```
class Person:

  #get prime number (q) and primitive root (alpha)
  def __init__(self,prime,root):

    assert root<prime
    self.q = prime
    self.alpha = root
    self.generate_private_key()
    self.generate_public_key()

    #These attributes are modified after key exchange
    self.received = False
    self.y_other = ''


  #private key is a random number between 1 and q-1
  #name mangling to avoid access
  def generate_private_key(self):
    from random import randint
    self.__x_priv = randint(1,self.q-1)


  #public_key = alpha^private_key mod prime
  def generate_public_key(self):
    self.y_pub = self.alpha**self.__x_priv % self.q


  # secret key generated after receiving public key from the other party
  # secret_key = y_other^private_key mod prime
  def generate_secret_key(self):
    self.__s_priv = self.y_other**self.__x_priv % self.q



def key_exchange(person1, person2):
  person1.received, person2.received = True, True
  person1.y_other, person2.y_other = person2.y_pub, person1.y_pub


def generate_secret_key(person1, person2):
  try:
    assert person1.y_pub == person2.y_other
    assert person2.y_pub == person1.y_other
    assert person1.received == True
    assert person2.received == True
    person1.generate_secret_key()
    person2.generate_secret_key()
    assert person1._Person__s_priv == person2._Person__s_priv
  except AssertionError as err:
    print(err)


prime = 8191
```

```
root = 17

print('Prime number =',prime)
print('Primitive root =',root)

# Generate Private Keys
alice = Person(prime, root)
bob = Person(prime, root)
print('Alice Private Key = ',alice._Person__x_priv)
print('Alice Public Key = ',alice.y_pub)
print('Bob Private Key = ',bob._Person__x_priv)
print('Bob Public Key = ',bob.y_pub)
print()

print('...Key Exchange...')
# Exchange Public Keys
key_exchange(alice, bob)

# Generate Secret Keys
generate_secret_key(alice, bob)
print('Alice Shared Key = ',alice._Person__s_priv)
print('Bob Shared Key = ',bob._Person__s_priv)
```

```
Prime number = 8191
Primitive root = 17
Alice Private Key =  3303
Alice Public Key =  2427
Bob Private Key =  5953
Bob Public Key =  549

...Key Exchange...
Alice Shared Key =  616
Bob Shared Key =  616
```