**Цели и задачи работы:** изучение основных принципов объектно-ориентированного программирования.

**Задание к работе:**Самостоятельно решить задачи в соответствии с индивидуальным вариантом на двух языках программирования высокого уровня (С++ и другой по выбору).

Реализовать криптографические протоколы Шамира, Диффи-Хеллмана, Эль-Гамаля, RSA с использованием классов для хранения данных.

**Методика выполнения работы:**

1. Разработать алгоритм решения задачи по индивидуальному заданию.

2. Написать и отладить программу решения задачи.

3. Протестировать работу программы на различных исходных данных. Контрольный пример  с результатами ручных расчетов представить в отчете.

4. Ответить на контрольные вопросы.

При **защите**лабораторной работы по требованию преподавателя необходимо модифицировать программу и устно ответить на контрольные вопросы.

**Контрольные вопросы:**

1. Что понимается под абстрактным типом данных?
2. Что такое класс? Понятие, назначение, пример использования.
3. Охарактеризуйте назначение секций класса.
4. Понятие односторонней функции.
5. Понятие и алгоритмы ассиметричного шифрования. Реализация в контексте ООП.
6. Понятие криптографического протокола.
7. Система с открытым ключом Диффи-Хеллмана. Математическое обоснование. Примеры.
8. Шифр Шамира. Математическое обоснование. Примеры.
9. Шифр Эль-Гамаля. Математическое обоснование. Примеры.
10. Шифр RSA. Математическое обоснование. Примеры.
11. Основные принципы создания объектной модели (абстрагирование инкапсуляция модульность, иерархия, типизация, параллелизм, сохраняемость).
12. Экземпляры класса. Перечислите и охарактеризуйте уровни доступа к членам класса.