Seminarthema Kryptographie

Kryptographie scheint mir für ein W–Seminar besonders gut geeignet zu sein, weil man hier zum einen Reine Mathematik (Zahlentheorie) behandeln kann und zum anderen lernen die Schüler, dass Mathematik nicht nur zum Selbstzweck betrieben werden kann, sondern im täglichen Leben sehr bedeutsame Anwendungen hat.

Themenvorschläge:

1. Primzahlen
2. Restklassen und ihre Verknüfungen
3. Verfahren

   Zu jedem der folgenden Verfahren kann es auch eine Programmieraufgabe geben. Man kann zur Veranschaulichung auch das CrypTool verwenden. Damit können die Schüler auch die Effizienz der Verfahren in der Praxis erproben, in dem man einen Text mit einem bestimmten Verfahren verschlüsselt und dann mit dem CrypTool oder einem eigenen Programm zu dechiffrieren versucht. Insbesondere soll auch darauf eingegegangen werden wie sicher ein Verfahren ist und eine Aufwandschätzung zur Entschlüsselung in der Praxis angegeben werden.

   a) Historisches: Caesar–Chiffre, Vigenère–Chiffre, Kasiski–Angriff, Friedmann–Angriff.
   b) Enigma
   c) RSA
   d) DES
   e) AES
   f) Diffie–Hellman–Schlüsselvereinbarung und ElGamal–Systeme
   g) Hashfunktionen
4. Schlüsselverwaltung
5. Authentizität
6. Internetsicherheit
7. Elektronisches Geld und elektronische Wahlen
8. Quantenkryptograhie

Literaturhinweise:

- Albrecht Beuteplspacher, Heike B. Neumann, Thomas Schwarzpaul: Kryptographie in Theorie und Praxis, Vieweg 2005
- Auf `http://www.cryptool.de/` findet man einen Link zum Download des CrypTools (OpenSource) und weitere interessante Informationen. Insbesondere wird bei der Installierung des Tools ein Skript skript-de.pdf zur Kryptographie mit heruntergeladen.