Indian Institute of Technology Kharagpur
Department of Computer Science and Engineering

CS60088 Foundations of Cryptography **Spring 2026**

End-Semester Examination | 28 April, 9 AM – 11 AM **Total Marks: 60**

---

*Answer **any four** questions. State all assumptions you make. Keep your answers concise.*

---

1. Give formal definitions of one-way function and hardcore predicate. For the statements below, answer True or False with proper justifications.
   (a) A 1-1 (i.e., bijective) function with a hard-core predicate is not a one-way function.
   (b) A one-way permutation f along with a hard-core predicate hc for f together imply a pseudorandom generator with expansion $\ell(n) = n + 10$.

4+5+6 = 15

2. Recall the group generation algorithm GGen discussed in class for a security parameter $\lambda \in \mathbb{N}$. Let us define $s = (\mathbb{G}, q, g, h)$, where $(\mathbb{G}, q, g) \leftarrow \mathsf{GGen}(1^\lambda)$ for $q = \Theta(2^\lambda), q \in \mathbb{P}$ and $h \leftarrow \mathbb{G}$ is sampled u.a.r. Consider the following function $H_s : \mathbb{Z}_q \times \mathbb{Z}_q \to \mathbb{G}$ defined as $H_s(x_1, x_2) := g^{x_1} h^{x_2} \in \mathbb{G}$.
   (a) Justify why H_s can be viewed as a compressing function.
   (b) Argue with a formal reduction that H_s is a (fixed-length) collision-resistant hash function, if the discrete logarithm problem is intractable relative to GGen.
   (c) Consider a generalization of H_s now. Define $\widehat{s} = (\mathbb{G}, q, (g_1, g_2, \ldots, g_t))$, where $(\mathbb{G}, q, g_1) \leftarrow \mathsf{GGen}(1^\lambda)$ for $q = \Theta(2^\lambda), q \in \mathbb{P}$ and $\forall i \in [2, t], g_i \leftarrow \mathbb{G}$ is sampled u.a.r. Further, consider the function $H_{\widehat{s}} : (\mathbb{Z}_q)^t \to \mathbb{G}$ such that $H_{\widehat{s}}(x_1, x_2, \ldots, x_t) := \prod_{i=1}^{t} g_i^{x_i} \in \mathbb{G}$. Prove that for any $t = \mathsf{poly}(\lambda)$, $H_{\widehat{s}}$ is a collision-resistant hash function if the discrete-logarithm problem is hard relative to GGen.

3+5+7 = 15

3. Recall the Diffie-Hellman problems discussed in class w.r.t. the algorithm GGen as in question 1.
   (a) Give formal definitions of the decisional and computational Diffie-Hellman (respectively, DDH and CDH) *assumptions* relative to GGen.
   (b) Construct a candidate PRG (pseudorandom generator) from the DDH problem. Show a formal security reduction to argue why your PRG construction is secure if the DDH problem is hard relative to GGen.
   (c) The Decision Linear (DLIN) problem relative to GGen is as follows. Assume $(\mathbb{G}, q, g) \leftarrow \mathsf{GGen}(1^\lambda)$ for $q = \Theta(2^\lambda), q \in \mathbb{P}$. Denote $1_\mathbb{G}$ as the identity of $\mathbb{G}$. For $u, v, h \leftarrow \mathbb{G} \setminus \{1_\mathbb{G}\}$ and $a, b \leftarrow \mathbb{Z}_q$, given a tuple (u, v, h, u^x, v^y, h^r), decide whether $r = x + y$ or not. Formally, we define the advantage of a PPT algorithm $\mathcal{A}$ in deciding the DLIN problem in $\mathbb{G}$ relative to GGen as:

$$\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{A}} := \Big| \Pr\left[\mathcal{A}\left(1^\lambda, u, v, h, u^x, v^y, h^{x+y}\right) = 1 : u, v, h \leftarrow \mathbb{G}, x, y \leftarrow \mathbb{Z}_q, (\mathbb{G}, q, g) \leftarrow \mathsf{GGen}(1^\lambda)\right] - \Pr\left[\mathcal{A}\left(1^\lambda, u, v, h, u^x, v^y, h^r\right) = 1 : u, v, h \leftarrow \mathbb{G}, x, y, r \leftarrow \mathbb{Z}_q, (\mathbb{G}, q, g) \leftarrow \mathsf{GGen}(1^\lambda)\right] \Big|,$$

   where, the probability is taken over the uniform random choice of the parameters input to $\mathcal{A}$, and over the random coin tosses possibly made by $\mathcal{A}$. Show that DLIN is hard to solve in $\mathbb{G}$, if it is so for DDH. [**Hint:** How can a reduction set a DLIN tuple (u, v, h, u^x, v^y, z), given a DDH challenge (g, g^a, g^b, t)?]

4+4+7 = 15

4. Consider an ElGamal-like public-key encryption scheme Π that is built upon the RSA problem. Let $M = r \cdot t$ (for $r, t \in \mathbb{P}$) be an RSA modulus and $(\mathsf{pk}, \mathsf{sk}) = ((u, M), (v, M))$ be public-secret key pair (i.e., formally $(M, u, v) \leftarrow \mathsf{GenRSA}(1^\lambda)$ for some $\lambda \in \mathbb{N}$). To encrypt any message $\mu \in \mathbb{Z}_M$ with pk, sample $w \leftarrow \mathbb{Z}_M$ u.a.r. and output the ciphertext as (α, β), where

$$\alpha = w^u \bmod M \qquad , \qquad \beta = \mu \cdot (w+1)^u \bmod M.$$

   (a) Recall that in class, we (informally) discussed the notions of malleable (and homomorphic) encryption. Is Π malleable and/or homomorphic? Justify your answers.

   (b) For $a, z \leftarrow \mathbb{Z}_M$, the decisional dependent-RSA problem (DDRSA) is to decide, given (M, u) and $(\alpha, \beta) \in \mathbb{Z}_M^2$, whether

$$(\alpha, \beta) = (a^u \bmod M \ , \ (a+1)^u \bmod M) \qquad \text{or} \qquad (\alpha, \beta) = (a^u \bmod M \ , \ z^u \bmod M) \, .$$

   Prove that Π is IND-CPA secure if the DDRSA problem in $\mathbb{Z}_M$ is intractable.

   (c) Modify Π to build a digital signature scheme Π'. In particular, you should describe *all* the algorithms of Π' explicitly, together with a proof of its *correctness*. Prove that Π' is *not* a secure digital signature. (That is, show a forgery against Π' by any PPT adversary $\mathcal{A}$.)

4+6+5 = 15

5. Recall the concept of one-time signatures (OTS) discussed in class with Lamport's OTS construction. A *strong* OTS scheme informally satisfies the following: given a valid message-signature pair (m', σ'), it is infeasible to output $(m, \sigma) \neq (m', \sigma')$ for which σ is a valid signature on m.

   (a) Give a formal security definition of strong OTS.

   (b) Recall that Lamport's OTS scheme uses a one-way function. Show a candidate one-way function for which Lamport's OTS is *not* a strong OTS scheme.

   (c) Is the textbook RSA signature a secure OTS? Is it a strong OTS? Justify your answers.

5+6+4 = 15