NAME : SRICHARAN R

ROLL NO: CS21M520

SOB : CS6530 - Assignment - 2.

Q1, Page 280, probl - 8.2:

a) what is the max period obtainable from the following generator?

$$x_{n+1} = (ax_n) \bmod 2^4.$$

where $m = 2^4$ and $c = 0$

$$\Rightarrow p = \frac{m}{4} = \frac{2^4}{4} = 2^{4-2} = 4.$$

b) $a = 3 + 8k$ or

$a = 5 + 8k$ for $k = 0, 1, 2, \ldots$

So a must be 3 or 5.

c) What restrictions are required on the seed?

x_0 seed should be odd.

Q2, (Page 280, prob-8.4):

With the L.C.A (Linear Congruential Algo)

Some Parameters that provides full period does not mean it gives 100% randomization.

For eg,

$$x_{n+1} = (6x_n) \bmod 13$$

$$x_{n+1} = (7x_n) \bmod 13$$

Assume $x_0 = 1$, So

(i) $x_{n+1} = (6x_n) \bmod 13$

$x_0 = 1$, $x_1 = (6) \bmod 13$, $x_2 = (6 \cdot 6) \bmod 13 = 10$

$x_3 = (6 \cdot 10) \bmod 13 = 8$

$x_4 = (6 \cdot 8) \bmod 13 = 9$

$x_5 = (6 \cdot 9) \bmod 13 = 2$

$x_6 = (6 \cdot 2) \bmod 13 = 12$

$x_7 = (6 \cdot 12) \bmod 13 = 7$

$x_8 = (6 \cdot 7) \bmod 13 = 3$

$x_9 = (6 \cdot 3) \bmod 13 = 5$

$x_{10} = (6 \cdot 5) \bmod 13 = 4$

$x_{11} = (6 \cdot 4) \bmod 13 = 11$

$x_{12} = (6 \cdot 11) \bmod 13 = 1$

$x_{13} = (6 \cdot 1) \bmod 13 = 6$

$x_{13} = x_1$ [Hence the Sequence repeats]

Finite Sequence.

b) $x_{n+1} = (7x_n) \bmod 13$

$x_0 = 1$

$x_1 = (7) \bmod 13 = 7$

$x_2 = (7 \cdot 7) \bmod 13 = 10$

$x_3 = (7 \cdot 10) \bmod 13 = 5$

$x_4 = (7 \cdot 5) \bmod 13 = 9$

$x_5 = (7 \cdot 9) \bmod 13 = 11$

$x_6 = (7 \cdot 11) \bmod 13 = 12$

$x_7 = (7 \cdot 12) \bmod 13 = 6$

$x_8 = (7 \cdot 6) \bmod 13 = 3$

$x_9 = (7 \cdot 3) \bmod 13 = 8$

$x_{10} = (7 \cdot 8) \bmod 13 = 4$

$x_{11} = (7 \cdot 4) \bmod 13 = 2$

$x_{12} = (7 \cdot 2) \bmod 13 = 1$

$\Rightarrow x_{12} = x_0$ [Finite Sequence repeats].

Which is more random?

F1 = {1, 6, 10, 8, 9, 2, 12, 7, 3, 5, 4, 11, 1, 6, ...}

F2 = {1, 7, 10, 5, 9, 11, 12, 6, 3, 8, 4, 2, 1, ...}

F2 has higher Sequence list. So F2 is more random Compared to F1.

Q4 - Page 281, prob 2.6:

What RC4 key value will leaves unchanged during intialized.?

After intial Compatation of S, entries will be equal to 0 to 255 in ascending order.

Let key length be 255 bytes.

K[0] = 0

K[1] = 0

K[2] = 255

K[3] = 254

:

K[255] = 2.

Q5: (Page 281, prob 8.7)

RC4 has a secret internal state which is a permutation of all possible values of the Vector S and two indices i and j

a) using straight forward scheme to store the internal state, how many bits are used?

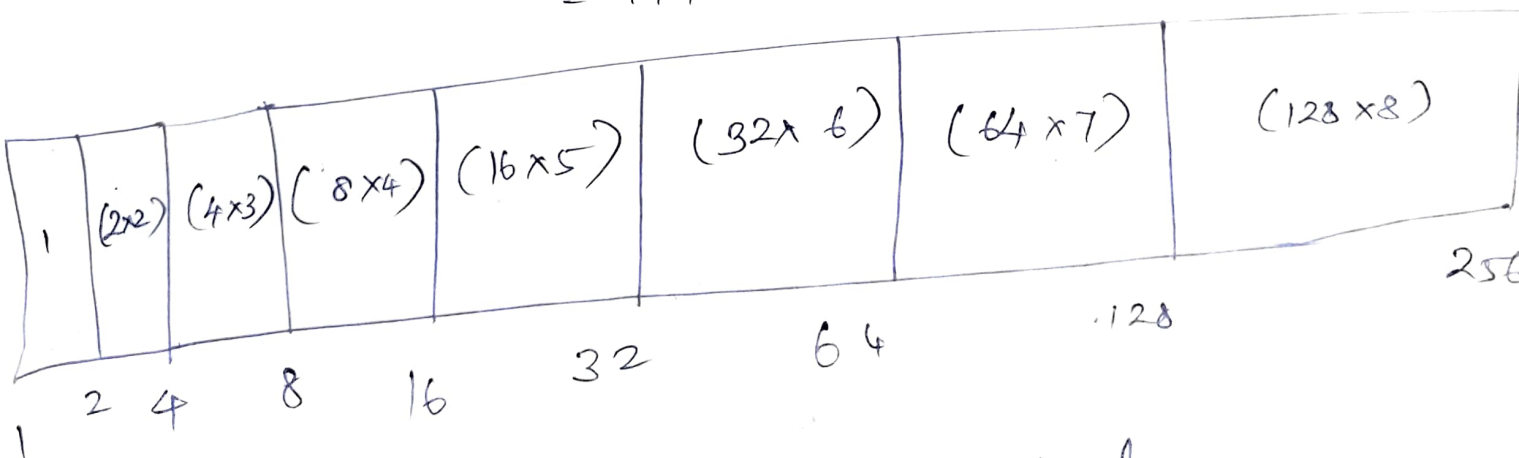
Save x, y and S, that requires

$8 + 8 + (256 \times 8)$

$= 2064$ bits.

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

$= 1791$



$\approx$ 1700 bits are required.

Q6: page 281, prob: 8.8:

Alice and Bob agree to Communicate privately via email using a Scheme based on RC4, but want to avoid using a new Secret key for each transmission, Alice and Bob privately agree on a 128 bit key k. To encrypt a message m, Consisting of string of bits, following procedure is used

1. choose a random 80-bit value v.
2. Generate a cipher text
$$C = RC4(v \| k) \oplus m$$
3. Send the bit string $(v \| c)$

a) Suppose Alice uses this procedure to Send a message m to bob. Describe how bob can recover the message or m from $(v \| c)$ using k.

b) Adversary observes Several values $(v_1 \| c_1), (v_2 \| c_2) \ldots\ldots$ transmitted

between Alice and Bob, how can he/she determine when the same key stream has been used to encrypt two messages?

(c) Approximately how many messages can Alice expect to send before the same key stream will be used twice? Use the result from the birthday pardox described in Appendix U.

(d) What does this imply about the lifetime of the key c (ie, the number of messages that can be encrypted using K)?

a) By taking the first 80 bits of V||C, we obtain the initialization Vector V. Since V, C, K are known, the message can be recovered (i.e decrypted) by computing: RC4(V||K) ⊕ C.

b) If the adversary observes that $V_i = V_j$ for distinct i, j the he/she knows that the same key stream

was used to encrypt both m_i and m_j.

(c) Since the key is fixed, the key stream varies with the choice of 80 bit V, which is selected randomly. Thus after approximately $\sqrt{\frac{\pi}{2} \cdot 2^{80}} \approx 2^{40}$. messages are sent, we expect the same V, hence the same key stream, to be used more than once.

(d) The key K should be changed sometime before 2^{40} messages are sent.

Q3: (page 281, P-8.5):

Please see the program that i have attached the source code in email along with output.