6 Komposition von Chiffrierverfahren

- Hintereinanderausführung zweier Chiffrierungen kann die Sicherheit erhöhen
- Positivbeispiel: überchiffrierter Code
- Negativbeispiel: doppelte CAESAR-Chiffrierung
- zu betrachten: Gruppeneigenschaft
  - seien $\boldsymbol{X}_{t_1}$ und $\boldsymbol{X}_{t_2}$ Chiffrierverfahren derselben Klasse mit den Schlüsseln t_1 und t_2
  - Gruppe, falls $\boldsymbol{X} = \boldsymbol{X}_{t_1}\boldsymbol{X}_{t_2}$ auch derselben Klasse angehört
  - dann existiert eine Operation $\bullet$, sodass $\boldsymbol{X}_t = \boldsymbol{X}_{t_1}\boldsymbol{X}_{t_2}$ mit $t = t_1 \bullet t_2$ (für CAESER z.B. $\bullet = +$)
  - ist $\bullet$ kommutativ, ist auch die Komposition kommutativ, also $\boldsymbol{X}_{t_1}\boldsymbol{X}_{t_2} = \boldsymbol{X}_{t_2}\boldsymbol{X}_{t_1}$ (aber auch Kommutativität ohne Gruppeneigenschaft möglich, Beispiel monographische, monoalphabetische Substitution und Transposition)
- Beispiele für Gruppen: CAESAR, VIGENÈRE gleicher Periodenlänge, allgemeine monoalphabetische Substitution
- keine Gruppen: vollzyklische Substitutionen, ALBERTI-Schritte, ROTOR-Schritte
- auch VIGENÈRE beliebiger Periodenlänge bildet Gruppe; Periode der Komposition ist kgv der Einzelperioden
- Komposition erhöht nur dann die Sicherheit, wenn man zu einer komplexeren Verfahrensklasse kommt
- zueinander *ähnliche* Verfahren ($X_2 = TX_1$, T schlüsselunabhängig) sind gleich sicher

- zur Erhöhung der Sicherheit sinnvoll, Verfahren zu kombinieren, die möglichst unterschiedlich arbeiten und nicht kommutativ sind (z.B. Substitution und Transposition unterschiedlicher Block- bzw. Periodenlänge)