ANUSHNA UPPU Assignment-2 CS21M504

8.2) Given $x_{n+1} = (ax_n) \bmod 2^4$

a) Maximum period $= 2^{4-2} = 4$

b) a should be either 5 or 11 $\quad 2^4 = 16$

if $a = 5$, $x_0 = 1$

then 1, 5, 9, 13, 1, 5, 9

period = 4

if $a = 11$, $x_0 = 1$

1, 11, 9, 3, 1, 11

period = 4

c) Seed must be odd

8.4) Assume $x_0 = 10$

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

then sequence 1, 6, 10, 8, 9, 2, 12, 7, 3, 5, 4, 11 = —

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

Sequence = 1, 7, 10, 5, 9, 11, 12, 6, 3, 8, 4, 2, 1 — —

Both are full period because the sequence contains all the integers between 1 and 12 (inclusive)

and the first sequence is more random because in the second sequence it contain 8, 4, 2, 1 which we can easily predict (by dividing with 2)

8.5] See attached file with the mail

8.6) After initialization we get S as

$S \rightarrow [0, 1, 2, \ldots 255]$

1) for i = 0 to 255 do
2) j = (j + S[i] + T[j]) mod 256
3) Swap (S[i], S[j])

Taking the keylength as 256

So $T[i] = K[i]$ ——— ①

Step: 1) i = 0 ; j = 0

then in order remain the S value as same we need to get i = j

At line 2: j = 0 + 0 + T[0] mod 256

j = T[0] mod 256

In order to get j = 0 we have to give T[0] as 0 **T[0] = 0**

Step: 2) i = 1 ; j = 0

We need to get j as 1

At line 2: j = 0 + 1 + T[1] mod 256

j = 1 + T[1] mod 256

In order to get j = 1 we have to give T[1] as 0 then j = 1

T[1] = 0

Step: 3) i = 2 ; j = 1

We need to get j as 2

At line 2: j = 1 + 2 + T[2] mod 256

j = 3 + T[2] mod 256

In order to get j = 2 we have to give T[2] as 255 then j = 2

T[2] = 255

Step: 4) i = 3 ; j = 2

we need to get j as 3

At line 2: j = 2 + 3 + T[3] mod 256

j = 5 + T[3] mod 256

In order to get i = 3 we have to give

T[3] as 254 then j = 3

T[3] = 254

⋮

Similarly T[4] = 253

T[5] = 252

⋮

T[255] = 2

from ① we know that T[i] = K[i]

So K should be [0, 0, 255, 254 --- 2]

(8.7)

a) In order to store i, j & S we require

$8 + 8 + (256 \times 8)$ bits

$= 16 + 2048$ bits

$= 2064$ bits

b) number of states are $256! \times 256^2 = 2^{1700}$

So we need 1700 bits to represent the states

(8.8)

a) Since V is 80-bit value

By taking first 80 bits from V||C, we can get the initialization vector V, so the remaining bits are C.

Since we know the values of V, K and C, we can get the message m by applying the following formulae $RC4(V||K) \oplus C$

b) If adversary observes $(V_1||C_1)$ & $(V_2||C_2)$ and get to know that the first 80 bits are same in both the message he can get to know about V. So he can easily get the message back

(8)

c) key is fixed & we know that v is an 80 bit value So By approximation

$\sqrt{\frac{\pi}{2} 2^{80}} \approx 2^{40}$ messages can be transmitted

d) The lifetime of the key will be 2^{40} messages