КОНТРОЛЬНАЯ РАБОТА

по курсу «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Задание №1. Шифр Цезаря.

Используя шифр Цезаря, зашифруйте свои данные: Фамилию Имя Отчество.

**Задание №2**. Алгоритм шифрования ГОСТ 28147-89.

Выполните первый цикл алгоритма шифрования ГОСТ 28147 89 в режиме простой замены. Для получения 64 бит исходного текста используйте 8 первых букв из своих данных: Фамилии Имени Отчества. Для получения ключа (256 бит) используют текст, состоящий из 32 букв. Фразу придумайте сами (не такую, как в примере). Первый подключ содержит первые 4 буквы.

**Задание №3**. Алгоритм шифрования RSA.

Сгенерируйте открытый и закрытый ключи в алгоритме шифрования RSA, выбрав простые числа p и q из первой сотни (не такие, как в примере). Зашифруйте сообщение, состоящее из ваших инициалов: ФИО.

**Задание №4**. Функция хеширования.

Найдите хеш-образ своей Фамилии, используя хеш-функцию

,где n = pq, p, q взять из Задания №3.

**Задание №5.** Электронная цифровая подпись.

Используя хеш-образ своей Фамилии, вычислите электронную цифровую подпись по схеме RSA.