Assignment three for 60-564 (Security and Privacy on the Internet)

9.16 Use the fast exponentiation algorithm of Figure 9.7 to determine 5^{596} mod 1234. Show the steps involved in the computation.

Answer:
My name is JIAYING SHI, so I mapped each character from ASCII code into Decimal format, like the following:

ASCII CODE	DECIMAL NO.	ASCII CODE	DECIMAL NO.
J	74	N	78
I	73	G	71
A	65	S	83
Y	89	H	72
I	73	I	73

J(74) I(73) A(65) Y(89) I(73) N(78) G(71) S(83) H(72) I(73)
Total is 751
The sequence number is counted by (751 mod 23) + 1=16
So I picked up the Question No.16. I implemented the fast exponentiation algorithm and the following lists the results.
As I set:
Input a=5, b=596, n=1234

i=9, b[i]=1, c=1, f=5
i=8, b[i]=0, c=2, f=25
i=7, b[i]=0, c=4, f=625
i=6, b[i]=1, c=9, f=937
i=5, b[i]=0, c=18, f=595
i=4, b[i]=1, c=37, f=569
i=3, b[i]=0, c=74, f=453
i=2, b[i]=1, c=149, f=591
i=1, b[i]=0, c=298, f=59
i=0, b[i]=0, c=596, f=1013

Final result = 1013

The above shows the result and the status of each specific step.

```
#include <stdio.h>
#define SIZE 32

int EMA(int,int,int, int[]);
int main ()
{    int a = 5, b = 596, n = 1234;
     int f=0, k=0, i=0, remainder=0;
     int binaryNumber[SIZE];
     for(i=0;i<SIZE;i++)
          binaryNumber[i]=0;
     printf("input a=%d, b=%d, n=%d\n\n",a,b,n);

     if(b<=1)
     {    binaryNumber[0]=b;
          k=1;
     }
     else
     {    for(i=0;i<SIZE;i++)
          {    binaryNumber[i]= b%2;
               b = b>>1;
          }
          k=SIZE;
          for(i=SIZE-1;i>=0;i--)
          {    if(binaryNumber[i]==0)
                    k--;
               else       break;
          }
     }
     f= EMA(a,k-1,n,binaryNumber);
     printf("\nfinal result = %d\n",f);
}
int EMA(int a, int k, int n, int b[])
{    int c=0,f=1,i;
     for (i=k; i>=0; i--)
     {    c*=2;
          f=(f*f)%n;
          if(b[i]==1)
          {    c+=1;
               f=(f*a)%n;
          }
          printf("i=%d, b[i]=%d, c=%d, f=%d\n",i,b[i],c,f);
     }
     return f;
}
```