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

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

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

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

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

$$f\left(\left(x^{e}\right)^{d}\right) = \left(\left[\left(x_{p}^{1 \mod \phi(N)}\right) \mod p\right], \left[\left(x_{q}^{1 \mod \phi(N)}\right) \mod q\right]\right)$$

$$= \left(\left[\left(x_{p}^{1 \mod \phi(p) \phi(q)}\right) \mod p\right], \left[\left(x_{q}^{1 \mod \phi(p) \phi(q)}\right) \mod q\right]\right) \tag{6.1}$$

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

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

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

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

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

$$f\left(\left(x^{e}\right)^{d}\right) = \left(\left[\left(\left(x^{1 \mod \phi(q)}\right) \mod p\right) \mod p\right], \left[\left(\left(x^{1 \mod \phi(p)}\right) \mod q\right) \mod q\right]\right)$$

$$= \left(\left[\left(x_{p} \mod (pq)\right) \mod p\right], \left[\left(x_{q} \mod (qp)\right) \mod q\right]\right) \tag{6.2}$$

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

$$f\left(\left(x^{e}\right)^{d}\right) = (\left[\left(x_{p} \mod (pq)\right) \mod p\right], \left[\left(x_{q} \mod (qp)\right) \mod q\right])$$
$$= (\left[\left(x_{p} \mod N\right) \mod p\right], \left[\left(x_{q} \mod N\right) \mod q\right])$$
$$= f\left(x \mod N\right)$$

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

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

as desired.