Prg2: date:20-5-2020

2.Write a simple Python program to implement Diffie–Hellman Key Exchange Example

sharedPrime = 23

sharedBase = 5

aliceSecret = 6

bobSecret = 15

print( "Publicly Shared Variables:")

print( " Publicly Shared Prime: " , sharedPrime )

print( " Publicly Shared Base: " , sharedBase )

A = (sharedBase\*\*aliceSecret) % sharedPrime

print( "\n Alice Sends Over Public Chanel: " , A )

B = (sharedBase \*\* bobSecret) % sharedPrime

print("\n Bob Sends Over Public Chanel: ", B )

print( "\n------------\n" )

print( "Privately Calculated Shared Secret:" )

# Alice Computes Shared Secret: s = B^a mod p

aliceSharedSecret = (B \*\* aliceSecret) % sharedPrime

print( " Alice Shared Secret: ", aliceSharedSecret )

bobSharedSecret = (A\*\*bobSecret) % sharedPrime

print( " Bob Shared Secret: ", bobSharedSecret )

Output:

