1.Цель работы

Исследование таких простых шифров как:

* Шифр Виженера;
* Метод квадрата Полибия;
* Метод Цезаря;
* Метод колонной(строчной) замены;
* Метод Вернама.

2.Вариант задания

Вариант 99

Вышел месяц из тумана.

3.Ход работы

Зашифруем сообщение **методом Виженера**. Имея алфавит следующего вида (табл.3.1.), используем ключевую фразу «свет». Эту фразу запишем столько раз циклически, чтобы она соответствовала каждому символу исходного сообщения.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| А-1 | Б-2 | В-3 | Г-4 | Д-5 | E-6 | Ж-7 | З-8 | И-9 | Й-10 | К-11 |
| Л-12 | М-13 | Н-14 | О-15 | П-16 | Р-17 | С-18 | Т-19 | У-20 | Ф-21 | Х-22 |
| Ц-23 | Ч-24 | Ш-25 | Щ-26 | Ъ-27 | Ы-28 | Ь-29 | Э-30 | Ю-31 | Я-32 | Пр.-33 |

Табл.3.1 - Алфавит.

Получим следующее соответствие символов. (табл.3.2)

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Исход | в | ы | ш | е | л | \_ | м | е | с | я | ц |
| Соотв. | с | в | е | т | с | в | е | т | с | е | т |
| Сдвиг | 18 | 3 | 6 | 19 | 18 | 3 | 6 | 19 | 18 | 3 | 6 |
| Итог | ф | ю | ю | ш | э | в | т | ш | в | б | ь |
|  | | | | | | | | | | | |
| Исход | и | з | \_ | т | У | м | а | н | а |  |  |
| Соотв. | с | в | е | т | С | в | е | т | с |  |  |
| Сдвиг | 19 | 18 | 3 | 6 | 19 | 18 | 3 | 6 | 19 |  |  |
| Итог | ы | щ | в | ш | Е | ю | г | у | у |  |  |

Таблица 3.2. - Шифрование сообщения.

Таки образом получим зашифрованную фразу: фюющэвтшвбьыщвшеюгуу.

Зашифруем сообщение методом **квадрата Полибия**.

Сначала создадим таблицу. Длинна русского алфавита равна 33 буквы, то есть размер таблицы должен быть не менее 33 ячеек. Оптимальный размер таблицы - 6х6 = 36 ячеек.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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 | Пр. | . | , | ? |

Таблица 3.3 – Квадрат Полибия.

Для шифрования сообщения необходимо брать символ, который в квадрате находится под исходным в таблице. В случае с последней строки, используется первая строка.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Исход | в | ы | ш | е | л | \_ | м | е | с | я | ц |
| Итог | и | . | ю | л | с | в | т | л | ч | б | ь |
|  |  |  |  |  |  |  |  |  |  |  |  |
| Исход | \_ | и | з | \_ | т | у | м | а | н | а |  |
| Итог | в | о | н | в | ш | щ | т | ж | у | ж |

Таблица 3.4 – Итоговое сообщение.

Получаем соответствия таблицы (3.5). Следовательно, получаем сообщение: и.юлсвтлчбьвонвшщтжуж

Зашифруем сообщение **методом Цезаря**.

Шифр Цезаря — это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите.

Воспользуемся сдвигом влево на 4. (табл.3.5)

Из сообщения «вышел месяц из тумана» получим следующее:

* жяьйпврйхбъвмлвцчрдсд

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Исход | Итог |  | Исход | Итог |
| А | Д | С | Х |
| Б | E | Т | Ц |
| В | Ж | У | Ч |
| Г | З | Ф | Ш |
| Д | И | Х | Щ |
| E | Й | Ц | Ъ |
| Ж | К | Ч | Ы |
| З | Л | Ш | Ь |
| И | М | Щ | Э |
| Й | Н | Ъ | Ю |
| К | О | Ы | Я |
| Л | П | Ь | Пр. |
| М | Р | Э | . |
| Н | С | Ю | А |
| О | Т | Я | Б |
| П | У | Пр. | В |
| Р | Ф | . | Г |

Таблица 3.5 – Таблица соответствий.

Зашифруем сообщение **методом Вернама**.

Пусть вспомогательной для шифрования комбинацией будет:

1010110111

Для данного кода между исходным сообщением и вспомогательным применяем умножение по модулю 2.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Исход | в | ы | ш | е | л | м | е | с | я | ц |
| Код | 00010 | 11011 | 11000 | 00101 | 01011 | 01100 | 00101 | 10001 | 11111 | 10110 |
| Вспом | 10101 | 10111 | 10101 | 10111 | 10101 | 10111 | 10101 | 10111 | 10101 | 10111 |
| Итог | 10111 | 01100 | 01101 | 10010 | 11110 | 11011 | 10000 | 00110 | 01010 | 00001 |
|  |  |  |  |  |  |  |  |  |  |  |
| Исход | и | з | т | у | м | а | н | а |  |  |
| Код | 01000 | 00111 | 10010 | 10011 | 01100 | 00000 | 01101 | 00000 |  |  |
| Вспом | 10101 | 10111 | 10101 | 10111 | 10101 | 10111 | 10101 | 10111 |  |  |
| Итог | 11101 | 10000 | 00111 | 00100 | 11001 | 10111 | 11000 | 10111 |  |  |

Таблица 3.6 - Метод Вермана.

Таким образом имеем следующее сообщение вида:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 10111 | 01100 | 01101 | 10010 | 11110 | 11011 | 10000 | 00110 | 01010 |
| 00001 | 11101 | 10000 | 00111 | 00100 | 11001 | 10111 | 11000 | 10111 |

Зашифруем сообщение **методом колонной (строчной) замены**.

Для этого составим таблицу из 6 столбцов и запишем в ней наше сообщение

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **1** | **2** | **3** | **4** | **5** | **6** |
| в | ы | ш | е | л |  |
| м | е | с | я | ц |  |
| и | з |  | т | у | м |
| а | н | а |  |  |  |

Таблица 3.6- Исходный текст.

При помощи комбинации состоящей из количества цифр, равному количества столбцов, составим кодовое слово.

* 451326

Получим следующую таблицу. (табл.3.7)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **4** | **5** | **1** | **3** | **2** | **6** |
| е | л | в | ш | ы |  |
| я | ц | м | с | е |  |
| т | у | и |  | з | м |
|  |  | а | а | н |  |

Таблица 3.6- Исходный текст.

Получим сообщение: елвшы яцмсе туи зм аан .

Выполним аналогичное действие, но для строчной замены при 3 стобцах.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **1** | **2** | **3** |
| **1** | в | ы | ш |
| **2** | е | л |  |
| **3** | м | е | с |
| **4** | я | ц |  |
| **5** | и | з |  |
| **6** | т | у | м |
| **7** | а | н | а |

Таблица 3.7-Исходная таблица.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **1** | **2** | **3** |
| **6** | т | у | м |
| **2** | е | л |  |
| **5** | и | з |  |
| **7** | а | н | а |
| **4** | я | ц |  |
| **1** | в | ы | ш |
| **3** | м | е | с |

Таблица 3.8 - Зашифрованная таблица.

Получаем сообщение «тумел из анаяц вышмес» с кодовой комбинацией 6257413.

ВЫВОД

В данной лабораторной работе мы исследовали простые шифры. Были рассмотрены алгоритмы смещения алфавита, основанные на шифре Цезаря. Также простейшие методы замены.