Assignment 2.

8.2. (a) What is the maximum period obtained from $X_{n+1} = aX_n \bmod 2^4$

(b) What should be value of a.

(c) What are restrictions on seed.

* Assume $X_n = 1$ $a = 1$

$X_{n+1} = 1 \bmod 16$.

$\{1\}$ periodic.

* $a = 2$; $X_n = 1$

$X_{n+1} = 2 \bmod 16 = 2$.

$X_{n+1} = 4 \bmod 16 = 4$

$X_{n+1} = 8 \bmod 16 = 8$

$X_{n+1} = 16 \bmod 16 = 0$

$= \{2, 4, 8, 0\} \cdots$

* $a = 3$ $X_n = 1$

Sequence $= \{3, 9, 11, 1 \cdots\}_{\text{Periodic}}$ — (1)

* $a = 4$ $X_n = 1$

Sequence $= 4, 0, 0 \cdots$

* $a = 5$ $X_n = 1$

Sequence $= \{5, 9, 13, 1 \cdots\}$ periodic. — (2)

* $a = 6$ $X_n = 1$

Sequence $= 6, 4, 8, 0, 0, 0 \cdots$

* $a = 7$ $X_n = 1$

Sequence $= \{7, 1\}$ periodic

* $a = 8$ $X_n = 1$

Sequence $= 8, 0, 0 \cdots$

* $a = 9$ $X_n = 1$

Sequence $= \{9, 1\}$ periodic

* $a = 10 \quad x_n = 1$

Sequence = 10, 4, 8, 0, 0 ....

* $a = 11, \quad x_n = 1$

Sequence
$= \{11, 9, 3, 1 ..\}$ periodic. — ③

* $a = 12 \quad x_n = 1$

Sequence = 12, 0 ....

* $a = 13 \quad x_n = 1$

Sequence = $\{13, 9, 5, 1\}$ periodic. — ④

* $a = 14 \quad x_n = 1$

Sequence = 14, 4, 8, 0

* $a = 15 \quad x_n = 1$

Sequence = $\{15, 1\}$ periodic.

Recompute $a - 1 = 15$ for $x_n = 2$

we get

x_{n+1}

* For $a = 1 \quad x_n = 2$

Sequence = 2.

* For $a = 2 \quad x_n = 2$

Sequence 4, 8, 0 .....

* For $a = 3 \quad x_n = 2$

sequence = $\{6, 2\}$ periodic.

* For $a = 4 \quad x_n = 2$

Sequence = 8, 0 ....

* For $a = 5 \quad x_n = 2$

Sequence = $\{10, 2\}$ periodic.

* For $a = 6 \quad x_n = 2$

Sequone = 12, 8, 0 .....

* For $a = 7 \quad x_n = 2$

Sequence = $\{14, 2\}$ periodic.

* For $a = 8 \quad x_n = 2$

Sequence = 0, 0 ....

* For a = 9 $x_n = 2$
  Sequence = 2, 2 ....
* For a = 10 $x_n = 2$
  Sequence = 4, 8, 0 .....
* For a = 11 $x_n = 2$
  Sequence = {6, 2} periodic.
* For a = 12 $x_n = 2$
  Sequence = 8, 0 .....
* For a = 13, $x_n = 2$
  Sequence = {10, 2} periodic.
* For a = 14 $x_n = 2$
  sequence = 12, 8, 0 ....
* For a = 15 $x_n = 2$
  Sequence = {14, 2} periodic.

(a) From the above sequence max period is 4.
ie.
$$x_{n+1} = (a x_i + c) \bmod m$$
When m is a power of 16 has period
$$= \frac{m}{4} = \frac{16}{4} = 4$$

(b) What should be the value of a.
From ① ② ③ and ④ value of a for max period is $a = 3$; $a = 5$; $a = 11$; $a = 13$
General result $a = 3 + 8k$ or $5 + 8k$ for integer k. for odd value of x_0

(c) What are the restriction on seed
Seed has to be odd as for even seed period has reduced to 2

8.4) with the linear Congruential algorithm, a choice of parameter that provides a full period does not necessarily provide a good randomization

Consider $X_{n+1} = 6X_n \bmod 13$.

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

Write out the sequence to show both are full period. Which one is more random to you.

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

$X_n = 1$

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

$X_{n+1} = 6 \times 6 \bmod 13 = 10$

$X_{n+1} = 6 \times 10 \bmod 13 = 8$

$X_{n+1} = 6 \times 8 \bmod 13 = 9$

$X_{n+1} = 6 \times 9 \bmod 13 = 2$

$X_{n+1} = 6 \times 2 \bmod 13 = 12$

$X_{n+1} = 6 \times 12 \bmod 13 = 7$

$X_{n+1} = 6 \times 7 \bmod 13 = 3$

$X_{n+1} = 6 \times 3 \bmod 13 = 5$

$X_{n+1} = 6 \times 5 \bmod 13 = 4$

$X_{n+1} = 6 \times 4 \bmod 13 = 11$

$X_{n+1} = 6 \times 11 \bmod 13 = 1$

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

Period = 13

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

$X_n = 1$

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

$X_{n+1} = 7 \times 7 \bmod 13 = 10$

$X_{n+1} = 7 \times 10 \bmod 13 = 5$

$X_{n+1} = 7 \times 5 \bmod 13 = 9$

$X_{n+1} = 7 \times 9 \bmod 13 = 11$

$X_{n+1} = 7 \times 11 \bmod 13 = 12$

$X_{n+1} = 7 \times 12 \bmod 13 = 6$

$X_{n+1} = 7 \times 6 \bmod 13 = 3$

$X_{n+1} = 7 \times 3 \bmod 13 = 8$

$X_{n+1} = 7 \times 8 \bmod 13 = 4$

$X_{n+1} = 7 \times 4 \bmod 13 = 2$

$X_{n+1} = 7 \times 2 \bmod 13 = 1$

Seq = {1, 7, 10, 5, 9, 11, 12, 6, 3, 8, 4, 2, 1 ...}; Period = 13

Second sequence is less random as the last part has a more predictable sequence where the number is preceding number divide by 2.

8.6 What RC_4 key will leave S unchanged during initialization. That is after initial permutation of S. the entries of S will be equal to the values 0 through 255 in ascending order

Initial permutation of S

```
j = 0
for i = 0 to 255 do
    j = (j + S[i] + T[i]) mod 256;
    Swap (S[i], S[j])
```

(a) For i=0 j has to 0.

$$j \leftarrow (0 + S[0] + T[0]) \bmod 256$$

$$S[0] = 0$$

$$\Rightarrow (0 + 0 + T[0]) \bmod 256 = 0$$

ie $\underline{T[0] = 0}$

(b) For i=1 j has to be 1

$$j \leftarrow (j_{previous} + S[i] + T[i]) \bmod 256$$

$$(0 + S[1] + T[1]) \bmod 256$$

$$(0 + 1 + T[1]) \bmod 256 = 1$$

$$\Rightarrow \underline{T[1] = 0}$$

(c) For $(i = 2)$; j has to be 2

$$j \leftarrow (j_{previous} + S[i] + T[i]) \bmod 256$$

$$j \leftarrow (1 + S[2] + T[2]) \bmod 256$$

$$(3 + T[2]) \bmod 256 = 2$$

$$T[2] + 3 = 258 \Rightarrow T[2] = \underline{\underline{255}}$$

(d) For $(i = 3)$; j has to be 3.

$$j \leftarrow (j_{previous} + S[i] + T[j]) \bmod 256$$

$$(2 + S[3] + T[3]) \bmod 256 = 3$$

$$5 + T[3] = 259$$

$$T[3] = \underline{\underline{254}}$$

IIIrdly $T[255] = 2$

use a key of length 255 bytes.

$K[0] = K[1] = 0$

$K[2] = 255$ .... $K[255] = 2$

$K[3] = 254$

8.7) RC4 has a secret state which is a permutation of all possible values of S, i, j

(a) Using a straightforward scheme to store interal states, how many bits are used.

i = 8 bits

j = 8 bits

S = 256 byte.

Total bits = 8 + 8 + 256 × 8 bits

= 2064

(b) Suppose we think of it from pain of view of how much information is represented by state. In that case, we need to find how many different states are there and log to base 2 to find out the information. Using this approach, how many bits are needed.

Total ways by which i can take values = $256 = 2^8$

Total combinations of i and j =

i, j can come with any state of S. $256 \times 256 = 256^2$

possible states in S = 256!

so total possible states

$$= 256! \times 256^2$$

Bits of information $= \frac{\log(256^2 \times 256!)}{\log 2} \approx 1700$

8.8) Alice and bob agree to communicate privately via email using a scheme based on RC_4. but wanted to avoid a new secret key for each transmission. Alice and bob agree on a 128 bit key k.

To encrpt a message m, following protocol is used

(1) Choose a random 80 bit value v.

(2) Generate $C = RC_4(V||K) \oplus m$

(3) Send bit$(V||C)$.

(a) Suppose Alice uses this procedure to send a message m to bob. Describe how bob can recover message m from $(V||C)$ using k.

Since V is a part of C, by taking first 80 bits of C V can be obtained

Since V, k, C are known to both parties message can be recovered by

$$RC_4(V||K) \oplus C$$

$$= RC_4(V||K) \oplus (m \oplus RC_4(V||K))$$

$$= m$$

(b) If an adversary observes several value $(V_1||C_1)$ $(V_2||C_2)$ ..... transmitted between Alice and bob. how can he determine when same key stream has been used to encrpt 2 message

If adversary observes V_i and V_j and notice $V_i = V_j$ for distinct i and j he will know that same key stream was used to encrpt both messages m_i and m_j

(c) Approximately how many message can Alice expect to send before the same key stream will be used twice. Refer to birthday paradox in Appendix U.

As per birthday paradox if m bit hash value if we pick data blocks at random we can expect to find two data blocks with same hash within $2^{m/2}$ attempts.

By the same principle, since key stream is fixed here

$$C = RC_4(V||K) \oplus m$$

variability is provided only by V with a 80 bit V vector. So by birthday paradox, after $2^{80/2} = 2^{40}$ message are sent, we can expect the same V to be used more than once.

(d) What does it imply about the lifetime of the key K (i.e the number of message that can be encrpled using K).

The key has to be changed before 2^{40} messages are sent, to avoid the same key stream getting used