Assignment - 2

Prob 8.2

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

a) Let us consider a random $x_0 = 1$

$2^4 = 16$

$1 \bmod 16 = 1$

(i) Let us assume $a = 3$

$x_1 = 3 \bmod 16 = 3$

$x_2 = 9 \bmod 16 = 9$

$x_3 = 27 \bmod 16 = 11$

$x_4 = 33 \bmod 16 = 1$

$x_5 = 3 \bmod 16 = 3$

$\{3, 9, 11, 1, \ldots\}$

(ii) Let us assume $a = 5$

$x_1 = 5 \bmod 16 = 5$

$x_2 = 25 \bmod 16 = 9$

$x_3 = 45 \bmod 16 = 13$

$x_4 = 65 \bmod 16 = 1$

$x_5 = 5 \bmod 16 = 5$

$\{5, 9, 13, 1, \ldots\}$

(iii) Assume $a = 7$

$x_1 = 7 \bmod 16 = 7$

$x_2 = 49 \bmod 16 = 1$

$x_3 = 7 \bmod 16 = 7$

$\{7, 1, \ldots\}$

(iv) Assume $a = 11$

$x_1 = 11 \bmod 16 = 11$

$x_2 = 121 \bmod 16 = 9$

$x_3 = 99 \bmod 16 = 3$

$x_4 = 33 \bmod 16 = 1$

$\{11, 9, 3, 1, \ldots\}$

(v) Assume $a = 13$

$x_1 = 13 \bmod 16 = 13$

$x_2 = 169 \bmod 16 = 9$

$x_3 = 117 \bmod 16 = 5$

$x_4 = 65 \bmod 16 = 1$

$\{13, 9, 5, 1, \ldots\}$

$\boxed{\text{Max period obtained is 4}}$

b) a can be 5, 3, 11, 13 for $x_0 = 1$

c) Restrictions on seed

It should be relatively prime with 16, i.e. $GCD(a, 16) = 1$.

Prob 8.4 $x_{n+1} = 6x_n \mod 13$

Let $x_0 = 1$.

$x_1 = 6 \mod 13 = 6$

$x_2 = 36 \mod 13 = 10$

$x_3 = 60 \mod 13 = 8$

$x_4 = 48 \mod 13 = 9$

$x_5 = 54 \mod 13 = 2$

$x_6 = 12 \mod 13 = 12$

$x_7 = 72 \mod 13 = 7$

$x_8 = 42 \mod 13 = 3$

$x_9 = 18 \mod 13 = 5$

$x_{10} = 30 \mod 13 = 4$

$x_{11} = 24 \mod 13 = 11$

$x_{12} = 66 \mod 13 = 1$

$x_{13} = 6 \mod 13 = 6$

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

Period has all numbers from 1 to 12.

So it is of full period.

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

$x_0 = 1$

$x_1 = 7 \mod 13 = 7$

$x_2 = 49 \mod 13 = 10$

$x_3 = 70 \mod 13 = 5$

$x_4 = 35 \mod 13 = 9$

$x_5 = 63 \bmod 13 = 11$

$x_6 = 77 \bmod 13 = 12$

$x_7 = 84 \bmod 13 = 6$

$x_8 = 42 \bmod 13 = 3$

$x_9 = 21 \bmod 13 = 8$

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

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

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

$x_{13} = 7 \bmod 13 = 7$

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

Period has all numbers from 1 to 12.

So it is of full period.

Prob 8.6 We have $s[0]=0, s[1]=1, \ldots s[255]=255$.

$j = (j + s[i] + T[i]) \bmod 256$

for $j = i$ the $s[i]$ remains unchanged.

for $i=0$, if $j=0$ then $T[i]=0$ i.e. $k[0]=0$

for $i=1$, if $j=1$ then $T[i]=0$ i.e. $k[1]=0$

$(\because s[i]=1, j=0+1+0=1)$.

for $i=2$, if $j=2$ then $T[i]=255$, i.e. $k[2]=255$

$(\because s[2]=2, j=((1)+(2)+255) \bmod 256)$

$j=2$.

for $i=3$, if $j=3$ then $T[i]=254$, i.e. $k[3]=254$

$(\because s[3]=3, j=((2)+(3)+254) \bmod 256 \Rightarrow j=3)$

⋮

for $i=255$, if $j=255$ then $T[i]=2$, i.e. $k[255]=2$.

$(\because s[255]=255, j=((254)+(255)+2) \bmod 256 \Rightarrow j=255)$

$\therefore$ key has to be of length 255 with below values for s to remain unchanged

$k[0]=k[1]=0$

$k[2]=255, k[3]=254, \ldots\ldots k[255]=2$.

for $i=0,1$ $k[i]=0$

for $i=2$ to 255 $k[i]=256-s[i]+1$

Prob 8.7:

a, We can store only i, j and $s \rightarrow$ this requires

$8+8+(256 * 8) = 2064$ bits

b, Number of states $[256 * 256^2] \approx 2^{1700} \rightarrow \therefore 1700$ bits are required.

Prob 8.8

$V = 80$ bit value

$K = 128$ bit value

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

(a) Retreiving 'm' from $v \| c$ & k

Take first 80 bits of $v \| c$, that gives v

Now we know v, c, k

So we can obtain

$$m = RC4(v \| k) \oplus c$$

(b) $(v_1 \| C_1), (v_2 \| C_2)$ - - -

$$m_1 = \underbrace{RC4(v_1 \| k)}_{\text{key stream (Random)}} \oplus c_1$$

Adversary can perform $m_1 \oplus c_1$ to get keystream k_1

$m_1 \oplus c_1 = k_1$

$m_2 \oplus c_2 = k_2$

⋮

$m_n \oplus c_n = k_n$

if any two $m_i \oplus c_i$ & $m_j \oplus c_j$ yield same k_i & k_j

then adv knows same keystream is used.

(c) $v \to 80$ bits $\to$ append 48 zeros to make it 128 bit.

for $i = 0$ to 127

$j = (j + v[i] + k[i]) \bmod 128$

swap $(v[i], v[j])$

$j = 0$

for $i = 0$ to 127

$i = (i+1) \bmod 128$

$j = (j + v[i]) \bmod 128$

swap $(v[i], v[j])$

$t = (v[i] + v[j]) \bmod 128$

$k = v[t]$

↓

$\oplus\, c[i]$.

c, for a given value of v & k the $RC4(v\|k)$ will be Same. As key k is already fixed, key stream depends on v. So for different values of v the RC4 generates diff key streams.

v is 80 bit values

So possible no. of values of v = 2^{80}

∴ For 2^{80} values of v, $RC4(v\|k)$ generates 2^{80} diff key streams.

Bob & Alice can communicate 2^{80} messages before the key streams repeats twice.

d, From 'c' we get the Lifetime of 'k' depends on value of v, range of v.

If v is 'n' bit value, 2^n messages can be encrypted.

So here 2^{80} messages can be sent.