**Integrating Quantum Concepts into Cybersecurity**

**Activity 3a: Tutorial**

1. Apply the BB84 protocol to the following:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Alice Candidate Key a | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 |
| Alice Encoding Basis b | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 |
| Alice Encoding Basis b | + | X | X | X | + | + | + | X | X | + | X | X | + | + | X | + | + | X | X | X |
| Alice Encoded State |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Bob Measuring basis | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 |
| Bob Decoding basis |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Bob Decoded bits |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Key |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

1. Describe in detail, the B92 quantum key agreement protocol. Compare and contrast the protocol to BB84. What part does *information reconciliation* and *privacy amplification* play in each of the protocols discussed?