

Angriffe auf RC4

Andreas Klein*

*Arbeitsgruppe Computational Mathematics, Universität Kassel

RC4 ist eine Stromchiffre die 1987 von Ron Rivest erfunden wurde. Die Chiffre ist sehr schnell und wird daher in Anwendungen wie SSL und WEP eingesetzt. Damit gehört sie zu den populärsten Stromchiffren. Der Algorithmus wurde als Firmengeheimnis von RSA Data Security Inc. behandelt. Die Beschreibung des Algorithmus wurde erst 1994 anonym auf der Mailing-Liste Cypherpunks veröffentlicht.

Die Struktur des Verfahrens ist recht einfach. Der Algorithmus arbeitet mit einer Permutation S_0, \dots, S_{255} der Zahlen von 0 bis 255. In jedem Schritt wird auf folgende Weise eine Pseudozufallszahl erzeugt.

$$\begin{aligned}i &= (i + 1) \pmod{256} \\j &= (j + S_i) \pmod{256} \\&\text{vertausche } S_i \text{ und } S_j \\t &= (S_i + S_j) \pmod{256} \\&\text{gebe } S_t \text{ aus}\end{aligned}$$

In meinem Vortrag möchte ich eine Schwäche der von RC4 erzeugten Pseudozufallsfolge vorstellen und zeigen wie diese zu einem Angriff ausgenutzt werden kann.

In Gegensatz zur bekannten FMS-Attacke [1] braucht der neue Angriff keine schwachen Schlüssel. Daher reichen jetzt bereits etwa 25000 statt 1000000 abgefangener Sitzungen zur Analyse aus. Mit der neuen Technik ist es auch dann möglich den Schlüssel zu rekonstruieren, wenn die ersten 256 Byte des Schlüsselstroms für eine Analyse nicht zu Verfügung stehen.

Literatur

- [1] S. Fluhrer, I. Mantin, and A. Shamir. Weakness in the Key Scheduling Algorithm of RC4. In *Selected areas in cryptography*, volume 2259 of *LNCS*, pages 1–24, Berlin, 2001. Springer.