Zur Geschichte der vertraulichen Kommunikation: Von der Kopfrasur zur Kopfakrobatik

Der Wunsch nach vertraulicher Kommunikation ist nicht neu. Schon seit der Antike versuchen Menschen, bestimmte Informationen bei der Übertragung vor anderen geheim zu halten. In diesem Vortrag werden die im Laufe der Zeit entwickelten Verfahren zur vertraulichen Kommunikation von den klassischen Chiffrierungsverfahren über die Grundlagen symmetrischer und asymmetrischer Verschlüsselung bis hin zu aktuellen Anwendungsmöglichkeiten kryptographischer Verfahren im heutigen Alltag vorgestellt:

- Klassische Verfahren
  (Transpositionschiffre, Substitutionschiffre, Polyalphabetische Chiffre)
- Symmetrische Verschlüsselung
  (Stromchiffren, Blockchiffren, Mehrfachverschlüsselungen)
- Asymmetrische Verschlüsselung und Einwegfunktionen
  (Hash-Funktionen, Primzahlmultiplikation, Potenzfunktionen und diskreter Logarithmus)
- Anwendungen für kryptographische Verfahren
  (Digitale Signaturen, SSL/TLS, SSH, IPSec, S/MIME, PGP)

Der Vortrag richtet sich an alle Interessierten, die etwas über die Geschichte und die Grundlagen der vertraulichen Kommunikation erfahren wollen. Die Erläuterungen sollen helfen, die vielen kryptographischen Verfahren, mit denen heutzutage der Datenaustausch abgesichert wird, leichter einzuordnen – und so Endanwendern im besten Falle ein wenig Verständnis zu geben und Angst zu nehmen. Der Vortrag bleibt bei den theoretischen Grundlagen. Spezielle Vorkenntnisse sind nicht erforderlich.