**Department of Computer Engineering**

**Name of the Student: Parth Das Roll Number: C-111**

**SAP ID: 60004220185 Class: Comps Division: C-2 Batch: 2**

**Subject: Information Security**

**DATE OF PERFORMANCE: 15/02/2025 DATE OF SUBMISION: 15/02/2025**

**EXPERIMENT NO: 4**

**AIM:** To Study and implement RSA Encryption Algorithm

**Theory:**

**SOURCE CODE WITH OUTPUTS:**

g = int(input(f"Enter G : "))

p = int(input(f"Enter P : "))

a = int(input(f"\nEnter A : "))

b = int(input(f"Enter B : "))

print(f"\nG : {g} & P : {p}")

print(f"A : {a} & B : {b}")

X\_a = (g\*\*a) % p

X\_b = (g\*\*b) % p

print(f"\nX(a) : {X\_a} & X(b) : {X\_b}")

print(f"\nA send [X(a) : {X\_a}] to B")

print(f"B send [X(b) : {X\_b}] to A")

A\_x = (X\_a\*\*b) % p

B\_x = (X\_b\*\*a) % p

print(f"\nA(x) : {A\_x} & B(x) : {B\_x}")

print(f"\nA calculate A(x) : {A\_x}")

print(f"B calculate B(x) : {B\_x}")

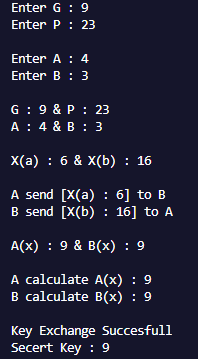
if A\_x == B\_x:

print(f"\nKey Exchange Succesfull\nSecert Key : {A\_x}")

else:

print("Error")

**Output:-**



**CONCLUSION:**

The Diffie-Hellman key exchange is a fundamental cryptographic protocol that enables two parties to securely establish a shared secret key over an insecure channel. It relies on the difficulty of solving the discrete logarithm problem, making it resistant to direct attacks. Although Diffie-Hellman ensures secure key exchange, it does not provide authentication, making it vulnerable to man-in-the-middle attacks if not properly implemented. Despite its limitations, Diffie-Hellman remains a widely used method for secure communication in cryptographic protocols.