Name _____

Quantum Computing and the Future of Cryptography

Short Answer Key

1. Shor's algorithm is significant because it can factor large numbers exponentially faster than classical computers. This poses a threat to widely used encryption methods that rely on the difficulty of factoring large numbers, such as RSA.
2. Post-quantum cryptography is the development of new encryption methods that are resistant to attacks by quantum computers. It is necessary to ensure the security of data and communications in a future where quantum computers could potentially break traditional encryption methods.
3. Quantum key distribution (QKD) works by using the principles of quantum mechanics to create encryption keys. It relies on the properties of quantum states, such as superposition and entanglement, to ensure that any attempt to intercept the keys would disrupt the quantum states, alerting the sender and receiver to a potential breach. This makes QKD considered unbreakable.
4. The impact of quantum computing on cryptography extends to various sectors such as finance, healthcare, and government. In finance, secure transactions rely on encryption. In healthcare, patient data must be protected. In government and military operations, classified information must remain confidential. The need for quantum-resistant encryption methods is critical to securing these areas.
5. The transition to quantum-resistant cryptography involves developing and implementing encryption methods that can withstand attacks by quantum computers. It is important for the future because as quantum computing technology advances, the risk of traditional encryption methods being compromised increases. Transitioning to quantum-resistant cryptography ensures the continued security of digital communications and data.