**Лабораторная работа №4**

**Тема:** шифрование с использованием системы Вижинера и шифра «двойной квадрат» Уитстона.

**Цель работы:** формирование умений шифрования с использованием системы Вижинера и шифра «двойной квадрат» Уитстона.

Задание 1. Используя систему Вижинера, зашифруйте сообщения. Текст сообщения и ключевое слово должны соответствовать варианту задания лабораторной работы 3.

Исходное сообщение: «ТОТ, КТО СМОТРИТ НА ДЕЛО С ОБЕИХ СТОРОН, ОБЫЧНО НЕ ВИДИТ НИ ОДНОЙ ИЗ НИХ».

Ключевое слово: «ЖИЗНЬ».

Таблица 1 – Таблица шифрования

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Сообщение | т | о | т |  | к | т | о |  | с | м | о | т | р | и | т |  |
| Ключ. слово | ж | и | з |  | н | ь | ж |  | и | з | н | ь | ж | и | з |  |
| Ключи | 6 | 8 | 7 |  | 13 | 28 | 6 |  | 8 | 7 | 13 | 28 | 6 | 8 | 7 |  |
| Шифртекст | ш | ц | щ |  | ч | о | ф |  | щ | у | ы | о | ц | р | щ |  |

Продолжение таблицы 1 – Таблица шифрования

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Сообщение | н | а |  | д | е | л | о |  | с |  | о | б | е | и | х |  |
| Ключ. слово | н | ь |  | ж | и | з | н |  | ь |  | ж | и | з | н | ь |  |
| Ключи | 13 | 28 |  | 6 | 8 | 7 | 13 |  | 28 |  | 6 | 8 | 7 | 13 | 28 |  |
| Шифртекст | ъ | ь |  | к | н | т | ы |  | н |  | ф | й | м | х | с |  |

Продолжение таблицы 1 – Таблица шифрования

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Сообщение | с | т | о | р | о | н |  | о | б | ы | ч | н | о |  | н | е |
| Ключ. слово | ж | и | з | н | ь | ж |  | и | з | н | ь | ж | и |  | з | н |
| Ключи | 6 | 8 | 7 | 13 | 28 | 6 |  | 8 | 7 | 13 | 28 | 6 | 8 |  | 7 | 13 |
| Шифртекст | ч | ъ | х | э | к | у |  | ц | и | и | у | у | ц |  | ф | т |

Продолжение таблицы 1 – Таблица шифрования

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Сообщение | в | и | д | и | т |  | н | и |  | о | д | н | о | й |  |  |
| Ключ. слово | ь | ж | и | з | н |  | ь | ж |  | и | з | н | ь | ж |  |  |
| Ключи | 28 | 6 | 8 | 7 | 13 |  | 28 | 6 |  | 8 | 7 | 13 | 28 | 6 |  |  |
| Шифртекст | ю | о | м | п | я |  | й | о |  | ц | д | ъ | к | п |  |  |

Продолжение таблицы 1 – Таблица шифрования

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Сообщение | и | з |  | н | и | х |  |  |  |  |  |  |  |  |  |  |
| Ключ. слово | и | з |  | н | ь | ж |  |  |  |  |  |  |  |  |  |  |
| Ключи | 8 | 7 |  | 13 | 28 | 6 |  |  |  |  |  |  |  |  |  |  |
| Шифртекст | р | о |  | ъ | д | ы |  |  |  |  |  |  |  |  |  |  |

В ходе шифрования сообщения:

«ТОТ, КТО СМОТРИТ НА ДЕЛО С ОБЕИХ СТОРОН, ОБЫЧНО НЕ ВИДИТ НИ ОДНОЙ ИЗ НИХ»

получаем шифртекст:

«ШЦЩ, ЧОФ ЩУЫОЦРЩ ЪЬ КНТЫ Н ФЙМХС ЧЪХЭКУ, ЦИИУУЦ ФТ ЮОМПЯ ЙО ЦЛЪКП РО ЪДЫ»

Задание 2. Используя шифр «двойной квадрат» Уитстона и шифрующие таблицы, представленные на рис. 4.1, выполните шифрование сообщения из задания лабораторной работы 3.

Таблицы 2, 3 – Шифрующие таблицы

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

Исходное сообщение: «ТОТ, КТО СМОТРИТ НА ДЕЛО С ОБЕИХ СТОРОН, ОБЫЧНО НЕ ВИДИТ НИ ОДНОЙ ИЗ НИХ».

Разобьём исходное сообщение на биграммы и сопоставим им соответствующие биграммы из таблицы

Таблица 4 – Биграммы

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| «ТО» | «Т,» | « К» | «ТО» | « С» | «МО» | «ТР» | «ИТ» | « Н» | «А » |
| «ЖБ» | «ЖИ» | «:Ш» | «ЖБ» | «ПШ» | «ЩТ» | «ЬМ» | «ОЖ» | «ПК» | «ФЪ» |
| «ДЕ» | «ЛО» | « С» | « О» | «БЕ» | «ИХ» | « С» | «ТО» | «РО» | «Н,» |
| «.Ы» | « Ц» | «ПШ» | «ЛБ» | «М » | «О:» | «ПШ» | «ЖБ» | «ТБ» | «ИЬ» |
| « О» | «БЫ» | «ЧН» | «О » | «НЕ» | « В» | «ИД» | «ИТ» | « Н» | «И » |
| «ЛБ» | «МЪ» | «ПО» | «ХЛ» | «ЯП» | «ЕС» | «ОЗ» | «ОЖ» | «ПК» | «ОЧ» |

Продолжение таблицы 4

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| «ОД» | «НО» | «Й » | «ИЗ» | « Н» | «ИХ» |  |  |  |  |
| «ХГ» | «ТЬ» | «ОЧ» | «,Я» | «ПК» | «О:» |  |  |  |  |

В ходе шифрования сообщения:

«ТОТ, КТО СМОТРИТ НА ДЕЛО С ОБЕИХ СТОРОН, ОБЫЧНО НЕ ВИДИТ НИ ОДНОЙ ИЗ НИХ»

получаем шифртекст:

«ЖБЖИ:ШЖБПШЩТЬМОЖПКФЪ.Ы\_ЦПШЛБМ\_О:ПШЖБТБИЬЛБМЪПОХЛЯПЕСОЗОЖПКОЧХГТЬОЧ,ЯПКО:»

**Контрольные вопросы**

1. Чем шифры сложной замены отличаются от шифров простой замены?

Шифры сложной замены отличаются от шифров простой замены тем, что они используют более сложные алгоритмы для замены символов текста. В шифрах простой замены каждая буква или символ заменяется однозначно другой буквой или символом (например, "А" заменяется на "X", "Б" на "Y" и так далее). В шифрах сложной замены, таких как шифр Вижинера или шифр «двойной квадрат» Уитстона, замены могут быть зависимыми от позиции символов или от предыдущих символов, что делает их более сложными для анализа и взлома.

2. Что используется в качестве ключа в системе Вижинера?

Таблица Вижинера имеет два входа:

* верхнюю строку подчеркнутых символов, используемую для считывания очередной буквы исходного открытого текста;
* крайний левый столбец ключа.

Последовательность ключей получают из порядковых номеров в алфавите букв ключевого слова (начиная с 0).

3. Как осуществляется шифрование текста с использованием системы Вижинера?

При шифровании исходного сообщения его выписывают в строку, а под ним записывают ключевое слово или фразу. Если ключ оказался короче сообщения, то его циклически повторяют. В процессе шифрования находят в верхней строке таблицы очередную букву исходного текста и в левом столбце очередное значение ключа. Очередная буква шифртекста находится на пересечении столбца, определяемого шифруемой буквой, и строки, определяемой числовым значением ключа.

4. Какие требования предъявляются к шифруемому тексту при использовании шифра «двойной квадрат» Уитстона?

Перед шифрованием исходное сообщение разбивают на биграммы. Каждая биграмма шифруется отдельно.

5. Как осуществляется шифрование текста с использованием шифра «двойной квадрат» Уитстона?

Шифр «двойной квадрат» использует две таблицы со случайно расположенными в них буквами русского алфавита, размещенными по одной горизонтали; шифрование идет биграммами, как в шифре Плейфейра. Перед шифрованием исходное сообщение разбивают на биграммы. Каждая биграмма шифруется отдельно. Первую букву биграммы находят в левой таблице, а вторую букву в правой. Затем мысленно строят прямоугольник так, чтобы буквы биграммы лежали в его противоположных вершинах. Другие две вершины этого прямоугольника дают буквы биграммы шифртекста.