**client.py**

**import socket**

**import random**

**def generate\_prime\_nos(num):**

**while True:**

**num = random.randint(100, 200)**

**if all(num % i != 0 for i in range(2, int(num \*\* 0.5) + 1)):**

**return num**

**def decrypt(encrypted\_message, key):**

**decrypted\_message = ""**

**for c in encrypted\_message:**

**if c.isalpha():**

**if c.isupper():**

**base = 'A'**

**else:**

**base = 'a'**

**decrypted\_message += chr((ord(c) - ord(base) - key) % 26 + ord(base))**

**else:**

**decrypted\_message += c**

**return decrypted\_message**

**client\_socket = socket.socket(socket.AF\_INET, socket.SOCK\_STREAM)**

**client\_socket.connect(("localhost", 9999))**

**num = random.randint(2, 200)**

**p = generate\_prime\_nos(num)**

**g = random.randint(2, p - 1)**

**print("Chosen prime number is ", p, "and the generator is ", g)**

**a = random.randint(1, p - 1)**

**print("Client's secret (a): ", a)**

**RA = pow(g, a, p)**

**print("Calculated RA = g^a mod p: ", RA)**

**data = f'{p}|{g}|{RA}'**

**client\_socket.send(data.encode('utf-8'))**

**RB = int(client\_socket.recv(1024).decode('utf-8'))**

**print("Received RB from the server: ", RB)**

**RAB = pow(RB, a, p)**

**print("Calculated shared key RAB: ", RAB)**

**encrypted\_message = client\_socket.recv(1024).decode('utf-8')**

**decrypted\_message = decrypt(encrypted\_message, RAB)**

**print("Message from the server: ", decrypted\_message)**

**client\_socket.close()**

**server.py**

**import socket**

**import random**

**def encrypt(message, key):**

**encrypted\_message = ""**

**for c in message:**

**if c.isalpha():**

**if c.isupper():**

**base = 'A'**

**else:**

**base = 'a'**

**encrypted\_message += chr((ord(c) - ord(base) + key) % 26 + ord(base))**

**else:**

**encrypted\_message += c**

**return encrypted\_message**

**server\_socket = socket.socket(socket.AF\_INET, socket.SOCK\_STREAM)**

**server\_socket.bind(("localhost", 9999))**

**server\_socket.listen(5)**

**print("Server is listening on port 9999.")**

**conn, addr = server\_socket.accept()**

**print("Connected to client at ", addr)**

**data = conn.recv(1024).decode('utf-8')**

**p, g, RA = data.split('|')**

**p = int(p)**

**g = int(g)**

**RA = int(RA)**

**print("Received from client:\np = ", p, "\ng = ", g, "\nRA = ", RA)**

**b = random.randint(1, p - 1)**

**print("Server's secret (b): ", b)**

**RB = pow(g, b, p)**

**print("Calculated RB = g^b mod p: ", RB)**

**conn.send(str(RB).encode('utf-8'))**

**RAB = pow(RA, b, p)**

**print("Calculated shared key RAB: ", RAB)**

**message = "Hello from Server!"**

**encrypted\_message = encrypt(message, RAB)**

**conn.send(encrypted\_message.encode('utf-8'))**

**server\_socket.close()**

**conn.close()**