QUANTUM CRYPTOGRAPHY
(IOT3103)

Time Allotted : 2½ hrs **Full Marks : 60**

Figures out of the right margin indicate full marks.

Candidates are required to answer Group A and any 4 (four) from Group B to E, taking one from each group.

Candidates are required to give answer in their own words as far as practicable.

Group – A

1. Answer any twelve: **12 × 1 = 12**

Choose the correct alternative for the following

(i) Which quantum gate acts as the quantum analogue of the NOT gate?
(a) Z gate (b) X gate
(c) H gate (d) CNOT gate

(ii) The most famous quantum cryptography protocol is:
(a) RSA. (b) BB84.
(c) AES. (d) ECC.

(iii) Shannon's principles of confusion and diffusion are applied in:
(a) Hash functions. (b) Block ciphers.
(c) RSA. (d) Digital signatures.

(iv) Elliptic Curve Cryptography (ECC) relies on:
(a) Quantum simulation. (b) Factoring integers.
(c) Balanced functions. (d) Hardness of ECC discrete log problem.

(v) Which algorithm solves the Hidden Subgroup Problem in polynomial time?
(a) Simon's (b) Deutsch–Jozsa
(c) Grover's (d) RSA

(vi) Which of the following is an example of a key exchange protocol?
(a) RSA (b) AES
(c) Diffie–Hellman (d) ElGamal

(vii) The Random Oracle Model assumes:
(a) The adversary has infinite computing power.
(b) The encryption is always probabilistic.
(c) The system is immune to chosen-ciphertext attacks.
(d) The hash function behaves as a truly random function.

(viii) The speedup in Shor's Algorithm comes from:
(a) Grover's quadratic search.
(b) Random Oracle access.
(c) Polynomial interpolation.
(d) Quantum Fourier Transform and period finding.

(ix) Lattice-based cryptography is considered:
(a) Only classical secure. (b) Symmetric-only.
(c) Random Oracle dependent. (d) Quantum-secure.

(x) The Quantum One-Time Pad encrypts qubits using:
(a) RSA keys. (b) Modular arithmetic.
(c) Pauli operators (X, Z). (d) Discrete logarithm.

Fill in the blanks with the correct word

(xi) The no-cloning theorem states that it is impossible to make an exact copy of an _____ quantum state.

(xii) The security of the Diffie–Hellman key exchange protocol is based on the hardness of the _____ problem.

(xiii) The _____ protocol was the first practical method for secure key exchange.

(xiv) The Dihedral HSP connects to lattice problems through _____.

(xv) The Quantum _____ applies random Pauli operators (X, Z) to qubits for perfect secrecy.

Group - B

2. Discuss the Controlled gate, the Swap gate, the Controlled-Z gate, and the Toffoli gate. *[(CO1)(Understand/IOCQ)]*
12

3. (a) State the postulates of quantum mechanics relevant to quantum computing. How does quantum error correction work to protect quantum information? *[(CO1)(Remember/LOCQ)]*

(b) Explain the fundamental differences between classical computing and quantum computing. How does quantum cryptography leverage quantum principles for secure communication? *[(CO1)(Remember/LOCQ)]*
6 + 6 = 12

Group - C

4. Describe Simon's algorithm and demonstrate its working with an example for n=4 and the secret string s=1001. *[(CO2)(Understand/IOCQ)]*
12

5. (a) Describe the RSA algorithm in detail. Explain key generation, encryption, and decryption steps with an example. *[(CO2)(Understand/LOCQ)]*

(b) What are the primary goals of cryptography? Briefly explain it.
[(CO3)(Remember/LOCQ)]

8 + 4 = 12

Group - D

6. (a) Explain how the quantum internet and quantum communication networks can enhance secure communications. Illustrate with examples of real-world applications. *[(CO6)(Understand/LOCQ)]*

(b) Compare classical digital signature schemes (RSA, ECC) with quantum-resistant schemes, focusing on security, efficiency, and vulnerability to quantum attacks.
[(CO4)(Understand/LOCQ)]

6 + 6 = 12

7. (a) Compare Grover's Algorithm and Shor's Algorithm with respect to their functionality, computational complexity, and implications for cryptography.
[(CO3)(Understand/LOCQ)]

(b) Describe the Quantum Fourier Transform (QFT). Why is it essential for Shor's Algorithm? *[(CO3)(Understand/LOCQ)]*

6 + 6 = 12

Group - E

8. (a) What is Quantum Public Key Encryption (QPKE)? How does it differ from classical public key cryptography, and why is it considered a necessary evolution in cybersecurity? *[(CO5)(Remember/LOCQ)]*

(b) How does the Quantum One-Time Pad (QOTP) relate to its classical counterpart? What makes the QOTP theoretically unbreakable, and what is the biggest practical challenge in implementing it? *[(CO5)(Understand/LOCQ)]*

6 + 6 = 12

9. (a) Explain the Learning with Errors (LWE) and Short Integer Solution (SIS) problems. Why are they considered the foundations of modern lattice-based cryptography? *[(CO4)(Understand/LOCQ)]*

(b) What is a lattice in the context of cryptography? Explain the concepts of a basis and a basis vector, and why a "good" basis is important for lattice-based cryptography. *[(CO4)(Remember/LOCQ)]*

(c) What is the Dihedral Hidden Subgroup Problem (DHSP), and why is it important in the context of post-quantum cryptography? *[(CO4)(Remember/LOCQ)]*

4 + 4 + 4 = 12

Cognition Level	LOCQ	IOCQ	HOCQ
Percentage distribution	75	25	0