Name: Ritesh Pawar

Batch: B4

Subject: CNS Lab

PRN: 2020BTECS00068

**Aim: Diffi-helman key exchange Algorithm**

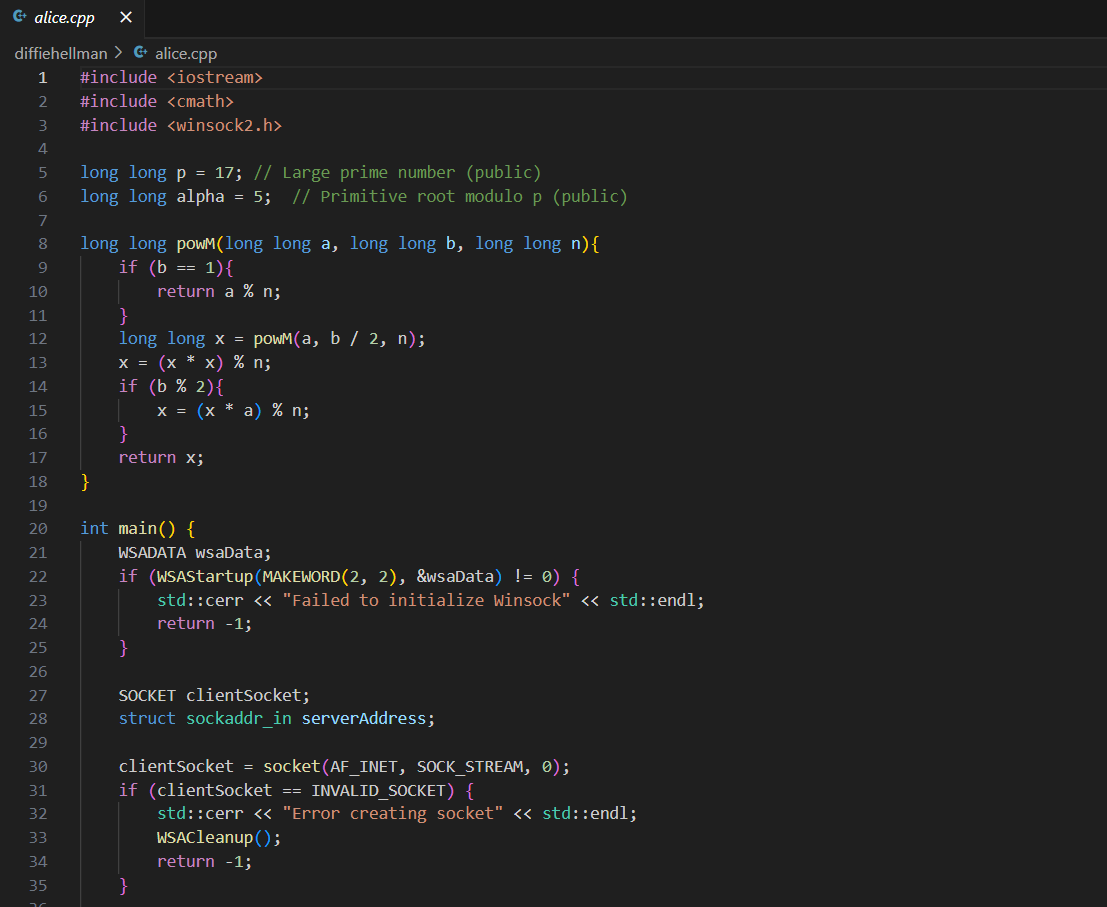
**Theory:**

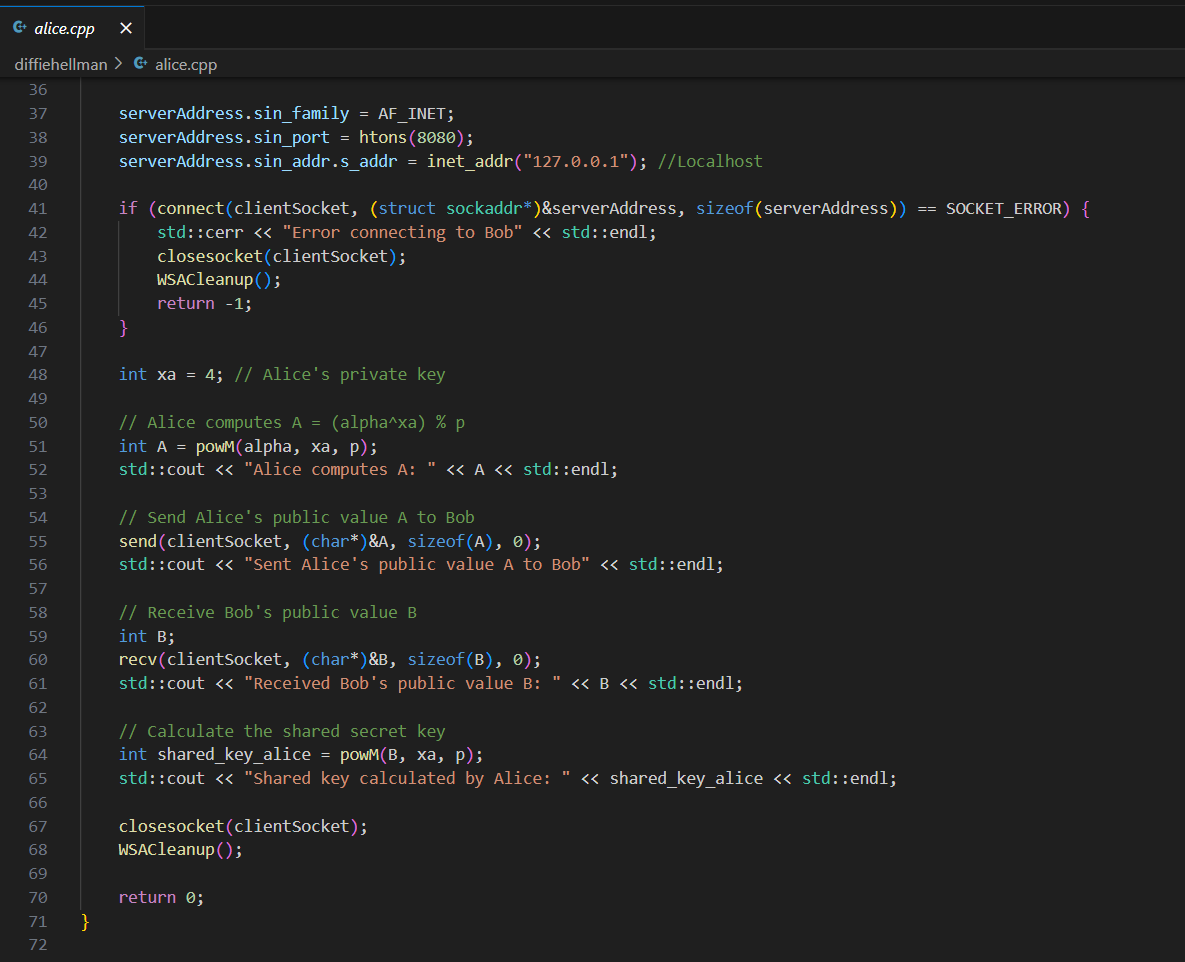
Diffie-Hellman algorithm is one of the most important algorithms used for establishing a shared secret. At the time of exchanging data over a public network, we can use the shared secret for secret communication. We use an elliptic curve for generating points and getting a secret key using the parameters.

1. We will take four variables, i.e., P (prime), G (the primitive root of P), and a and b(private values).
2. The variables P and G both are publicly available. The sender selects a privatevalue, either a or b, for generating a key to exchange publicly. The receiver receives the key, and that generates a secret key, after which the sender and receiver both have the same secret key to encrypt.

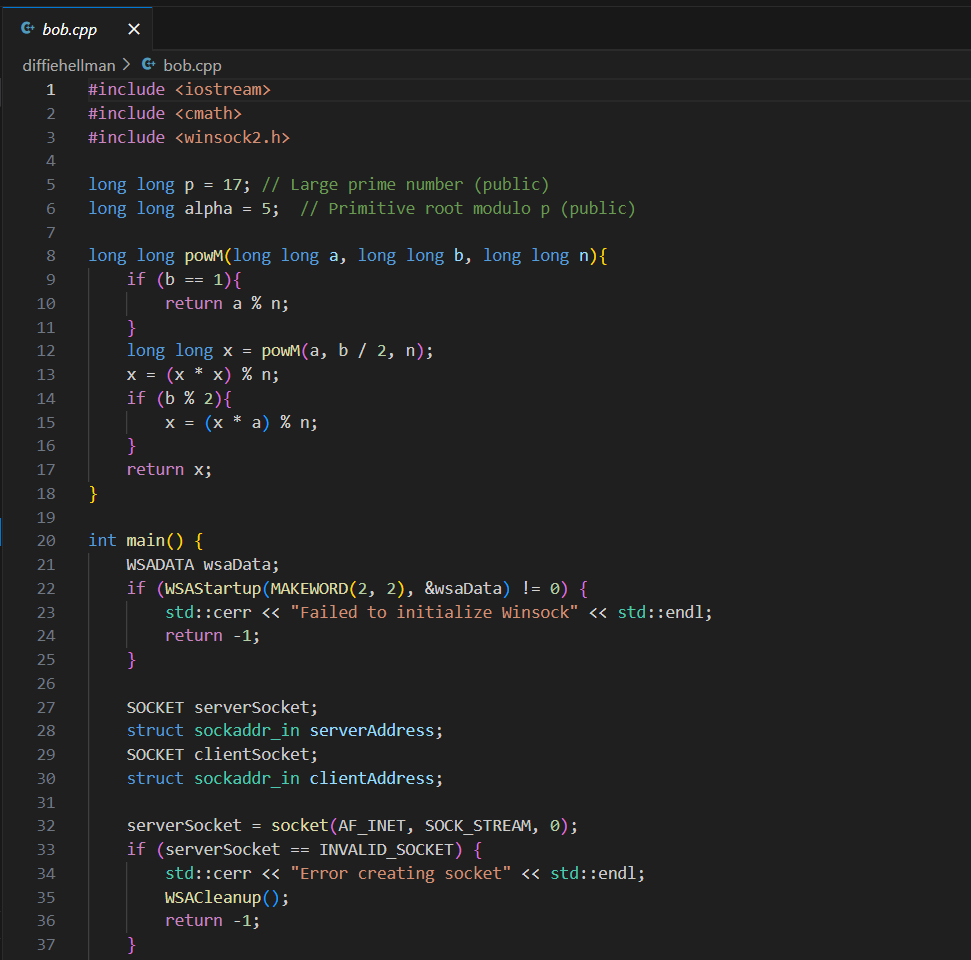
**Code:**

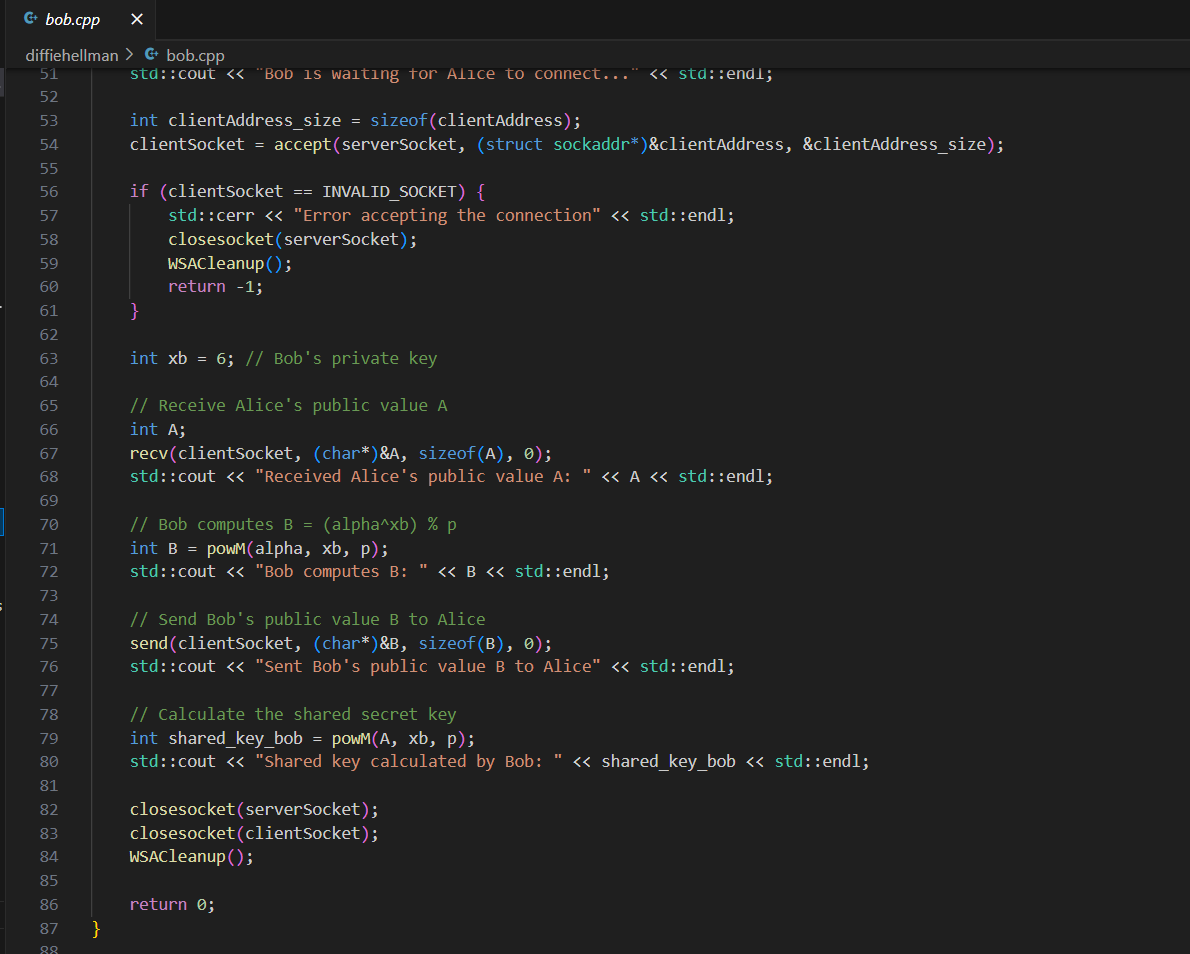
**Alice.cpp**





**Bob.cpp**





**Output:**



