Kryptoanalyse – Angriffstypen

- **Ciphertext-only-Angriff:** Die Kryptoanalytikerin kennt nur einige Schlüsseltexte und sie versucht daraus, die Klartexte oder die Schlüssel zu bestimmen. Hält ein Kryptosystem diesem Angriff nicht stand, so sollte es nicht verwendet werden.
- **Known-Plaintext-Angriff:** Die Kryptoanalytikerin kennt nur einige Paare von Schlüsseltexten und zugehörigen Klartexten, aus denen sie die verwendeten Schlüssel ermittelt oder andere Schlüsseltexte entschlüsselt.
- **Chosen-Plaintext-Angriff:** Die Kryptoanalytikerin kann Klartexte nach Belieben auswählen und erfährt die zugehörigen Schlüsseltexte, aus denen sie die Schlüssel bestimmen möchte.
- **Chosen-Ciphertext-Angriff:** Die Kryptoanalytikerin hat Zugang zum Entschlüsselungsgerät und kann einen Schlüsseltext wählen, um den zugehörigen Klartext zu konstruieren.
- **Key-only-Angriff:** Die Kryptoanalytikerin kennt nur den öffentlichen Schlüssel, aber sie hat noch keine Schlüsseltexte abgefangen. Sie versucht nun, den entsprechenden privaten Schlüssel zu bestimmen. Im Unterschied zu den vorgenannten Angriffsarten besteht darin, dass die Angreiferin nun so viel Zeit hat, wie sie möchte, um ihre Berechnungen durchzuführen.

. . . . . .

Man könnte sich fragen, ob vielleicht auch geheim gehalten werden sollte, welches Kryptosystem verwendet wird. Sicherlich könnte es die Aufgabe der Kryptoanalytikerin beträchtlich erschweren, wenn ihr das verwendete Kryptosystem verborgen bleibt (Security by obscurity).

Diese Annahme kann – und dies ist geschichtlich immer wieder bestätigt worden – nicht eingehalten werden. Daher hat man sich in der Kryptologie ein Prinzip zu Eigen gemacht, welches erstmals von dem niederländischen Philologen und Kryptologen Jean Guillaume Hubert Victor François Alexandre Auguste Kerckhoffs von Nieuwenhof (1835 bis 1903) in seinem Buch »La cryptographie militaire« formuliert wurde.

Kerckhoffssches Prinzip

Die Sicherheit eines Kryptosystems darf nicht von der Geheimhaltung des verwendeten Systems abhängen. Stattdessen darf die Sicherheit eines Kryptosystems nur von der Geheimhaltung der verwendeten Schlüssel abhängen.

. . . . . .

Die in diesem Informationsblatt angegebenen Elemente orientieren sich an den Einordnungen in (**Rothe2008**).