

Solutions

ENEE/CMSC/MATH 456: Cryptography Stream Cipher Class Exercise 3/28/22

ALGORITHM 6.1

Init algorithm for RC4

Input: 16-byte key k

Output: Initial state (S, i, j)

(Note: All addition is done modulo 256)

for $i = 0$ to 255:

$S[i] := i$

$k[i] := k[i \bmod 16]$

$j := 0$

for $i = 0$ to 255:

$j := j + S[i] + k[i]$

Swap $S[i]$ and $S[j]$

$j := 0, i := 0$

return (S, i, j)

ALGORITHM 6.2

GetBits algorithm for RC4

Input: Current state (S, i, j)

Output: Updated state (S, i, j) ; output byte y

(Note: All addition is done modulo 256)

$i := i + 1$

$j := j + S[i]$

Swap $S[i]$ and $S[j]$

$t := S[i] + S[j]$

$y := S[t]$

return $(S, i, j), y$

Let S^0 denote the initial state, S^i denote the state after i calls to **GetBits**.

Consider Event 1: $(S^0[2] = 0) \wedge (S^0[1] = X \neq 2)$

What is the probability that Event 1 occurs? (For this part, assume Init outputs a perfectly random permutation of the values from 0 to 255) $\frac{1}{256} \cdot (1 - \frac{1}{256}) \sim \frac{1}{256}$

Assuming Event 1 occurs, what is the value of $S^1[X]$ (i.e. the value in position $S[X]$ after the first iteration)? X

Assuming Event 1 occurs, what is the value of $S^2[X], S^2[2]$ (i.e. the values in positions $S[X]$ and $S[2]$ after the second iteration)? 0, X

Assuming Event 1 occurs, what value (call this V) is outputted in the second iteration?

0

Assuming Event 1 does not occur, V is uniformly distributed.

Towards what value is V biased and with what probability? $\frac{1}{256} + \frac{1}{256} (1 - \frac{1}{256}) \sim \frac{2}{256}$.
biased towards 0.

First iteration:

$i = 1$

$j = S[1] = X$

Swap $S[1]$ and $S[X]$

$S[1] = S[X]$

$S[X] = X$

Second iteration:

$i = 2$

$j = X + S[2] = X + 0 = X$

Swap $S[2]$ and $S[X]$

$S[2] = S[X] = X$

$S[X] = 0$

$t := S[2] + S[X] = X$

$y := S[t] = S[X] = 0$

return, 0.

