МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «Белорусский государственный технологический университет»

Кафедра информационных технологий

**Практическое занятие №5**

**Тема «Криптографическая защита информации»**

Выполнила:

Студентка 2 курса, 7 группы

Курносенко Софья Андреевна

Проверил:

Барковский Евгений Валерьевич

Цель: Овладение основными криптографическими алгоритмами симметричного шифрования.

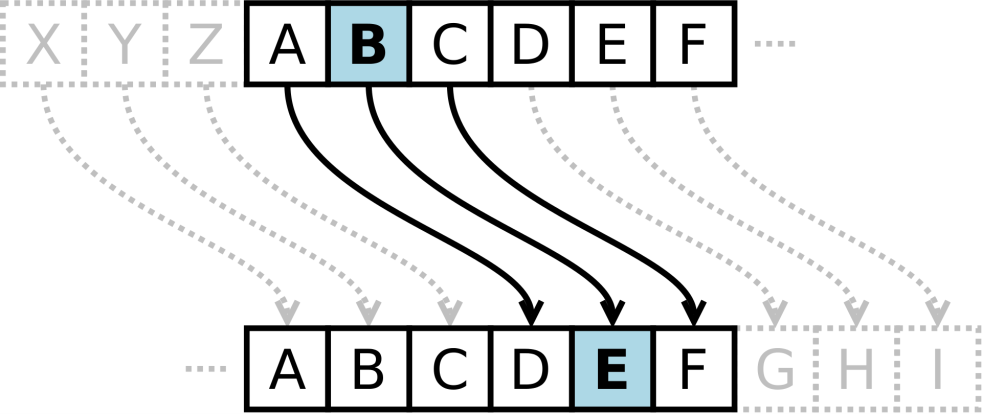
**ВАРИАНТ 13**

**Задание к выполнению**

1. Изучить теоретические сведения по данной теме.
2. Зашифровать сообщение с использованием шифра Цезаря, Трисемуса, Плейфейра и Вижинера и полученного секретного ключа (по номеру варианта и ключевому слову «Защита»). В качестве сообщения использовать свою Фамилию Имя Отчество.

2.1) **Шифр 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. Например, в шифре со сдвигом вправо на 3, А была бы заменена на Г, Б станет Д, и так далее.



Шифр Цезаря со сдвигом на 3:

A заменяется на D

B заменяется на E

и так далее

Z заменяется на C

Выполнение задания

Ключ = 13.

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

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Сообщение | К | У | Р | Н | О | С | Е | Н | К | О |  | С | О | Ф | Ь | Я |  | А | Н | Д | Р | Е | Е | В | Н | А |
| Номер |  |  | 18 | 15 | 16 | 19 | 6 | 15 | 12 | 16 |  | 19 | 16 | 22 | 30 | 33 |  | 1 | 15 | 5 | 18 | 6 | 6 | 3 | 15 | 1 |
| Номер + 13 | 25 |  | 31 | 28 | 29 | 32 | 19 | 28 | 25 | 29 |  | 32 | 29 |  |  |  |  | 14 | 28 | 18 | 31 | 19 | 19 | 16 | 28 | 14 |
| Итог |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Сообщение | Номер | Номер + 13 | Итог |
| К | 12 | 25 | Ч |
| У | 21 | 34 → 1 | А |
| Р | 18 | 31 | Э |
| Н | 15 | 28 | Ъ |
| О | 16 | 29 | Ы |
| С | 19 | 32 | Ю |
| Е | 6 | 19 | С |
| Н | 15 | 28 | Ъ |
| К | 12 | 25 | Ч |
| О | 16 | 29 | Ы |
|  |  |  |  |
| С | 19 | 32 | Ю |
| О | 16 | 29 | Ы |
| Ф | 22 | 35 →2 | Б |
| Ь | 30 | 43 → 10 | И |
| Я | 33 | 46 → 13 | Л |
|  |  |  |  |
| А | 1 | 14 | М |
| Н | 15 | 28 | Ъ |
| Д | 5 | 18 | Р |
| Р | 18 | 31 | Э |
| Е | 6 | 19 | С |
| Е | 6 | 19 | С |
| В | 3 | 16 | О |
| Н | 15 | 28 | Ъ |
| А | 1 | 14 | М |

Результат:

«ЧАЭЪЫЮСЪЧЫ ЮЫБИЛ МЪРЭССОЪМ»

2.2) **Шифр Тритемиуса**

Шифр Тритемиуса — система шифрования, разработанная Иоганном Тритемием. Представляет собой усовершенствованный шифр Цезаря, то есть шифр подстановки. По алгоритму шифрования, каждый символ сообщения смещается на символ, отстающий от данного на некоторый шаг. Здесь шаг смещения делается переменным, то есть зависящим от каких-либо дополнительных факторов.

Таблица Трисемуса заполняется с помощью ключевого слова, повторяющиеся буквы которого отбрасываются. Затем таблица дополняется не вошедшими в нее буквами алфавита по порядку как в системе Цезаря с ключевым словом. Таким образом, ключом в таблицах Трисемуса является ключевое слово и размер таблицы.

При шифровании буква открытого текста заменяется буквой, расположенной ниже нее в том же столбце.

Выполнение задания

С помощью ключевого слова – ЗАЩИТА и таблицы размером 5×7 зашифрую сообщение «КУРНОСЕНКО СОФЬЯ АНДРЕЕВНА».

Сначала подготовим ключевое слово, убрав из него повторяющиеся буквы. Полученное буквосочетание «ЗАЩИТ» запишем построчно в таблицу. После этого дополняем таблицу оставшимися буквами алфавита, пробелом, запятой и точкой

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

Например, для буквы К в строке расположенной ниже находим С, для буквы Ь возвращаемся к первой строке таблицы и берем значение З.

Сообщение: КУРНОСЕНКО СОФЬЯ АНДРЕЕВНА.

*Зашифрованное сообщение*: СЫШХЦЪОХСЦТЪЦЬЗИТДХНШООЛХД.

2.3) **Шифр Плейфера**

Шифр Плейфера использует матрицу 5х5 (для латинского алфавита, для кириллического алфавита необходимо увеличить размер матрицы до 4х8), содержащую ключевое слово или фразу. Для создания матрицы и использования шифра достаточно запомнить ключевое слово и четыре простых правила. Чтобы составить ключевую матрицу, в первую очередь нужно заполнить пустые ячейки матрицы буквами ключевого слова (не записывая повторяющиеся символы), потом заполнить оставшиеся ячейки матрицы символами алфавита, не встречающимися в ключевом слове, по порядку (в английских текстах обычно опускается символ «Q», чтобы уменьшить алфавит, в других версиях «I» и «J» объединяются в одну ячейку). Ключевое слово может быть записано в верхней строке матрицы слева направо, либо по спирали из левого верхнего угла к центру. Ключевое слово, дополненное алфавитом, составляет матрицу 5х5 и является ключом шифра.

Для шифрования сообщения необходимо разбить его на биграммы (группы из двух символов), при этом, если в биграмме встретятся два одинаковых символа, то между ними добавляется заранее оговоренный вспомогательный символ (в оригинале – X, для русского алфавита — Я). Например, «зашифрованное сообщение» становится «за ши фр ов ан но ес оЯ об ще ни еЯ». Для формирования ключевой таблицы выбирается лозунг и далее она заполняется по правилам шифрующей системы Трисемуса. Например, лозунг «ДЯДИНА»



Ключевая таблица для шифра Плейфера

Затем, руководствуясь следующими правилами, выполняется зашифровывание пар символов исходного текста:

1. Если символы биграммы исходного текста встречаются в одной строке, то эти символы замещаются на символы, расположенные в ближайших столбцах справа от соответствующих символов. Если символ является последним в строке, то он заменяется на первый символ этой же строки.

2. Если символы биграммы исходного текста встречаются в одном столбце, то они преобразуются в символы того же столбца, находящимися непосредственно под ними. Если символ является нижним в столбце, то он заменяется на первый символ этого же столбца.

3. Если символы биграммы исходного текста находятся в разных столбцах и разных строках, то они заменяются на символы, находящиеся в тех же строках, но соответствующие другим углам прямоугольника.

*Пример шифрования:*

— биграмма «за» формирует прямоугольник – заменяется на «жб»;

— биграмма «ши» находятся в одном столбце – заменяется на «юе»;

— биграмма «фр» находятся в одной строке – заменяется на «хс»;

— биграмма «ов» формирует прямоугольник – заменяется на «йж»;

— биграмма «ан» находятся в одной строке – заменяется на «ба»;

— биграмма «но» формирует прямоугольник – заменяется на «ам»;

— биграмма «ес» формирует прямоугольник – заменяется на «гт»;

— биграмма «оя» формирует прямоугольник – заменяется на «ка»;

— биграмма «об» формирует прямоугольник – заменяется на «па»;

— биграмма «ще» формирует прямоугольник – заменяется на «шё»;

— биграмма «ни» формирует прямоугольник – заменяется на «ан»;

— биграмма «ея» формирует прямоугольник – заменяется на «ги».

Шифрограмма – «жб юе хс йж ба ам гт ка па шё ан ги».

Для расшифровки необходимо использовать инверсию этих правил, откидывая символы Я (или Х), если они не несут смысла в исходном сообщении.

Выполнение задания

С помощью ключевого слова – ЗАЩИТА и таблицы размером 4×8 зашифрую сообщение «КУРНОСЕНКО СОФЬЯ АНДРЕЕВНА».

Сначала подготовим ключевое слово, убрав из него повторяющиеся буквы. Полученное буквосочетание «ЗАЩИТ» запишем построчно в таблицу. После этого дополняем таблицу оставшимися буквами алфавита.

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

Сообщение: КУРНОСЕНКО СОФЬЯ АНДРЕЕВНА

Сообщение, разбитое на биграммы: КУ РН ОС ЕН КО СО ФЬ ЯА НД РЕ ЕВ НА

─ биграмма КУ расположена в одном столбце, заменяем на УЬ

─ биграмма РН формирует прямоугольник, заменяем на ЦЖ

─ биграмма ОС расположена в одной строке, заменяем на ПУ

─ биграмма ЕН расположена в одной строке, заменяем на ЖД

─ биграмма КО формирует прямоугольник, заменяем на ДУ

─ биграмма СО расположена в одной строке, заменяем на УП

─ биграмма ФЬ формирует прямоугольник, заменяем на УЭ

─ биграмма ЯА формирует прямоугольник, заменяем на ШГ

─ биграмма НД расположена в одной строке, заменяем на ДЕ

─ биграмма РЕ формирует прямоугольник, заменяем на ПЖ

─ биграмма ЕВ формирует прямоугольник, заменяем на МА

─ биграмма НА формирует прямоугольник, заменяем на ЕГ

*Зашифрованное сообщение*: УЬЦЖПУЖДДУУППЭШГДЕПЖМАЕГ

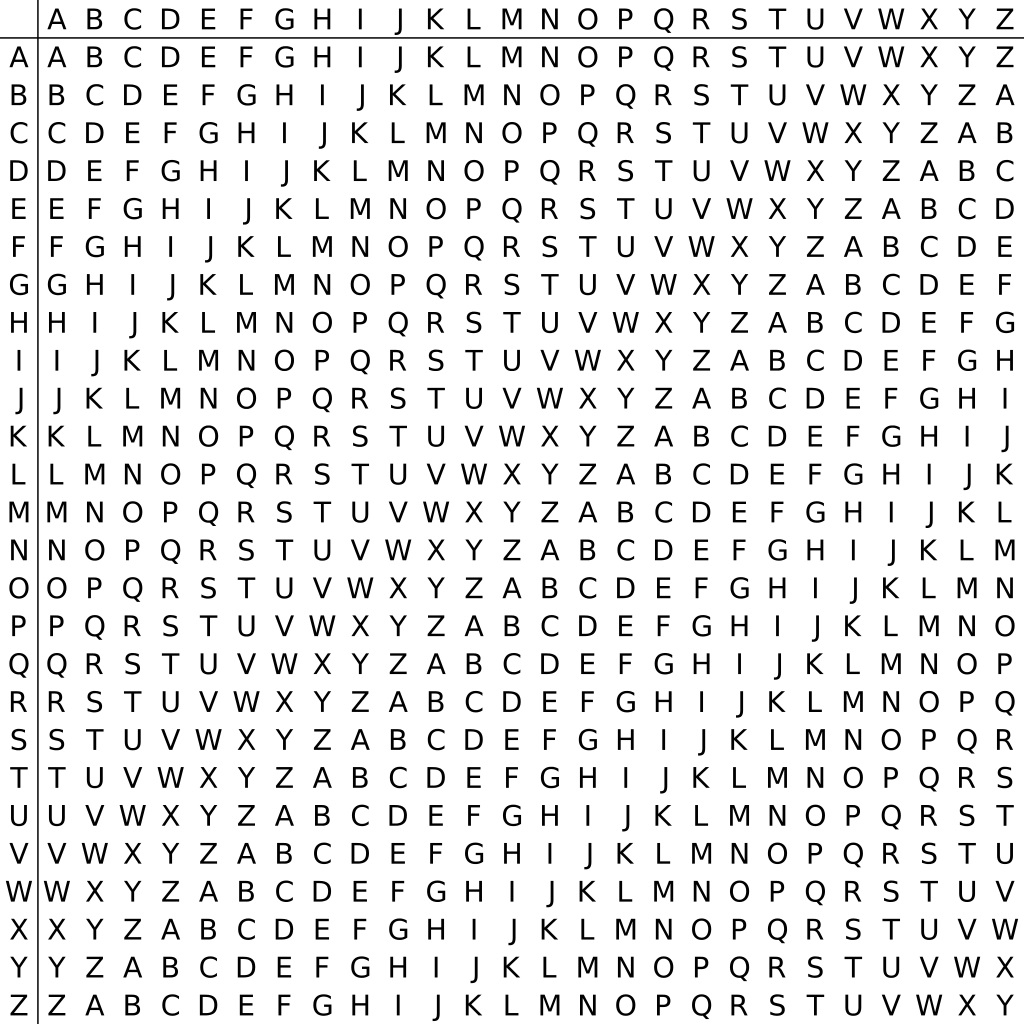
2.4) **Шифр Вижинера**

В [шифре Цезаря](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%A6%D0%B5%D0%B7%D0%B0%D1%80%D1%8F) каждая буква алфавита сдвигается на несколько строк; например в шифре Цезаря при сдвиге +3, A стало бы D, B стало бы E и так далее. Шифр Виженера состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига. Для зашифровывания может использоваться таблица алфавитов, называемая tabula recta или квадрат (таблица) Виженера. Применительно к латинскому алфавиту таблица Виженера составляется из строк по 26 символов, причём каждая следующая строка сдвигается на несколько позиций. Таким образом, в таблице получается 26 различных шифров Цезаря. На каждом этапе шифрования используются различные алфавиты, выбираемые в зависимости от символа ключевого слова. Например, предположим, что исходный текст имеет вид:

ATTACKATDOWN

Человек, посылающий сообщение, записывает ключевое слово («LEMON») циклически до тех пор, пока его длина не будет соответствовать длине исходного текста:

LEMONLEMONLE



Первый символ исходного текста A зашифрован последовательностью L, которая является первым символом ключа. Первый символ L шифрованного текста находится на пересечении строки L и столбца A в таблице Виженера. Точно так же для второго символа исходного текста используется второй символ ключа; то есть второй символ шифрованного текста X получается на пересечении строки E и столбца T. Остальная часть исходного текста шифруется подобным способом.

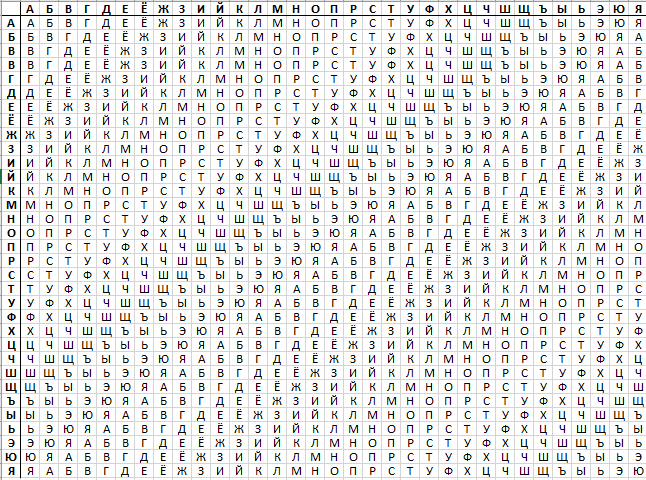
*Исходный текст: ATTACKATDAWN*

*Ключ: LEMONLEMONLE*

*Зашифрованный текст: LXFOPVEFRNHR*

Расшифровывание производится следующим образом: находим в таблице Виженера строку, соответствующую первому символу ключевого слова; в данной строке находим первый символ зашифрованного текста. Столбец, в котором находится данный символ, соответствует первому символу исходного текста. Следующие символы зашифрованного текста расшифровываются подобным образом.

Таблица Виженера для русского алфавита



Выполнение задания

С помощью ключевого слова – ЗАЩИТА и таблицы Вижинера зашифрую сообщение «КУРНОСЕНКО СОФЬЯ АНДРЕЕВНА».

Сначала подготовим ключевое слово, прописывая его циклически до тех пор, пока его длина не будет соответствовать длине исходного текста: ЗАЩИТАЗАЩИТАЗАЩИТАЗАЩИТА.

Шифрую, находя соответствующий символ шифрованного текста на пересечении строки с буквой ключа и столбца с буквой исходного сообщения:

Исходный текст: КУРНОСЕНКОСОФЬЯАНДРЕЕВНА

Ключ: ЗАЩИТАЗАЩИТАЗАЩИТАЗАЩИТА

Зашифрованный текст: ТУЙЦБСМНДЧДОЬЬЯИАДШЕЮКАА

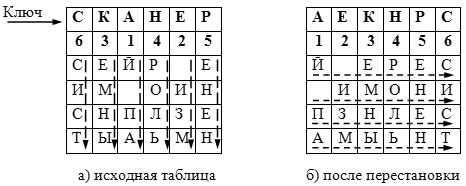
1. Расшифровать следующее сообщение:

|  |  |  |
| --- | --- | --- |
|  | **\_яетож\_нксучнтуотдеыужбьатйдны\_,**  **с\_ао\_о\_яс,\_ндк,е\_иаиу\_ккддндаруто\_**  **а\_еди.в\_нта\_ \_ахе:\_** | Расшифровать с помощью **Одиночной перестановки по ключу.**  **Ключ – СЧАСТЬЕ Таблица 12х7** |

Метод шифрующих таблиц с одиночной перестановкой по ключу заключается в перестановке столбцов таблицы по ключевому слову после заполнения таблицы исходным текстом. Длина ключевого слова, фразы или числа, задающего способ перестановки, должна быть равна числу столбцов таблицы. Столбцы переставляются в порядке следования в алфавите символов ключевого слова.

Пример 3. Зашифруем фразу «СИСТЕМНЫЙ ПАРОЛЬ ИЗМЕНЕН» с помощью таблицы размером 4х6 и ключевого слова «СКАНЕР».

Для записи заданной фразы достаточно одной таблицы. Сначала ее заполняют по столбцам исходной фразой, затем переставляют столбцы по ключевому слову «СКАНЕР» и считывают символы по строкам. В результате получаем шифрованное сообщение: «Й\_ЕРЕС\_ИМОНИПЗНЛЕСАМЫЬНТ».



Реализация шифрующих таблиц с одиночной перестановкой по ключу

Выполнение задания

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Ключ | С | Ч | А | С | Т | Ь | Е |
| Очередность буквы в алфавите | 19 | 25 | 1 | 19 | 20 | 30 | 6 |
| Очередность буквы для упорядочения букв ключа по алфавиту | 3 | 6 | 1 | 4 | 5 | 7 | 2 |
| Расположение букв ключа в алфавитном порядке | А | Е | С | С | Т | Ч | Ь |

Записываем построчно зашифрованное сообщение:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| А | Е | С | С | Т | Ч | Ь |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|  | я | е | т | о | ж |  |
| н | к | с | у | ч | н | т |
| у | о | т | д | е | ы | у |
| ж | б | ь | а | т | й | д |
| н | ы |  | , | с |  | а |
| о |  | о |  | я | с | , |
|  | н | д | к | , | е |  |
| и | а | и | у |  | к | к |
| д | д | н | д | а | р | у |
| т | о |  | а |  | е | д |
| и | . | в |  | н | т | а |
|  |  | а | х | е |  |  |

Переставляем столбцы, так чтобы в верхней строке сложилось ключевое слово:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| С | Ч | А | С | Т | Ь | Е |
| 3 | 6 | 1 | 4 | 5 | 7 | 2 |
| е | ж |  | т | о |  | я |
| с | н | н | у | ч | т | к |
| т | ы | у | д | е | у | о |
| ь | й | ж | а | т | д | б |
|  |  | н | , | с | а | ы |
| о | с | о |  | я | , |  |
| д | е |  | к | , |  | н |
| и | к | и | у |  | к | а |
| н | р | д | д | а | у | д |
|  | е | т | а |  | д | о |
| в | т | и |  | н | а | . |
| а |  |  | х | е |  |  |

*Расшифровка: есть один важный секрет нужно идти туда, куда хочется, а не туда, куда якобы надо.*