



Aufgaben

1. a) *Erstelle ein Diagramm „Verschlüsselungsverfahren“ mit den Begriffen Substitutionsverfahren, mono-/polyalphabetische Verfahren, symmetrische Verfahren, asymmetrische Verfahren, Transpositionsverfahren und erkläre jeden Begriff kurz.*
- b) *Notiere alle bisher kennengelernten Verschlüsselungsverfahren und ordne sie den Typen aus (a) zu.*

2. *Erstelle eine Übersicht über alle Verfahren:*

Verfahren	(Wie) kann es gebrochen werden? z.B. Anzahl der Möglichkeiten bei brute force	Bewertung: Wie sicher ist das Verfahren?
...		

3. a) *Was ist eine aktuell sichere Schlüssellänge bei RSA-Verfahren?*
- b) *Was ist eine aktuell sichere Schlüssellänge bei AES-Verfahren?*