

Solutions to RSA Exercise

a) $n = 13 \cdot 19$

b) $\phi = 12 \cdot 18 = 216$

c)

$$216 = 6(31) + 30$$

$$31 = 1(30) + 1$$

Now working backwards:

$$1 = 31 - 1(30)$$

$$= 31 - 1(216 - 6(31))$$

$$= 7(31) - 1(216)$$

We have found the private decryption key $d = 7$.

d)

$$45^2 \equiv 49 \pmod{247}, 45^4 \equiv 178 \pmod{247}$$

$$\Rightarrow 45^7 \equiv 178 \cdot 49 \cdot 45 \pmod{247} \equiv 7 \pmod{247}.$$

$$199^2 \equiv 81 \pmod{247}, 199^4 \equiv 139 \pmod{247}$$

$$\Rightarrow 199^7 \equiv 139 \cdot 81 \cdot 199 \pmod{247} \equiv 4 \pmod{247}.$$

$$106^2 \equiv 121 \pmod{247}, 106^4 \equiv 68 \pmod{247}$$

$$\Rightarrow 106^7 \equiv 68 \cdot 121 \cdot 106 \pmod{247} \equiv 11 \pmod{247}.$$

$$219^2 \equiv 43 \pmod{247}, 219^4 \equiv 120 \pmod{247}$$

$$\Rightarrow 219^7 \equiv 120 \cdot 43 \cdot 219 \pmod{247} \equiv 15 \pmod{247}.$$

The original message was 007 004 011 015.

e) The plaintext of the message is HELP. Note that in practice the public exponent e is usually chosen so that d is much larger than e .