Reg.no: 210701092

Experiment no: 2b Date: 27/2/24	Diffie Hellman Key Exchange Algorithm

AIM:

To Write the C program to Exchange Keys Using Diffie Hellman key ~~Exan~~ Exchange Algorithm

ALGORITHM:

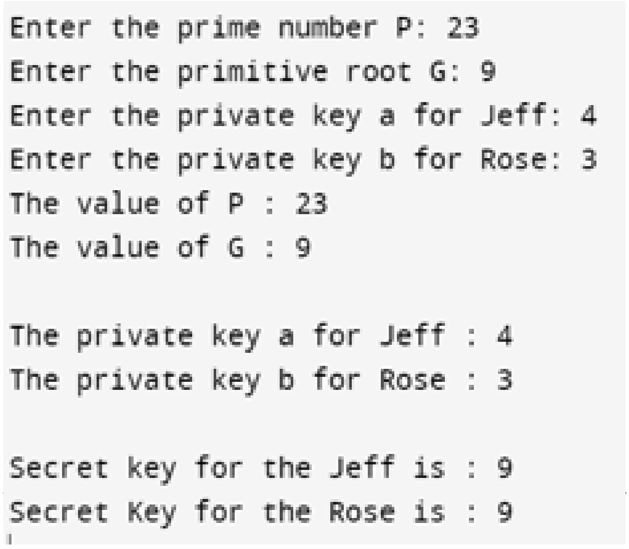
```
Step 1: START
Step 2: Get the two prime Numbers P and G
Step 3: Get the Private key a and b from
        the User
Step 4: perform Calculations to generate key
        $x = G^a \bmod p$ and $y = G^b \bmod p$
Step 5: After Exchanging key, User 1 Recives key y
        ~~And Exchange~~ After Exchanging keys,
        User 2 Recives key x
Step 6: If the Secret key of the Both
        Users are Same, then the Message
        Is Verified
Step 7: STOP
```

Exp 2b : Diffie-Hellman Key Exchange Algorithm

Code:

```
#include <math.h>
#include <stdio.h>

long long int power(long long int a, long long int b,
long long int P)
{
    if (b == 1)
        return a;
    else
        return (((long long int)pow(a, b)) % P);
}

int main()
{
    long long int P, G, x, a, y, b, ka, kb;

    printf("Enter the prime number P: ");
scanf("%lld", &P);

    printf("Enter the primitive root G: ");
scanf("%lld", &G);

    printf("Enter the private key a for Jeff: ");
scanf("%lld", &a);
    x = power(G, a, P);

    printf("Enter the private key b for Rose: ");
scanf("%lld", &b);
    y = power(G, b, P);

    ka  =  power(y,  a,  P);
kb = power(x, b, P);

    printf("The value of P : %lld\n", P);
    printf("The value of G : %lld\n\n", G);

    printf("The private key a for Jeff : %lld\n", a);
    printf("The private key b for Rose : %lld\n\n", b);

    printf("Secret key for the Jeff is : %lld\n", ka);
    printf("Secret Key for the Rose is : %lld\n", kb);

    return 0;
}
```

Output:



```
Enter the prime number P: 23
Enter the primitive root G: 9
Enter the private key a for Jeff: 4
Enter the private key b for Rose: 3
The value of P : 23
The value of G : 9

The private key a for Jeff : 4
The private key b for Rose : 3

Secret key for the Jeff is : 9
Secret Key for the Rose is : 9
```