Indian Institute of Technology Kharagpur | Department of Computer Science & Engineering

Spring 2026 | CS60088: Foundations of Cryptography | Short Test - 2

Full Marks: 10 **Time: 60 minutes | Date: April 6, 2026**

State any assumptions you make. Keep your answers concise. Ensure your handwriting is legible.

---

1. Show how to modify the Diffie-Hellman key-exchange protocol to build the ElGamal public-key encryption scheme. Use the DDH assumption to formally prove that the scheme is secure against chosen plaintext (CPA) attacks. Recall the security definition of a key-exchange protocol against an eavesdropping adversary that we discussed in class. Show that *any* two-round key-exchange protocol (where each party sends a single message to the other one) satisfying the above security definition can be converted into a CPA-secure public-key encryption scheme. **[2+4+4 = 10]**

Indian Institute of Technology Kharagpur | Department of Computer Science & Engineering

Spring 2026 | CS60088: Foundations of Cryptography | Short Test - 2

Full Marks: 10 **Time: 60 minutes | Date: April 6, 2026**

State any assumptions you make. Keep your answers concise. Ensure your handwriting is legible.

---

1. Describe the textbook RSA public-key encryption scheme discussed in class. Prove its correctness formally *without* using Chinese Remainder Theorem. Recall that we had discussed the Factoring and RSA problems, and their associated computational assumptions. Formally prove that the hardness of Factoring is a weaker computational assumption than that of RSA. **[3+4+3 = 10]**

Indian Institute of Technology Kharagpur | Department of Computer Science & Engineering

Spring 2026 | CS60088: Foundations of Cryptography | Short Test - 2

Full Marks: 10 **Time: 60 minutes | Date: April 6, 2026**

State any assumptions you make. Keep your answers concise. Ensure your handwriting is legible.

---

1. Consider a ElGamal-like public-key encryption scheme based upon the RSA problem. Let $M = r \cdot t$ (for $r, t \in \mathbb{P}$) be an RSA modulus, and (u, v) be public-secret key pair under M. For encrypting $\mu \in \mathbb{Z}_M$, sample $w \leftarrow \mathbb{Z}_M$ u.a.r., and compute

$$\alpha = w^u (\text{mod } M) \qquad , \qquad \beta = \mu \cdot (w+1)^u (\text{mod } M).$$

Output the ciphertext as (α, β). Explain how a ciphertext (α, β) can be decrypted. Formally justify if the encryption scheme is malleable or not. For some $a, z \leftarrow \mathbb{Z}_M$, the decisional dependent-RSA problem (DDRSA) is to decide, given (M, u) and $(\alpha, \beta) \leftarrow \mathbb{Z}_M^2$, whether

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

Formalize the problem to define it as a cryptographic assumption. **[3+2+5 = 10]**
