

6) Routine calculation

7) Let  $x = \gcd(a, b) = ua + vb$  with  $u, v \in \mathbb{Z}$

$$\text{Then } g^x \equiv g^{ua+vb} \equiv (g^a)^u (g^b)^v$$

$$\equiv 1^u \cdot 1^v \equiv 1 \pmod{m}$$

8) No, because we don't know that 16 is the smallest such number. (In fact

$$4^4 \equiv 1 \pmod{17}.)$$

$$9) 2^{1643} \equiv 1558 \pmod{1643}.$$

↑  
Routine calc

If 1643 was prime, by Fermat's Little Thm. this would have to be  $\equiv 2$ , so 1643 cannot be prime.

b) Calculations are routine.

This does not imply that 561 is prime, because Fermat's Little Theorem is necessary, but not sufficient. (Numbers (such as 561) that fulfill the condition of the theorem but are not prime are called Carmichael-Numbers)

10) Calculate  $g = \text{gcd}(m_1, m_2)$ . The messages are  $m_1/g$  and  $m_2/g$ .

11) See solution Link on web pages.