

Problem 7): We start with $a^{\phi(N)} = 1 \pmod{N}$ and note $\phi(N) = \phi(p) \phi(q)$ to obtain

$$a^{\phi(N)} = 1 \pmod{N} = a^{\phi(p) \phi(q)}$$

Since $\phi(p) = p - 1$ and $\phi(q) = q - 1$, the previous result is equivalent to

$$\begin{aligned} a^{\phi(N)} &= 1 \pmod{N} = a^{\phi(p) \phi(q)} \\ &= 1 \pmod{N} = a^{(p-1)(q-1)} \end{aligned}$$

$a^{p-1} = 1 \pmod{p}$, and $a^{q-1} = 1 \pmod{q}$