**AP25122050004**

**Avisikta Mandal Das**

**Applied Cryptography: Implementation of Diffie-Helman Algorithm**

**Github Link:** <https://github.com/AvisiktaMandalDas/Cryptography_Lab5>

**Code:**

P = 23

G = 9

print("Publicly Shared Variables:")

print(f"P (Prime): {P}")

print(f"G (Primitive Root): {G}\n")

a = 4 # Alice's private key

print(f"Alice's private key (a): {a}")

x = (G \*\* a) % P

print(f"Alice's public key (x): {x}\n")

b = 3 # Bob's private key

print(f"Bob's private key (b): {b}")

y = (G \*\* b) % P

print(f"Bob's public key (y): {y}\n")

ka = (y \*\* a) % P

kb = (x \*\* b) % P

print("Shared Secret Computation:")

print(f"Alice's computed key: {ka}")

print(f"Bob's computed key: {kb}")

if ka == kb:

print(f"\n✅ Shared Secret Key Established Successfully: {ka}")

else:

print("\n❌ Key mismatch! Something went wrong.")

