

CRYPTOGRAPHY- LAB-8

NAME: SHLOK KAMATH

REG NO: 21BAI1844

1) DIFFIE HELLMAN KEY ECXHANGE ALGORITHM
CODE:

```
main.py
1- def power(a, b, p):
2-     if b == 1:
3-         return a
4-     else:
5-         return pow(a, b) % p
6
7 # Main function
8- def main():
9     P = 23
10    print("The value of P:", P)
11    G = 9
12    print("The value of G:", G)
13    a = 4
14    print("The private key a for Alice:", a)
15    x = power(G, a, P)
16    b = 3
17    print("The private key b for Bob:", b)
18    y = power(G, b, P)
19    ka = power(y, a, P) # Secret key for Alice
20    kb = power(x, b, P) # Secret key for Bob
21
22    print("Secret key for Alice is:", ka)
23    print("Secret key for Bob is:", kb)
24
25- if __name__ == "__main__":
26    main()
```

OUTPUT:

Output
The value of P: 23
The value of G: 9
The private key a for Alice: 4
The private key b for Bob: 3
Secret key for Alice is: 9
Secret key for Bob is: 9
=== Code Execution Successful ===