

L3 Verlaufsplanung Stunden 14/15: Sicherheit von RSA

Zeit	Phase	Aktivitäten der SuS	Impulse von L	Medien/Soz.form
10 Min.	Vorbereitung	Die SuS führen das RSA-Verfahren computer-gestützt durch. Sie erarbeiten sich die Bedienung der RSA-Demo von CrypTool	L gibt den SuS Hilfestellung bei der Nutzung des Programms RSA-Demo von CrypTool.	AB „RSA-Demo von CrypTool“
20 Min.	Erarbeitung I	SuS wenden die RSA-Demo selbstständig zur Erstellung eines Schlüssels geeigneter Größe an. Sie ver- und entschlüsseln Geburtstage als Zahlen (23.5.1991 → 23051991)	L teilt den AB „Mit RSA Daten verschlüsselt austauschen“ aus und erläutert den Arbeitsauftrag. Er/Sie gibt erforderlichenfalls Hilfestellung.	AB „Mit RSA Daten verschlüsselt austauschen“
5 Min.	Sicherung I	SuS tauschen sich über die Lösung der Aufgabe aus, ggf. auftretende Probleme werden geklärt.	L moderiert die Diskussion und gibt ggf. Lösungshinweise	
10 Min.	Erarbeitung II	SuS versuchen zunächst, die Aufgabe selbstständig zu lösen. Erforderlichenfalls holen sie sich den AB	L stellt die Aufgabe: „Alice übermittelt Bob ihr verschlüsseltes Geburtsdatum. Der öffentliche Schlüssel von Bob lautet 65537, der Modul N ist 32442353. Könnt Ihr das Geburtsdatum von Alice auch ohne Bobs geheimen Schlüssel ermitteln?“ L legt den AB „RSA mit CrypTool knacken“ am Lehrertisch aus.	AB „RSA mit CrypTool knacken“
5 Min.	Sicherung II	SuS tauschen sich über die Lösung der Aufgabe aus, ggf. auftretende Probleme werden geklärt.	L moderiert die Diskussion und gibt ggf. Lösungshinweise	
20 Min.	Erarbeitung III	SuS bearbeiten die Aufgabe.	L stellt die Aufgabe: „Wie groß muss der RSA-Schlüssel sein, damit er mit CrypTool nicht so schnell geknackt werden kann?“ L gibt Hinweise, wie mit der RSA-Demo ein Schlüssel mit vorgegebener Bit-Länge erzeugt werden kann.	
10 Min.	Sicherung III	SuS vergleichen Ergebnisse (128-Bit-Schlüssel können von CrypTool < 1Min. geknackt werden).		
10 Min.	Vertiefung	Die SuS recherchieren, was die größte bisher faktorisierte Zahl ist. Basierend darauf, diskutieren sie, wie sicher das RSA-Verfahren ist.	L erläutert den Arbeitsauftrag. Er / Sie moderiert die Diskussion über die Sicherheit des RSA-Verfahrens.	Recherche, Diskussion im Plenum