Quiz Assignment 5

Note: All multi-qubit state representations are written with LSB on the left, unless specified otherwise

Quantum Key Distribution

1. The key generated during BB84 is. (1 point)
   - A. Predictable
   - B. Random
2. It is possibly to detect an 'Intercept and Resend' attack on BB84? (1 point)
   - A. True
   - B. False
3. The quantum channel used in the BB84 protocol is: (1 point)
   - A. Bidirectional
   - B. Unidirectional
4. Is it possible for Oscar to copy any state Alice sends without being detected? (1 point)
   - A. Possible
   - B. Impossible
5. Given the following information, find the key generated by the BB84 QKD protocol: (3 points)

Alice's State:	11100010000001001001010111011000
Alice's Bases:	10111010110100111101111011110001
Bob's Bases:	00000101011110000100010111010000

   - A. 00010000011000
   - B. 0000000000010011
   - C. 1001001111100
   - D. 11000111110
6. Out of all the qubits that Alice sends to Bob, what fraction (on average) of it will be a part of the key after comparing basis choices? (3 points)
   - A. 1/2
   - B. 1/4
   - C. 1/3
   - D. 3/4
7. For large enough key length, the key generated by BB84 will have an equal number of zeros and ones. (3 points)
   - A. True
   - B. False
8. In the presence of an eavesdropper and under the 'intercept and re-send' attack model, what is the probability of a bit mismatch when Alice and Bob compare their key bits? (2 points)
   - A. 1/2
   - B. 1/4
   - C. 1/3
   - D. 3/4

9. Given the following information for a BB84 process with an ‘intercept and re-send’ adversary Oscar,

Alice's State:	00001111110110011010110111100100
Alice's Bases:	11011110011000110111110111111001
Oscar's Bases:	11111010101111001011000110000011
Bob's Bases:	10001101001001111010001000010001

Find the length of the key generated by the BB84 QKD protocol after sifting: (2 points)

A. 11
B. 15
C. 17
D. 28

10. Using the information in Q9, what is the least number of key bits that Oscar knows? (3 points)

A. 2
B. 4
C. 5
D. 6