**DIFFIE HELLMAN EXCHANGE – MAN IN THE MIDDLE ATTACK**

**BY-**

**AAKRITI MEHROTRA**

**22BCE1954**

**CODE**

**SERVER.PY**

import random

import socket

class Server:

def \_\_init\_\_(self, p, g):

self.p = p

self.g = g

self.b = random.randint(1, p)

self.public\_value = None

self.secret\_key = None

def generate\_public\_value(self):

self.public\_value = (self.g \*\* self.b) % self.p

return self.public\_value

def compute\_secret\_key(self, client\_public\_value):

self.secret\_key = (client\_public\_value \*\* self.b) % self.p

return self.secret\_key

def start(self, host, port):

server\_socket = socket.socket(socket.AF\_INET, socket.SOCK\_STREAM)

server\_socket.bind((host, port))

server\_socket.listen(1)

print(f"Server (Bob) listening on {host}:{port}...")

conn, addr = server\_socket.accept()

print(f"Connected to client (Alice) at {addr}")

bob\_public\_value = self.generate\_public\_value()

conn.send(str(bob\_public\_value).encode())

print(f"Bob's public value (gb): {bob\_public\_value}")

alice\_public\_value = int(conn.recv(1024).decode())

print(f"Received Alice's public value (ga): {alice\_public\_value}")

secret\_key = self.compute\_secret\_key(alice\_public\_value)

print(f"Bob's computed secret key: {secret\_key}")

conn.close()

if \_\_name\_\_ == "\_\_main\_\_":

p = int(input("Enter a prime number (p): "))

g = int(input("Enter a number (g): "))

server = Server(p, g)

server.start("127.0.0.1", 12345)

**CLIENT.PY**

import random

import socket

class Client:

def \_\_init\_\_(self, p, g):

self.p = p

self.g = g

self.a = random.randint(1, p)

self.public\_value = None

self.secret\_key = None

def generate\_public\_value(self):

self.public\_value = (self.g \*\* self.a) % self.p

return self.public\_value

def compute\_secret\_key(self, server\_public\_value):

self.secret\_key = (server\_public\_value \*\* self.a) % self.p

return self.secret\_key

def start(self, host, port):

client\_socket = socket.socket(socket.AF\_INET, socket.SOCK\_STREAM)

client\_socket.connect((host, port))

print(f"Connected to server (Bob) at {host}:{port}")

alice\_public\_value = self.generate\_public\_value()

client\_socket.send(str(alice\_public\_value).encode())

print(f"Alice's public value (ga): {alice\_public\_value}")

bob\_public\_value = int(client\_socket.recv(1024).decode())

print(f"Received Bob's public value (gb): {bob\_public\_value}")

secret\_key = self.compute\_secret\_key(bob\_public\_value)

print(f"Alice's computed secret key: {secret\_key}")

client\_socket.close()

if \_\_name\_\_ == "\_\_main\_\_":

p = int(input("Enter a prime number (p): "))

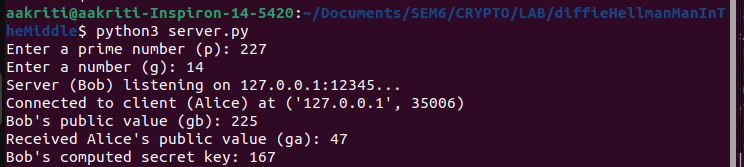
g = int(input("Enter a number (g): "))

client = Client(p, g)

client.start("127.0.0.1", 12345)

**OUTPUT**

**SERVER**

****

**CLIENT**

