# STOFFVERTEILUNGSPLAN

## Informationsgesellschaft und Datensicherheit (3.3.1.4)

| Std. | Bildungsplan, inhaltsbezogene Kompetenzen | Inhalt / Material |
|---|---|---|
| 1 | | *01_iud_ab_wdh.odt*<br>*00_krypto.odp*<br>WDH Kryptoziele,<br>Problem des Schlüsseltauschs |
| 2-3 | (1) das Konzept der *asymmetrischen Verschlüsselung* (*privater*/*öffentlicher Schlüssel*) erklären (keine mathematischen Grundlagen!)<br>(2) erklären, wie Nachrichten mit *asymmetrischer Verschlüsselung signiert* werden können<br>(4) *asymmetrische* und *symmetrische Verschlüsselung* vergleichen (Schlüsselverwaltung, Schlüsseltausch, Geschwindigkeit) | *02_iud_ab_asym.odt*<br>*00_krypto.odp*<br>*RSA-Chat-Tool*<br>Symmetrisches – asymmetrisches Verfahren<br>öffentlicher/privater Schlüssel |
| 4-5 | (5) die Notwendigkeit eines Zertifizierungssystems für die öffentlichen Schlüssel erläutern | *03_iud_ab_man-in-the-middle.odt*<br>*04_iud_ab_zertifikate.odt*<br>*00_krypto.odp*<br>*RSA-Chat-Tool*<br>Man-in-the-middle-Angriff<br>Zertifikat |
| 6-7 | (2) erklären, wie Nachrichten mit *asymmetrischer Verschlüsselung signiert* werden können<br>(3) die *Verschlüsselung*, *Entschlüsselung* und *Signierung* eigener Nachrichten mit einem geeigneten (didaktischen) Tool durchführen | *05_iud_ab_digit_signatur.odt*<br>*00_krypto.odp*<br>*RSA-Chat-Tool*<br>Digitale Signatur<br>(Hashfunktion) |
| 8 | Aus Bildungsplan Mathematik:<br>(9) die behandelten Verschlüsselungsverfahren vergleichend beurteilen | *06_iud_ab_vergleich_verfahren.odt*<br>Vergleich und Bewertung aller bisher kennengelernten Kryptoverfahren |