Zusatzaufgabe. Zum Abschluß des Kryptographiekapitels und anläßlich des verregneten langen Wochenendes gibt es einen Wettbewerb: Am Freitag 14.5. werden um 14:00 im Teachcenter zwei verschlüsselte Texte angezeigt. Für die jeweils ersten drei abgegebenen Lösungen (inklusive Lösungsweg) gibt es Extrapunkte.

Aufgabe 41. Das folgende Beispiel illustriert, daß die Wahl kleiner Schlüssel die Sicherheit des RSA-Verfahrens verringert.

Tom schickt die gleiche Botschaft an seine Freundinnen Gernot, Wolfi und Sebastian, die ihm vorher die öffentlichen Schlüssel $(m_1 = 1219, r_1 = 3)$, $(m_2 = 799, r_2 = 3)$ und $(m_3 = 1189, r_3 = 3)$ bekanntgegeben haben. Die drei Botschaften sind $y_1 = (248, 1093, 354)$, $y_2 = (274, 648, 178)$ und $y_3 = (682, 40, 1140)$. Entschlüssle die Botschaft, ohne die Primfaktorzerlegung der Schlüssel m_i durchzuführen (Computer oder Taschenrechner für Zwischenrechnungen ist zugelassen).

Aufgabe 42. Überprüfe anhand von Wahrheitstafeln, ob die folgenden Aussageformen äquivalent sind:

(a) $(A \to B) \to C$ und $A \to (B \to C)$

(b) $(\neg A \to B) \to (B \vee C)$ und $(A \to B) \vee C$.

Aufgabe 43. Der Speiseplan einer Mensa folgt folgenden Regeln:

(i) Wenn es keine Mehlspeise gibt, dann muß es eine Suppe geben.

(ii) Wenn es Suppe und Mehlspeise gibt, dann gibt es keinen Salat.

(iii) Wenn es Salat gibt oder keine Mehlspeise dabei ist, darf es keine Suppe geben.

Stelle die Bedingungen als logische Aussageformen P_1, P_2, P_3 dar und bestimme eine möglichst einfache Formel, die zu $P_1 \wedge P_2 \wedge P_3$ äquivalent ist.

Aufgabe 44. Orpheus steht in der Unterwelt vor drei Türen, von denen genau eine in die Freiheit führt.

- Auf der linken Tür steht: hier geht es hinaus.
- Auf der mittleren Tür steht: rechts geht es nicht hinaus.
- Auf der rechten Tür steht: hier geht es nicht hinaus.

Mindestens eine Aufschrift ist wahr und mindestens eine Aufschrift ist falsch. Wo geht es hinaus?

Aufgabe 45. Beweise mit den Regeln des logischen Schließens[3] den **Modus Tollens**

$$((P \to Q) \wedge \neg Q) \to \neg P.$$

Aufgabe 46. Beweise mit den Regeln des logischen Schließens das Klammer-Änderungsgesetz für "$\to$":

$$A \to (B \to C) \iff (A \wedge B) \to C$$

[3]siehe `https://www.math.tugraz.at/idm-lv/dmi/2021/Uebungsblaetter/logikregeln.pdf`