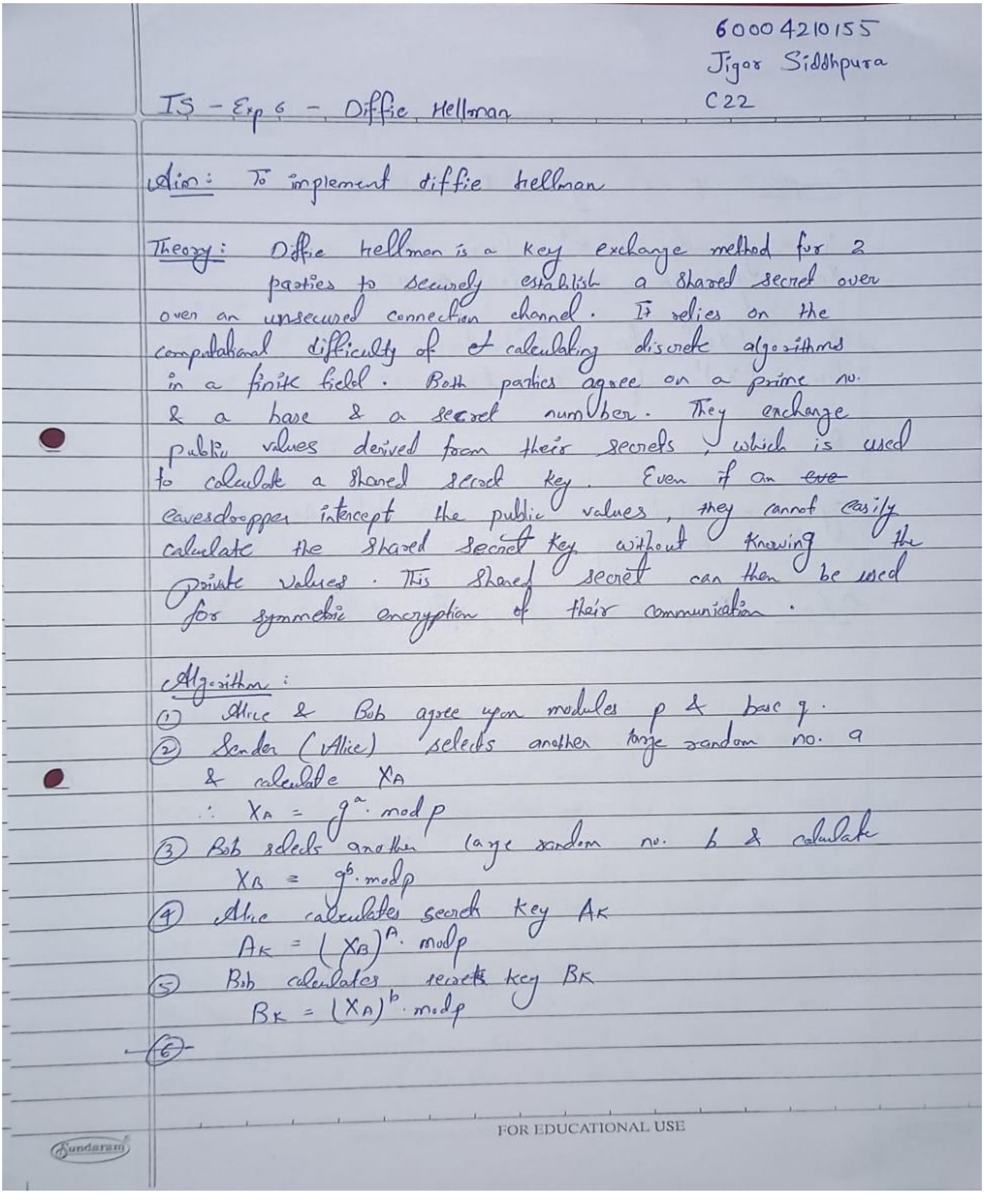
Name: Jigar Siddhpura **SAPID:** 60004200155

DIV: C/C2 **Branch:** Computer Engineering

IS - Experiment 6 - Diffie Hellman



60004210155
Jigar Siddhpura
C22

IS - Exp 6 - Diffie Hellman

Aim: To implement diffie hellman

Theory: Diffie hellman is a key exchange method for 2 parties to securely establish a shared secret over over an unsecured connection channel. It relies on the computational difficulty of ~~of~~ calculating discrete algorithms in a finite field. Both parties agree on a prime no. & a base & a secret number. They exchange public values derived from their secrets, which is used to calculate a shared secret key. Even if an ~~eve~~ eavesdropper intercept the public values, they cannot easily calculate the shared secret key without knowing the private values. This shared secret can then be used for symmetric encryption of their communication.

Algorithm:

1. Alice & Bob agree upon modules p & base g.
2. Sender (Alice) selects another large random no. a & calculate X_A
   $\therefore X_A = g^a \cdot \mod p$
3. Bob selects another large random no. b & calculate
   $X_B = g^b \cdot \mod p$
4. Alice calculates secrets key A_K
   $A_K = (X_B)^A \cdot \mod p$
5. Bob calculates secrets key B_K
   $B_K = (X_A)^b \cdot \mod p$
6.

Example: $p = 23$, $g = 5$, $A = 4$, $b = 3$

$X_A = g^a \cdot \text{mod}\, p = 5^4 \cdot \text{mod}\, 23 = 4$

$X_B = g^b \cdot \text{mod}\, p = 5^3 \cdot \text{mod}\, 23 = 10$

$A_K = (X_B)^a \cdot \text{mod}\, p = 10^4 \cdot \text{mod}\, 23 = 18$

$B_K = (X_A)^b \cdot \text{mod}\, p = 4^3 \cdot \text{mod}\, 23 = 18$

$A_K = B_K$

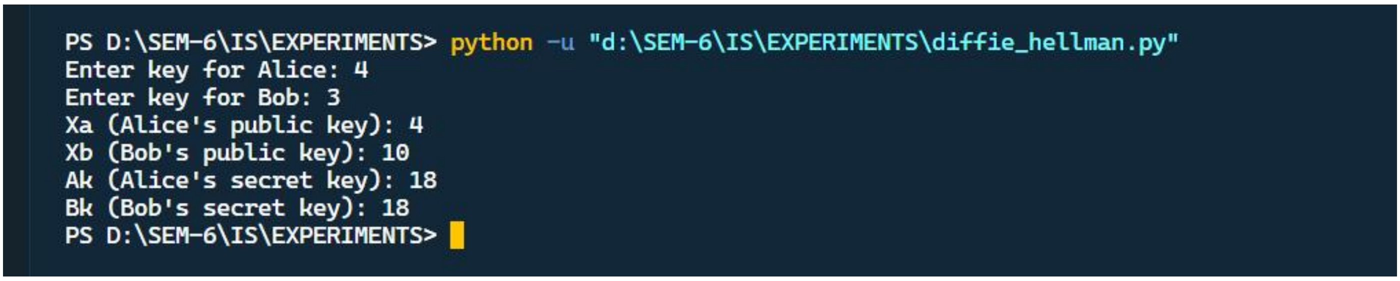
They can now start communicating with each other using this Shared secret key.

Conclusion: Thus, we implemented Diffie Hellman.

CODE

```
p = 23
g = 5

# Alice's private key
private_key_A = int(input("Enter key for Alice: "))
# Bob's private key
private_key_B = int(input("Enter key for Bob: "))
# Calculate Xa (Alice's public key)

Xa = (g ** private_key_A) % p
# Calculate Xb (Bob's public key)
Xb = (g ** private_key_B) % p

# Calculate Ak (Alice's secret key)
Ak = (Xb ** private_key_A) % p
# Calculate Bk (Bob's secret key)
Bk = (Xa ** private_key_B) % p

print("Xa (Alice's public key):", Xa)
print("Xb (Bob's public key):", Xb)
print("Ak (Alice's secret key):", Ak)
print("Bk (Bob's secret key):", Bk)
```

OUTPUT



```
PS D:\SEM-6\IS\EXPERIMENTS> python -u "d:\SEM-6\IS\EXPERIMENTS\diffie_hellman.py"
Enter key for Alice: 4
Enter key for Bob: 3
Xa (Alice's public key): 4
Xb (Bob's public key): 10
Ak (Alice's secret key): 18
Bk (Bob's secret key): 18
PS D:\SEM-6\IS\EXPERIMENTS> 
```