Assignment -2	NARESH GUNDU	Roll no: CS21M514

8.2 What is the maximum period obtainable from following generators?

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

Answer (a) If $m = 2^k$ maximum period is 2^{k-2}

So max. period $= 2^{4-2} = 2^2 = 4$

(b) What should be the value of a?

Ans: a must be 5 or 11

(c) Ans) The seed must be odd

8.3 Let us start with seed 1. $X_0 = 1$

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

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

(1) → 1, 6, 10, 8, 9, 2, 12, 7, 3, 5, 4, 11, 1, ...

(2) → 1, 7, 10, 5, 9, 11, 12, 6, 3, 8, 4, 2, 1, ...

In 2nd generator O/P, second half contain less random

8.6 What RC4 Key Value leave S unchanged during initialization? That is, after the initial permutation of S, The entries of S will be equal to the values from 0 through 255 in ascending order?

Answer

Use a key length of 255 bytes.

First two bytes are zero. i.e. $K[0] = K[1] = 0$.

Thereafter we have $K[2] = 255$, $K[3] = 254$, ... $K[255] = 2$

8.7 (a) how many bits are used to store internal state?

Ans: Simply store i, j, and S $8 + 8 + 256 \times 8 = 2064$ bits

(b) How many bits would need to represent the state?

Ans: The number of States is

$$[256! \times 256^4] \simeq 2^{1700}$$

So 1700 bits are required.

8.8 (1) Choose a random 80 bit value V.

(2) $C = RC4(V||K) \oplus m$

(3) Send the bit string $(V||C)$

(a) First 80 bits of $V||C$ = we obtain V.

Since V, C, K are known.

$m = RC4(V||K) \oplus C$

8.8 (b) If the adversary observes $V_i = V_j$ then he/she knows that the same key stream was used to encrypt both m_i & m_j. In this case, the messages m_i & m_j are vulnerable to the type of cryptanalysis carried out in part (a).

8.8 (c) Since the key is fixed, the key stream varies with the choice of the the 80-bit V, which is selected randomly. Thus, after approximately 2^{40} messages are sent, we expect the same V, and then the same key stream, to be used more than once.

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