**Information Security**

* **Practical 9: Implement a digital signature algorithm.**

**CODE:**

#include<stdio.h>

#include<conio.h>

#include<math.h>

long int distance(long int m,long int b)

{

int a1=1,a2=0,a3=m,b1=0,b2=1,b3=b,q,t1,t2,t3;

while(1)

{

if(b3==0)

{

return 0;

}

if(b3==1)

{

if(b2<0)

b2+=m;

return b2;

}

q=a3/b3;

t1=a1-(q\*b1);

t2=a2-(q\*b2);

t3=a3-(q\*b3);

a1=b1;

a2=b2;

a3=b3;

b1=t1;

b2=t2;

b3=t3;

}

}

long int powerr(long int a, long int j, long int c)

{

int f,i;

f=1;

for(i=1;i<=j;i++)

{

f=(f\*a)%c;

}

f=f%c;

return f;

}

int main()

{

long int p,q,g,x,hm,k,y,r,s,s1,w,u1,u2,v,v1,v2,v3;

printf("\nDigital Signeture\n");

printf("\n-------------------------\n");

printf("Enter the value of p:");

scanf("%ld",&p);

printf("Enter the value of q:");

scanf("%ld",&q);

printf("Enter the value of g:");

scanf("%ld",&g);

printf("Enter the value of x:");

scanf("%ld",&x);

printf("Enter the value of hm:");

scanf("%ld",&hm);

printf("Enter the value of k:");

scanf("%ld",&k);

printf("\n-------------------------\n");

y=powerr(g,x,p);

printf("\nValue of y:%ld",y);

r=powerr(g,k,p);

r=r%q;

printf("\nValue of r:%ld",r);

s=distance(q,k);

s1=(hm+(x\*r));

s=(s\*s1)%q;

printf("\nValue of s:%ld",s);

w=distance(q,s);

printf("\nSignature (r,s):%ld %ld",r,s);

printf("\nvalue of w:%ld",w);

u1=(hm\*w)%q;

printf("\nValue of u1:%ld",u1);

u2=(r\*w)%q;

printf("\nValue of u2:%ld",u2);

v=powerr(g,u1,p);

v1=powerr(y,u2,p);

v2=(v\*v1)%p;

v3=v2%q;

printf("\nValue of v:%ld",v3);

printf("\n-------------------------\n");

getch();

return 0; }

**Output:**

