Experiment 4: Diffie Hellman Key Exchange algorithm

Aim: Write a program to implement Diffie Hellman Key Exchange Algorithm.

Learning Outcomes:
After completion of this experiment, student should be able to
1. Explain the concept of asymmetric key cryptography
2. Describe working of DH algorithm.
3. List the application of DH algorithm along with its advantage and limitations.

Theory:
The Diffie–Hellman (DH) Algorithm is a key-exchange protocol that enables two parties communicating over public channel to establish a mutual secret without it being transmitted over the Internet.

Algorithm for DH key exchange is given below.

1. Alice and Bob agree on two large prime numbers, n and g. these two prime numbers need not be kept secret and may be shared over the insecure channel.
2. Alice chooses another large random number x, and calculates A such that: $A = g^x \bmod n$
3. Alice sends the number A to Bob.
4. Bob independently chooses another large random integer y and calculates B such that: $B = g^y \bmod n$.
5. Bob sends the number B to Alice.
6. Alice now computes the secret key K1 as follows: $K1 = B^x \bmod n$.
7. Bob now computes the secret key K2 as follows: $K2 = A^y \bmod n$.

Procedure:

1. Write a program to implement DH key exchange algorithm.
2. Accept two prime numbers from the end user and validate user input.
3. Accept two integer numbers x and y from the user.
4. Compute the secret keys, K1 and K2.
5. Display the secret keys.
6. Create a word document for your observation and answer the following questions.
7. Upload your document on Student Portal along with your code.

Note: Code should have proper comments.

Questions:

1. Explain DH key exchange algorithm.
2. List some of the protocols where DH algorithm is used.
3. List advantages and limitations of DH.