L3 Verlaufsplanung Stunde 8: Polyalphabetische Kryptographie – Vigenère und One-Time-Pads

Zeit	*Phase*	*Aktivitäten der SuS*	*Impulse von L*	*Medien/Soz.form*
5 Min.	Einführung und Brainstorming	Die SuS überlegen, wie man Verschlüsselungen gegen Häufigkeitsanalysen schützen kann (Aufgabe 1). Wenn sie dabei nicht auf das Prinzip der polyalphabetischen Verfahren kommen, ist dies nicht weiter schlimm, da diese in Aufgabe 2) eingeführt werden.	L gibt einen kurzen Ausblick auf die Doppelstunde. Der Lehrer/ Die Lehrerin teilt den Arbeitsbogen der Stunde aus. Er / Sie lenkt die Aufmerksamkeit der SuS auf Frage 1).	AB „Häufigkeitsanalyse mit Vigenère verhindern“
15 Min.	Erarbeitung I	Die SuS nutzen das Programm „Cryptool“ in Partnerarbeit, um per Vigenère-Verfahren einen eingegebenen Text zu verschlüsseln. Dabei sollen sie anhand der Analyse der Animation der Verschlüsselung die Arbeitsweise des Verfahrens erkennen und schriftlich festhalten. Anschließend nutzen sie die Verschlüsselung, um ihrem Partner eine verschlüsselte E-Mail zuzusenden.	L erläutert den Arbeitsauftrag (Aufgaben 2 und 3) und gibt den SuS Hilfestellung bei der Benutzung des Programms „Cryptool“.	Partnerarbeit; „Cryptool“; Thunderbird
10 Min.	Sicherung I	Eine Schülerin / Ein Schüler beschreiben das Verfahren, ein(e) weitere(r) Schüler(in) hält dabei die Schrittfolge des Verfahrens an der Tafel (oder auf dem Beamer) fest. Die anderen SuS korrigieren und erweitern wenn nötig die Beschreibung des Verfahrens und halten das Ergebnis schriftlich fest.	L moderiert den Schülervortrag.	Schülervortrag mit Tafelanschrieb
10 Min.	Erarbeitung II	Sie SuS lesen die verschlüsselte E-Mail und kennen ihren Arbeitsauftrag (Aufgabe 4). Die SuS nutzen „Cryptool“, um die E-Mail zu entschlüsseln.Sie stellen fest, dass sich mit Kenntnis der Schlüssellänge die polyalphabetische Verschlüsselung auf eine monoalphabetische reduzieren lässt. Weiterhin erkennen sie, dass bei einer Schlüssellänge > Textlänge eine solche Reduktion unmöglich ist.	L verschickt die „verschlüsselte E-Mail der Polizei“ an die SuS und fordert sie anschließend auf, ihr Postfach zu überprüfen (Aufgabe 4). L gibt den SuS Hilfestellung bei der Benutzung von „Cryptool“.	„Cryptool“, „Verschlüsselte E-Mail der Polizei“, Thunderbird
5 Min.	Sicherung und Transfer	Die SuS erläutern ihre Antworten auf Aufgabe 4). Hinweis: Falls die SuS erhebliche Schwierigkeiten mit Aufgabe 4 zeigen, so wird empfohlen, die optionale Stunde „Vigenère per Hand knacken“ durchzuführen!	L erläutert das One-Time-Pad-Verfahren und berichtet über dessen historische Bedeutung.	