**Задания на контрольную работу**

**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. 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. Зашифруйте сообщение, состоящее из ваших инициалов: ФИО.

**Задание №4. Функция хеширования.**

Найти хеш–образ своей Фамилии, используя хеш–функцию Hi=(Hi-1+Mi) 2

, 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.

**1 вариант** – Пережогина Ольга Владимировна (была моя ошибка с отчеством)

**4 вариант** – Дубровин Дмитрий Евгеньевич

**Вариант№1**

**Задание №1. Шифр Цезаря**

Используя шифр Цезаря, зашифруйте свои данные: Пережогина Ольга Георгиевна.

Для шифрования будем пользоваться формулой Сi=(Рi+k) mod n. Мощность алфавита n=33. Выберем ключ шифрования k=3.

Алфавит с соответствующими номерами букв.

A-1; Б-2; В-3; Г-4; Д-5; Е-6; Ё-7; Ж-8; З-9; И-10; Й-11; К-12; Л-13; М-14; Н-15; О-16; П-17; Р-18; С-19; Т-20; У-21; Ф-22; Х-23; Ц-24; Ч-25; Ш-26; Щ-27; Ъ-28; Ы-29; Ь-30; Э-31; Ю-32; Я-33.

Таким образом сообщение “Пережогина Ольга Георгиевна” можно представить в виде:

(17;6;18;6;8;16;4;10;15;1; 16;13;30;4;1; 4;6;16;18;4;10;6;3;15;1)

Используя формулу шифрования Сi=(Рi+k) mod n зашифруем исходное сообщение

С1 = (Р1+k) mod 33 = (17 + 3) mod 33 = 20 (Т)

С2 = (Р2+k) mod 33 = (6 + 3) mod 33 = 9 (З)

С3 = (Р3+k) mod 33 = (18 + 3) mod 33 = 21 (У)

С4 = (Р4+k) mod 33 = (6 + 3) mod 33 = 9 (З)

С5 = (Р5+k) mod 33 = (8 + 3) mod 33 = 11 (Й)

С6 = (Р6+k) mod 33 = (16 + 3) mod 33 = 19 (С)

С7 = (Р7+k) mod 33 = (4 + 3) mod 33 = 7 (Ё)

С8 = (Р8+k) mod 33 = (10 + 3) mod 33 = 13 (Л)

С9 = (Р9+k) mod 33 = (15 + 3) mod 33 = 18 (Р)

С10 = (Р10+k) mod 33 = (1 + 3) mod 33 = 4 (Г)

С11 = (Р11+k) mod 33 = (16 + 3) mod 33 = 19 (С)

С12 = (Р12+k) mod 33 = (13 + 3) mod 33 = 16 (О)

С13 = (Р13+k) mod 33 = (30 + 3) mod 33 = 33 (Я)

С14 = (Р14+k) mod 33 = (4 + 3) mod 33 = 7 (Ё)

С15 = (Р15+k) mod 33 = (1 + 3) mod 33 = 4 (Г)

С16 = (Р16+k) mod 33 = (4 + 3) mod 33 = 7 (Ё)

С17 = (Р17+k) mod 33 = (6 + 3) mod 33 = 9 (З)

С18 = (Р18+k) mod 33 = (16 + 3) mod 33 = 19 (С)

С19 = (Р19+k) mod 33 = (18 + 3) mod 33 = 21 (У)

С20 = (Р20+k) mod 33 = (4 + 3) mod 33 = 7 (Ё)

С21 = (Р21+k) mod 33 = (10 + 3) mod 33 = 13 (Л)

С22 = (Р22+k) mod 33 = (6 + 3) mod 33 = 9 (З)

С23 = (Р23+k) mod 33 = (3 + 3) mod 33 = 6 (Е)

С24 = (Р24+k) mod 33 = (15 + 3) mod 33 = 18 (Р)

С25 = (Р25+k) mod 33 = (1 + 3) mod 33 = 4 (Г)

Сообщение, зашифрованное шифром Цезаря будет “ТЗУЗЙСЁЛРГ СОЯЁГ ЁЗСУЁЛЗЕРГ”

**Вариант №4**

**Задание №1. Функция хеширования.**

Найти хеш–образ своей фамилии, используя хеш–функцию Hi=(Hi-1+Mi) 2

Возьмем два простых числа *p*=3, *q*=11. Определим *n*=*p\*q*=3\*11=33. Вектор инициализации H0 выберем равным 8 (выбор – случайным образом). Слово “ДУБРОВИН” **м**ожно представить последовательностью чисел (5;21;2;18;16;3;10;15) по номерам букв в алфавите.

Таким образом:

*n*=33;

H0=8;

M1= 5 - Д;

M2=21 - У;

M3= 2 - Б;

M4=18 - Р;

M5=16 - О;

M6= 3 - В;

M7=10 - И;

M8=15 - Н.

Используя формулу H*i*=( H*i-1*+M*i*) 2 mod *n* получим хэш-образ сообщения:

H1=(H0+M1) 2 mod n= (8+5) 2 mod 33 = 169 mod 33=4

H2=(H1+M2) 2 mod n= (4+21) 2 mod 33 = 625 mod 33=31

H3=(H2+M3) 2 mod n= (31+2) 2 mod 33 = 33 mod 33=0

H4=(H3+M4) 2 mod n= (0+18) 2 mod 33 = 324 mod 33=27

H5=(H4+M5) 2 mod n= (27+16) 2 mod 33 = 100 mod 33=1

H6=(H5+M6) 2 mod n= (1+3) 2 mod 33 = 16 mod 33=16

H7=(H6+M7) 2 mod n= (16+10) 2 mod 33 = 676 mod 33=16

H8=(H7+M8) 2 mod n= (16+15) 2 mod 33 = 961 mod 33=4

Таким образом хеш-образом “ДУБРОВИН” будет значение 4.