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

Endsem Exam: 40 points — Date: November 11, 2025

---

1. [5 points] Let G be a finite group of order m. Prove that $g^m = 1$ for all $g \in G$ where 1 is the identity of the group.

2. Let $N = pq$ where p and q are integers greater than 1 such $\gcd(p,q) = 1$. Consider the mapping f from $\mathbb{Z}_N$ to $\mathbb{Z}_p \times \mathbb{Z}_q$ given by $f(x) = (x \bmod p, x \bmod q)$.
   (a) [2 points] Prove that if p divides M and q divides M, then N divides M for some integer M. Use this result, to prove that the map f is a bijection from $\mathbb{Z}_N$ to $\mathbb{Z}_p \times \mathbb{Z}_q$.
   (b) [3 points] For $(a,b) \in \mathbb{Z}_p \times \mathbb{Z}_q$, find $f^{-1}((a,b)) \in \mathbb{Z}_N$ as a function of a and b. For $(a,b) \in \mathbb{Z}_p^* \times \mathbb{Z}_q^*$, show that $f^{-1}((a,b))$ belongs to $\mathbb{Z}_N^*$.

3. [5 points] Solve the following system of congruences using the Chinese remainder theorem. Show your steps and reduce your answer to an element in $\mathbb{Z}_{67830}$.

$$\begin{aligned} x &= 2 \bmod 14,\\ x &= 3 \bmod 15,\\ x &= 4 \bmod 17,\\ x &= 5 \bmod 19. \end{aligned}$$

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 the following.
   (a) The only square roots of 1 in $\mathbb{Z}_p$ are $+1$ and -1.
   (b) $\mathcal{J}_p(x) = x^{\frac{p-1}{2}} \bmod p$
   Hint: You can assume that $\mathbb{Z}_p^*$ is cyclic without proof.

5. [5 points] In the coin-flipping over telephone protocol, Alice initially sends the integer N to Bob where $N = pq$ for distinct odd primes p and q. Assume that $p = q = 3 \bmod 4$. Describe the rest of the protocol by
   - specifying the sequence of messages exchanged between Alice and Bob,
   - the computations performed by Alice and Bob, and
   - the conditions under which Alice wins and the conditions under which Bob wins.

6. Let G be a cyclic group of order q and generator g.
   (a) [3 points] Describe the Schnorr identification scheme over G where an identity corresponds to the knowledge of the discrete logarithm x of an element $h = g^x$ in G.
   (b) [2 points] Explain how the Schnorr signature scheme is derived from the Schnorr identification scheme. Specify the signing and verification algorithms.

7. Let $\mathsf{GenModulus}$ be a PPT algorithm that on input 1^n outputs (N, p, q) where $N = pq$ and p, q are n-bit primes except with probability negligible in n.
   (a) [2 points] Using $\mathsf{GenModulus}$, describe the Goldwasser-Micali encryption scheme for a message space $\mathcal{M} = \{0, 1\}$.
   (b) [3 points] Prove that the Goldwasser-Micali encryption scheme is CPA-secure if the quadratic residuosity problem is hard relative to $\mathsf{GenModulus}$.

Note 1: We say that **deciding quadratic residuosity is hard relative to** $\mathsf{GenModulus}$ if for all PPT algorithms D there exists a negligible function negl such that

$$\left| \Pr\left[D(N, \mathsf{qr}) = 1\right] - \Pr\left[D(N, \mathsf{qnr}) = 1\right] \right| \leq \mathsf{negl}(n)$$

where in each case the probabilities are taken over the experiment in which $\mathsf{GenModulus}(1^n)$ is run to give (N, p, q), qr is chosen uniformly from $\mathcal{QR}_N$, and qnr is chosen uniformly from $\mathcal{QNR}_N^{+1}$

Note 2: The **eavesdropping indistinguishability experiment** $\mathtt{PubK}^{\mathtt{eav}}_{\mathcal{A},\Pi}(n)$ where $\Pi = (\mathtt{Gen}, \mathtt{Enc}, \mathtt{Dec})$ is described below.

1. A key pair (pk, sk) is generated by running $\mathtt{Gen}(1^n)$.
2. The adversary $\mathcal{A}$ is given pk. It outputs a pair of messages $m_0, m_1 \in \mathcal{M}_{pk}$ of the same length.
3. A uniform bit $b \in \{0, 1\}$ is chosen. Ciphertext $c \leftarrow \mathtt{Enc}_{pk}(m_b)$ is computed and given to $\mathcal{A}$. c is called the *challenge ciphertext.*
4. The output of the experiment is defined to be 1 if $b' = b$, and 0 otherwise. If output is 1, we say that $\mathcal{A}$ succeeds.

Note 3: A public-key encryption scheme $\Pi = (\mathtt{Gen}, \mathtt{Enc}, \mathtt{Dec})$ has **indistinguishable encryptions in the presence of an eavesdropper**, or is **EAV-secure**, if for all probabilistic polynomial-time adversaries $\mathcal{A}$ there is a negligible function $\mathtt{negl}$ such that, for all n,

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

Note 4: A public-key encryption scheme which is EAV-secure is also CPA-secure since the adversary already has access to an encryption oracle (through the public key).

8. Let $\mathcal{G}$ be a cyclic group generation algorithm that on input 1^n outputs a triple (G, q, g) where G is a cyclic group of prime order q having generator g.
   (a) [2 points] Using $\mathcal{G}$, describe the El Gamal encryption scheme.
   (b) [3 points] Prove that the El Gamal encryption scheme is CPA-secure if the decisional Diffie-Hellman (DDH) problem is hard relative to a cyclic group generation algorithm $\mathcal{G}$.

Note 1: Let $\mathcal{G}$ be a cyclic group generation algorithm that on input 1^n outputs a triple (G, q, g) where G is a cyclic group of prime order q having generator g.

We say the **DDH 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