Diffie Hellman

Software: Scilab

```
clc;

g=7;

p=23;

printf("\n The resuls are as follows:\n\n");

x=3;

y=6;

R1=modulo(g^x,p);

R2=modulo(g^y,p);

printf("1)Alice choose x=%d & calculates R1=%d\n\n 2)Bob chooses y=%d & calculates R2=%d\n\n
3)Alice sends the number %d to Bob \n\n 4)Bob sends the number %d to Alice \n\n",x,R1,y,R2,R1,R2);

K_Alice =modulo((R2)^x,p);

K_Bob=modulo((R1)^y,p);

K_Final=modulo(g^(x*y),p);

printf('5)Alice calculates the symmetric key K=%d \n\n6)Bob calculates the symmetric key
k=%d\n\n7)K_Final=%d \n\n',K_Alice,K_Bob,K_Final);
```

Result:

```
 The resuls are as follows:
1)Alice choose x=3 & calculates R1=21
 2)Bob chooses y=6 & calculates R2=4
 3)Alice sends the number 21 to Bob
 4)Bob sends the number 4 to Alice
5)Alice calculates the symmetric key K=18
6)Bob calculates the symmetric key k=18
7)K_Final=18
```