Problem 6): We begin by applying the function mapping $\mathbb{Z}_N$ to $\mathbb{Z}_p \times \mathbb{Z}_q$ (denoted f) to $(x^e)^d$. This gives us

$$\begin{aligned} f\left((x^e)^d\right) &= \left(\left[\left(x_p^e\right)^d \mod p\right], \left[\left(x_q^e\right)^d \mod q\right]\right) \\ &= \left(\left[\left(x_p^{e\,d}\right) \mod p\right], \left[\left(x_q^{e\,d}\right) \mod q\right]\right) \end{aligned}$$

We now substitute $ed = 1 \mod \phi(N)$ into our previous result to obtain

$$\begin{aligned} f\left((x^e)^d\right) &= \left(\left[\left(x_p^{e\,d}\right) \mod p\right], \left[\left(x_q^{e\,d}\right) \mod q\right]\right) \\ &= \left(\left[\left(x_p^{1 \mod \phi(N)}\right) \mod p\right], \left[\left(x_q^{1 \mod \phi(N)}\right) \mod q\right]\right) \end{aligned}$$

Using the definition of $\phi(\cdots)$ as well as the fact that $N = pq$, where p and q are distinct primes, we note that $\phi(N) = \phi(p)\ \phi(q)$. Therefore, our previous result can be rewritten as

$$\begin{aligned} f\left((x^e)^d\right) &= \left(\left[\left(x_p^{1 \mod \phi(N)}\right) \mod p\right], \left[\left(x_q^{1 \mod \phi(N)}\right) \mod q\right]\right) \\ &= \left(\left[\left(x_p^{1 \mod \phi(p)\,\phi(q)}\right) \mod p\right], \left[\left(x_q^{1 \mod \phi(p)\,\phi(q)}\right) \mod q\right]\right) \end{aligned} \tag{6.1}$$

Using the relation $a^{\phi(N)} = 1 \mod N$, we see that $\phi(q)$ will cancel from the exponent in the first part of the left-hand-term in 6.1. Similarly, $\phi(q)$ will also cancel from the second part of the left-hand-term in 6.1. Therefore, our expression in 6.1 can be simplified to give

$$\begin{aligned} f\left((x^e)^d\right) &= \left(\left[\left(x_p^{1 \mod \phi(p)\,\phi(q)}\right) \mod p\right], \left[\left(x_q^{1 \mod \phi(p)\,\phi(q)}\right) \mod q\right]\right) \\ &= \left(\left[\left(x_p^{1 \mod \phi(q)}\right) \mod p\right], \left[\left(q^{1 \mod \phi(p)}\right) \mod q\right]\right) \end{aligned}$$

Noting that $b \mod p = [b \mod c] \mod c$, we modify our previous result to give

$$
\begin{aligned}
f\left((x^e)^d\right) &= \left(\left[\left(x_p^{1 \mod \phi(q)}\right) \mod p\right], \left[\left(x_q^{1 \mod \phi(p)}\right) \mod q\right]\right) \\
&= \left(\left[\left(\left(x_p^{1 \mod \phi(q)}\right) \mod p\right) \mod p\right], \left[\left(\left(x_q^{1 \mod \phi(p)}\right) \mod q\right) \mod q\right]\right)
\end{aligned}
$$

Again using the relation $a^{\phi(N)} = 1 \mod N$, we are able to simplify our previous result as

$$
\begin{aligned}
f\left((x^e)^d\right) &= \left(\left[\left(\left(x^{1 \mod \phi(q)}\right) \mod p\right) \mod p\right], \left[\left(\left(x^{1 \mod \phi(p)}\right) \mod q\right) \mod q\right]\right) \\
&= \left(\left[(x_p \mod (pq)) \mod p\right], \left[(x_q \mod (qp)) \mod q\right]\right) \qquad (6.2)
\end{aligned}
$$

Finally, we note that $pq = qp = N$ and recall the definition of $f(\cdots)$. These relations allow us to rewrite our result in expression 6.2 to give

$$
\begin{aligned}
f\left((x^e)^d\right) &= \left(\left[(x_p \mod (pq)) \mod p\right], \left[(x_q \mod (qp)) \mod q\right]\right) \\
&= \left(\left[(x_p \mod N) \mod p\right], \left[(x_q \mod N) \mod q\right]\right) \\
&= f(x \mod N)
\end{aligned}
$$

We then take the inverse of $f(\cdots)$ to ultimately give

$$
f\left((x^e)^d\right) = f(x \mod N) \implies (x^e)^d = x \mod N
$$

as desired.

□