CS6530 - Cryptography Basics

Vaishnav. J
EE20M544

Assignment 2

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

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

b) What should be the value of a?

c) What restrictions are required on the seed?

Ans → Consider $x_0 = 1$

1) $a = 1 \Rightarrow \{1, 1, 1, 1 -- \}$
2) $a = 2 \Rightarrow \{2, 4, 8, 0, 0 -- \}$
3) $a = 3 \Rightarrow \{3, 9, 11, 1, -- \} \Rightarrow$ Period $= 4$
4) $a = 4 \Rightarrow \{4, 0, 0 --- \}$
5) $a = 5 \Rightarrow \{5, 9, 13, 1 -- \} \Rightarrow$ Period $= 4$
6) $a = 6 \Rightarrow \{6, 4, 8, 0, 0 -- \}$
7) $a = 7 \Rightarrow \{7, 1, 7, 1 -- \}$
8) $a = 8 \Rightarrow \{8, 0, 0 --- \}$
9) $a = 9 \Rightarrow \{9, 1, 9, 1 -- \}$
10) $a = 10 \Rightarrow \{10, 4, 8, 0, 0 -- \}$
11) $a = 11 \Rightarrow \{11, 9, 3, 1, 11, -- \} \Rightarrow$ Period $= 4$
12) $a = 12 \Rightarrow \{12, 0, 0 --- \}$
13) $a = 13 \Rightarrow \{13, 9, 5, 1, 13 -- \} \Rightarrow$ Period $= 4$
14) $a = 14 \Rightarrow \{14, 4, 8, 0, 0 -- \}$
15) $a = 15 \Rightarrow \{15, 1, 15, 1 -- \}$

a) Maximum period $= \frac{2^4}{4} = 4$ // (Also verified above)

b) Value of a as obtained above $= 3, 5, 11, 13$

In general : $a = 3 + 8K$ or $5 + 8K$ where K is an integer.

c) Consider an even seed : $x_0 = 2$

1) $a = 1 \Rightarrow \{2, 2, 2 \ldots\}$

2) $a = 2 \Rightarrow \{4, 8, 0, 0 \ldots\}$

3) $a = 3 \Rightarrow \{6, 2, 6, 2 \ldots\}$

4) $a = 4 \Rightarrow \{8, 0, 0, \ldots\}$

5) $a = 5 \Rightarrow \{10, 2, 10, 2 \ldots\}$

⋮

11) $a = 11 \Rightarrow \{6, 2, 6, 2 \ldots\}$

12) $a = 12 \Rightarrow \{8, 0, 0 \ldots\}$

13) $a = 13 \Rightarrow \{10, 2, 10, 2 \ldots\}$

⋮

∴ When seed is even, in no case we can see maximum period as shown above.

∴ Seed has to be odd.

---

2) 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 :

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

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

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

Ans

Consider an initial seed $x_0 = 1$.

Sequence 1

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

$X_1 = 6 \bmod 13 = 6$

$X_2 = 36 \bmod 13 = 10$

$X_3 = 60 \bmod 13 = 8$

$X_4 = 48 \bmod 13 = 9$

$X_5 = 54 \bmod 13 = 2$

$X_6 = 12 \bmod 13 = 12$

$X_7 = 72 \bmod 13 = 7$

$X_8 = 42 \bmod 13 = 3$

$X_9 = 18 \bmod 13 = 5$

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

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

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

Sequence 2

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

$X_1 = 7 \bmod 13 = 7$

$X_2 = 49 \bmod 13 = 10$

$X_3 = 70 \bmod 13 = 5$

$X_4 = 35 \bmod 13 = 9$

$X_5 = 63 \bmod 13 = 11$

$X_6 = 77 \bmod 13 = 12$

$X_7 = 84 \bmod 13 = 6$

$X_8 = 42 \bmod 13 = 3$

$X_9 = 21 \bmod 13 = 8$

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

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

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

Sequence 1 is $\{13, 6, 10, 8, 9, 2, 12, 7, 3, 5, 4, 11, 1 \ldots\}$

Sequence 2 is $\{7, 10, 5, 9, 11, 12, 6, 3, 8, 4, 2, 1 \ldots\}$

Sequence 1 appears more random because seq 2 contains div by 2 patterns like $\{12, 6, 3\}$, $\{8, 4, 2, 1\}$.

3) What RC_4 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.

Ans: RC_4 algorithm outputs a key stream.

Initialization part logic is as below:

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

To leave S unchanged, $j = i$.

Key values are stored in $T[i]$ which is of length 256.

$S[i]$ is also initialized to i.

For above configuration:

$T(0) = 0$

$T(1) = 0$

$T(2) = 255$

$T(3) = 254$

$T(4) = 253$

$\vdots$

$T(255) = 2$

$$\therefore \quad T(i) = \begin{cases} 0 \; ; & i = 0, 1 \\ 257 - i \; ; & i = 2 \text{ to } 255 \end{cases}$$

The above RC_4 key value 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 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?

Ans

a) In the RC4 algorithm, a variable key-length of the form 1 to 256 bytes (8 to 2048 bits) is used to initialize a 256-byte state vector S with elements S[0], S[1] --- S[255]. RC4 stores permutation of all possible values of vector S along with 2 indices i and j.

$\therefore$ Number of bytes stored in internal state $= i + j + S$

$= 1 \text{ byte} + 1 \text{ byte} + 256 \text{ bytes}$

$= 8 + 8 + 2048$

$= 2064$ bits

b) Number of states $= 256! \times 256 \times 256$

Number of bits $= \log_2(256! \times 256 \times 256)$

$= \log_2(256!) + 16$

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

$= \dfrac{256 \ln(256) - 256}{\ln 2} + 16$ (By Stirling's Approx)

$= 1678.67 + 16$

≈ 1700 bits

5) Alice and Bob agree to communicate privately via email using a scheme based on RC_4, 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 a string of bits, 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 a 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 $(V_1 \| C_1), (V_2 \| C_2)$ -- 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.

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

Ans

a) 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 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 the message becomes vulnerable and can be cracked.

c) The key stream varies with selection of 80 bit v as key K is fixed.

$\therefore$ No of bits to be encrypted using same key $= 2^{40}$

$\therefore$ Number of messages Alice can send before same key stream used twice $= 2^{40}$.

d) Lifetime of key K = No of message that can be encrypted with same key K

$= 2^{40}$