1. Explain Quantum Cryptography and its basic principles. (5 marks)

Quantum Cryptography is a modern security technique that uses the laws of quantum physics to protect communication. Its main purpose is to securely share secret keys between two parties so that data cannot be intercepted by attackers.

It works based on the behavior of quantum particles like photons. If anyone tries to observe or measure these particles, their state changes automatically, which helps in detecting eavesdropping.

Basic Principles:
- Quantum Superposition: A particle can exist in multiple states at the same time until it is measured.
- Quantum Entanglement: Two particles are linked together, and a change in one affects the other instantly.
- Heisenberg's Uncertainty Principle: It is impossible to measure a quantum state without disturbing it.
- No-Cloning Theorem: Quantum information cannot be copied exactly.

Conclusion:
These principles ensure that any unauthorized access can be detected, making communication highly secure.

2. Describe the BB84 Quantum Key Distribution protocol. (5 marks)

BB84 is one of the first and most widely used Quantum Key Distribution (QKD) protocols. It allows two users (usually called sender and receiver) to generate a shared secret key securely.

Working of BB84:
1. The sender transmits photons encoded in different polarization bases (randomly chosen).
2. The receiver measures these photons using randomly selected bases.
3. After transmission, both compare their chosen bases over a public channel.
4. Only the matching measurements are kept to form the secret key.

If an attacker tries to intercept the photons, it changes their state and introduces errors. These errors can be detected, and the communication is discarded.

Conclusion:
BB84 ensures secure key exchange and detects any eavesdropping, making it a fundamental protocol in quantum cryptography.

3. Explain Post-Quantum Cryptography and the Kyber algorithm. (5 marks)

Post-Quantum Cryptography (PQC) refers to cryptographic techniques that are designed to remain secure even when quantum computers become powerful enough to break traditional

encryption methods like RSA and ECC.

PQC algorithms are based on complex mathematical problems that are difficult for both classical and quantum computers to solve.

Kyber Algorithm:
Kyber is a popular lattice-based PQC algorithm used for secure key exchange.

Features of Kyber:
- Based on the Module Learning With Errors (Module-LWE) problem
- Efficient and fast
- Suitable for real-world applications

Main Steps:
1. Key Generation: Public and private keys are created
2. Encapsulation: A secret key is encrypted using the public key
3. Decapsulation: The receiver decrypts the key using the private key

Conclusion:
Kyber provides strong security against quantum attacks and is suitable for future communication systems.

4. Explain the Hybrid QC + PQC approach and its workflow. (5 marks)

The Hybrid QC + PQC approach combines Quantum Cryptography and Post-Quantum Cryptography to achieve stronger and future-proof security.

Workflow:
1. Quantum Key Distribution (QKD):
Secure keys are generated using quantum communication. Any eavesdropping is detected immediately.

2. Classical Communication:
A classical channel is used for error correction, basis comparison, and authentication.

3. Authentication:
Hash functions and authentication techniques verify the identity of users.

4. Post-Quantum Cryptography:
Algorithms like Kyber encrypt the actual data using the secure keys.

Advantages:
- Provides multi-layer security
- Protects against both classical and quantum attacks

- Ensures long-term secure communication

Conclusion:
This hybrid model is considered a future-proof solution for secure communication systems.