EE 720: Introduction to Number Theory and Cryptography (Autumn 2025)
Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay

Assignment 4: 20 points Date: October 21, 2025

1. [5 points] Suppose an RSA encryption scheme has public key $\langle N, e \rangle = \langle 2537, 13 \rangle$. Find the decryption exponent d.

2. [5 points] Suppose the GenRSA algorithm is used to generate two encryption-decryption exponent pairs (e_1, d_1) and (e_2, d_2) for the same modulus N, where we have $e_1 \neq e_2$ and $\gcd(e_1, e_2) = 1$. Also, suppose the same message $m \in \mathbb{Z}_N^*$ is encrypted via plain RSA using both the exponents to get ciphertexts c_1, c_2 given by

$$c_1 = m^{e_1} \bmod N,$$
$$c_2 = m^{e_2} \bmod N.$$

   Show how a PPT adversary can recover m from c_1, c_2 using the public information N, e_1, e_2.

3. [5 points] An element $x \in \mathbb{Z}_N^*$ which satisfies $x^{N-1} \neq 1 \bmod N$ is said to be a *witness* that N is composite.

   For a given N, suppose there exists a witness that N is composite. Prove that at least half the elements of $\mathbb{Z}_N^*$ are witnesses that N is composite.

4. [5 points] For an odd integer N, let $N - 1 = 2^r u$ where u is odd and $r \geq 1$. An integer $x \in \mathbb{Z}_N^*$ is said to be a *strong witness* that N is composite if

   (i) $x^u \neq 1 \bmod N$ and

   (ii) $x^{2^i u} \neq -1 \bmod N$ for all $i \in \{0, 1, 2, \ldots, r-1\}$.

   If $x \in \mathbb{Z}_N^*$ is a witness, prove that it is also a strong witness. The definition of a witness is given in question 1.