REG NO : 21BCE1019

NAME : VARUN VETRIVENDAN

CRYPTOGRAPHY LAB ASSIGNMENT – DIFFIE HELMAN WITH MAN IN THE ATTACK

CODE:

```
# Input prime number and primitive root
prime = int(input("Enter the prime number to be considered: "))
root = int(input("Enter the primitive root: "))

# Party1 chooses a secret number
alicesecret = int(input("Enter a secret number for Party1: "))

# Party2 chooses a secret number
bobsecret = int(input("Enter a secret number for Party2: "))
print("\n")

# Attacker intercepts Party1's public key
attacker_public_to_bob = (root ** alicesecret) % prime
print("Attacker intercepts Party1's public key intended for Party2:",
attacker_public_to_bob)

# Attacker intercepts Party2's public key
attacker_public_to_alice = (root ** bobsecret) % prime
print("Attacker intercepts Party2's public key intended for Party1:",
attacker_public_to_alice)
print("\n")

# Attacker can now compute their own shared keys with Party1 and Party2
attacker_key_with_alice = (attacker_public_to_alice ** alicesecret) % prime
attacker_key_with_bob = (attacker_public_to_bob ** bobsecret) % prime

# Both Party1 and Party2 now believe they are communicating securely with each
other,
# but in reality, the attacker is intercepting and possibly altering the
communication.
print("Attacker calculates the shared key with Party1:",
attacker_key_with_alice)
print("Attacker calculates the shared key with Party2:",
attacker_key_with_bob)
print("\n")
```

```
print("Both Alice and Bob are unaware that the attacker has intercepted the communication.")
```

OUTPUT: