Вариант 9

Задание 1. Алгоритмы замены

Используя шифр простой замены одной буквы на соответствующую другую, ключ <оыблеякэщмчжьфхйвёстюършпизаднугц> , расшифруйте:

жмвм, июфм, стёяфмсн фцтяэхяч,
люем, сяейч бйейбйёйт,
еоч бяёмтн, птй ц тйэя вёяэхмч
стйг хое ёосвёяч вёяэхмр бйе!

Задание 2. Алгоритм шифрования гост 28147-89.

Выполните два цикла алгоритма шифрования ГОСТ 28147 89 в режиме простой замены. Для получения 32 бит исходного текста используйте 6 букв, начиная с 4 буквы, из своих данных: Фамилии Имени Отчества. Для получения ключа (256 бит) используют текст, состоящий из 50 символов. Первый подключ содержит 8 символов, начиная с десятого

Задание 3. Алгоритм шифрования rsa.

Сгенерируйте открытый и закрытый ключи в алгоритме шифрования RSA, используя простые числа p=277 и q=521. Зашифруйте сообщение, состоящее из вашей фамилии и инициалов.

Задание 4. Функция хеширования.

Найти хеш–образ своей Фамилии, используя хеш–функцию (выбрать свою) , где n = pq.

Задание 5. Электронная цифровая подпись

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