Vorschlag für eine Stoffverteilung

Die Tabelle enthält einen Vorschlag für eine Stoffverteilung. Die Prioritäten A und B summieren sich auf 13 Einzelstunden. Die Ideen der fünften Spalte sollten langfristig hängenbleiben, die der sechsten stellen Zusammenhänge innerhalb der Krypto-Einheit her.

Beachten Sie, dass gegenwärtig (2021) Teile davon in IMP bzw. im Brückenkurs Informatik verortet sind. Ein durchgängiger Kryptografieunterricht wie hier skizziert kann aber im zweistündigen Wahlfach Informatik erfolgen.

Prio, h		Thema	Methodenvorschlag und Stoff	Langfristiges Lernziel	Mittelfristiges Lernziel
Symmetrische Kryptosysteme					
B	1	Vertrauen	UG: 2-3 Beispiele aus dem Skript, z.B.: Unterschrift, Geld, Personalausweis	„Krypto (und damit Informatik) betrifft etwas zutiefst Menschliches“	Krypto ist nicht nur Chiffrieren
A	1	Caesar	LV Prinzip Ü chiffrieren, dechiffrieren, angreifen UG: Schwachstelle?	Begriffe Chiffre, Schlüssel, Klartext, Geheim-(Chiffre-)text, Angriff	Abk. K, M, C Brute-force-Angr.
A	1	Substitution	LV Prinzip UG Schwachstelle noch da? UG Brute-force-Angriff unmöglich Ü chiffrieren/dechiffrieren UG mögliche Schwachstelle	„Es reicht nicht, gegen den Angriff von gestern immun zu sein“	Monoalphabetisch
B	1	Substitution	Ü Angriff mit Cryptool	„Eine gute Idee bringt mehr als 1000 schnelle Rechner“	Wenn man OTP machen will: „nicht alle Klartexte passen dazu“
B	1	Vigenère	LV Prinzip UG Schwachstelle noch da? Ü chiffrieren und dechiffrieren UG mögliche Schwachstelle und Angriff darauf	Galt 300 Jahre lang als unknackbar, und doch...	Wenn man Enigma machen will: „Chiffre hat kurze Periode“
C	1	Vigenère	Ü Angriff mit Autokorrelation oder Kasiski-Test		„Jede Chiffre wird gebrochen.“
D	1	Enigma	LV oder vorbereitende Lese-HA: Prinzip Ü chiffrieren und dechiffrieren mit Simulator		
D	1	Enigma	LV, Ü: Rejewski-Angriff	Informatik entscheidet Kriege	

Prio, h		Thema	Methodenvorschlag und Stoff	Langfristiges Lernziel	Mittelfristiges Lernziel
C	2	One-Time-Pad	LV, UG: Prinzip, 3 Kriterien absolut sicher und doch unpraktisch	NICHT jede Chiffre kann gebrochen werden!! Nichtexistenz-beweis	
Asymmetrische Kryptosysteme:					
A	1	Asymmetrische Krypto-systeme	UG Motivation UG mit Vorhängeschloss chiffrieren/dechiffrieren UG MITM-Angriff auf Schlüsselaustausch	Unterschied öffentlicher/ privater Schlüssel	
B	1	Modulare Arithmetik	UG und Ü	Gewohnte Rechenregeln gelten auch in anderen Mengen	
B	1	Schnelle Potenzie-rung	UG Motivation Ü Beispiele von Hand	„Eine gute Idee bringt mehr als 1000…“ (s.o.)	
C	1-2	schnelle Pot. implemen-tieren	UG Iteration und/oder rekursive Fallunterscheidung Ü programmieren		Ab und zu mal wieder program-mieren… :-)
A	2	Chiffrieren mit RSA	LV, Ü Schlüsselerzeugung von Hand Ü Schlüsselverteilung im Klassenzimmer Ü kurze „Nachrichten“ an anndere Schüler chiffrieren		
B	2	Signaturen mit RSA	LV, Ü	Krypto ist mehr als Chiffrieren (s.o.)	
B	1	Geheim und authentisch	Siehe Skript		
A	2	Zertifkate SSL/TLS	Siehe Skript		
A	2	Hashfunktio nen	Siehe Skript CS Unplugged	Kryptowissen ist essenziell für Nutzung von Diensten; Folgen mangelnden Infor-matikwissens für die Gesellschaft	

Auswahl einiger Bonusthemen

Prio, h		Thema	Methodenvorschlag und Stoff	Langfristiges Lernziel	Mittelfr. Lernziel
D	1-2	Secret Sharing	Optisch mit Folien; unplugged mit Zahlenschlössern; algebraisch mit ganzrationalen Fkt; geometrisch mit Ebenen.	Vielfalt der Kryptografie als „Informatik des Vertrauens“	
D	2	ITG für Fortgeschritten: Enigmail	Derzeit (2021) im Skript noch nicht enthalten. Anleitung unter *Piratenwiki*[48]		
D	1-2	Zero-knowledge-Protokoll	Derzeit (2021) im Skript noch nicht enthalten. Vollständiges Modul CS Unplugged: *Information Hiding*[49]	Vielfalt der Kryptografie als „Informatik des Vertrauens“	

48 *https://wiki.piratenpartei.de/HowTo_Emails_verschlüsseln_mit_PGP_mit_Thunderbird*
49 *http://csunplugged.org/information-hiding/*