L1 Verlaufsplanung Stunde 1: Regeln zur Kommunikation aufstellen – ein eigenes Protokoll entwerfen

Zeit	*Phase*	*Aktivitäten der SuS*	*Impulse von L*	*Medien/Sozialform*
5 Min.	Einführung: Zur Unterrichtsreihe		L gibt einen kurzen Ausblick über die Unterrichtseinheit.	Vortrag
10 Min.	Entwicklungsphase	Die SuS einigen sich in Kleingruppen auf ein geeignetes Protokoll zur Übertragung von Nachrichten mittels einer Schnur.	L gibt den Arbeitsauftrag; Beobachtet den Arbeitsfortschritt	Hilfen: Aufgabenzettel, Morsecode / durchnummerierte Aufstellung des Alphabets; Signalschnur;
15 Min.	Experimentierphase	Die SuS signalisieren sich mittels ihrer erstellten Kommunikationsregeln Worte durch eine Tür hindurch. Dabei überprüfen und verändern sie das von ihnen erstellte Protokoll bei Bedarf.	L organisiert die räumliche Einteilung und beobachtet den Arbeitsfortschritt.	Signalschnur; in Entwicklungsphase erstellte Kommunikationsregeln
15 Min.	Auswertung	Die einzelnen Schülergruppen führen im Plenum ihre Kommunikationsmethode vor. Sie sammeln dabei an der Tafel Eigenschaften des Protokolls: Geschwindigkeit, Fehleranfälligkeit, Signaltypen und definieren anschließend den Begriff „Protokoll“. (~ „Ein Protokoll ist eine Regel/Absprache/ Vereinbarung über die Form einer Kommunikation“)	L moderiert die Auswertung und fertigt eine Tafelanschrift an (Tabelle: „Eigenschaften des Protokolls“). L beendet die Stunde mit der Frage nach der Definition des Begriffs „Protokoll“.	Signalschnur, Tafelanschrift

L1 Verlaufsplanung Stunden 2/3: SMTP- und POP3-Protokoll mit einem Netzwerkanalyse-Werkzeug erfassen und die Protokolle rekonstruieren

Zeit	*Phase*	*Aktivitäten der SuS*	*Impulse von L*	*Medien/Sozialform*
Vor der Stunde	Vorbereitung		Starten des Hamsters	Lehrerrechner / Hamster-Installation
5 Min	Einleitung		L gibt Warnhinweise an die SuS: Keine privaten Passwörter benutzen. Alle Kommunikation kann mitgelesen werden. Nennt Ziel der Stunde: „Echte“ Protokolle kennen lernen → Anknüpfen an letzte Stunde.	Vortrag
15 Min.	Vorbereitungsphase	Die SuS richten auf ihren Arbeitsplätzen den Thunderbird ein. Anschließend kommen sie zum Lehrer und richten sich ein Profil auf dem Hamster-Server ein (Benutzername+Passwort). Die SuS unterstützen sich untereinander bei der Fehlerbehebung.	L unterstützt die SuS beim Einrichten von Thunderbird.	Arbeit am Rechner /Anleitung zum Thunderbird
20 Min	Testphase *Die Phase gilt als abgeschlossen, wenn alle SuS erfolgreich Mails gesendet und empfangen haben.*	Die SuS senden und empfangen untereinander E-Mails über ihr eingerichtetes Mailkonto. Die SuS unterstützen sich untereinander bei der Fehlerbehebung.	Bei auftretenden Problemen hilft L bei der Behebung der Fehler.	Arbeit am Rechner /Thunderbird
5 Min	Ausblick		L erläutert das weitere Vorgehen in der nächsten Stunde.	Vortrag

5 Min.	Einleitung		L erläutert den Arbeitsauftrag: Es gilt herauszufinden, welche Protokolle der Rechner nutzt, um die Kommunikation erfolgreich zu gestalten. Das Protokoll besitzt verschiedene Bestandteile und einen festen Ablauf – diesen zu erkennen ist Ziel der Aufgabe. L verteilt jeweils Schüleranzahl:2 Arbeitsbögen zu POP/SMTP und die Anleitung zu „Socket Sniff“.	Arbeitsbögen zu POP & SMTP; Anleitung Socket Sniff
20 Min.	Arbeitsphase	Die SuS ermitteln mittels „Socket Sniff“ die Funktionsweise von POP/SMTP. Dazu empfangen, bzw. senden sie nach dem Start von „Socket Sniff“ eine E-Mail. Durch das Protokoll von „Socket Sniff“ sind sie in der Lage den Arbeitsbogen auszufüllen.	L hilft bei auftretenden Problemen mit dem Programm „Socket Sniff“.	Socket Sniff / Arbeitsbögen POP & SMTP Einzelarbeit
20 Min.	Auswertung	Jeweils ein/e Schüler/in stellt seine Lösung an der Tafel vor. Dazu erläutert er/sie, welche Bedeutung die einzelnen Bestandteile des Protokolls besitzen. Die anderen SuS leisten Hilfestellung. (Bestandteile: ~ Begrüßung, Authentifizierung, Versenden der E-Mail, Abmeldung)	L moderiert die Auswertung.	Tafel / moderierte Auswertung im Plenum

L2 Verlaufsplanung Stunden 4/5: Gefahren bei der Kommunikation über öffentliche Netzwerke entdecken

Zeit	*Phase*	*Aktivitäten der SuS*	*Impulse von L*	*Medien/Soz.form*
Vor der Stunde	Vorbereitung		1. „Man-in-the-middle-attack“ vorbereiten 2. Hamster starten 3. Kanzlerin-E-Mail vorbereiten (neues Mailkonto einrichten)	
10 Min.	Einführung	Fassen auf Aufforderung des Lehrers /der Lehrerin die letzten Stunden zusammen.	1. L stellt Anschluss zur letzten Stunde her . 2. L nennt Thema der heutigen Stunden.	Vortrag
10 Min.	„Funktionstest“ + Szenario „Kanzlerin“	Senden sich E-Mails um „zu probieren, ob das Netz noch läuft“.	1. L fängt Nachrichten ab, um später ein Mailkonto zu hacken. 2. L verschickt die „Kanzlerinnen-Mail“ → Anlass zur Feststellung bei den SuS, dass hier etwas nicht richtig läuft!	Thunderbird, Wireshark
10 Min.	Ergebnissicherung Szenario „Kanzlerin“	Erkennen und benennen das Problem mangelnder Authentizität bei Mailkommunikation.	Arbeitsauftrag: „Notiert: Welche Gefahren bei der Kommunikation über das Internet lassen sich beobachten?“ → Vortäuschen „falscher Identität“ mit Thunderbird auf Beamer zeigen.	Thunderbird, Beamer
15 Min.	Szenario „gefakter Schüler“	Die SuS vermuten hinter dem Absender der Mails den Schüler und reagieren ungehalten.	1. L versendet mittels eines gehackten Schülerkontos eine provokative Mail. 2. L löst die Situation auf, indem er die wahre Identität des Senders preisgibt.	Thunderbird
15 Min.	Ergebnissicherung Szenario „gefakter Schüler“	Die SuS spekulieren begründet über die Vorgehensweise des Lehrers / der Lehrerin im vorangegangenen Szenario.	L erläutert, wie man mittels spezieller Programme Mailkonten „knacken“ kann. Das eigentliche Programm „Wireshark“ wird dabei nicht vorgeführt, sondern nur die durch Wireshark erzeugten Protokolle.	Wireshark-Protokolle

10 Min.	Szenario „Manipulation auf E-Mail-Server“	1. Ein Schüler verschickt auf Bitten des Lehrers / der Lehrerin eine Einladung an einen anderen Schüler.	1.L bittet einen S einem anderen eine Einladung zu schicken. 2. L führt vor, wie man als Serveradmin fremde Mails verändern kann.	Beamer, Hamster
10 Min	Ergebnissicherung Szenario „Manipulation auf E-Mail-Server“	Die SuS antworten auf die Fragen „Welche Folgen kann das falsche Handeln eines Server-Admins haben?“ und „Wenn sich alle Mitarbeiter des Mail-Servers korrekt verhalten – ist dann eine Manipulation ausgeschlossen?“		Unterrichts-gespräch
10 Min.	Ergebnissicherung – Fazit	Die SuS fassen die Gefahren der E-Mail-Kommunikation zusammen.	L moderiert und übernimmt den TA und ergänzt anschließend das Tafelbild „Anforderungen an eine sichere Kommunikation“ L gibt Ausblick über die nächsten Stunden.	TA

L3 *Verlaufsplanung optionaler Einstieg in Lernabschnitt 3: „Der Goldkäfer“ (zwischen Stunden 4/5 und 6/7)*

Zeit	*Phase*	*Aktivitäten der SuS*	*Impulse von L*	*Medien/Sozialform*
5 Min	Einführung	Die SuS nennen die in der letzten Stunde erarbeiteten Anforderungen an sichere Kommunikation.	L fragt nach den Arbeitsergebnissen der letzten Stunde. → Überleitung: Heute Beschäftigung mit der Anforderung „Vertraulichkeit“.	---
15 Min	Motivation	Ein(e) Schüler(in) liest den ersten Textausschnitt aus „Der Goldkäfer“.	L teilt die AB aus und gibt Hinweise zur Aufgabenstellung.	AB „Der Goldkäfer“
10 Min	Brainstorming	Die SuS nennen Ideen zur Entschlüsselung des chiffrierten Textes: ~ - „Ausprobieren“ - „Welcher Buchstabe kommt am Häufigsten vor?“	L stellt dar, warum ein bloßes ausprobieren nicht zu einer Lösung führt (schiere Anzahl der zu testenden Möglichkeiten). Falls die SuS nicht auf die Möglichkeit der Häufigkeitsanalyse kommen, wird diese durch L erläutert.	Tafel zum Festhalten der Ideen
5 Min	Erläuterung	Die SuS lesen und verstehen den Bogen zu Häufigkeiten von Buchstaben in deutschen und englischen Texten.	L erläutert, warum man mit einer Häufigkeitsanalyse zum Ziel kommt und verdeutlicht den Unterschied zwischen Häufigkeiten von Buchstaben in deutschen und englischen Texten.	AB „Häufigkeiten“
10 Min	Erarbeitung I	Die SuS zählen arbeitsteilig die Häufigkeiten der einzelnen Zeichen im Text.	L gibt den Auftrag, die Häufigkeiten der Buchstaben im Text zu zählen.	AB „Häufigkeiten“
5 Min	Pause		L wirft mittels Beamer die Folie zum chiffrierten Text an die Wand	Beamer, Folie zum chiffrierten Text
10 Min	Erarbeitung II	Die SuS nennen die Häufigkeiten der Buchstaben.	L trägt die Häufigkeiten der Buchstaben in die Folie ein.	Beamer, Folie zum chiffrierten Text
5 Min	Erarbeitung II.1	Die SuS suchen nach Vorkommen von häufigen Tripeln und identifizieren das „;“ als t und die „4“ als h.	L verweist auf das häufigste Tripel in der englischen Sprache	Beamer, Folie zum chiffrierten Text; Arbeit im Plenum

5 Min	Erarbeitung II.2	Durch Heuristiken finden die SuS weitere Buchstaben des chiffrierten Textes und lösen ihn somit schrittweise.	Fall die Erarbeitung der SuS ins Stocken gerät, kann L durch Hinweise das Fortkommen sichern. Bei völligem Stillstand kann die Fortsetzung des GK und somit die Lösung des Rätsels verteilt werden.	Beamer, Folie zum chiffrierten Text Bei Bedarf: Fortsetzung des GK; Arbeit im Plenum
10 Min.	Erarbeitung II.3	Die SuS führen das Lösen des Textes durch Heuristiken in Kleingruppen fort und lösen den Text somit weiter auf.	L steht für Rückfragen bereit und hilft Gruppen, die nicht weiterkommen.	AB „Der Goldkäfer“, AB „Häufigkeiten“; Arbeit in Kleingruppen
15 Min	Sicherung	Die SuS reflektieren über ihre Arbeit und entwickeln dadurch ein Vorgehensmuster bei der Entschlüsselung monoalphabetisch verschlüsselter Texte.	L stellt die Frage nach welchen Schritten bei einer Dechiffrierung vorgegangen werden kann. L hält die Lösungen der SuS an der Tafel fest.	Tafel
Eventuelle Restzeit	„Puffer“	Die SuS üben das Verfahren der Entschlüsselung monoalphabetischer Verschlüsselungen.	L teilt Zusatzaufgaben aus.	AB „Zusatzaufgaben“

L3 Verlaufsplanung Stunden 6/7: Monoalphabetische Kryptographie – Caesars Geheimcode

Zeit	*Phase*	*Aktivitäten der SuS*	*Impulse von L*	*Medien/Soz.form*
10 Min	Einstieg	Die SuS fertigen eine Mitschrift an.	L gibt einen Ausblick über die folgenden Stunden und klärt erste Begriffe: Kryptographie, Kryptoanalyse, Kryptologie (Tafelanschrieb).	Tafel
20 Min	Lernaktion I	Die SuS bearbeiten Aufgabe 1 mit Hilfe der Doppelalphabetstreifen. Sie vervollständigen ihre Mitschrift der Begrifflichkeiten.	"Wir lernen heute eine berühmte Verschlüsselung kennen: Das Caesar-Verfahren". L teilt die AB aus, mit der Aufgabe, den Text zu lesen und Aufgabe 1 zu bearbeiten. Klärung der Begriffe Klartext, Geheimtext, Klartextalphabet, Geheimtextalphabet, Schlüssel (Tafelanschrieb).	AB, Doppelalphabet-streifen
5 Min	Sicherung I	Die SuS tauschen ihre Erfahrungen bei der Bearbeitung von Aufgabe 1 aus. Dabei soll auf den korrekten Gebrauch der Fachsprache geachtet werden.	L achtet vor allem auf den korrekten Gebrauch der Fachbegriffe und greift – wenn notwendig – korrigierend ein.	Plenum
15 Min	Lernaktion II	Die SuS lösen mit Hilfe des Programms „Krypto" Aufgabe II des Arbeitbogens in Partnerarbeit.	L stellt das Programm „Krypto" von Michael Kühn vor und demonstriert die damit die Caesar-Verschlüsselung. Anschließend gibt er / sie den Auftrag, Aufgabe II zu bearbeiten.	AB; „Krypto"
10 Min	Sicherung II	Die SuS erkennen, dass die Caesar-Verschlüsselung nur unzulängliche Sicherheit bietet. Sie notieren die Begriffsdefinitionen.	L fragt nach der Sicherheit des Caesar Verfahrens und führt die Begriffe monoalphabetisches Verschlüsselungsverfahren, Schlüsselraum und Verschlüsselungsalgorithmus ein.	Diskussion
15 Min	Vertiefung	Die SuS üben sich in der Arbeit mit „Krypto", indem sie den Arbeitsbogen „Sprüche bearbeiten".	L gibt den Arbeitsbogen „Sprüche" aus.	„Krypto", AB-Sprüche
	Hausaufgabe		L gibt die Hausaufgabe aus: Die SuS bekommen die Aufgabe, sich über das Kerckhoffs'sche Prinzip zu informieren.	

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.	

L3 *Verlaufsplanung optionaler Exkurs: Vigenère per Hand knacken (zwischen Stunden 8 und 9)*

Zeit	*Phase*	*Aktivitäten der SuS*	*Impulse von L*	*Medien/Sozialform*
5 Min.	Wiederholung	Ein(e) Schüler(in) erläutert kurz an der Tafel das Vigenere-Verfahren.	L bittet eine(n) Schüler(in) das aus der letzten Stunde bekannte Vigenere-Verfahren zu erläutern.	Schülervortrag
20 Min.	Vorbereitung der Arbeitsphase	Die SuS ermitteln die Länge des Schlüsselwortes indem sie die Abstände zwischen Buchstabengruppen zählen und anschließend deren GGT ausrechnen.	L erläutert, wie man in einem Vigenère-verschlüsselten Text die Länge des Schlüsselwortes herausfindet. Zu diesem Zweck wiederholt er/sie das Verfahren zu Bestimmung des GGT. Anschließende Frage: ~*“Wie könntet ihr nun vorgehen, um den Text weiter zu entschlüsseln?“* ->Reduzierung auf Caesar	Unterrichtsgespräch ; Beamer mit Seite 1 des AB „Vigenère knacken“
10 Min.	Arbeitsphase	Die SuS entschlüsseln den Text, indem Sie das Vigenère-Verfahren auf das Caesar-Verfahren reduzieren und anschließend (arbeitsteilig mit anderen Gruppen) eine Häufigkeitsanalyse durchführen.	L gibt Seiten 2 und 3 des AB „Vigenere knacken“ aus und erläutert das weitere Vorgehen. (Abzählen der Gruppen von 2 bis 7)	Partnerarbeit Seiten 2 und 3 des AB „Vigenère knacken“
10 Min.	Sicherung	Die SuS nennen die durch Häufigkeitsanalyse herausgefundenen Buchstaben des Schlüsselwortes. Anschließend nennen und erklären die SuS die einzelnen Schritte des Verfahrens.	L gibt den Geheimtext und den Schlüssel in „Krypto“ ein und entschlüsselt den Text. Anschließend hält er das Vorgehen beim Entschlüsseln an der Tafel fest.	Beamer, Programm „Krypto“, TA

L3 *Verlaufsplanung optionaler Exkurs: Film „Krieg der Buchstaben“ (zwischen Stunden 8 und 9)*

Zeit	*Phase*	*Aktivitäten der SuS*	*Impulse von L*	*Medien/Sozialform*
5 Min.	Einführung	Die SuS kennen ihren Arbeitsauftrag.	L gibt eine Einführung zum folgenden Film, teilt die Arbeitsaufträge aus und erläutert das weitere Vorgehen.	Arbeitsbogen „Arbeitsauftrag zum Film“
45 Min.	Film	Die SuS machen sich Notizen zu den Arbeitsaufträgen.		Film „Krieg der Buchstaben“
10 Min.	Austausch in Partnerarbeit	Die SuS tauschen sich mit ihren Sitzpartnern aus. Dabei ergänzen sie fehlende Informationen und diskutieren ihre Standpunkte zu Aufgabe 2 und 6.	L fordert die SuS auf, sich auszutauschen und ihrem Nachbarn den eigenen Standpunkt bzgl. Aufgabe 2 u. 6 mitzuteilen.	Arbeitbogen „ Arbeitsauftrag zum Film“
15 Min.	Sicherung	Die SuS teilen im Plenum ihre Ergebnisse zu den Aufgaben 1, 3, 4 und 5 mit. Dabei korrigieren und ergänzen die SuS die Ergebnisse ihre Mitschülerinnen. Anschließend legen sie begründet ihre Standpunkte zu den Arbeitsaufträgen 2 und 6 dar.	L fordert die SuS zunächst auf, ihre Lösungen zu den Aufgaben 1, 3, 4 und 5 im Plenum mitzuteilen. Anschließend erfragt L die Perspektiven der SuS zu den Arbeitsaufträgen 2 und 6.	Vorstellung im Plenum
15 Min.	Diskussion	Die SuS legen begründet ihre Standpunkte zu den Arbeitsaufträgen 2 und 6 dar.	L erfragt die Perspektiven der SuS zu den Arbeitsaufträgen 2 und 6 und moderiert die Diskussion.	Diskussion

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

L3 Verlaufsplanung Stunde 10: Das Prinzip der asymmetrischen Kryptologie

Zeit	*Phase*	*Aktivitäten der SuS*	*Impulse von L*	*Medien/Sozialform*
5 Min.	Einführung	Sie SuS starten in Paaren die Animation und Lesen die Erläuterungen und Aufgaben des AB.	L gibt einen Ausblick auf die Stunde knüpft an das Schlüsselaustauschverfahren der letzten Stunde an. Dieses soll nun in den Kontext „E-Mail“ gesetzt werden. L erläutert, wie die SuS die Animation starten können und verteilt die AB.	AB, Animation
30 Min.	Analyse	Die SuS bedienen die Animation und analysieren die Funktionsweise der asymmetrischen Kryptographie, indem sie in die Rolle von Alice und Bob schlüpfen und Nachrichten sowie digitale Unterschriften versenden. Sie bereiten sich auf die Präsentation ihrer Lösungen vor.	L steht für Nachfragen bereit und hilft bei der Bedienung der Animation.	AB, Animation
10 Min.	Präsentation/ Sicherung	Einzelne Paare stellen ihre Lösung vor.	L moderiert die Präsentation und greift – wenn nötig – korrigierend ein.	

L3 Verlaufsplanung Stunde 11: Konstruktion einer mathematischen Falltürfunktion – Semiprimzahlen und Zerlegung in Primfaktoren

Zeit	*Phase*	*Aktivitäten der SuS*	*Impulse von L*	*Medien/Sozialform*
5 Min.	Einführung	Die SuS rufen sich die aus dem Mathematikunterricht bekannten Primzahlen ins Gedächtnis. Sie nennen Beispiele für Primzahlen (Aufgabe 1) und zusammengesetzte Zahlen (Aufgabe 2).	L verteilt die AB und erläutert die Bedeutung der Primzahlen für die asymmetrische Kryptographie. L wiederholt die Definition einer Primzahl.	AB
10 Min.	Erarbeitung	Die SuS entdecken mittels einer Online-Animation eine Methode zum Auffinden von Primzahlen: Das Sieb des Eratosthenes.	L gibt Hilfestellung bei der Bedienung der Animation.	AB, Online-Animation
5 Min.	Sicherung	Die SuS erläutern unter Beachtung der Fachsprache das Sieb des Eratosthenes und den Zusammenhang zwischen (Semi)Primzahlen und der Kryptographie.	L fragt nach der Funktionsweise des Siebs des Eratosthenes.	
10 Min.	Vertiefung	Die SuS bearbeiten Aufgabe 4 und 5 des AB. Dabei nutzen sie CrypTool, um zu bestimmen, ob eine Zahl Primzahl ist und geben die Faktoren der Semiprimzahlen an.	L hilft einzelnen SuS, die mit der Bedienung von CrypTool Schwierigkeiten haben. Er / Sie fragt nach den Lösungen für Aufgabe 4.	Tabellarische Darstellung der Primzahlen bis 16200, AB
5 Min.		Recherche zur RSA Factoring Challange	L gibt Startschuss zur Recherche	Internet
10 Min.		Diskussion über die Rechercheergebnisse	L moderiert die Diskussion und gibt ggf. weitere Informationen	Tabelle mit RSA-Zahlen

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

Zeit	*Phase*	*Aktivitäten der SuS*	*Impulse von L*	*Medien/Soz.form*
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“ 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

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

L4 Verlaufsplanung Stunde 16: Prinzip der digitalen Unterschrift

Zeit	*Phase*	*Aktivitäten der SuS*	*Impulse von L*	*Medien/Sozialform*
15 Min.	Einführung	Sie SuS starten in Paaren die Animation und Lesen die Erläuterungen und Aufgaben des AB.	L verweist auf die Leitfrage der UE → „Wie können Vertraulichkeit, Authentizität und Integrität bei E-Mail-Kommunikation gewährleistet werden.“ Er / Sie gibt einen Ausblick auf die Stunde, die der Beantwortung der Frage nach Authentizität und Integrität gewidmet ist. L verteilt die Arbeitsbögen und erläutert die Aufgabenstellung.	AB, Animation
15 Min.	Analyse	Die SuS bedienen die Animation und verstehen die Funktionsweise der digitalen Signatur, indem sie in die Rolle von Alice und Bob schlüpfen und Nachrichten versenden.	L steht für Nachfragen bereit und hilft bei der Bedienung der Animation.	AB, Animation
15 Min.	Sicherung	Ein(e) Schüler(in) erläutert das Verfahren der digitalen Signatur. Ein(e) weitere(r) Schüler(in) hält die Schrittfolge des Verfahrens an der Tafel fest. Die Lerngruppe hilft bei der Erstellung des Tafelbildes.	L moderiert die Sicherung.	Schülervortrag, TA

L4 Verlaufsplanung Stunde 17: Digitale Unterschrift anwenden

Zeit	*Phase*	*Aktivitäten der SuS*	*Impulse von L*	*Medien/Sozialform*
3 Min.	Einführung	Die SuS kennen den Ablauf und Ziel der Stunde.	L knüpft an die letzten Stunden an und gibt einen Ausblick auf die Unterrichtsstunde.	
15 Min.	Vorbereitung	Die SuS installieren OpenPGP und erzeugen ein Schlüsselpaar. (Resp.: Holen sich ein Zertifikat von einem Trustcenter) Sie installieren das Plugin *Enigmail.*	L teilt die Anleitung aus und erläutert die Aufgabe und gibt Hilfestellung bei der Installation der Programme.	Anleitung, *OpenPGP* und *Enigmail*, bzw. *PGP4Win*
15 Min.	Erarbeitung	Die SuS tauschen ihre öffentlichen Schlüssel aus, senden und empfangen verschlüsselte und signierte E-Mails. Sie überprüfen mittels Socket Sniff, ob die E-Mails noch sensible Informationen im Klartextformat enthalten.	L erläutert das weitere Vorgehen und gibt Hilfestellung bei der Bedienung der Programme.	Anleitung, *Thunderbird* bzw. *Outlook*
12 Min.	Sicherung	Ein(e) Schüler(in) führt vor, welches Format die verschlüsselten E-Mails besitzen (Socket Sniff). Die SuS beschreiben, wie Authentizität, Vertraulichkeit und Integrität der E-Mail-Kommunikation gewährleistet wurde.	L fragt, wie die drei Anforderungen an sichere Kommunikation erreicht wurden und hält die Antworten der SuS an der Tafel fest.	TA

L5 Verlaufsplanung Stunden 18/19: Gruppenpuzzle zur Informationsfreiheit

Zeit	*Phase*	*Aktivitäten der SuS*	*Impulse von L*	*Medien/Sozialform*
10 Min.	Einführung	Die SuS finden sich in Stammgruppen zusammen und kennen ihren Arbeitsauftrag und den Ablauf der Stunde.	L verteilt die Arbeitsbögen und erläutert den Ablauf der Stunde.	AB Gruppenpuzzle
35 Min.	Expertenphase	Die SuS finden sich in den Expertengruppen zusammen. Sie erfassen ihr Thema zunächst in Einzelarbeit und erarbeiten anschließend innerhalb der Gruppe einen Vortrag zu ihrem Thema.	L organisiert die räumliche Aufteilung der SuS und gibt – wenn nötig – Hilfestellung.	AB Gruppenpuzzle
25 Min.	Vortragsphase	Die SuS kehren in ihre Stammgruppen zurück und halten einen Vortrag zu ihrem Thema. Die Zuhörer machen sich Notizen.	L organisiert den Gruppenwechsel.	Schülervortrag
20 Min.	Sicherung/Diskussion	Die SuS beantworten die Leitfragen des Gruppenpuzzles. Ausgehend von den Leitfragen der Gruppe „Kommunikationsfreiheit“ diskutieren die SuS über den Wert der Informationsfreiheit.	L projiziert die Leitfragen des Gruppenpuzzles. Zuletzt sollten die Fragen der Gruppe „Kommunikationsfreiheit“ behandelt werden. Diese Leitfrage dient als Grundlage für eine Diskussion, die L moderiert.	Beamer/OH-Projektor; Diskussion