CS6530 - ASSIGNMENT 2

THARUN VK
CS21M508

1) (a) What is the maximum period obtainable for the following generator?

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

Ans:

Let's assume $X_0 = 1$

a can take one of 2^4 values. Consider each value:

a		Period
1	→	{1, 1}
2	→	{2, 4, 8, 0}
3	→	{3, 9, 11, 1}
4	→	{4, 0}
5	→	{5, 9, 13, 1}
6	→	{6, 4, 8, 0}
7	→	{7, 1}
8	→	{8, 0}
9	→	{9, 1}
10	→	{10, 4, 8, 0}
11	→	{11, 9, 3, 1}
12	→	{12, 0}
13	→	{13, 9, 5, 1}
14	→	{14, 4, 8, 0}
15	→	{15, 1}

∴ we can say that the maximum period is 4.

Also $\frac{2^4}{4} = 4$.

(b) What should be the value of 'a'?

Ans: The values of a can be 3, 5, 11 or 13.

In general $a = 3+8k$ or $5+8k$.

(c) What restrictions are required on the seed?

Ans: Consider an even seed

$X_0 = 2$.

The maximum is 2 when the seed is even.

∴ The seed has to be odd to get maximum period, which is 4 in our case.

2) With the linear congruential algorithm, a choice of parameters that provides a full period doesn't necessarily provide a good randomization. Consider the following 2 generators:

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

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

Write out the 2 sequences to show that both are full period. Which one appears more random to you?

Ans: Let's consider $X_0 = 1$

1st generator

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

$X_1 = 6 \bmod 13 = 6$

$X_2 = 36 \bmod 13 = 10$

$X_3 = 60 \bmod 13 = 8$

$X_4 = 48 \bmod 13 = 9$

$X_5 = 54 \bmod 13 = 2$

$X_6 = 12 \bmod 13 = 12$

$X_7 = 72 \bmod 13 = 7$

$X_8 = 42 \bmod 13 = 3$

$X_9 = 18 \bmod 13 = 5$

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

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

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

2nd generator

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

$X_1 = 7 \bmod 13 = 7$

$X_2 = 49 \bmod 13 = 10$

$X_3 = 70 \bmod 13 = 5$

$X_4 = 35 \bmod 13 = 9$

$X_5 = 63 \bmod 13 = 11$

$X_6 = 77 \bmod 13 = 12$

$X_7 = 84 \bmod 13 = 6$

$X_8 = 42 \bmod 13 = 3$

$X_9 = 21 \bmod 13 = 8$

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

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

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

Sequence 2 contains patterns which are multiples
For example: {1,2,6,3} and {8,4,2,1}

∴ We can say that "Sequence 1" is more random.

3) What RC_4 key value will leave S unchanged during initialization? That is, after initial permutation of S, the entries of S will be equal to the values from 0 through 255 in ascending order

Ans:

Initialization logic of RC_4:

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

S can be unchanged if $j = i$ in every iteration.
T[i] is the key of length 256.
The below key config will ensure $j = i$

T[0] = 0
T[1] = 0
T[2] = 255
T[3] = 254
⋮
T[255] = 2

i.e $$T[i] = \begin{cases} 0 & | \ i = 0, 1 \\ 257 - i & | \ i = 2 \text{ to } 255 \end{cases}$$

∴ This key will leave S unchanged during initialization.

4) RC4 has a secret internal state which is a permutation of all the possible values of the vector S and the 2 indices i & j

(a) Using a straightforward scheme to store internal state, how many bits are used?

Ans: In RC4 algorithm a variable 1-256 bytes key T is used to initialize a 256-byte vector S from S[0] ··· S[255].

Number of bytes in total in internal state = i + j + S.

= 1 byte + 1 byte + 256 bytes.

= 2064 bits.

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

Ans: Number of states = $256 \times 256 \times 256!$

Total no. of bits = $\log_2(256^2 \times 256!)$

$= 16 + \log_2(256!)$

$= 16 + \frac{\ln(256!)}{\ln 2}$

$= \frac{256\ln(256) - 256}{\ln 2} + 16.$

$\approx$ 1700 bits.

5) 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 & Bob privately agree on a 128 bit key K. To encrypt a message m, consisting of a string of bytes, the following procedure is used.

1) Choose a random bit value V (80-bit)
2) Generate a cipher text $c = RC_4(V||K) \oplus m$.
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 message m from (V||c) using K.

Ans: By considering first 80 bits of V||c we get initialization vector V.

Since V, c, K are known, the message can be decrypted by:

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

(b) If an adversary observes several values $(V_1||c_1)$, $(V_2||c_2)$ transmitted b/w Alice & Bob how can he/she determine when same key stream was used to encrypt 2 messages?

Ans: If the adversary knows that $V_i = V_j$ for unique i, j then he knows that the same key stream was used to encrypt m_i and m_j.

Thus message becomes vulnerable & can be cracked.

(c) Approx. how many messages can Alice except to send before the same key stream will be used twice? Use result from birthday paradox

Ans: The key stream varies with selection of 80 bit V as key K is fixed.

∴ No. of bits to be encrypted using same key = 2^{40}

∴ No. of messages Alice can send

$= 2^{40}$.

(d) What does this imply about lifetime of key K?

Ans: lifetime of key K = No. of message that can be encrypted with same key K.

$= 2^{40}$.