Name: Abeer Ur Rahim

Id: 15849

IS LAB 08

long long power(long long base, long long exp,long long mod){

long long result=1;

int i;

for (i = 0; i < exp; i++)

{

result=(result\*base)%mod;

}

return result;

}

int main(){

long long p=6;

long long g =5;

//secret

long long a=6,b=15,c=13, d=9;

//A send A=g\*a%p

long long A= power(g,a,p);

//b send b=g\*b%p

long long B=power(g,b,p);

//C send c=g^c %p

long long C=power(g,c,p);

//D send d=g^d %p

long long D=power(g,d,p);

//alice get (B^a)^c%p

long long AB = power(B,a,p);

long long ABC=power(AB,c,p);

//bob get (C^b)^a%p

long long CB = power(C,b,p);

long long CBA = power(CB,a,p);

//carol get (A^c)^b%p

long long AC = power(A,c,p);

long long ACB = power(AC,b,p);

//david get (A^d)^b%p

long long AD = power(A,d,p);

long long ADB = power(AD,c,p);

printf("shared key(alice): %lld\n",ABC);

printf("shared key(bob): %lld\n",CBA);

printf("shared key(carol): %lld\n",ACB);

printf("shared key(david): %lld\n",ADB);

if (ABC==CBA==ACB==ADB)

{

printf("key shared succesfully");

}

else{

printf("key not shared succesfully");

}

getchar();

return 0;

}

