Exercise 1

Show that for any $x \in \mathbb{Z}_n$, we have $D_{n,d}(E_{n,e}(x)) \equiv x \pmod{n}$.

Solution: Let $x \in \mathbb{Z}_n$. Then, as per the RSA specification, we have

$$ed \equiv 1 \pmod{\varphi(n)}.$$

So:

$$\phi(n) | ed - 1.$$

And there exists $k \in \mathbb{Z}$ so that:

$$k\phi(n) = ed - 1,$$

$$k\phi(n) + 1 = ed.$$

By Fermat's little theorem (or Lagrange theorem if you like),

$$\begin{aligned} x^{p-1} &\equiv 1 \pmod{p}, & x^{q-1} &\equiv 1 \pmod{q} \\ x^{(p-1)(q-1)} &\equiv 1 \pmod{p}, & x^{(p-1)(q-1)} &\equiv 1 \pmod{q} \\ x^{k\varphi(n)} &\equiv 1 \pmod{p}, & x^{k\varphi(n)} &\equiv 1 \pmod{q} \\ x^{k\varphi(n)+1} &\equiv 1 \pmod{p}, & x^{k\varphi(n)+1} &\equiv 1 \pmod{q} \\ x^{ed} &\equiv x \pmod{p}, & x^{ed} &\equiv x \pmod{q}. \end{aligned}$$

Then by the Chinese remainder theorem, we must have

$$x^{ed} \equiv x \pmod{pq}.$$