QUANTUM ENCRYPTION LAB QUIZ: SPY VS SPY CHALLENGE

QUIZ STRUCTURE

Total Time: 30 minutes
Total Points: 100
Format: Multiple Choice, True/False, Short Answer, Scenario Analysis

---

SECTION 1: BASIC CONCEPTS (20 points)

1. Multiple Choice (4 points each)

Q1.1: The primary security advantage of quantum cryptography over classical cryptography is:

- A) Faster computation speed
- B) Information-theoretic security based on physics principles ✓
- C) Smaller key sizes
- D) Easier implementation

Q1.2: In the BB84 protocol, what does Alice do before sending qubits to Bob?

- A) Encrypts the message with a public key
- B) Randomly chooses bases (Z or X) for each qubit ✓
- C) Shares a secret key with Bob through a secure channel
- D) Encodes all qubits in the same basis for consistency

Q1.3: What principle prevents Eve from perfectly copying quantum states?

- A) Heisenberg's Uncertainty Principle
- B) Quantum Entanglement
- C) No-Cloning Theorem ✓
- D) Superposition Principle

Q1.4: When Bob measures a qubit in the wrong basis (different from Alice's encoding basis), what happens?

- A) He always gets the wrong result
- B) He gets a random result (0 or 1 with 50% probability) ✓
- C) The qubit is destroyed
- D) He gets an error message

Q1.5: The sifting process in BB84 involves:

- A) Comparing bases publicly and keeping only matching measurements ✓
- B) Encrypting the quantum states
- C) Adding error correction codes
- D) Measuring all qubits multiple times

SECTION 2: EAVESDROPPER ANALYSIS (25 points)

2. True/False with Justification (5 points each)

Q2.1: If Eve intercepts and measures all qubits in the Z basis, she will always get the correct values for qubits encoded in the X basis.

- False ✓
- *Justification: When Eve measures X-basis qubits in the Z basis, she gets random results (0 or 1 with 50% probability), not the correct values.*

Q2.2: A 10% error rate in the sifted key always indicates eavesdropping.

- False ✓
- *Justification: Real quantum systems have natural noise (1-2% error rate). An error rate of 10% could be due to eavesdropping OR high channel noise, requiring statistical analysis to determine the cause.*

Q2.3: If Alice and Bob use all the same bases (all Z or all X), the protocol becomes more secure.

- False ✓

- *Justification: Using all the same bases makes the protocol vulnerable because Eve can use the same basis and intercept without introducing errors. Random basis choice is essential for security.*

Q2.4: Eve's sophisticated attack (randomly guessing bases) introduces a lower error rate than her unsophisticated attack (always using Z basis).

- True ✓
- *Justification: Sophisticated attack error rate = 25% × 50% = 12.5%, while unsophisticated attack error rate = 25% for X-basis qubits + 0% for Z-basis qubits = average 12.5% if equal bases, but potentially higher if Alice uses mostly X basis.*

Q2.5: Privacy amplification can completely eliminate any information Eve gained from interception.

- True ✓
- *Justification: Privacy amplification uses hash functions to distill a shorter, completely secure key from the partially compromised sifted key, reducing Eve's information to negligible levels.*

SECTION 3: ERROR RATE CALCULATIONS (25 points)

3. Scenario Analysis (5 points each)

Scenario: Alice sends 100 qubits to Bob using random bases. Eve intercepts using the strategy described below. Calculate the expected error rate in the sifted key.

Q3.1: Eve uses an unsophisticated attack (measures all in Z basis). Alice uses 50% Z basis, 50% X basis.

- Calculation: Error only occurs when Alice uses X basis (50%) AND Bob uses same basis as Alice (50% of those). When wrong basis measurement: 50% error. So: 50% × 50% × 50% = 12.5%
- Answer: 12.5% ✓

Q3.2: Eve uses a sophisticated attack (randomly guesses Z or X). Both Alice and Bob use random bases.

- Calculation: Eve guesses wrong basis 50% of the time. When she guesses wrong: causes error 25% of the time (when Bob uses same basis as Alice, which happens 50% of the time, and measurement gives wrong result 50% of those). So: 50% × 50% × 50% = 12.5%
- Answer: 12.5% ✓

Q3.3: Eve intercepts only 30% of the qubits (random selection) using sophisticated attack.

- Calculation: For intercepted qubits: 12.5% error rate. For non-intercepted qubits: only natural noise (assume 1%). Weighted average: (30% × 12.5%) + (70% × 1%) = 3.75% + 0.7% = 4.45%
- Answer: ~4.45% ✓

Q3.4: In the lab, you observed a 15% error rate with 200 sifted bits. The expected natural noise is 1%. What's the Z-score for detecting eavesdropping? (Use: Z = (observed - expected)/√[p(1-p)/n])

- Calculation: p_observed = 0.15, p_expected = 0.01, n = 200
  Z = (0.15 - 0.01)/√[0.01×0.99/200] = 0.14/√[0.0099/200] = 0.14/√0.0000495 = 0.14/0.007036 = 19.9
- Answer: Z ≈ 19.9 ✓

Q3.5: If the security threshold is set at 11% error rate, and you observe 9% error with 1000 sifted bits (natural noise = 1%), should you accept or reject the key?

- Calculation: Need to check statistical significance, not just compare to threshold.
  Z = (0.09 - 0.01)/√[0.01×0.99/1000] = 0.08/√0.0000099 = 0.08/0.003146 = 25.4
  This is highly significant (p-value < 0.0001), even though 9% < 11%.
- Answer: Reject the key - significant evidence of eavesdropping ✓

SECTION 4: PROTOCOL DESIGN (30 points)

4. Short Answer (10 points each)

Q4.1: During the lab, you tested different encoding strategies. Compare the security of these two approaches:

- Strategy A: Always use Z basis
- Strategy B: Use random Z/X bases

Answer:

- *Strategy A (all Z):* Extremely insecure. Eve can measure all qubits in Z basis without introducing errors. She learns the entire key undetected. No quantum advantage is utilized.
- *Strategy B (random bases):* Secure when properly implemented. Random basis choice forces Eve to guess, introducing detectable errors when she guesses wrong. This leverages quantum principles for security.
- *Key difference:* Randomness in basis choice is essential for detecting eavesdropping through error analysis. ✓

Q4.2: Describe how the "decoy state" method (mentioned in security challenges) improves upon basic BB84. Include what problem it solves and how it works.

Answer:

- *Problem solved:* Photon Number Splitting (PNS) attack where Eve steals one photon from multi-photon pulses without detection.
- *How it works:* Alice randomly inserts decoy pulses with different intensities (weak coherent pulses) among the signal pulses. Eve cannot distinguish decoys from signals.
- *Detection:* Eve's interception changes the transmission statistics of decoy states differently than signal states. By monitoring arrival rates of decoys vs. signals, Alice/Bob can detect the PNS attack.
- *Advantage:* Provides additional layer of security against sophisticated attacks on practical implementations. ✓

Q4.3: In the final mission, you had to choose a strategy. Explain why checking a larger sample (e.g., 50% instead of 25% of bits) for error estimation improves security but has a trade-off.

Answer:

- *Improvement:* Larger sample gives better statistical power to detect small deviations. Reduces false negatives (failing to detect Eve) because smaller error rate increases can be detected as statistically significant.
- *Trade-off:* More bits sacrificed for testing means fewer bits remain for the final key. This reduces key rate/throughput.
- *Optimal balance:* Need sufficient samples for reliable detection while maintaining reasonable key generation rate. Typically 25-50% is used depending on security requirements.
- *Mathematical reason:* Standard error decreases with √n, so quadrupling sample size halves the minimum detectable error rate increase. ✓

BONUS SECTION: ADVANCED ANALYSIS (Extra 10 points)

5. Critical Thinking

Q5: Real quantum channels have natural noise (typically 1-2% error rate). How does this affect the security analysis compared to the idealized simulations in the lab? Propose a modified protocol that accounts for this reality.

Answer:

- *Effect on analysis:* Natural noise creates a "background" error rate that Eve's errors add to. This makes distinguishing eavesdropping from channel noise more challenging.
- *Statistical solution:* Use hypothesis testing instead of fixed thresholds. Test H_0: errors = natural noise vs. H_1: errors > natural noise.
- *Modified protocol ideas:*
    1. Error correction: First correct natural errors using codes like Cascade or Winnow.
    2. Privacy amplification: Hash the corrected key to reduce Eve's partial information.
    3. Adaptive thresholds: Set thresholds based on measured natural noise characteristics.
    4. Decoy states: As mentioned, to detect photon-number splitting attacks.

5. Device-independent QKD: Protocols that don't require assumptions about device imperfections.

- *Key insight:* Real-world QKD must account for and separate channel noise from eavesdropper-induced noise through statistical methods and additional protocol layers. ✓

QUIZ ANSWER KEY & GRADING RUBRIC

Scoring:

- Section 1: 20 points (4 per question)
- Section 2: 25 points (5 per question: 2 for T/F, 3 for justification)
- Section 3: 25 points (5 per question)
- Section 4: 30 points (10 per question)
- Total: 100 points
- Bonus: Up to 10 extra points

Grading Scale:

- 90-100: A - Excellent understanding of quantum encryption principles
- 80-89: B - Good understanding with minor gaps
- 70-79: C - Basic understanding but needs review of key concepts
- 60-69: D - Significant gaps in understanding
- Below 60: F - Needs to retake the lab and review fundamentals

Common Misconceptions to Address:

1. Quantum encryption vs. quantum-resistant encryption: Emphasize that QKD provides key distribution, not encryption of messages.
2. Perfect security misconception: Clarify that QKD provides information-theoretic security under ideal conditions, but practical implementations have limitations.

3. Error rate interpretation: Stress that error rates must be interpreted statistically, not as absolute thresholds.
4. Role of randomness: Highlight that security depends on genuine randomness in basis choices.

Discussion Points for Post-Quiz Review:

1. How does the spy vs. spy narrative help understand real security challenges?
2. What real-world implementations of QKD exist today?
3. How might quantum computing eventually break classical encryption, making QKD more important?
4. What are the practical limitations of deploying QKD in real communication networks?

This quiz assesses not just factual recall but also analytical skills, error calculation abilities, and protocol design thinking - mirroring the hands-on, problem-solving approach of the interactive lab.