Криптосистема RSA

Задача 1.

Предположим, вы хотите отправить зашифрованное по RSA. Даны следующие параметры:

1. Простые числа $p = 101$, $q = 113$.
2. Открытая экспонента $e = 7$.
3. Сообщение, которое нужно зашифровать: $m = 567$.

Найти:

1. Найдите модуль n и функцию Эйлера $\varphi(n)$.
2. Зашифруйте сообщение m и найдите зашифрованное сообщение c.

Решение 1.

1. $n = pq = 101 \cdot 113 = 11413$

   $\varphi(n) = (p-1)(q-1) = 100 \cdot 112 = 11200$

2. $c = m^e = 567^7 = 3292$

Задача 2.

В криптосистеме RSA известны следующие данные:

1. $p = 89,\ q = 97$.
2. Открытая экспонента $e = 5$.
3. Зашифрованное сообщение: $c = 2789$.

Найти:

1. Найдите секретный ключ d, используя информацию о p и q.
2. Расшифруйте сообщение c и определите исходное значение m.

Решение 2. Найдем n и $\varphi(n)$: $n = pq = 89 \cdot 97 = 8633$ и $\varphi(n) = (p-1)(q-1) = 88 \cdot 96 = 8448$

1. Найдем $d = e^{-1} \mod \varphi(n)$:

$$ed = 1 \pmod{8448}$$

$$5d = 1 \pmod{8448}$$

$$5d = 25345 \pmod{8448}$$

$$d = 5069 \pmod{8448}$$

2. Расшифруем сообщение c:

$$m = c^d = 2789^{5069} = 6605$$