|  |
| --- |
|  |
| #Write a simple Python program to implement Diffie–Hellman Key Exchange Example |
|  | # Variables Used |
|  | sharedPrime = int(input("\nEnter the value of p(shared prime)")) #23 |
|  | sharedBase = int(input("\nEnter the value of g(shared base)")) #5 |
|  |  |
|  | aliceSecret = int(input("\nEnter the value of a(alice secret)")) #6 |
|  | bobSecret = int(input("\nEnter the value of a(bob secret)")) #15 |
|  |  |
|  | # Begin |
|  | print( "\nPublicly Shared Variables:") |
|  | print( " Publicly Shared Prime: " , sharedPrime ) |
|  | print( " Publicly Shared Base: " , sharedBase ) |
|  |  |
|  | # Alice Sends Bob A = g^a mod p |
|  | A = (sharedBase\*\*aliceSecret) % sharedPrime |
|  | print( "\n Alice Sends Over Public Chanel: " , A ) |
|  |  |
|  | # Bob Sends Alice B = g^b mod p |
|  | B = (sharedBase \*\* bobSecret) % sharedPrime |
|  | print( " 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 ) |
|  |  |
|  | # Bob Computes Shared Secret: s = A^b mod p |
|  | bobSharedSecret = (A\*\*bobSecret) % sharedPrime |
|  | print( " Bob Shared Secret: ", bobSharedSecret ) |
|  |  |