Name: Kejal Kumari
Roll No: CS21M506
ASSIGNMENT-2

Q1 8.2

a) $X_{n+1} = (aX_n) \bmod 2^4$

We know that the above is of form
$X_{n+1} = (aX_n + c) \bmod m$, here $c=0$ & $m=2^4$

Max period $= \frac{m}{4} = \frac{2^4}{4} = 2^{4-2} = 4$

b) Value of a should be :

$a = 3 + 8k$ or
$a = 5 + 8k$
where K is an integer.

(c) Seed X_0 must be odd.

8.4

$X_{n+1} = (6X_n) \bmod 13$

Let $X_0 = 1$.

$X_1 = 6 \bmod 13 = 6$

$X_2 = 36 \bmod 13 = 10$

$X_3 = 60 \bmod 13 = 8$

$X_4 = 48 \bmod 13 = 9$

$X_5 = 54 \bmod 13 = 2$

$X_6 = 12 \bmod 13 = 12$

$X_7 = 72 \bmod 13 = 7$

$X_8 = 42 \bmod 13 = 3$

$X_9 = 18 \bmod 13 = 5$

$X_{10} = 30 \bmod 13 = 4$

$X_{11} = 24 \bmod 13 = 11$

$X_{12} = 66 \bmod 13 = 1$

$X_{13} = 6 \bmod 13 = 6$

$\therefore$ Sequence is $\{1, 6, 10, 8, 9, 2, 12, 7, 3, 5, 4, 11, 1\}$

All the digits are unique in this sequence,
$\therefore$ Its a full period ~~seq.~~ generator.

$X_{n+1} = (7X_n) \bmod 13$

$X_0 = 1$

$X_1 = 7 \bmod 13 = 7$

$X_2 = 49 \bmod 13 = 10$

$X_3 = 70 \bmod 13 = 5$

$X_4 = 35 \bmod 13 = 9$

$X_5 = 63 \bmod 13 = 11$

$X_6 = 77 \bmod 13 = 12$

$X_7 = 84 \bmod 13 = 6$

$X_8 = 42 \bmod 13 = 3$

$X_9 = 21 \bmod 13 = 8$

$X_{10} = 56 \bmod 13 = 4$

$X_{11} = 28 \bmod 13 = 2$

$X_{12} = 14 \bmod 13 = 1$

Sequence is : $\{1, 7, 10, 5, 9, 11, 12, 6, 3, 8, 4, 2\}$.

$\therefore$ Its a full period generator.

8.5

Q3

```
#include <stdio.h>
#include <math.h>
#include <string.h>
#include <stdlib.h>

void main (int argc, char* argv)
{
 int i = 0, s ;
 int j, count = 0;
 douple pi ;
 double z;

 printf ("Enter the number of trials");
 scanf ("%d", & i);
 printf ("Enter the seed value :");
 scanf ("%d", s);

 srand (s);
 count = 0;
 for (j=0; j< i; i++)
  {
   x = (double) rand ()/RAND_MAX;
   y = (double)rand()/RAND_MAX;
   z = x*x + y*y;
   if (z <=1) count ++;
   }
   pi = (double) count/i*4;
   ~~printf(~~
  }
```

Q4 8.6

RC4 Question

We will use a key of length 255 bytes. The first 2 bytes are $K[0] = K[1] = 0$.

$K[2] = 255$

$K[3] = 254$

$K[4] = 253$

⋮

$K[255] = 2$.

Q5 8.7

a) Storing x, y & S requires $8+8+(256 * 8)$ bits

$= 8+8+(2048)$

$= 2064$ bits

b) The number of states is $[256! \times 256^2]$

$= 2^{1700}$

Hence, we require 1700 bits.

8.8

a) By taking the first 80 bits of $V||C$, we will have vector V.

Message after decrypt by company : $RC4(V||K) \oplus C$

b) If $V_i = V_j \rightarrow$ if the adversary sees this, he knows that the same key was used to encrypt both m_i & m_j.

(c) Key is fixed, so after sending $\sqrt{\frac{\pi}{2} 2^{80}}$ where 80 bit V is used, $\sqrt{\frac{\pi}{2} 2^{80}} \approx 2^{40}$ messages are sent, we expect the same V, & hence same key stream to be used more than once.

(d) The key should change before 2^{40} messages are sent using the same key.