**Лабораторная работа №1. Шифрование-дешифорвание**

**Цель работы.** Изучить шифры и коды, а также получить практические навыки шифрования и дешифрования текстовых данных.

**Общее задание.** Написать программу, осуществляющую шифрование и дешифрование каких-либо данных. Для проверки работоспособности программ необходимо предоставить не менее 3-х контрольных примеров. В некоторых пунктах вариантов присутствуют пункты А) и Б), в которых студентам предлагается на выбор один из способов шифрования, в случае возникновения затруднений по какому-либо пункту. В квадратных скобках указана ссылка на справочный источник.

**Варианты заданий.**

1. А) Тип шифрования — перемножение матрицы данных на матрицу ключа. Матрица ключа — квазиединичная матрица 8x8.   
   Б) Шифр с паролем [1]
2. Тип шифрования — перемножение матрицы данных на матрицу ключа. Матрица ключа — матрица размещения 8 ферзей на шахматной доске (что бы они не атаковали друг-друга).
3. Тип шифрования — шифр Цезаря.
4. Тип шифрования — шифр Скитала.
5. Тип шифрования – Полибианский квадрат
6. Тип шифрования – шифр Гронсфельда
7. Тип шифрования – таблицы Виженера (Вижанера)
8. Тип шифрования – простая перестановка
9. Тип шифрования – таблицы двойная перестановка
10. Тип шифрования – регулярные перестановочные таблицы
11. Тип шифрования — «революционный код». Последовательное выписывание групп по 8 символов, ключ задается матрицей с 8-ю единицами, размещенных таким образом, чтобы они, при повороте матрицы на 90° 3 раза, не совпадали.
12. Тип шифрования — шифр Цезаря.
13. Тип шифрования — шифр Скитала.
14. Тип шифрования – шифр Гронсфельда
15. Тип шифрования – таблицы Виженера (Вижанера)
16. Тип шифрования – простая перестановка
17. Тип шифрования – таблицы двойная перестановка
18. Тип шифрования – регулярные перестановочные таблицы
19. Тип шифрования – шифр Трисемуса
20. Тип шифрования – шифрование методом решеток
21. Тип шифрования – двойной квадрат
22. A) Тип шифрования — замена значащих символов на символы псевдографики и аналогичные.   
    Б) Шифр - перевернутые пары [1]

**Список источников**

1. Адаменко М. В. Основы классической криптологии: секреты шифров и кодов. -М: ДМК Пресс, 2012. - 256 с.
2. Мао В. Современная криптография: теория и практика. : Пер. с англ. — М. Издательский дом "Вильяме", 2005. — 768 с.