Министерство образования и науки Российской Федерации

Севастопольский государственный университет

Кафедра ИС

ОТЧЕТ

по дисциплине «Информационные технологии»

к лабораторной работе № 4

«Исследование простых шифров»

Выполнил:

ст. гр. ИСб-21

Куркчи А.Э.

Проверила:

Маслова М. А.

Севастополь

2015

1. Цель работы

Исследование простых шифров Виженера, квадрата Полибия, Цезаря, колонной (строчной) замены, Вернама.

2. Постановка задачи

1. Записать текстовое сообщение на естественном языке в соответствии с вариантом задания (ЛР №1).
2. Закодировать сообщение п.1 по методу

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

1. Сделать выводы по работе

3. Ход работы

1. Текстовое сообщение на естественном языке: не\_хвались\_умом,\_коли\_берешь\_все\_хребтом
2. Кодирование методом Виженера.

Этот метод является простой формой многоалфавитной замены. Квадрат Виженера или таблица Виженера, может быть использована для заширования и расшифрования. На разных этапах кодировки шифр Виженера использует различные алфавиты из этой таблицы. На каждом этапе шифрования используются различные алфавиты, выбираемые в зависимости от символа ключевого слова.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | а | б | в | е | и | к | л | м | н | о | п | р | с | т | у | х | ш | ь | \_ | , |
| а | а | б | в | е | и | к | л | м | н | о | п | р | с | т | у | х | ш | ь | \_ | , |
| б | б | в | е | и | к | л | м | н | о | п | р | с | т | у | х | ш | ь | \_ | , | а |
| в | в | е | и | к | л | м | н | о | п | р | с | т | у | х | ш | ь | \_ | , | а | б |
| е | е | и | к | л | м | н | о | п | р | с | т | у | х | ш | ь | \_ | , | а | б | в |
| и | и | к | л | м | н | о | п | р | с | т | у | х | ш | ь | \_ | , | а | б | в | е |
| к | к | л | м | н | о | п | р | с | т | у | х | ш | ь | \_ | , | а | б | в | е | и |
| л | л | м | н | о | п | р | с | т | у | х | ш | ь | \_ | , | а | б | в | е | и | к |
| м | м | н | о | п | р | с | т | у | х | ш | ь | \_ | , | а | б | в | е | и | к | л |
| н | н | о | п | р | с | т | у | х | ш | ь | \_ | , | а | б | в | е | и | к | л | м |
| о | о | п | р | с | т | у | х | ш | ь | \_ | , | а | б | в | е | и | к | л | м | н |
| п | п | р | с | т | у | х | ш | ь | \_ | , | а | б | в | е | и | к | л | м | н | о |
| р | р | с | т | у | х | ш | ь | \_ | , | а | б | в | е | и | к | л | м | н | о | п |
| с | с | т | у | х | ш | ь | \_ | , | а | б | в | е | и | к | л | м | н | о | п | р |
| т | т | у | х | ш | ь | \_ | , | а | б | в | е | и | к | л | м | н | о | п | р | с |
| у | у | х | ш | ь | \_ | , | а | б | в | е | и | к | л | м | н | о | п | р | с | т |
| х | х | ш | ь | \_ | , | а | б | в | е | и | к | л | м | н | о | п | р | с | т | у |
| ш | ш | ь | \_ | , | а | б | в | е | и | к | л | м | н | о | п | р | с | т | у | х |
| ь | ь | \_ | , | а | б | в | е | и | к | л | м | н | о | п | р | с | т | у | х | ш |
| \_ | \_ | , | а | б | в | е | и | к | л | м | н | о | п | р | с | т | у | х | ш | ь |
| , | , | а | б | в | е | и | к | л | м | н | о | п | р | с | т | у | х | ш | ь | \_ |

Таблица 1 – Таблица Виженера.

Исходный текст: не\_хвались\_умом,\_коли\_берешь\_все\_хребтом

Кодовое слово: шишка

Человек, посылающий сообщение, записывает ключевое слово("шишка") циклически до тех пор, пока его длина не будет соответствовать длине исходного текста.

Первый символ исходного текста х зашифрован последовательностью о, которая является первым символом ключа. Первый символ о шифрованного текста находится на пересечении строки я и столбца х в таблице Виженера. Точно так же для второго символа исходного текста используется второй символ ключа. Остальная часть исходного текста шифруется подобным способом.

|  |  |  |
| --- | --- | --- |
| символ | ключ | шифр |
| н | ш | и |
| е | и | м |
| \_ | ш | у |
| х | к | а |
| в | а | в |
| а | ш | ш |
| л | и | п |
| и | ш | а |
| с | к | ь |
| ь | а | ь |
| \_ | ш | у |
| у | и | \_ |
| м | ш | е |
| о | к | у |
| м | а | м |
| , | ш | х |
| \_ | и | в |
| к | ш | б |
| о | к | у |
| л | а | л |
| и | ш | а |
| \_ | и | в |
| б | ш | ь |
| е | к | н |
| р | а | р |
| е | ш | , |
| ш | и | а |
| ь | ш | т |
| \_ | к | е |
| в | а | в |
| с | ш | н |
| е | и | м |
| \_ | ш | у |
| х | к | а |
| р | а | р |
| е | ш | , |
| б | и | к |
| т | ш | о |
| о | к | у |
| м | а | м |

Таблица 2 – Шифрование методом Виженера.

Зашифрованный текст: имуавшпаььу\_еумхвбулавьнр,атевнмуар,коум

1. Кодирование методом квадрата Полибия:

Для начала надо создать таблицу, размер таблицы должен быть более или равным размера алфавита языка. Длинна алфавита сообщения равна 18 буквы, то есть размер таблицы должен быть не менее 20 ячеек. Оптимальный размер таблицы - 5х5 = 25 ячеек, что вписывается в наш размер. Теперь требуется заполнить таблицу алфавитом языка. Заполняется таблица по строкам.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| а | б | в | е | и |
| к | л | м | н | о |
| п | р | с | т | у |
| х | ш | ь | \_ | , |
| 1 | 2 | 3 | 4 | 5 |

Таблица 3 – Квадрат Полибия.

При создании и заполнении таблицы у нас появились 6 лишних клетки, их можно заполнить другими символами(1 2 3 4 5). На этом этапе шифровании происходит собственно шифрование текста. Для шифрования требуется найти букву слова в таблице, затем чтобы получить шифровку надо взять букву под ней. Если буква текста находится на последней строке, то букву берем из первой строки.

|  |  |
| --- | --- |
| символ | шифр |
| н | т |
| е | н |
| \_ | 4 |
| х | 1 |
| в | м |
| а | к |
| л | р |
| и | о |
| с | ь |
| ь | 3 |
| \_ | 4 |
| у | , |
| м | с |
| о | у |
| м | с |
| , | 5 |
| \_ | 4 |
| к | п |
| о | у |
| л | р |
| и | о |
| \_ | 4 |
| б | л |
| е | н |
| р | ш |
| е | н |
| ш | 2 |
| ь | 3 |
| \_ | 4 |
| в | м |
| с | ь |
| е | н |
| \_ | 4 |
| х | 1 |
| р | ш |
| е | н |
| б | л |
| т | \_ |
| о | у |
| м | с |

Таблица 4 – Таблица шифра.

Зашифрованный текст: тн41мкроь34,сус54пуро4лншн234мьн41шнл\_ус

1. Кодирование методом Цезаря:

Для начала надо создать таблицу с алфавитом сообщения.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| а | б | в | е | и |
| 6 | 7 | 8 | 9 | 10 |
| к | л | м | н | о |
| 11 | 12 | 13 | 14 | 15 |
| п | р | с | т | у |
| 16 | 17 | 18 | 19 | 20 |
| х | ш | ь | \_ | , |

Таблица 4 – Таблица алфавита.

Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 1), то шифрование можно выразить формулой http://pastexen.com/i/8ORJZ2CBa4.png,где x — символ открытого текста, y — символ шифрованного текста , n — мощность алфавита (кол-во символов), k — ключ.

n = 20

k = 43

|  |  |  |  |
| --- | --- | --- | --- |
| исходный текст | | шифрованный текст | |
| н | 9 | 12 | р |
| е | 4 | 7 | л |
| \_ | 19 | 2 | б |
| х | 16 | 19 | \_ |
| в | 3 | 6 | к |
| а | 1 | 4 | е |
| л | 7 | 10 | о |
| и | 5 | 8 | м |
| с | 13 | 16 | х |
| ь | 18 | 1 | а |
| \_ | 19 | 2 | б |
| у | 15 | 18 | ь |
| м | 8 | 11 | п |
| о | 10 | 13 | с |
| м | 8 | 11 | п |
| , | 20 | 3 | в |
| \_ | 19 | 2 | б |
| к | 6 | 9 | н |
| о | 10 | 13 | с |
| л | 7 | 10 | о |
| и | 5 | 8 | м |
| \_ | 19 | 2 | б |
| б | 2 | 5 | и |
| е | 4 | 7 | л |
| р | 12 | 15 | у |
| е | 4 | 7 | л |
| ш | 17 | 20 | , |
| ь | 18 | 1 | а |
| \_ | 19 | 2 | б |
| в | 3 | 6 | к |
| с | 13 | 16 | х |
| е | 4 | 7 | л |
| \_ | 19 | 2 | б |
| х | 16 | 19 | \_ |
| р | 12 | 15 | у |
| е | 4 | 7 | л |
| б | 2 | 5 | и |
| т | 14 | 17 | ш |
| о | 10 | 13 | с |
| м | 8 | 11 | п |

Таблица 5 – Шифрование текста.

Зашифрованный текст: рлб\_кеомхабьпспвбнсомбилул,абкхлб\_улишсп

1. Кодирование методом колонной (строчной) замены:

Смысл этого метода в том, чтобы составить таблицу сообщения и пронумеровать столбцы(строки), затем шифровщик задает ключ и перемещает колонны(строки) таблицы и получим зашифрованный текст.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 1 | н | е | \_ | х | в | а | л | и |
| 2 | с | ь | \_ | у | м | о | м | , |
| 3 | \_ | к | о | л | и | \_ | б | е |
| 4 | р | е | ш | ь | \_ | в | с | е |
| 5 | \_ | х | р | е | б | т | о | м |

Таблица 6 – Исходное сообщение.

Для колонной замены шифр 58137246, а для строчной 53142.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 5 | 8 | 1 | 3 | 7 | 2 | 4 | 6 |
| в | и | н | \_ | л | е | х | а |
| м | , | с | \_ | м | ь | у | о |
| и | е | \_ | о | б | к | л | \_ |
| \_ | е | р | ш | с | е | ь | в |
| б | м | \_ | р | о | х | е | т |

Таблица 7 – Колонная замена.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 5 | \_ | х | р | е | б | т | о | м |
| 3 | \_ | к | о | л | и | \_ | б | е |
| 1 | н | е | \_ | х | в | а | л | и |
| 4 | р | е | ш | ь | \_ | в | с | е |
| 2 | с | ь | \_ | у | м | о | м | , |

Таблица 8 – Строчная замена.

1. Кодирование методом Вернама:

Для получения шифротекста открытый текст объединяется операцией «исключающее ИЛИ» с секретным ключом( в нашем случае ключ k= 10110). Перед началом шифрованием надо закодировать алфавит сообщение безизбыточным кодом.

|  |  |  |  |
| --- | --- | --- | --- |
| символ | двоичный код | ⊕ | код |
| а | 00000 | 00000⊕10110 | 10110 |
| б | 00001 | 00001⊕10110 | 10111 |
| в | 00010 | 00010⊕10110 | 10100 |
| е | 00011 | 00011⊕10110 | 10101 |
| и | 00100 | 00100⊕10110 | 10010 |
| к | 00101 | 00101⊕10110 | 10011 |
| л | 00110 | 00110⊕10110 | 10000 |
| м | 00111 | 00111⊕10110 | 10001 |
| н | 01000 | 01000⊕10110 | 11110 |
| о | 01001 | 01001⊕10110 | 11111 |
| п | 01010 | 01010⊕10110 | 11100 |
| р | 01011 | 01011⊕10110 | 11101 |
| с | 01100 | 01100⊕10110 | 11010 |
| т | 01101 | 01101⊕10110 | 11011 |
| у | 01110 | 01110⊕10110 | 11000 |
| х | 01111 | 01111⊕10110 | 11001 |
| ш | 10000 | 10000⊕10110 | 00110 |
| ь | 10001 | 10001⊕10110 | 00111 |
| \_ | 10010 | 10010⊕10110 | 00100 |
| , | 10011 | 10011⊕10110 | 00101 |

Таблица 9 – Шифрование Вернама.

Закодированное сообщение: 11110 10101 00100 11001 10100 10110 10000 10010 11010 00111 00100 11000 10001 11111 10001 00101 00100 10011 11111 10000 10010 00100 10111 10101 11101 10101 00110 00111 00100 10100 1101010101 0010011001 1110110101 10111 11011 11111 10001

ВЫВОДЫ

В ходе лабораторной работы были исследованы простые шифры Виженера, квадрата Полибия, Цезаря, колонной (строчной) замены, Вернама.