Mathematische Grundlagen der Kryptologie

Stunden	Inhaltsbezogene Kompetenzen	Inhalt / *Material (in Ordner 2_kopiervorlagen und 4_Lösungen)*
1 – 3	Wiederholung aus Klasse 8/9: CÄSAR-Verfahren, modulo-Operation, Kongruenzrelation	*01a.0_mgk_Caesar bzw.* *01a.1_mgk_Alternative_Caesar* *01b_mgk_mod_und_Kongruenz*
4, 5	Modulares Addieren	Kennenlernen des benötigten Gesetzes, Vertiefung des Unterschiedes „=“ und „≡“. *optional:* Beweis der Regel (binnendiff.) *02a_mgk_Modulares_ Addieren*
6, 7	Modulares Multiplizieren	Kennenlernen des benötigten Gesetzes, Vertiefung des Unterschiedes „=“ und „≡“. *optional:* Beweis der Regel (binnendiff.) *02b_mgk_Modulares_ Multiplizieren*
8 – 10	Modulares Potenzieren	grundlegendes Rechengesetz, Problem der Reste großer Potenzen und dessen Lösung, Umsetzung mit dem WTR *optional:* Beweis der Regel *02c_mgk_Mod._Potenzieren_(Version_CASIO)* *bzw.* *02c_mgk_Mod._Potenzieren_(Version_TI)*
11 – 15	Ver- und Entschlüsseln durch (modulare) Multiplikation	Multiplikation und Faktorisierung im Vergleich, Prinzip der Ver- und Entschlüsselung durch Mult. Info-Block: Übertragbarkeit der Ergebnisse auf Bearbeitung des Problems mit Computern, Größe real verwendeter Primzahlen. *03a_mgk_ Einstieg - Verschlüsseln_durch_Mult* *03b.0_mgk_Verschlüsseln durch modulare Mult*
	optionaler Exkurs: diophantische Gleichungen	*03b.1_mgk_diophantische_Gln* Lösung linearer Kongruenzgleichungen, Lösungsansätze zur Lösung linearer Gleichungen in zwei Variablen
+2h *(optional)*	Bestimmung des multiplikativen Inversen in mod	Erweiterter Euklidischer Algorithmus. Empfehlung: Erarbeitung im U-Gespräch (siehe *00_mgk_hintergrund*). Für starke Gruppen: Vorschlag einer S-zentrierten Erarbeitung im AB *03c_mgk_Erw_Euklid_Alg_S-zentriertS*

+1h (optional)	*Optionaler Exkurs: Einweg- und Falltürfunktionen*	Kennenlernen der Begriffe, auch Beispiele im nichtmathematischen Zusammenhang. Ebenfalls als Hausaufgabe geeignet. *03d_mgk_Einweg-und_Falltürfunktionen*
+2h (optional)	*Optionaler Exkurs: Neutrale und Inverse Elemente*	Ein Ausflug in die mathematischen Grundlagen: Genauere Betrachtungen der Begriffe und Beispiele. *03e_mgk_ Neutrale_und_inverse_Elemente*
16 - 18	RSA an einfachen Beispielen	Kennenlernen der RSA-Verschlüsselung. Abschließende Übung durch Ver- und Entschlüsseln *04_mgk_Das_RSA-Verfahren* Das Prinzip des Schlüsseltauschverfahrens bleibt hier unberücksichtigt, da es im Themenbereich „Informationsgesellschaft und Datensicherheit“ ausführlich behandelt wird. Es kann (mit zusätzlichem Zeitaufwand) jedoch auch sinnvoll hier bei der Einführung des RSA-Verfahrens behandelt werden (siehe *00_hintergrund*)
	Das BP-Item (9) „die behandelten Verschlüsselungsverfahren vergleichend behandeln“ findet sich im Themenbereich IuD	*06_iud_ab_vergleich_verfahren*