**Алгоритм шифрования RSA**

1. **Генерация ключей**

Выберем два простых числа p = 61 и q = 103

Тогда модуль n = p\*q = 6283

Вычислим функцию Эйлера:

ϕ(n) = (p - 1)(q - 1) = 60 \* 102 = 6120

Закрытый ключ d: d < ϕ(n) и d взаимно просто с ϕ(n).

Пусть d = 121.

Открытый ключ e: e < ϕ(n) и d\*e=1(mod ϕ(n)):

e < 6120

121e=1(mod 6120).

121e-1=6120k.

При k=19 получаем 121e = 116280

e=961.

В итоге

(961, 6283) - открытый ключ

(121, 6283) - секретный ключ.

1. **Шифрование**

Представим шифруемое сообщение «ДИЕ» как последовательность целых

чисел:

Д – 5

И – 10

Е – 6

С1 = (5961)mod 6283 = 5068

С2 = (10961)mod 6283 = 1840

С3 = (6961)mod 6283 = 2019

Исходному сообщению (5, 10, 6) соответствует криптограмма (5068, 1840, 2019)

1. **Расшифрование**

M1 = (5068121)mod 6283 = 5

M2 = (1840121)mod 6283 = 10

M3 = (2019121)mod 6283 = 6

В результате расшифрования было получено исходное сообщение (5, 10, 6), то есть "ДИЕ".

**Функция хеширования**

p = 61, q = 103

n = p \* q = 6283

Выберем случайно H0 = 24

Хешируемое сообщение: «ДАКУКИН».

Д А К У К И Н

5 1 12 21 12 10 15

Таким образом:

n = 6283, H0 = 24, M1 = 5, M2 = 1, M3 = 12, M4 = 21, M5 = 12, M6 = 10, M7 = 15

Используя формулу:

Hi = (Hi-1 + Mi)2 mod n,

Получим хеш-образ сообщения «ДАКУКИН»:

Н1 = (Н0 + М1)2 mod n = (24 + 5)2 mod 6283 = 841

Н2 = (Н1 + М2)2 mod n = (841 + 1)2 mod 6283 = 5268

Н3 = (Н2 + М3)2 mod n = (5268 + 12)2 mod 6283 = 729

Н4 = (Н3 + М4)2 mod n = (729 + 21)2 mod 6283 = 3313

Н5 = (Н4 + М5)2 mod n = (3313 + 12)2 mod 6283 = 3828

Н6 = (Н5 + М6)2 mod n = (3828 + 10)2 mod 6283 = 2892

Н7 = (Н6 + М7)2 mod n = (2892 + 15)2 mod 6283 = 14

В итоге получаем хеш-образ сообщения «ДАКУКИН», равный 14.

**Электронная цифровая подпись**

Хеш-образ фамилии равен 14, а закрытый ключ алгоритма RSA равен (121, 6283). Тогда электронная цифровая подпись сообщения, состоящего из фамилии, вычисляется по правилу:

s = 14121mod 6283 = 1844

Для проверки ЭЦП, используя открытый ключ (961, 6283), найдем:

H = 1844961mod 6283 = 14

Поскольку хеш-образ сообщения совпадает с найденным значением Н, подпись признаётся подлинной.