Lab 9

MAN IN THE MIDDLE ATTACK

Name: Shlok Kamath

Reg No.: 21BAI1844

Professor Name: Dr. Rajesh R

Subject: Cryptography and network security Lab

Subject Code: BCSE309P

21BAI1844
Shlok Kamath

Code:

```
import random

p = int(input('Enter a prime number : '))
g = int(input('Enter a number : '))


class A:
    def __init__(self):
        # Generating a random private number selected by alice
        self.n = random.randint(1, p)

    def publish(self):
        # generating public values
        return (g**self.n)%p

    def compute_secret(self, gb):
        # computing secret key
        return (gb**self.n)%p


class B:
    def __init__(self):
        # Generating a random private number selected for alice
        self.a = random.randint(1, p)
        # Generating a random private number selected for bob
        self.b = random.randint(1, p)
        self.arr = [self.a,self.b]

    def publish(self, i):
        # generating public values
        return (g**self.arr[i])%p

    def compute_secret(self, ga, i):
        # computing secret key
        return (ga**self.arr[i])%p


alice = A()
bob = A()
eve = B()

# Printing out the private selected number by Alice and Bob
print(f'Alice selected (a) : {alice.n}')
print(f'Bob selected (b) : {bob.n}')
print(f'Eve selected private number for Alice (c) : {eve.a}')
print(f'Eve selected private number for Bob (d) : {eve.b}')
```

```
# Generating public values
ga = alice.publish()
gb = bob.publish()
gea = eve.publish(0)
geb = eve.publish(1)
print(f'Alice published (ga): {ga}')
print(f'Bob published (gb): {gb}')
print(f'Eve published value for Alice (gc): {gea}')
print(f'Eve published value for Bob (gd): {geb}')

# Computing the secret key
sa = alice.compute_secret(gea)
sea = eve.compute_secret(ga,0)
sb = bob.compute_secret(geb)
seb = eve.compute_secret(gb,1)
print(f'Alice computed (S1) : {sa}')
print(f'Eve computed key for Alice (S1) : {sea}')
print(f'Bob computed (S2) : {sb}')
print(f'Eve computed key for Bob (S2) : {seb}')
```

Input and Output: