

Chapter 6 #9

a)

Since $n = pq$, p and q prime, $\Phi(n) = \Phi(p)\Phi(q)$, $\gcd(x, n) = 1$.

Thus, we can rewrite $x^{(1/2)\Phi(n)}$ as $x^{(1/2)\Phi(p)\Phi(q)}$

Since $\gcd(x, pq) = 1$, we know that $\gcd(x, p) = 1$ and $\gcd(x, q) = 1$. Furthermore, any power of x will be relatively prime to p and q .

Thus, using Euler's Theorem, we can say that $(x^{(1/2)\Phi(p)})^{\Phi(q)} \equiv 1 \pmod{q}$ and $(x^{(1/2)\Phi(q)})^{\Phi(p)} \equiv 1 \pmod{p}$

Thus $x^{(1/2)\Phi(n)} \equiv 1 \pmod{p}$ and $x^{(1/2)\Phi(n)} \equiv 1 \pmod{q}$

b)

Since p and q are relatively prime, the fact that $x^{(1/2)\Phi(n)} \equiv 1 \pmod{p}$ and $x^{(1/2)\Phi(n)} \equiv 1 \pmod{q}$

means that $x^{(1/2)\Phi(n)} \equiv 1 \pmod{pq = n}$ by the Chinese Remainder Theorem.

c)

Suppose $ed \equiv 1 \pmod{(1/2)\Phi(n)}$

Then $(1/2)\Phi(n) \mid (ed - 1)$, so can write $ed - 1 = k((1/2)\Phi(n))$ for some positive integer k .

Thus $x^{ed - 1} \equiv x^{((1/2)\Phi(n))k} \equiv 1^k \equiv 1 \pmod{n}$.

Thus $x^{ed} \equiv x \pmod{n}$. We conclude that we could choose our deciphering key to the modulus $(1/2)\Phi(n)$ instead of $\Phi(n)$.