Assignment-5
Due date: 26th March, 2022

Let's explore why in the RSA trapdoor permutation every party has to be assigned a different modulus $\mathbf{n = pq}$. Suppose we try to use the same modulus $\mathbf{n = pq}$ for everyone. Every party is assigned a public exponent $\mathbf{e_i \in Z}$ and a private exponent $\mathbf{d_i \in Z}$ such that $\mathbf{e_i \cdot d_i = 1 \bmod \phi(n)}$. At first this appears to work fine: to sign a message $\mathbf{m \in M}$, Alice would publish the signature $\boldsymbol{\sigma_a} \leftarrow \mathbf{H(m)^{da} \in Z_n}$ where $\mathbf{H : M \to Z^*_n}$ is a hash function. Similarly, Bob would publish the signature $\boldsymbol{\sigma_b} \leftarrow \mathbf{H(m)^{db} \in Z_n}$. Since Alice is the only one who knows $\mathbf{d_a \in Z}$ and Bob is the only one who knows $\mathbf{d_b \in Z}$, this seems fine. Let's show that this is completely insecure: Bob can use his secret key $\mathbf{d_b}$ to sign messages on behalf of Alice.

(1) Show that Bob can use his public-private key pair $\mathbf{(e_b, d_b)}$ to obtain a multiple of $\boldsymbol{\phi}\mathbf{(n)}$. Let us denote that integer by $\mathbf{V}$.

(2) Now, suppose Bob knows Alice's public key $\mathbf{e_a}$. Show that for any message $\mathbf{m \in M}$, Bob can compute $\boldsymbol{\sigma} \leftarrow \mathbf{H(m)^{1/ea} \in Z_n}$. In other words, Bob can invert Alice's trapdoor permutation and obtain her signature on $\mathbf{m}$. Hint: First, suppose $\mathbf{e_a}$ is relatively prime to $\mathbf{V}$. Then Bob can find an integer $\mathbf{d}$ such that $\mathbf{d \cdot e_a = 1 \bmod V}$. Show that $\mathbf{d}$ can be used to efficiently compute $\boldsymbol{\sigma}$.

(3) Next, show how to make your algorithm work even if $\mathbf{e_a}$ is not relatively prime to $\mathbf{V}$.