Netzsicherheit I, WS 2011
Übung 2

Prof. Dr. Jörg Schwenk

Betreuer: Florian Feldmann, Florian Giesen

Abgabe: Montag, 07. November 2011, 11:00h
In der Übung, am Kasten vor ID 2/467, oder per Mail an Florian.Giesen AT rub.de
Gruppenarbeit bis max. 3 Studenten pro Gruppe ist erlaubt und erwünscht.

1 Paper Lesen

Lesen Sie das Paper von Fluhrer, Mantin und Schamir: "Weaknesses in the Key Scheduling Algorithm of RC4" genau durch.
URL: `http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf`.

2 WLAN & RC4 (Klausur)

Gegeben sei die RC4-Stromchiffre mit einer Wortgröße von 4 Bit, d.h. $N=2^4=16$. Der Initialisierungsvektor IV = K[0...2] besteht aus drei Worten (4, 14, 9). Bekannt sind auch die ersten drei Worte des Schlüssels K[3...5] = (13, 11, 7). Das erste Output-Wort der Chiffre ist z = OUT[0] = 5.

a) Funktioniert der Angriff von Fluhrer, Mantin und Shamir für die gegebenen Werte, um das nächste Schlüsselwort K[6] zu berechnen? Erläutern Sie, warum die Berechnung möglich bzw. nicht möglich ist! Korrigieren Sie gegebenenfalls die angegebenen Werte, damit die Berechnung von K[6] durchgeführt werden kann.

   Anmerkung: Führen Sie ausschließlich notwendige Änderungen an den gegebenen Werten durch!

b) Führen Sie die Berechnung von K[6] durch!

   Anmerkung: Sie können Tabelle 1 als Hilfsmittel benutzen.

c) Ist die Berechnung des nächsten Schlüsselwortes immer korrekt, wenn ein passender Initialisierungsvektor gegeben ist? Kann der Angreifer überprüfen, ob das berechnete Schlüsselwort korrekt ist?

		S[0]	S[1]	S[2]	S[3]	S[4]	S[5]	S[6]	S[7]	S[8]	S[9]	S[10]	S[11]	S[12]	S[13]	S[14]	S[15]
		00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
i	j	S[0]	S[1]	S[2]	S[3]	S[4]	S[5]	S[6]	S[7]	S[8]	S[9]	S[10]	S[11]	S[12]	S[13]	S[14]	S[15]
i	j	S[0]	S[1]	S[2]	S[3]	S[4]	S[5]	S[6]	S[7]	S[8]	S[9]	S[10]	S[11]	S[12]	S[13]	S[14]	S[15]
i	j	S[0]	S[1]	S[2]	S[3]	S[4]	S[5]	S[6]	S[7]	S[8]	S[9]	S[10]	S[11]	S[12]	S[13]	S[14]	S[15]
i	j	S[0]	S[1]	S[2]	S[3]	S[4]	S[5]	S[6]	S[7]	S[8]	S[9]	S[10]	S[11]	S[12]	S[13]	S[14]	S[15]
i	j	S[0]	S[1]	S[2]	S[3]	S[4]	S[5]	S[6]	S[7]	S[8]	S[9]	S[10]	S[11]	S[12]	S[13]	S[14]	S[15]
i	j	S[0]	S[1]	S[2]	S[3]	S[4]	S[5]	S[6]	S[7]	S[8]	S[9]	S[10]	S[11]	S[12]	S[13]	S[14]	S[15]
i	j	S[0]	S[1]	S[2]	S[3]	S[4]	S[5]	S[6]	S[7]	S[8]	S[9]	S[10]	S[11]	S[12]	S[13]	S[14]	S[15]
i	j	S[0]	S[1]	S[2]	S[3]	S[4]	S[5]	S[6]	S[7]	S[8]	S[9]	S[10]	S[11]	S[12]	S[13]	S[14]	S[15]
i	j	S[0]	S[1]	S[2]	S[3]	S[4]	S[5]	S[6]	S[7]	S[8]	S[9]	S[10]	S[11]	S[12]	S[13]	S[14]	S[15]
i	j	S[0]	S[1]	S[2]	S[3]	S[4]	S[5]	S[6]	S[7]	S[8]	S[9]	S[10]	S[11]	S[12]	S[13]	S[14]	S[15]

Tabelle 1: Hilfsmittel zur KSA-Berechnung