1. Solve for x

$$(a)\quad \begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 4 \end{cases} \qquad (b)\quad \begin{cases} x \equiv 0 \pmod 4 \\ x \equiv 3 \pmod 7 \end{cases}$$

$$(c)\quad \begin{cases} x \equiv 10 \pmod{12} \\ x \equiv 3 \pmod 5 \end{cases} \qquad (d)\quad \begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 5 \pmod 6 \end{cases}$$

2. Solve for x

$$(a)\quad \begin{cases} x \equiv 0 \pmod 2 \\ x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \end{cases} \qquad (b)\quad \begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 5 \pmod 7 \end{cases}$$

3. Modified RSA signature scheme. First, let's recall the regular RSA signatures.

   (a) Alice selects sufficiently large primes p and q and calculates $n = pq$.

   (b) Alice selects her public exponent $e \in \mathbb{Z}^{\times}_{\varphi(n)}$.

   (c) Alice calculates her private exponent $d \in \mathbb{Z}^{\times}_{\varphi(n)}$ such that $d \cdot e \equiv 1 \pmod{\varphi(n)}$.

   (d) Alice publishes her public key (e, n) to the key server, and keeps her private key (d, n) to herself.

   (e) To sign a document $\hat{d}$, Alice takes a hash of it $m = H(\hat{d}) \in \mathbb{Z}_n$.

   (f) The signature of Alice is $m^d \bmod n$, she distributes it together with the document.

   (g) To verify the signature, Bob downloads Alice's public key (e, n) and computes

$$\Big(m^d \bmod n\Big)^e \bmod n = m^{de} \bmod n = m \ .$$

   If $m = H(\hat{d})$, the signature is valid.

   Now consider a modification to this scheme. Assume we do not need CRT to combine elements in $\mathbb{Z}^{\times}_p$ and $\mathbb{Z}^{\times}_q$ into one structure $\mathbb{Z}^{\times}_{pq}$. Instead, let's just work in one ring $\mathbb{Z}^{\times}_n$, where n is sufficiently large prime. The modified scheme works as follows.

   (a) Alice selects a sufficiently large prime n and selects her public exponent $e \in \mathbb{Z}^{\times}_{\varphi(n)}$.

   (b) Alice calculates her private exponent $d \in \mathbb{Z}^{\times}_{\varphi(n)}$ such that $d \cdot e \equiv 1 \pmod{\varphi(n)}$.

   (c) Alice publishes her public key (e, n) to the key server and keeps her private key (d, n) to herself. To sign a document $\hat{d}$, Alice takes a hash of it $m = H(\hat{d}) \in \mathbb{Z}_n$.

   (d) The signature of Alice is $m^d \bmod n$, she distributes it together with the document.

   (e) To verify the signature, Bob downloads Alice's public key (e, n) and computes

$$\Big(m^d \bmod n\Big)^e \bmod n = m^{de} \bmod n = m \ .$$

   If $m = H(\hat{d})$, the signature is valid.

This scheme is not secure against passive adversary Carol. It turns out that Carol can obtain Alice's private key from her public key (e, n) and only just one sample of her signature $m^d \bmod n$. This will allow Carol to make as many fake signatures on behalf of Alice as she wants with Alice being completely unaware of it. How can Carol obtain Alice's private key (d, n)?

4. Alice sends the same message $m = 10$ encrypted using the RSA algorithm to three different people with public keys $(n = 87, e = 3), (n = 115, e = 3), (n = 187, e = 3)$. Adversary Eve recovers three cryptograms $c_1 = 43, c_2 = 80, c_3 = 65$ and knows the public keys (n_i, e_i) of all the recipients. Can Eve recover the message without factoring the moduli?