Netzsicherheit I, WS 2011, Übung 2

Tilman Bender 108011247244
Christian Kröger 108011250663
Thomas Tacke 108011267882

7. November 2011

WLAN & RC4

a) Wie man anhand der Tabelle Hilfsmittel zur KSA-Berechnung a) sieht, funktioniert der Angriff nicht, da der Output nicht stimmig ist.
Dies ist daran zu sehen, das die 5 der erste z Wert ist, und dieser daher in der nächste Operation an die Stelle bewegt werden müsste, auf die durch S[S[1]+S[S[1]] verwiesen wird. In diesem Fall wäre dies die Position 8.
Die 5 kann jedoch nicht auf diese Position bewegt werden, da i auf Position 6 zeigt, was bedeutet das ein beliebiges Element mit dem an Position 6 getauscht werden kann jedoch nicht mit dem an Position 8 (bzw. es ist nicht möglich Position 3 mit 8 zu tauschen, was nötig wäre um die 5 auf Position 8 zu verschieben, da eine der beiden zu vertauschenden Positionen aufjedenfall Position 6 ist).
Um es zu ermöglichen, das im nächsten Schritt die Position der 5 verändert werden kann, ist es nötig diese auf Position 6 zu verschieben (denn dadurch wird i im folgenden Schritt auf die 5 verweisen und es ist möglich die 5 mit Hilfe des zu berechnenden $K[6]$ an die korrekte Position zu verschieben).
Die 5 kann durch folgende Änderung auf Position 6 verschoben werden:
$K[5] = 10 \wedge \neq 7$
Sprich, wenn $K[5]$ auf den Wert 10 gesetzt wird, steht der Wert 5 auf Position 6 und kann durch $K[6]$ im nächsten Schritt an die benötigte Position verschoben werden.

i	j	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	4	4	1	2	3	0	5	6	7	8	9	10	11	12	13	14	15
1	3	4	3	2	1	0	5	6	7	8	9	10	11	12	13	14	15
2	14	4	3	14	1	0	5	6	7	8	9	10	11	12	13	2	15
3	12	4	3	14	12	0	5	6	7	8	9	10	11	1	13	2	15
4	7	4	3	14	12	7	5	6	0	8	9	10	11	1	13	2	15
5	3	4	3	14	5	7	12	6	0	8	9	10	11	1	13	2	15

Tabelle 1: Hilfsmittel zur KSA-Berechnung a)

b) $K[6 = 4]$
Dies ist zu sehen durch:
$z[0] = 5 = S[S[1] + S[S[1]]] = S[3 + S[3]] = S[3 + 12] = S[15]$. Daher muss

an Position 15 der Wert 5 stehen, was durch $K[6]$ zu erreichen ist.
Dies führt zu der Berechnung:
$j = (j + S[i] + k[6]) \mod 16$
$j = 6$ (alter j Wert) $+5 + k[6]$
$15 = 11 + k[6]$
$K[6] = 4$

i	j	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	4	4	1	2	3	0	5	6	7	8	9	10	11	12	13	14	15
1	3	4	3	2	1	0	5	6	7	8	9	10	11	12	13	14	15
2	14	4	3	14	1	0	5	6	7	8	9	10	11	12	13	2	15
3	12	4	3	14	12	0	5	6	7	8	9	10	11	1	13	2	15
4	7	4	3	14	12	7	5	6	0	8	9	10	11	1	13	2	15
5	6	4	3	14	12	7	6	5	0	8	9	10	11	1	13	2	15
6	15	4	3	14	12	7	6	15	0	8	9	10	11	1	13	2	5

Tabelle 2: Hilfsmittel zur KSA-Berechnung b)

c) Die Berechnung des Schlüsselwortes ist nicht immer korrekt, was daran gesehen werden kann, das im Durchschnitt ca. 60 verschiedene Werte benötigt werden um ein folgendes Schlüssel Element (von K) zu errechnen.
Die Wahrscheinlichkeit, das dies für einen passenden IV funktioniert ist ca. 5 Prozent, daher ist man mit ca. 60 Werten jenseits der 50 Prozent.
Der Angreifer kann nicht direkt Prüfen ob ein errechnetes Wort richtig ist. Er kann prüfen ob es häufiger errechnet würde und wenn dies der Fall ist, ist es Wahrscheinlicher, dass es korrekt ist.