**EXP 5**

**Program:**

clc;

g=7;

p=23;

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

x=3;

y=6;

R1=modulo(g^x,p);

R2=modulo(g^y,p);

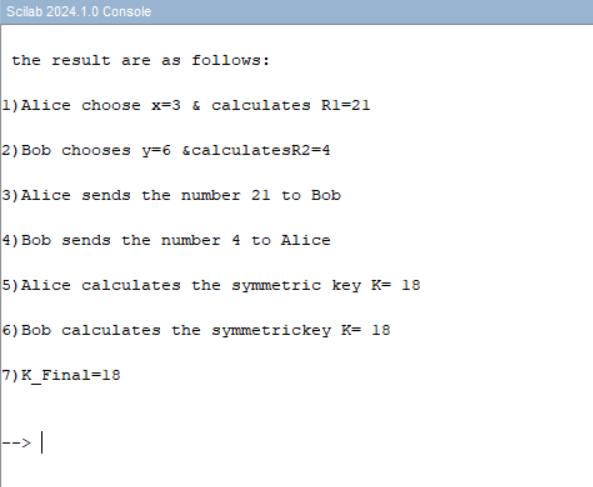
printf("1)Alice choose x=%d & calculates R1=%d\n\n2)Bob chooses y=%d &calculatesR2=%d\n\n3)Alice sends the number %d to Bob \n\n4)Bob sends the number %d to Alice\n\n",x,R1,y,R2,R1,R2);

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 symmetrickey K= %d\n\n7)K\_Final=%d\n\n",K\_Alice,K\_Bob,K\_Final);

**Output: **