PROJECT REPORT: ENCRYPTION IN PYTHON

Introduction:

The project consists of implementing the BB84 quantum key distribution protocol along with encryption and decryption functions in Python. The primary goal is to establish a secure communication channel between two parties, Alice and Bob, using quantum principles.

- **Function Design and Implementation (Encryption and Decryption Functions):**

  The `encrypt_message` and `decrypt_message` functions were designed to provide a secure method for encoding and decoding messages using a shared secret key. These functions take into account the need for secure communication and leverage the properties of symmetric encryption for data confidentiality.

```python
# Function to encrypt the message using the key
def encrypt_message(message, key):
    encrypted_message = ""
    for i in range(len(message)):
        char = message[i]
        key_char = key[i % len(key)]
        encrypted_char = chr((ord(char) + ord(str(key_char))) % 256)
        encrypted_message += encrypted_char
    return encrypted_message
```

```python
# Function to decrypt the message using the key
def decrypt_message(encrypted_message, key):
    decrypted_message = ""
    for i in range(len(encrypted_message)):
        char = encrypted_message[i]
        key_char = key[i % len(key)]
        decrypted_char = chr((ord(char) - ord(str(key_char))) % 256)
        decrypted_message += decrypted_char
    return decrypted_message
```

- **Consideration taken into account:**

  Considerations for the encryption and decryption functions included security via a BB84-derived shared key, efficiency for reasonable execution, and scalability to handle messages of variable lengths.

- **Difficulties Encountered:**

  Understanding quantum principles for key distribution, implementing them in Python, and ensuring robust error handling posed significant challenges during development. Additionally, translating theoretical quantum cryptography concepts into practical code demanded careful consideration and thorough testing.

Analysis (How would an eavesdropper impact the encryption and decryption of your data?):-

An eavesdropper could compromise the security of encryption and decryption by intercepting the quantum communication between Alice and Bob, potentially accessing the shared secret key. This would lead to the encryption key being compromised, allowing the eavesdropper to decrypt the data and potentially tamper with or read sensitive information.

To mitigate this threat, the BB84 protocol incorporates quantum principles to detect eavesdropping attempts. The protocol ensures that any attempt by an eavesdropper to intercept the qubits alters their quantum state, thus introducing errors in the shared key that can be detected by Alice and Bob.

Here's how the code snippet that addresses this problem:-

```python
# Loop to run the protocol multiple times
secure_key_found = False
while not secure_key_found:
    alice_key, alice_bases, alice_circuit = alice_sends()
    eve_key = eve_intercepts(alice_circuit)
    bob_key, bob_bases = bob_receives(alice_circuit, alice_bases)
    # Compare keys to check for eavesdropping
    eavesdropping_detected = False
    for i in range(num_bits):
        if alice_bases[i] == bob_bases[i] and alice_key[i] != bob_key[i]:
            eavesdropping_detected = True
            break

    if not eavesdropping_detected:
        secure_key_found = True
        secure_key = bob_key
        print("Secure key found:", secure_key)
```

In the above code snippet:

- Alice and Bob compare their measurement bases and keys to detect any inconsistencies that could indicate eavesdropping.
- If the bases match and the keys don't, it suggests interference, and the communication is considered compromised.
- The protocol repeats until a secure key is established, ensuring the integrity of the encryption process.

Conclusion:-

The development of quantum encryption important for the future of secure communication

- **Unbreakable Security**: Quantum encryption offers theoretically unbreakable security due to its reliance on fundamental quantum principles.
- **Resistance to Quantum Attacks**: It provides resistance against attacks from quantum computers, which could compromise traditional cryptographic algorithms.
- **Quantum Key Distribution**: Protocols like BB84 enable secure key distribution over quantum channels, ensuring confidentiality even in the presence of eavesdroppers.
- **Global Secure Communication**: Quantum repeaters and communication satellites pave the way for secure quantum communication networks on a global scale.
- **Privacy Preservation**: Quantum encryption ensures the confidentiality and integrity of sensitive information, addressing privacy concerns across various sectors.