Cryptography DA-5

Question

Activity -5

Diffie- Hellman: Simulate the Man- in the -Middle Attack.

Code:-

```
# tom is a hacker or attacker!!
#2 Large prime numbers n and g these numbers are publicly known
n=int(input("Enter the value for n:(Must be a prime value):>>  "))
g=int(input("Enter the value for g:(Must be a prime value):>>  "))


#alice
x=int(input("Enter the value for alice's key:-> "))
A_a=(g**x)%n


#bob
y=int(input("Enter the value for bob's key:-> "))
B_b=(g**y)%n

#tom(hacker)
x_tom=int(input("Enter the value for tom's key :-> "))
y_tom=int(input("Enter the value for tom's key:-> "))
T_a=(g**x_tom)%n
T_b=(g**y_tom)%n
```

```
#Key gen in alice
k1=(T_b**x)%n
#Key gen in bob
k2=(T_a**y)%n
#Key gen in tom
k1_tom=(B_b**x_tom)%n
k2_tom=(A_a**y_tom)%n

print("\n\nAlice's Key "+ str(k1))
print("Tom's key "+ str(k2_tom))
print("\n\nBob's Key "+ str(k2))
print("Tom's key "+ str(k1_tom))
```

Input and Output

```
Enter the value for n:(Must be a prime value):>>  11
Enter the value for g:(Must be a prime value):>>  7
Enter the value for alice's key:-> 3
Enter the value for bob's key:-> 9
Enter the value for tom's key :-> 8
Enter the value for tom's key:-> 6


Alice's Key 9
Tom's key 9


Bob's Key 5
Tom's key 5
```

Name: Aena Verma

ID:- 19BCI0221