Integrating Quantum Concepts into Cybersecurity

Activity 2a: Tutorial

1. Draw the quantum communication model from the slides.

2. Explain what is meant by entanglement.

3. Draw the circuit for generating EPR (Einstein, Podolsky, Rosen) pairs and derive the four Bell states that can be produced.

4. Alice the sender encodes bits using the Z basis and sends these as photons to Bob the receiver. Describe a possible threat to the quantum channel. What steps would you advise to block the threat described? Hence describe an improved model for the communication protocol. Could entanglement help?

5. What threats do you feel the above protocol could be susceptible to if entanglement was employed?