

**L3 Verlaufsplanung Stunden 12/13:****Implementierung asymmetrischer Kryptologie am Beispiel RSA**

| <i>Zeit</i> | <i>Phase</i>   | <i>Aktivitäten der SuS</i>   | <i>Impulse von L</i>  | <i>Medien/Soz.form</i>                                    |
|-------------|----------------|--|---|---|
| 5 Min.      | Wiedereinstieg | Die SuS rufen sich die Funktion der (Semi)Primzahlen für die asymmetrische Verschlüsselung ins Gedächtnis und kennen den Ablauf der Stunde.  | L knüpft an die letzte Stunde an, indem er / sie die Bedeutung der (Semi)Primzahlen für die asymmetrische Kryptographie erläutert. Er / Sie gibt einen Ausblick auf das RSA-Verfahren und die Doppelstunde und das dafür benötigte modulare Rechnen.  |   |
| 10 Min.     | Erarbeitung I  | SuS bearbeiten den AB „Modulares Rechnen“ - Rechnen mit Resten   | L gibt ggf. Hilfestellung.  | AB „Rechnen mit Resten“                                   |
| 5 Min.      | Sicherung I    | SuS vergleichen die Ergebnisse ihrer Rechnungen  | L moderiert (Lösungsbogen zur Kontrolle)  |   |
| 25 Min.     | Erarbeitung II | Die SuS erstellen in Partnerarbeit ein Schlüsselsystem und Ver- und Entschlüsseln eine einfache Zahl.  | L gibt den AB „Das RSA-Verfahren“ aus und erläutert den Arbeitsauftrag: Erstellung eines Schlüsselpaares und Bearbeitung eines einfachen Beispiels zum Ver- und Entschlüsseln. Er / Sie steht für Nachfragen bereit und erläutert – wenn nötig – im Plenum einzelne Schritte des Verfahrens, insbes. wie der Rest großer Potenzen mit „Modularem Potenzieren“ zu berechnen ist. | AB „Das RSA-Verfahren“<br>ggf. AB „Modulares Potenzieren“ |
| 5 Min.      | Sicherung II   | SuS vergleichen die Ergebnisse ihrer Rechnungen  | L moderiert (Lösungsbogen zur Kontrolle)  |   |
| 20 Min.     | Anwendung      | Die SuS tauschen ihren öffentlichen Schlüssel mit einem Partner (!= Partner aus Erarbeitung I) aus und verschlüsseln ihr Geburtsdatum. Sie übermitteln das Chiffre an den Partner und entschlüsseln selber dessen Geburtsdatum.  | L teilt den AB „Mit RSA Daten verschlüsselt austauschen“ aus und erläutert die Aufgabenstellung. Er / Sie steht für Rückfragen bereit.  | AB „Mit RSA Daten verschlüsselt austauschen“              |
| 20 Min.     | Transfer       | Einzelne SuS stellen ihren öffentlichen Schlüssel und ein Chiffre an der Tafel zur Verfügung. Sie SuS überlegen, wie man mit diesen Informationen das Chiffre knacken kann und überlegen, wie man das Knacken verhindern könnte. | L gibt – wenn nötig – Hinweise darauf, wie man mit den gegebenen Informationen die Chiffre knacken kann. Bei genügend Zeit kann ein kleiner „Entschlüsselungs-Wettbewerb“ durchgeführt werden.  | TA, Plenum  |