**Assignment-1**

**Problem: Secure communication between a client and a server**

**Use Case:**
A company is developing a new messaging service that allows clients to communicate securely with a server. The company wants to ensure that all messages sent between the client and the server are encrypted and secure.

**Assignment:**
Your task is to write an implementation of the AES or RSA encryption algorithm in Python that will be used to encrypt and decrypt messages sent between the client and the server. The implementation should include the ability to generate a key for encryption/decryption and should be able to handle large amounts of data. The code should also include a mechanism for securely exchanging the encryption key between the client and the server.

**Implementation details:**

- The program should be able to encrypt and decrypt data using AES or RSA algorithm.
- The encryption key should be generated randomly and securely.
- The key should be exchanged between the client and the server securely (e.g. by using asymmetric encryption).
- The program should be able to handle large amounts of data.
- The program should be well-documented and easy to understand.
- The program should be compatible with Python 3.

**Deliverables:**

- The implementation of the AES or RSA encryption algorithm in Python.
- A brief report explaining the design choices made in the implementation and the trade-offs between different options.
- A test plan and test cases to show that the implementation is working correctly.

**Submission Due Date: Feb 3, 2022**

You can drop email at sureshpro@gmail.com if you have any further queries or confusion.