PSEUDORANDOM NUMBERS:

Pseudorandom numbers are used in [simulation](http://dictionary.reference.com/browse/simulation) and [encryption](http://dictionary.reference.com/browse/encryption). They arepseudorandom not random because the sequence eventually repeatsexactly and is entirely determined by the initial conditions.   
One of the simplest algorithms is   
x[i+1] = (a \* x[i] + c) mod m

SOURCE CODE:

#include<stdio.h>

int main(){

int x[1000],a,m,c;

int i,j,count=0;

printf("Enter initial value x[0]= ");

scanf("%d",&x[0]);

printf("Enter the value of a ,c ,m : ");

scanf("%d%d%d",&a,&c,&m);

for(i=0;;i++){

x[i+1]=(a\*x[i]+c)%m;

count++;

printf(" %d",x[i+1]);

if(x[0]==x[i+1])

break;

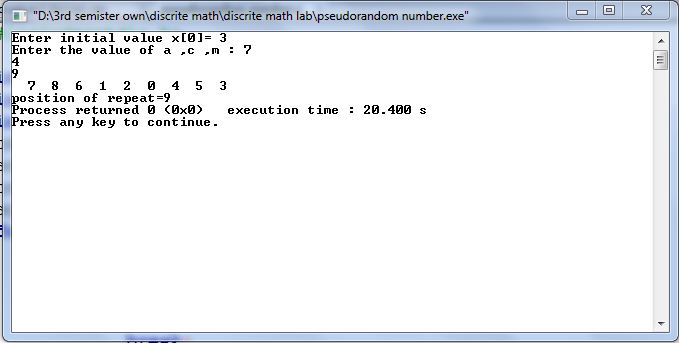
}

printf("\nposition of repeat=%d",count);

return 0;

}

OUTPUT:



CRYPTOLOGY:

The process of determining the original message from the encrypted message is called decryption.

f(p)=(p-k) mod 26

for encryption:

f(p)=(p+k) mod 26

SOURCE CODE:

#include<bits/stdc++.h>

using namespace std;

int main()

{

char str1[100],str2[100];

int k,len,x,y,p;

cout<<"enter a string:\n";

gets(str1);

cout<<"enter the value of k:\n";

cin>>k;

len=strlen(str1);

cout<<"ENCRYPTION\n";

for(int i=0;i<len;i++)

{

if(str1[i]==32)

{

cout<<" ";

str1[i]=32;

}

if(str1[i]>=65 && str1[i]<=90){

p=str1[i]-65;

y=(p+k)%26;

y=y+65;

printf("%c",y);

str1[i]=y;

}

if(str1[i]>=97 && str1[i]<=122){

p=str1[i]-97;

y=(p+k)%26;

y=y+97;

printf("%c",y);

str1[i]=y;

}

}

cout<<endl;

cout<<"DECRYPTION\n";

for(int i=0;i<len;i++)

{

if(str1[i]==32)

{

cout<<" ";

}

if(str1[i]>=65 && str1[i]<=90){

p=str1[i]-65;

if(p==0)

y=88;

else if(p==1)

y=89;

else if(p==2)

y=90;

else{

y=(p-k)%26;

y=y+65;

}

printf("%c",y);

}

if(str1[i]>=97 && str1[i]<=122){

p=str1[i]-97;

if(p==0)

y=120;

else if(p==1)

y=121;

else if(p==2)

y=122;

else{

y=(p-k)%26;

y=y+97;

}

printf("%c",y);

}

}

return 0;

}

OUTPUT:

