**Лабораторная работа № 3**

# **Шифрование с использованием: систем Цезаря и системы Трисемуса**

1. **Цель работы: изучить и закрепить умение шифровать информацию системой цезаря и системой Трисемуса.**

**2 Порядок выполнения работы:**

**2.1 Выбрать язык программирования.**

**2.2 Изучить материал.**

**2.3 Выполнить задания.**

**2.4 Ответьте на контрольные вопросы.**

**2.4.1 Опишите шифр Цезаря.**

**2.4.2 Опишите алгоритм системы Трисемуса.**

**2.5 Оформить отчет**

**Теоретические сведенья:**

## **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*

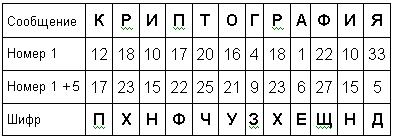
*n — мощность алфавита (кол-во символов)*

*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

**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 методом Трисемуса индивидуальную фразу.

В качестве индивидуальной фразы использовать «Название предмета который мы проходим».

В качестве коэффициентов использовать цифры из таблицы

|  |  |  |  |
| --- | --- | --- | --- |
| # | A | B | C |
| 1 | 1 | 4 | -3 |
| 2 | 2 | -1 | 2 |
| 3 | 3 | 2 | 1 |
| 4 | 2 | 5 | 2 |
| 5 | 4 | 1 | 4 |
| 6 | 2 | -1 | 7 |
| 7 | 3 | 3 | -2 |
| 8 | 1 | 4 | 2 |
| 9 | 2 | 2 | 3 |
| 10 | 1 | 5 | 1 |

**3 Содержание отчета:**

3.1 Наименование и цель работы.

3.2 Описание порядка выполнения работы.

3.3 Ответы на контрольные вопросы.

3.4 Выводы по работе.

**Оформите отчет. Запишите результаты выполнения заданий в отчет.**