Assignment 2

Question 8.2

a. What is the maximum period obtainable from the following generator?

$$X_{+1} = (aX\quad) \bmod 2^4$$

b. What should be the value of a?

c. What restrictions are required on the seed?

Solution:

a. For m = 2^k we can get the maximum period of 2^(k-2) = 2^(4-2) = 2^2 = 4.

b. THe value of a can be 3,5,11,13

Let us take the example of X0 = 1 and a = 3

The sequence will be of the form {3,9,11,1,3,9,…} period is 4

c. The seed must be odd and less than m i.e < 16

Question 8.4 With the linear congruential algorithm, a choice of parameters that provides a full period does not necessarily provide a good randomization. For example, consider the following two generators: Xn+1 = (11Xn) mod 13

Xn+1 = (2Xn) mod 13

Write out the two sequences to show that both are full periods.

Which one appears more random to you?

Solution: Let us start with an initial seed of 1.

The first generator yields the sequence:

11,4,5,3,7,12,2,9,8,10,6,1,11,4, . . Period of 12.

The second generator yields the sequence:

2,4,8,3,6,12,11,9,5,10,7,1,2,4, . . . Period of 12

First one appears more random to me based on number spacing.

Question 8.6 What RC4 key value will 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.

Solution:

Use a key of length 255 bytes. The first two bytes are zero; that is K[0] = K[1] = 0. Thereafter, we have: K[2] = 255; K[3] = 254; … K[255]= 2.

Question 8.7 RC4 has a secret internal state which is a permutation of all the possible values of the vector S and the two indices i and j.

a. Using a straightforward scheme to store the internal state, how many bits are used?

b. Suppose we think of it from the point of view of how much information is represented by the state. In that case, we need to determine how many different states there are, then take the log to base 2 to find out how many bits of information this represents. Using this approach, how many bits would be needed to represent the state?

Solution:

a. Simply we will store i, j and S, which requires 8 + 8 + (256 × 8) = 2064 bits

b. The number of states is [256! × 256^2] = 2^1700. Therefore, 1700 bits are required to represent the information for these states

Question 8.8 Alice and Bob agree to communicate privately via email using a scheme based on RC4, but they 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 a string of bits, the following procedure is used.

1. Choose a random 64-bit value v
2. Generate the ciphertext 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 m from (v || c) using k.

b. If an adversary observes several values (v1 ||c1), (v2 || c2), … 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 paradox described in Appendix U.

d. What does this imply about the lifetime of the key k (i.e., the number of messages that can be encrypted using k)?

Solution:

a. By taking the first 64 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) $\oplus$ c.

b. If the adversary observes that vi = vj for distinct i, j then he/she knows that the same key stream was used to encrypt both mi and mj.

c. Since the key is fixed, the key stream varies with the choice of the 64-bit v, which is selected randomly. Thus, after approximately   messages are sent, we expect the same v, and hence the same key stream, to be used more than once.

d. The key k should be changed sometime before 2^32 messages are sent