IIT MADRAS

Indian Institute of Technology Madras

M.Tech Computer Science Information security.

Cryptography Basic.(CS6530)

Assignment-2.

Roll Number - CS21M515

Name – Ayub Shaikh.

Batch Year-2021

Select "C:\Users\DELL\Desktop\IIT Mtech\Crypto\newProg\PseudorandomNumbersVerification\bin\Debug\PseudorandomNumbersVerification.exe"

Assignment :- 2

8.2 What is maximum period obtainable from the following generators?

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

a) **Answer:** A widely used tech is linear congruent method. The algo is parameterised with 4 numbers.

m the modulus $m > 0$
a the multiplier $0 < a < m$
c the increment $0 \le c < m$
x_0 the starting value or seed $0 \le X_0 < m$

For example when $a = 5$ & $x_0 = 1$

$x_1 = (5 \times 1) \bmod 16 = 5$
$x_2 = (5 \times 5) \bmod 16 = 9$
$x_3 = (5 \times 9) \bmod 16 = 13$
$x_4 = (5 \times 13) \bmod 16 = 1$
$x_5 = (5 \times 1) \bmod 16 = 5$
$x_6 = (5 \times 5) \bmod 16 = 9$
$x_7 = (5 \times 9) \bmod 16 = 13$
$x_8 = (5 \times 13) \bmod 16 = 1$

and Example $a = 3$ & $x_0 = 1$

$x_1 = (3 \times 1) \bmod 16 = 3$
$x_2 = (3 \times 3) \bmod 16 = 9$
$x_3 = (3 \times 9) \bmod 16 = 11$
$x_4 = (3 \times 11) \bmod 16 = 1$
$x_5 = (3 \times 1) \bmod 16 = 3$
$x_6 = (3 \times 3) \bmod 16 = 9$
$x_7 = (3 \times 9) \bmod 16 = 11$

So values are getting repeated after 4 values it means it is having maximum period is 4

which is $2^{4-2} = 4$ - max period.

b) What should be value of a.

= a must be 5 or 11. (from calculation)

c) what restrictions required on seed.

= ~~The seed must be odd number.~~

from above calculation we can conclude seed must be odd.

8.4

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

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

Write out two sequences to show which one is more random.

Answer:-

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

- Lets start with seed = 1 $x_0 = 1$

$x_1 = (6) \bmod 13 = 6$

$x_2 = (6\times6) \bmod 13 = 36 \bmod 13 = 10$

$x_3 = (6\times10) \bmod 13 = 60 \% 13 = 8$

$x_4 = (6\times8) \bmod 13 = 48 \bmod 13 = 9$

$x_5 = (6\times9) \bmod 13 = 54 \bmod 13 = 2$

$x_6 = (6\times2) \bmod 13 = 12 \bmod 13 = 12$

$x_7 = (6\times12) \bmod 13 = 72 \bmod 13 = 7$

$x_8 = (6\times7) \bmod 13 = 42 \bmod 13 = 3$

$x_9 = (6\times3) \bmod 13 = 18 \bmod 13 = 5$

$x_{10} = (6\times5) \bmod 13 = 30 \bmod 13 = 4$

$x_{11} = (6\times4) \bmod 13 = 24 \bmod 13 = 11$

$x_{12} = (6\times11) \bmod 13 = 66 \bmod 13 = 1$

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

- Lets start with seed = 1 $x_0 = 1$

$x_1 = (7\times1) \bmod 13 = 7$

$x_2 = (7\times7) \bmod 13 = 49 \bmod 13 = 10$

$x_3 = (7\times10) \bmod 13 = 70 \% 13 = 5$

$x_4 = (35) \bmod 13 = 9$

$x_5 = (63) \bmod 13 = 11$

$x_6 = (7\times11) \bmod 13 = 12$

$x_7 = (84) \bmod 13 = 6$

$x_8 = (42) \bmod 13 = 3$

$x_9 = (21) \bmod 13 = 8$

$x_{10} = (7\times8) \bmod 13 = 4$

$x_{11} = (28) \bmod 13 = 2$

$x_{12} = (14) \bmod 13 = 1$

Date
Page

1* So The random Number generator sequence for $X_{n+1} = (6 X_n) \bmod 13$

is ⇒ 1, 6, 10, 8, 9, 2, 12, 7, 3, 5, 4, 11, 1

2* Random Number sequence for

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

is ⇒ 1, 7, 10, 5, 9, 11, 12, 6, 3, 8, 4, 2, 1.

In above Sequence because the patterns evident in the 2nd half of the latter Sequence so we mostly consider this is to be less random than the First sequence

First $X_{n+1} = (6 X_n) \bmod 13$ is more random than $X_{n+1} = (7 (X_n) \bmod 13$

Q. 8.6 What RC4 key value will leave S unchanged during initilization - - -

- - - - - - - - 0 through 255 in ascending order

Answer ⇒ RC4 is a stream cipher designed in 1987 by Ron Rivest for RSA security. It is a variable key size stream cipher with byte oriented operations. This algo is based on random permutation.

A variable length key of form 1 to 256 byte (8 to 2048 bits) is used to initilize a 256 byte vector S. which is S[0], S[1], ... S[255]

use a key length 255 bytes.
So the first two bytes are zero
that is -

$K[0] = 0$ &

$K[1] = 0$.

Therefore we have

$K[2] = 255$, $K[3] = 254$, $K[4] = 253$

.... $K[5] = 252$ .... $K[255] = 2$.

Q. 8.7 a) using straight forward scheme to store the internal state how many bits are used.?

Answer:- So to store it i we need 8 bits, for to store j we need 8 bits and for S we need (256 × 8) so it is totally we can say as.

$$i + j + S$$

$$\Downarrow \quad \Downarrow \quad \Downarrow$$

$$(8 \text{ bits}) + (8 \text{ bits}) + (256 \times 8)$$

$$= 8 + 8 + 2048 \text{ bits}.$$

$$= 2064 \text{ bits}.$$

8.7 b)

Answer: so the number of states used is

$$[256! \times 256^2]$$

permutation of 256 'es (0 to 255) so

(0 to 255 so total 256).

$$[256! \times 256^2]$$

$$\approx 2^{1700}$$

Therefore 1700 bits are required.

Q. 8.8 (a)

Answer:- So by taking the first 80 bits of $V \| C$.

Bob can obtain the initilization vector V.

As we know that the V, C and K are known, so the message can be recovered and decrypted by computing

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

(b) So if the adversary observes that the $(V_1 \| C_1); (V_2 \| C_2)$ .... transmitted we can that $V_i = V_j$ for distinct i, j, then adversary knows that the same key stream was used to encrypt both messages for example m_i & m_j. So in this case the messages are vlunerable to by using the first 80 bits of $V \| C$ we get the initilization vector so then as he knows these then by using

$$RC4(V \| K) \oplus C.$$

Adversary can compute the message.

8.8 (c)

Birthday paradox is type of cryptographic attack which is class of Brute force attack. The success of this attack is depends on likelihood of collisions found betⁿ random attack attempts.

Now here in this example since key is fixed, the key stream varies and we know it is 80 bit vector which selected random. so it is 2^{80} messages

~~but these send by alice & bob so, but~~

to consider only Alice messages send will be half of it so ~~ap~~ it is $\approx 2^{40}$

so it ~~could be~~ approximately $\approx 2^{40}$

messages are sent we expect same V. (vector) and same key stream to be used more than once.

8.8 d

So in the life time of key the number of message can be encrypted by K, So from above point C we can approximately say $\sqrt{\frac{\pi}{2} 2^{80}} \approx 2^{40}$ messages.

So a key should be changed before 2^{40} messages are sent. So that it won't used twice.

* Thank - You - SiR *