# BB84 Quantum Cryptography Protocol Worksheet

Maqsad: Duniya ka pehla quantum cryptography protocol samjhein interactive sawalaat aur mashq ke zariye.

---

## Part A: Quantum Bases Ki Samajh

### Sawalaat:

1. Z basis ki measurements se humein milta hai
   _____
   *Hint: Standard computational basis ke baare mein sochein*
2. X basis ki measurements se humein milta hai
   _____
   *Hint: Is mein Hadamard gate shamil hai*
3. Hum Z aur X dono bases ek saath kyun nahi measure kar sakte?
   _____
   _____
   *Hint: Yeh ek bunyadi quantum principle hai*

---

## Part B: Protocol Steps Ki Tarteeb

Hidayat: Steps ko sahi chronological order mein number dein (1-4):

- Step _____: Alice aur Bob aam tour par compare karte hain ke unhoun ne kaun se bases istemal kiye
- Step _____: Alice random bits ko random chosen bases (Z ya X) istemal karte huwe encode karti hai
- Step _____: Bob mile huwe qubits ko random chosen bases (Z ya X) istemal karte huwe measure karta hai

- Step _____: Woh sirf un bits ko rakhte hain jahan unke bases match karte hain

Sahi Tarteeb: _____ → _____ → _____ → _____

---

## Part C: Security Analysis

### Security Sawalaat:

1. Agar Eve (eavesdropper) galat basis mein measure kare, to kya hota hai?
   - A) Use 100% accuracy ke saath sahi bit milta hai
   - B) Use random results milte hain (50% 0, 50% 1)
   - C) Qubit tabah ho jata hai
   - D) Kuch nahi hota
2. Alice aur Bob Eve ki mojoodgi ka pata kaise lagate hain?
   - A) Ye check kar ke ke unki keys identical hain ya nahi
   - B) Aam tour par bits ke subset ko compare kar ke
   - C) Entanglement measure kar ke
   - D) Woh Eve ka pata nahi laga sakte
3. BB84 ke liye approximate maximum safe error rate kya hai?
   - A) 5%
   - B) 11%
   - C) 25%
   - D) 50%

---

## Part D: Code Implementation

Task: BB84 ke liye quantum encoding function complete karein:

```
python
```

```python
def encode_qubit(bit, basis):
    """
    BB84 protocol ke liye classical bit ko quantum state mein encode karein
```

```
    Parameters:
    bit (int): 0 ya 1
    basis (str): 'Z' ya 'X'

    Returns:
    QuantumCircuit: Bit ko encode karta hua circuit
    """
    qc = QuantumCircuit(1, 1)

    if basis == 'Z':
        # Z basis: 0 ke liye |0⟩, 1 ke liye |1⟩
        if bit == 1:
            qc._____(0)  # Konsa gate lagayein takay |1⟩ ban jaye?
    else:  # X basis
        # X basis: 0 ke liye |+⟩, 1 ke liye |-⟩
        if bit == 0:
            qc._____(0)  # Konsa gate lagayein takay |+⟩ ban jaye?
        else:
            qc._____(0)  # Pehle |1⟩ banayein
            qc._____(0)  # Phir |-⟩ mein transform karein

    return qc
```

Missing Gates: Inmein se chunein: `h`, `x`, `y`, `z`

---

## Part E: Critical Thinking

### Scenario Analysis:

Imagine karein Eve ye attacks koshish karti hai. Har case mein kya hota hai?

1. Intercept-Resend Attack: Eve tamam qubits ko Z basis mein measure karti hai aur naye bhejti hai.
   Error rate jo aati hai: _____%

2. Partial Attack: Eve sirf 30% qubits measure karti hai.
   Detection ki probability: _____%
3. Basis Guessing: Eve har qubit ke liye randomly Z ya X guess karti hai.
   Average information jo milti hai har qubit se: _____ bits

---

## Part F: Quantum Principles Review

Har quantum principle ko BB84 mein iske role se match karein:

| Principle | BB84 Mein Role |
|---|---|
| No-Cloning Theorem | |
| Uncertainty Principle | |
| Measurement Collapse | |
| Superposition | |

Options:

- A) Quantum states ki perfect copying se rokta hai
- B) Galat basis measurements ko random banata hai
- C) Eve ke measure karne par state ko disturb karta hai
- D) Multiple bases mein encoding ki ijazat deta hai

---

## Part G: Short Answer Questions

1. "BB84" ka matlab kya hai?

---

2. Quantum cryptography ki ek real-world implementation ka naam dein:

   _____

3. Quantum key distribution classical encryption se kaise different hai?

   _____

   _____

4. Agar Alice aur Bob high error rates discover karein to kya hota hai?

   _____

   _____

---

## Part H: Learning Objectives Checklist

- Samjhein Z aur X basis measurements ka farq
- Sequence karein BB84 protocol steps ko sahi tarteeb se
- Samjhaayein quantum mechanics security kaise mumkin banati hai
- Implement karein basic quantum encoding code mein
- Calculate karein eavesdropping detection ke liye error rates
- Connect karein quantum principles ko practical cryptography se
- Analyze karein different eavesdropping strategies
- Compare karein quantum vs classical security approaches

---

## Jawaboon Ki Key Section *(Teachers/Instructors Ke Liye)*

### Part A Jawab:

1. $|0\rangle$ ya $|1\rangle$ (computational basis states)
2. $|+\rangle$ ya $|-\rangle$ (Hadamard basis states)
3. Heisenberg Uncertainty Principle ki wajah se - Z aur X complementary observables hain jo bina uncertainty ke ek saath measure nahi kiye ja sakte

### Part B Jawab:

Sahi tarteeb: 2 → 3 → 1 → 4

## Part C Jawab:

1. B) Use random results milte hain (50% 0, 50% 1)
2. B) Aam tour par bits ke subset ko compare kar ke
3. B) 11%

## Part D Jawab:

Missing gates tarteeb se: `x`, `h`, `x`, `h`

## Part E Jawab:

1. 25%
2. Sample size par depend karta hai, lekin sample size ke sath probability barhti hai
3. 0.5 bits (50% chance sahi guess karne ka)

## Part F Jawab:

- No-Cloning Theorem → A
- Uncertainty Principle → B
- Measurement Collapse → C
- Superposition → D

## Part G Jawab:

1. Bennett & Brassard 1984 (inventors aur saal)
2. Misal: ID Quantique systems, Chinese quantum satellite, waghaira
3. Quantum physics istemal karta hai security ke liye, classical mathematical complexity istemal karta hai
4. Woh key discard karte hain aur phir se shuru karte hain - high errors possible eavesdropping ki nishani hai

---

## Scoring Rubric

| Section | Max Points | Scoring Criteria |
|---|---|---|
| Part A | 6 | Har sahi jawab ke 2 points |
| Part B | 4 | Har sahi sequence ke 1 point |
| Part C | 6 | Har sahi jawab ke 2 points |
| Part D | 4 | Har sahi gate ke 1 point |
| Part E | 6 | Har sahi calculation ke 2 points |
| Part F | 8 | Har sahi match ke 2 points |
| Part G | 8 | Har sahi jawab ke 2 points |
| Total | 42 | |

Grade Scale:

- 38-42: Behtareen (A)
- 34-37: Bohat Acha (B)
- 30-33: Acha (C)
- 25-29: Qabil Qubool (D)
- 25 se kam: Behtar honay ki zaroorat

---

## Additional Resources & References

1. Textbook References:

    - Nielsen & Chuang, "Quantum Computation and Quantum Information"
    - Scarani et al., "The Security of Practical Quantum Key Distribution"
2. Online Resources:
    - Qiskit Textbook: Quantum Cryptography Chapter
    - IBM Quantum Experience Lab
    - MIT OpenCourseWare: Quantum Information Science
3. Software Tools:
    - Qiskit (Python library)
    - IBM Quantum Lab (online platform)
    - Quirk (quantum circuit simulator)
4. Further Reading:
    - Original BB84 Paper: Bennett & Brassard (1984)
    - Quantum Hacking aur Countermeasures
    - Post-Quantum Cryptography

---

## Worksheet Information

Course: Quantum Computing Fundamentals
Module: Quantum Cryptography
Duration: 60-90 minutes
Difficulty Level: Intermediate
Prerequisites: Basic quantum mechanics, Python programming
Created: [Date]
Last Updated: [Date]
Version: 1.0

Instructor Notes:

- Yeh worksheet individual ya group work ke liye acha kaam karti hai
- Code section ke liye Qiskit installation ki zaroorat hai
- Hands-on quantum simulation ke sath pair karna sochein
- Jawaboon ki discussion learning ko behtar banati hai