

Netzicherheit I, WS 2011, Übung 2

Tilman Bender Christian Kröger Thomas Tacke
108011247244 108011250663 108011267882

5. November 2011

WLAN & RC4

- a) Wie man anhand der Tabelle Hilfsmittel zur KSA-Berechnung b) sieht, ist der Output nicht stimmig.

$K[5] = 10 \wedge \neq 7$ TODO: Yaddda Yadda dings da.

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) $K[6 = 13]$

Yadda Yadda dings da TODO.

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

Tabelle 2: Hilfsmittel zur KSA-Berechnung b)

- c) Yadda Yadda dings da TODO

wharscheinlichkeiten ≈ 60 dingsdas, weist schon qed.