Student Number: [redacted] Name: Bryan Hoang

7. (10 points)

(a) **Answer:**
With $\gcd(c, N) = 1$, then the formula in Exercise 3.4(c) says that

$$c^{\phi(N)} \equiv 1 \pmod{N}. \tag{1}$$

Taking both sides of the congruence to the power of ϕN yields

$$\begin{aligned}\left(x^e\right)^{\phi(N)} &\equiv c^{\phi(N)} \pmod{N} \\ \left(x^e\right)^{\phi(N)} &\equiv 1 \pmod{N}.\end{aligned}$$

To have the LHS satisfy the formula in Exercise 3.4(c), let $d \equiv e^{-1} \pmod{\phi N}$. Then it is sufficient to find $x = c^d$.

(b)

(i) **Answer:**
To solve $x^{577} \equiv 60 \pmod{1463}$, we first note that $N = 7 \cdot 11 \cdot 19$. By the formula in Exercise 3.5(d),

$$\begin{aligned}\phi(1463) &= 1463\left(1 - \frac{1}{7}\right)\left(1 - \frac{1}{11}\right)\left(1 - \frac{1}{19}\right) \\ &= 1080.\end{aligned}$$

Then $d \equiv 577^{-1} \equiv 73 \pmod{1080}$. Therefore,

$$\boxed{x = 60^{73} \equiv 1390 \pmod{1463}}.$$

(ii) **Answer:**
To solve $x^{959} \equiv 1583 \pmod{1625}$, we first note that $N = 5^3 \cdot 13$. By the formula in Exercise 3.5(d),

$$\begin{aligned}\phi(1625) &= 1625\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{13}\right) \\ &= 1200.\end{aligned}$$

Then $d \equiv 959^{-1} \equiv 239 \pmod{1200}$. Therefore,

$$\boxed{x = 1583^{239} \equiv 147 \pmod{1625}}.$$

(iii) **Answer:**
To solve $x^{133957} \equiv 224689 \pmod{2134440}$, we first note that $N = 2^3 \cdot 3^2 \cdot 5 \cdot 7^2 \cdot 11^2$. By the formula in Exercise 3.5(d),

$$\begin{aligned}\phi(2134440) &= 2134440\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{7}\right)\left(1 - \frac{1}{11}\right) \\ &= 443520.\end{aligned}$$

Then $d \equiv 133957^{-1} \equiv 326413 \pmod{443520}$. Therefore,

$$\boxed{x = 224689^{326413} \equiv 1892929 \pmod{2134440}}.$$