L3 Verlaufsplanung Stunde 9: Trennung von Ver- und Entschlüsseln mittels Falltürfunktion

Zeit	*Phase*	*Aktivitäten der SuS*	*Impulse von L*	*Medien/Sozialform*
5 Min.	Einführung	Die SuS rufen sich die Problematik der letzten Stunde in Gedächtnis: Trotz 100%ig sicherer Verschlüsselungsverfahren (One-Time-Pad), stellt die Schlüsselübermittlung eine Schwachstelle dar.	L knüpft an die letzte Stunde (Vigenère) an und nennt die Fragestellung für die heutige Stunde: Wie kann das Problem der Schlüsselübermittlung gelöst werden?	Kurs
15 Min.	Entwickeln und Testen des Verfahrens	Die in zwei Gruppen aufgeteilten SuS entwickeln ein Verfahren, bei dem sie mittels ihrer Schlösser und einem Karton eine Nachricht sicher übermitteln können. Sie führen das Verfahren anschließend durch.	L teilt die AB aus. Er / Sie teilt die SuS in zwei Gruppen auf und erläutert die Aufgabenstellung des Rollenspiels. Während des Spiels versucht L, die übermittelte Nachricht zu lesen. Dies kann durch die SuS nur verhindert werden, wenn sie ein geschicktes Schlüsselaustauschverfahren nutzen.	AB „Einführung in die asymmetrische Kryptographie“; Rollenspiel; 2 Vorhängeschlösser, 1 Karton
5 Min.	Demonstration eines man-in-the-middle-Angriffs	Entscheiden sich die SuS für das Diffie-Hellman- Verfahren, so führen Sie das Verfahren erneut durch und beobachten dabei, wie die Übermittlung der Nachricht durch den Lehrer / die Lehrerin angegriffen wird.	L fordert die SuS auf, das Szenario noch einmal durchzuspielen, greift die Nachrichtenübermittlung an, indem er/sie 1. die Nachricht abfängt, mit einem eigenen Schloss versieht und wieder zurückschickt und 2. den Karton austauscht und weiter schickt.	3 Vorhängeschlösser, 2 Kartons
10 Min.	Abwandlung des Verfahrens	Die SuS erarbeiten, ggf. durch geeignete Einhilfen von L, ein Verfahren mit vorangehendem Austausch der geöffneten Schlösser. Die SuS testen das Verfahren im Rollenspiel.	L erweitert die Situationsbeschreibung um die Möglichkeit, dass die Gruppen die Kommunikation in einem einmaligen Treffen vorbereiten.	
10 Min.	Sicherung	Ein(e) Schüler(in) hält die Schrittfolge des Verfahrens an der Tafel fest, die anderen SuS unterstützen ihn / sie dabei. Die SuS halten die Schrittfolge auf dem AB fest. Die SuS benennen die Trennung von Schließ- und Öffnungsfunktion als Lösung.	L bittet eine(e) Schüler(in) die Schrittfolge des Verfahrens an der Tafel festzuhalten. L fragt nach der zentralen Idee des gewählten Lösungsansatzes.	Schülervortrag, Tafelanschrieb, AB