PROBLEM B – PART B

Name: Rijul

Q1: What happens if an eavesdropper intercepts the qubit sent from Alice to Bob?

If an eavesdropper (Eve) intercepts Alice's qubit *after* encoding but *before* it reaches Bob, she holds only **one qubit** of a two-qubit entangled Bell state. Critically:

- The single intercepted qubit is in a **maximally mixed state**: its reduced density matrix is $\rho = I/2$, meaning it appears completely random regardless of what message Alice encoded.
- Eve gains **zero information** about the 2-bit message from measuring just one qubit — any measurement she makes will yield 0 or 1 with equal 50% probability for any basis.
- Furthermore, Eve's measurement *destroys the entanglement*. When Bob receives the (now collapsed) qubit and attempts Bell-basis decoding with his half of the original pair, he will get **random, incorrect results**, alerting Alice and Bob to the presence of an eavesdropper.

This demonstrates that superdense coding inherits the security properties of quantum entanglement — the information is non-locally encoded and cannot be extracted by intercepting only one particle of the pair.

Q2: Give one application or implication of superdense coding.

Application: Quantum-Enhanced Communication Capacity

Superdense coding demonstrates that a **pre-shared entangled resource** can double the classical information capacity of a quantum channel. Specifically, transmitting only 1 qubit conveys 2 classical bits of information — achieving a **communication capacity of 2 bits/qubit**, compared to 1 bit/qubit for classical systems.

Implication for Quantum Networks: In future quantum communication networks (quantum internet), superdense coding could be used to boost the effective bandwidth of quantum links. Nodes that pre-share entangled pairs (distributed via entanglement distribution protocols) can communicate classical data at twice the rate using the same quantum channel. This has practical implications for satellite-based quantum communication, secure data transmission, and quantum-assisted classical networking where generating entangled pairs is a one-time investment that enhances future communication efficiency.