



Übungsaufgaben zur Bearbeitung **zu Hause** vor der Übungsstunde

Aufgabe 1

Bob sendet Alice die Nachricht `LOESUNG`. Die beiden haben die Verwendung der 26 lateinischen Buchstaben vereinbart ($A \rightarrow 0$, $B \rightarrow 1$, ...) und sie benutzen zur Verschlüsselung ein Transpositions-Chiffre mit multiplikativem Schlüssel 7 und additivem Schlüssel 9.

- Wie lautet der verschlüsselte Text?
- Wie bestimmt Alice aus der empfangenen verschlüsselten Nachricht den Klartext?

Aufgabe 2

Der Text „GDINF“ wurde unter Verwendung des 7-Bit ASCII-Codes mit einem One-Time-Pad verschlüsselt. Das Ergebnis ist „SUPER“. Wie lautet der One-Time-Pad?