# **Лабораторная работа №3 Шифрование методами замены**

**Цель работы:** закрепить умение шифровать информацию системой Цезаря, системой Трисемуса, алгоритмом Плейфера и реализовать алгоритмы в программном коде

**Порядок выполнения работы:**

1. Изучить теоретический материал
2. Выбрать язык программирования
3. Выполнить практическую часть.
4. Оформить отчет. Отчет должен содержать:
   * наименование и цель работы;
   * ответы на контрольные вопросы;
   * код на выбранном языке программирования соответствующих заданий и скриншоты выполнения написанных программ;
   * выводы к выполненной лабораторной работе.

Отчет переименовать следующим образом: **ЗКИ\_ЛР3\_Фамилия\_№группы** и сдать на проверку преподавателю.

**Теоретическая часть**

## Система Цезаря

Шифр Цезаря — один из древнейших шифров. При шифровании каждый символ заменяется другим, отстоящим от него в алфавите на фиксированное число позиций. Шифр Цезаря можно классифицировать как шифр подстановки, при более узкой классификации — шифр простой замены.

Шифр назван в честь римского императора Гая Юлия Цезаря, использовавшего его для секретной переписки.

Математическая модель

Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование и дешифрование можно выразить формулами:

http://kriptografea.narod.ru/13.png

http://kriptografea.narod.ru/14.png

*где x — символ открытого текста*

*y — символ шифрованного текста*

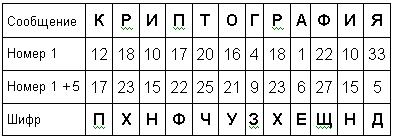
*n — мощность алфавита (кол-во символов)*

*k — ключ.*

Алфавит:



Пример:



Ответ: «Пхнфчузхещнд» Ключ: 5

## Система Трисемуса

Шифрующая система Трисемуса (Тритемия). В 1508 г. аббат из Германии Иоганн Трисемус написал печатную работу по криптологии под названием «Полиграфия». В этой книге он впервые систематически описал применение модифицированного шифра Цезаря.

Здесь шаг смещения делается переменным, то есть зависящим от каких-либо дополнительных факторов. Например, можно задать закон смещения в виде линейной функции (уравнения зашифрования) позиции шифруемой буквы.

Сама функция должна гарантировать целочисленное значение. Прямая функция шифрования должна иметь обратную функцию шифрования, тоже целочисленную.

Уравнение зашифрования для шифра Тритемиуса имеет следующий вид:

Некоторые варианты вычисления шага смещения k:

,

,

где p — позиция буквы в сообщении; A, B, C — ключи.

*Алгоритм шифрования с использованием системы Трисемуса:*

1. Определяем порядковый номер шифруемой буквы в тексте.
2. Определяем код буквы в алфавите.
3. Вычисляем смещение k.
4. Находим код зашифрованной буквы, пользуясь нашим уравнением зашифрования. Расшифрование
5. По коду L восстанавливаем очередную букву криптограммы.
6. Повторяем пункты 1..5 до окончания текста шифрограммы.

Для k=2p^2+5p+3 и алфавита:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 |
| С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я |  | , | . |
| 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 |

Оригинальный текст:

Съешь же ещё этих мягких французских булок, да выпей чаю.

Шифрованный текст:

ФБЩШЛГД Ч.ЪСЧДП ЕО,ЧЁЬЙЙЛЮЩЛ РЬА РЙХАКЕЛ,РЮШЮЭ,НТЩВ,ПЁФЦВ

**Реализация алгоритма шифрования 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 того чтобы зашифровать сообщение, необходимо разбить его на биграммы (группы из двух символов), например «Hello World» становится «HE LL OW OR LD», и отыскать эти биграммы в таблице. Два символа биграммы соответствуют углам прямоугольника в ключевой матрице. Определяем положения углов этого прямоугольника относительно друг друга. Затем, руководствуясь следующими 4 правилами, зашифровываем пары символов исходного текста:

1. Если два символа биграммы совпадают (или если остался один символ), добавляем после первого символа «Х», зашифровываем новую пару символов и продолжаем. В некоторых вариантах шифра Плейфера вместо «Х» используется «Q».

2. 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.

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

4. 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.

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

Пример. Используем ключ «playfair example», тогда матрица примет вид:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| P | L | A | Y | F |
| I | R | E | X | M |
| B | C | D | G | H |
| J | K | N | O | S |
| T | U | V | W | Z |

Зашифруем сообщение «Hide the gold in the tree stump»  
HI DE TH EG OL DI NT HE TR EX ES TU MP  
1. Биграмма HI формирует прямоугольник, заменяем её на BM.  
2. Биграмма DE расположена в одном столбце, заменяем её на ND.  
3. Биграмма TH формирует прямоугольник, заменяем её на ZB.  
4. Биграмма EG формирует прямоугольник, заменяем её на XD.  
5. Биграмма OL формирует прямоугольник, заменяем её на KY.  
6. Биграмма DI формирует прямоугольник, заменяем её на BE.  
7. Биграмма NT формирует прямоугольник, заменяем её на JV.  
8. Биграмма HE формирует прямоугольник, заменяем её на DM.  
9. Биграмма TR формирует прямоугольник, заменяем её на UI.  
10. Биграмма EX находится в одной строке, заменяем её на XM.  
11. Биграмма ES формирует прямоугольник, заменяем её на MN.  
12. Биграмма TU находится в одной строке, заменяем её на UV.  
13. Биграмма MP формирует прямоугольник, заменяем её на IF.

Получаем зашифрованный текст «BM ND ZB XD KY BE JV DM UI XM MN UV IF»

Таким образом сообщение «Hide the gold in the tree stump» преобразуется в «BMNDZBXDKYBEJVDMUIXMMNUVIF»

**Практическая часть**

**Задание №1**

Зашифровать системой Цезаря индивидуальную фразу.

В качестве индивидуальной фразы зашифровать *«Свое Имя Отчество Фамилию».*

В качестве ключа использовать свой номер в списке.

**Задание №2**

Зашифровать системой Плейфера индивидуальную фразу.

В качестве индивидуальной фразы зашифровать «Название любимой книги и ее автора».

В качестве ключа использовать слово из таблицы.

|  |  |
| --- | --- |
| 1 вариант: буйвол  2 вариант: мальта  3 вариант: портрет  4 вариант: архив  5 вариант: совершенство  6 вариант: удар  7 вариант: алгоритм  8 вариант: советник | 9 вариант: мгновенье  10 вариант: гвардия  11 вариант: колонна  12 вариант: сплав  13 вариант: призыв  14 вариант: шерсть  15 вариант: фамилия  16 вариант: парус |

# **Контрольные вопросы:**

1. **Опишите шифр Цезаря.**
2. **Опишите алгоритм системы Трисемуса.**
3. **Как зашифровывается сообщение в шифре Плейфера?**