RC4 : The algorithm

The RC4 algorithm has two main parts:

(i) KSA (Key Scheduling Algorithm)

and (ii) PRGA (Pseudo Random Generation Algorithm)

KSA

```
initialization:
   j = 0
   for i = 0 to N-1
      S[i] = i
scrambling:
   for i = 0 to N-1
      j = (j + S[i] + k[i mod l]) mod N;
      swap (S[i], S[j])
```

PRGA

```
initialization:
   i = 0
   j = 0
generation loop:
   i = (i + 1)mod N
   j = (j + S[i]) mod N
   swap (S[i], S[j])
   Output Z = S[ S[i] + S[j] ]
```

where ‘k’ is the key of length ‘l’; S = {0,1…N-1} is the initial permutation

RC4 : Example

We give a simple example with 4-byte state S.
Let the key be k = [2, 4]. Here N = 4 and key-length 'l' = 2.

KSA:

iteration:1

S[] = [s_0,s_1,s_2,s_3] = [0,1,2,3]

k[] = [k_0,k_1] = [2,5]

i=0, j=0

j = (j + s_0 + k_0) mod4 = 2

swap (s_0, s_2)

New array S = [2,1,0,3]

RC4 : Example

KSA:

iteration:2

$S[] = [s_0, s_1, s_2, s_3] = [2,1,0,3]$

$k[] = [k_0, k_1] = [2,5]$

$i=1,\ j=2$

$j = (j + s_1 + k_1) \bmod 4 = 0$

swap (s_1, s_0)

New array $S = [1,2,0,3]$

RC4 : Example

KSA:

iteration:3

$S[] = [s_0,s_1,s_2,s_3] = [1,2,0,3]$

$k[] = [k_0,k_1] = [2,5]$

$i=2,\ j=0$

$j = (j + s_2 + k_0) \bmod 4 = 2$

swap (s_2, s_2)

New array S = [1,2,0,3]

RC4 : Example

KSA:

iteration:4

$S[] = [s_0,s_1,s_2,s_3] = [1,2,0,3]$

$k[] = [k_0,k_1] = [2,5]$

$i=3,\ j=2$

$j = (j + s_3 + k_1) \bmod 4 = 2$

swap (s_3, s_2)

New array $S = [1,2,3,0]$

RC4 : Example

PRGA:

Set i=j=0

S = $[s_0,s_1,s_2,s_3]$ = [1,2,3,0]

i = (i + 1) mod N = 1

j = (j + s[i]) mod N = 1

swap (s_1, s_1)

new array S = [1,2,3,0]

output Z = $S[s_1 + s_1] = s_2$ = 3.