**Задание No3. 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 No4. Функция хеширования.**

Найти хеш–образ своей Фамилии, используя хеш–функцию, где n = pq, p, q взять из Задания No3

**Задание No5. Электронная цифровая подпись.**

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

*Примеры решения:*

**Задание No3.** 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.

I.Генерация ключей (см. Приложение Г).Выберем два простых числа р= 13 и q= 19 (см. Приложение Д).

Тогда модуль n=pq=13\*19 = 247

и функция Эйлераϕ(n)=(p-1)(q-1)= 12\*18 = 216.

Закрытый ключ d выбираем из условий d<ϕ(n) и d взаимно просто с ϕ (n), т.е. d и ϕ(n)не имеют общих делителей.

Пусть d= 25.

Открытый ключ e выбираем из условий e < ϕ(n)

И de=1(mod ϕ(n)): e<216,25 e=1(mod 216).

Последнее условие означает, что число 25 e- 1 должно делиться на 216 без остатка.

Таким образом, для определения e нужно подобрать такое число k, что 25 e - 1 = 216k.

При k=14 получаем 25 e =3024+1 или e=121.

В нашем примере(121, 247) –открытый ключ,( 25, 247) –

секретный ключ.

II. Шифрование.

Представим шифруемое сообщение «КГЛ» как последовательность целых чисел. Пусть буква «К» соответствует числу 12, буква «Г» - числу 4 и буква

«Л» -числу 13.

Зашифруем сообщение, используя открытый ключ (121, 247):С1 = () mod 247= 12

С2= () mod 247=199

С3= () mod 247= 91

Таким образом, исходному сообщению (12, 4, 13) соответствует криптограмма (12, 199, 91).

III. Расшифрование

Расшифруем сообщение (12, 199, 91), пользуясь секретным ключом (25,247):М1= () mod 247=12

М2= () mod 247= 4

МЗ= () mod 247=13

В результате расшифрования было получено исходное сообщение (12, 4, 13), то есть "КГЛ".

**Задание No4**. Функция хеширования.

Найти хеш–образ своей Фамилии, используя хеш–функцию, где n = pq, p, q взять из Задания No3.

Хешируемое сообщение «КОЗИНА». Возьмем два простых числа p=13,q=19

Определим n=pq=13\*19=247. Вектор

Инициализации выберем равным 8 (выбираем случайным образом). Слово «КОЗИНА» можно представить последовательностью чисел (12, 16, 9, 10,

15, 1) по номерам букв в алфавите. Таким о

бразом,

n=247, H0=8, M1=12, M2=16, M3=9, M4=10, M5=15, M6=1.

Используя формулу,получим хеш-образ сообщения «КОЗИНА»:

H1=(H0+M1)2mod n =( 8 + 12)2mod247 =400 mod 247=153

H2=(H1+M2)2mod n =(153 + 16)2mod247 = 28561mod 247=156

H3=(H2+M3)2mod n =(156 + 9)2mod247 = 27225mod 247=55

H4=(H3+M4)2mod n =( 55 + 10)2mod247 = 4225mod 247=26

H5=(H4+M5)2mod n =( 26 + 15)2mod247 = 1681mod 247=199

H6=(H5+M6)2mod n =(199 + 1)2mod247 = 40000mod 247=233

В итоге получаем хеш-образ сообщения «КОЗИНА», равный 233

**Задание No5**. Электронная цифровая подпись.

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

Пусть хеш-образ Фамилии равен 233, а закрытый ключ алгоритма RSA равен (25, 247). Тогда электронная цифровая подпись сообщения, состоящего из

Фамилии, вычисляется по правилу

s= 23325mod 247 = 168.

Для проверки ЭЦП, используя открытый ключ (121, 247), найдем

H = 168121mod 247 = 233.

Поскольку хеш-образ сообщения совпадает с найденным значением H, то подпись признается подлинной.