Расшифрование RSA по китайской теореме об остатках

Аметов Имиль, гр. M07-903

24 мая 2020 г.

Задача:

Расшифровать сообщение $c = 251$ для $p = 67$, $q = 31$ и $d = 463$ зашифрованное с помощью RSA. При расшифровании использовать китайскую теорему об остатках.

Решение:

Находим $n = p \cdot q = 67 \cdot 31 = 2077$.

Находим $m_p = c^{d \mod (p-1)} \mod p = 251^{463 \mod 66} \mod 67 = 251^{1} \mod 67 = 50$.

Находим $m_q = c^{d \mod (q-1)} \mod q = 251^{463 \mod 30} \mod 31 = 251^{13} \mod 31 = 24$.

Вычисляем открытое сообщение m по формуле:

$$m = m_p \cdot q \cdot (q^{-1} \mod p) + m_q \cdot p \cdot (p^{-1} \mod q) \mod n.$$

Получаем:

$$m = 50 \cdot 31 \cdot (31^{-1} \mod 67) + 24 \cdot 67 \cdot (67^{-1} \mod 31) \mod 2077 =$$

$$= 1550 \cdot (13 \mod 67) + 1608 \cdot (25 \mod 31) \mod 2077 =$$

$$= 1550 \cdot 13 + 1608 \cdot 25 \mod 2077 =$$

$$= 20150 + 40200 \mod 2077 = 60350 \mod 2077 = 117.$$

Ответ: $m = 117$.