CSE 5351 Homework 8

Due: Wednesday, April 22 by class time

1. Describe the encryption key space of RSA? What is its cardinality? Answer the same questions for the decryption key space.

2. Compute $101^{4,800,000,023} \bmod 35$ (without using a calculator).

3. Test if 769 is a prime using the Miller-Rabin algorithm, with $t = 3,\ a = 3, 5, 7$.

4. Suppose three users have public keys (N_1, 3), (N_2, 3), (N_3, 3) (i.e., they all have e=3)), with $N_1 < N_2 < N_3$. Consider the following method for sending the same message $m \in \{0,1\}^\ell$ to these users: choose $r \leftarrow \mathbb{Z}^*_{N_1}$ and send to everyone the same ciphertext

$$\left\langle r^3 \bmod N_1,\ r^3 \bmod N_2,\ r^3 \bmod N_3,\ H(r) \oplus m \right\rangle$$

where $H : \mathbb{Z}^*_{N_1} \to \{0,1\}^\ell$ is a collision-resistant hash function. Assume $\ell \gg n = \|N_3\|$.

(a) Show that this method is not secure --- an adversary can recover m from the ciphertext.

(b) Show a simple way to fix this using a ciphertext of length $3\ell + O(n)$.

(c) Show a better approach that is CPA-secure but with a ciphertext of length $\ell + O(n)$. Assume H is modeled as a random oracle.

In (b) and (c), just show the modified methods; you don't need to *prove* the security.