EE 720: Introduction to Number Theory and Cryptography (Autumn 2023)
Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay

Quiz 3: 20 points Date: November 8, 2023

---

1. [5 points] Suppose an RSA encryption scheme has public key $\langle N, e \rangle = \langle 2537, 13 \rangle$. Find the decryption exponent d. Show your steps (to convince me that you did not eavesdrop the solution). *Hint:* $2537 = 43 \times 59$.

2. [5 points] Prove that the El Gamal encryption scheme is not CCA-secure.

3. [5 points] Consider a padded RSA signature scheme where the public key is $\langle N, e \rangle$ and private key is $\langle N, d \rangle$. The modulus N is the product of two n-bit primes. For $1 \leq l < 2n - 1$, the signature on a message $m \in \{0,1\}^l$ is computed by choosing uniform $r \in \{0,1\}^{2n-l-1}$ and outputting $\left[(r \| m)^d \bmod N\right]$.

   (a) How can verification be done in this scheme?

   (b) Show that this scheme is insecure.

4. [5 points] For prime $p > 2$ and $x \in \mathbb{Z}_p^*$, the Jacobi symbol of x modulo p is given by

$$\mathcal{J}_p(x) = \begin{cases} +1 & \text{if } x \in \mathcal{QR}_p, \\ -1 & \text{if } x \in \mathcal{QNR}_p. \end{cases}$$

   In the above definition, the sets $\mathcal{QR}_p$ and $\mathcal{QNR}_p$ correspond to quadratic residues and quadratic non-residues modulo p, respectively. Prove that

$$\mathcal{J}_p(x) = x^{\frac{p-1}{2}} \bmod p.$$