Question # 1

a) **Suppose you have received the following encrypted messages from the sender and you have been told that RSA algorithm is used to encrypt this information and the public key to decrypt the message is {7, 187}. Your task is to retrieve the original messages.**
C1 = 16
C2 = 24

b. **Show the process of Diffie-Helman key exchange using a prime 47 and generator 11. Suppose Alice chooses a secret 9 and Bob chooses 16.**

Question # 2

Describe the key development mechanism using RSA when the values of p and q are given to be 7 and 11 respectively? Although there are multiple options for choosing the encryption value 'e', let's choose 7 that fulfill the criteria and then find 'd' accordingly. You should provide all details and outcome should be written in the form of private and public keys. Demonstrate the working of your system by encrypting a number and then retrieving it back using decryption.

Question # 3

a) **Given two prime numbers p=61 and q=53, encrypt and decrypt the message m=10 using RSA**

b) **Follow the following steps using RSA**

1. Choose two primes $p = 11$ and $q = 13$.
2. Use $e = 7$ as the public exponent.
3. Calculate the public and private keys.
4. Encrypt the message $m = 9$.
5. Decrypt the ciphertext to retrieve the original message.

Question # 4

Find out the shared key value using Diffie-Hellman (DH) public-key encryption algorithm for each of following:

a) **p=23 and g=5**
b) **with p=11 and g=2, Alice and Bob choose private keys x=5 and y = 12, respectively.**