

2. Suppose your RSA modulus is 55, $e = 3$. Note that $\varphi(55) = \varphi(5)\varphi(11) = 4 * 10 = 40$.
- a) The encryption modulus d must have the property that $d * e \equiv 1 \pmod{40}$. Given that $e = 3$, we quickly see that $d=27$ is a solution; since $27 * 3 = 81$
- b) Now, assuming $\gcd(m, 55) = 1$ for some message m we want to show that if c is the cipher text, then $m \equiv c^{27} \pmod{55}$ is the plain text. Notice, since $27 * 3 \equiv 1 \pmod{40}$ we have that $d * e = 1 + 2 * 40$. Thus, $c^{27} \equiv (m^3)^{27} \pmod{55}$ and $(m^3)^{27} \equiv m^{(1+80)} \equiv m * (m^{80}) \equiv m * (m^{40})^2 \equiv m * 1^2 \equiv m \pmod{55}$. Notice, that $m^{40} \equiv 1 \pmod{55}$ by Eulers theorem since $\gcd(m, 55) = 1$ implies that $m^{40} \equiv 1 \pmod{55}$.