***Задание 5***

**Задача №1. Алгоритмы замены**

Сообщение, зaписaнноe в алфавите АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯ зашифровывается при помощи последовательности букв этого же алфавита. Длина последовательности равна длине сообщения. Шифрование каждой буквы исходного сообщения состоит в сложении ее порядкового номера в алфавите c порядковым номером соответствующей буквы шифрующей последовательности и замене такой суммы на букву алфaвитa, порядковый номер которой имеет тот же остаток от деления на 30, что и эта сумма.

Восстановите два исходных сообщения, каждое из которых содержит слово КОРАБЛИ, если результат их зашифрования при ПОМОЩИ ОДНОЙ и той же шифрующей последовательности известен: ЮПТЦАРГШАЛЖЖЕВЦЩЫРВУУ и ЮПЯТБНЩМСДТЛЖГПСГХСЦЦ

**Задача №2. Алгоритм шифрования гост 28147-89.**

Выполните два цикла алгоритма шифрования ГОСТ 28147 89 в режиме простой замены. Для получения 28 бит исходного текста используйте 8 букв, начиная с 5 буквы, из своих данных: Фамилии Имени Отчества. Для получения ключа (256 бит) используют текст, состоящий из 24 букв. Первый подключ содержит последние 6 букв.

**Задача №3. Алгоритм шифрования rsa.**

Сгенерируйте открытый и закрытый ключи в алгоритме шифрования RSA, выбрав простые числа p и q из пятой сотни. Зашифруйте сообщение, состоящее из ваших инициалов: ФИО.

**Задача №4. Функция хеширования.**

Найти хеш–образ своей Фамилии, используя хеш–функцию HL=(HL-1+ML)2 , где n = pq.

**Задача №5. Электронная цифровая подпись.**

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