Informationsgesellschaft und Datensicherheit (3.1.1.4)

Std.	Bildungsplan, inhaltsbezogene Kompetenzen	Inhalt / Material
1	(7) Anwendungsbereiche beschreiben, in denen Verschlüsselung eingesetzt wird	Datensicherheit – Wozu? *01_iud_ab_DatensicherheitWozu.odt*
2	(2) *Transpositionsverfahren* (z.B. Skytale), *monoalphabetische Substitution* und *polyalphabetische Substitution* vergleichen (s.u.)	Skytale (als Transpositionsverfahren) *02_iud_ab_Skytale.odt* *02_iud_Skytale_Vorlage.pdf*
3	(Wdh aus Klasse 7)	Cäsar-Verfahren mit Verbesserungen *03_iud_ab_Caesar.odt* *04_iud_ab_VerbesserungCaesar.odt*
4, 5, 6	(1) Das *Vigenère-Verfahren* erklären und durchführen (3) Eine grundlegende Angriffsstrategie auf das *Vigenère-Verfahren* erklären und an einfachen Beispielen durchführen PBK: 2.11 (6) Teillösungen zur Lösung des Gesamtproblems nutzen	Vigenère-Verfahren *05_iud_ab_Vigenere.odt* *05_iud_Vigenere_Vorlage.pdf* *06_iud_ab_BrechenTeil2.odt* *07_iud_ab_BrechenTeil1.odt*
7	(4) das *One-Time-Pad*-Verfahren erklären und begründen, dass es sich um ein absolut sicheres Verschlüsselungsverfahren handelt PBK: 2.14 (7) Entscheidungen auf der Grundlage informatischen Sachverstands treffen und diese sachegrecht begründen	One-Time-Pad-Verfahren *08_iud_ab_OneTimePad.odt*
8	(2) *Transpositionsverfahren* (z.B. Skytale), *monoalphabetische Substitution* und *polyalphabetische Substitution* vergleichen (s.o.) PBK: 2.14 (3) unterschiedliche Lösungsansätze und Vorgehensweisen miteinander vergleichen und bewerten	*Vergleich und Zuordnung der kennengelernten Verfahren* *09_iud_ab_TypenStruktur.odt*
	(6) erläutern, dass die Sicherheit von Verschlüsselungsverfahren nicht von der Geheimhaltung des *Algorithmus* abhängen darf (*Kerckhoffs'sches Prinzip*)	Das Kerckhoffs'sche Prinzip *10_iud_ab_Kerckhoffs.odt*

	PBK: 2.14 (7) Entscheidungen auf der Grundlage informatischen Sachverstands treffen und diese sachegrecht begründen	
9	(5) erläutern, dass moderne *symmetrische Verschlüsselungsverfahren* auf elementaren Verschlüsselungsverfahren basieren und einen Kompromiss zwischen Sicherheit und Praktikabilität sind PBK: 2.14 (5) Kenntnisse über den inneren Ablauf informatischer Systeme im Alltag nutzen (7) Entscheidungen auf der Grundlage informatischen Sachverstands treffen und diese sachegrecht begründen	AES *CrypTool 1*[1]
10	(8) die Verschlüsselung eigener Daten mit Hilfe eines geeigneten Programms durchführen PBK: 2.14 (5) Kenntnisse über den inneren Ablauf informatischer Systeme im Alltag nutzen 2.11 (1) mit dem Schulnetz (zum Beispiel Homeverzeichnis, Tauschverzeichnis, mobile Datenträger, Netzwerkdrucker) zielorientiert arbeiten	Daten verschlüsseln mit VeraCrypt *11_iud_VeraCrypt_Anleitung.odt*
11, 12	(9) eine aktuell eingesetzte Technologie erläutern, mit der *personenbezogene Daten* gesammelt werden (z.B. Webtracking, Cookies, Geodaten) (10) Möglichkeiten erläutern, um das Sammeln *personenbezogener Daten* einzuschränken (z.B. anonymes Surfen, Rechteverwaltung von Apps, Standortfreigabe) PBK: 2.14 (8)Auswirkungen von Computersystemen auf Gesellschaft, Berufswelt und persönliches Lebensumfeld aus verschiedenen Perspektiven bewerten 2.14 (9) im Zusammenhang einer digitalisierten Gesellschaft einen eigenen Standpunkt zu ethischen Fragen in der Informatik einnehmen und ihn argumentativ vertreten	Internet-Tracking klicksafe-Modul „*Datensatz – Datenschatz?*[2] *Internet*

1 *https://www.cryptool.org/de/* (Abgerufen am 8.5.18)
2 *https://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_Allgemein/ks_to_go_Datensatz_-_Datenschatz.pdf* (Abgerufen am 8.5.18)