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

Quiz 2: 20 points — Date: October 30, 2025

1. [5 points] Let a, b be positive integers. Prove the following statements.
   - There exist integers X, Y such that $Xa + Yb = \gcd(a, b)$.
   - $\gcd(a, b)$ is the smallest positive integer that can be expressed as an integer linear combination of a and b.

2. Let G be a finite group. Let H be a subgroup of G. For $g \in G$, the set $H + g = \{h + g \mid h \in H\}$ is called a right coset of H. Prove the following.
   (a) [3 points] Two right cosets of H are either disjoint or equal.
   (b) [2 points] All right cosets of H have the same size.

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] Prove that the Diffie-Hellman key exchange protocol is secure in the presence of an eavesdropper if the decisional Diffie-Hellman problem is hard relative to a cyclic group generation algorithm $\mathcal{G}$.

   Note: The key-exchange experiment $\mathsf{KE}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n)$:

   - Two parties holding 1^n execute protocol Π. This results in a
     - transcript trans containing all the messages sent by the parties, and
     - a key k output by each of the parties which belongs to some set $\mathcal{K}$.
   - A uniform bit $b \in \{0, 1\}$ is chosen.
     - If $b = 0$, set $\hat{k} := k$
     - If $b = 1$, then choose uniform $\hat{k} \in \mathcal{K}$.
   - $\mathcal{A}$ is given trans and $\hat{k}$, and outputs a bit b'
   - The output of the experiment is defined to be 1 if $b = b'$, and other 0 otherwise.

   Note: A key-exchange protocol Π is **secure in the presence of an eavesdropper** if for all PPT adversaries $\mathcal{A}$ there is a negligible function negl such that

   $$\Pr\left[\mathsf{KE}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n) = 1\right] \leq \frac{1}{2} + \mathsf{negl}(n).$$

   Note: Let $\mathcal{G}$ denote a polynomial-time, cyclic group generation algorithm. Run $\mathcal{G}(1^n)$ to obtain (G, q, g), where G is a cyclic group of order q (with $\|q\| = n$), and g is a generator of G. We say that the decisional Diffie-Hellman problem is hard relative to $\mathcal{G}$ if for all PPT algorithms $\mathcal{A}$ there exists a negligible function negl such that

   $$\left| \Pr[\mathcal{A}(G, q, g, g^x, g^y, g^z) = 1] - \Pr[\mathcal{A}(G, q, g, g^x, g^y, g^{xy}) = 1] \right| \leq \mathsf{negl}(n)$$

   where $x, y, z \in \mathbb{Z}_q$ are uniformly chosen