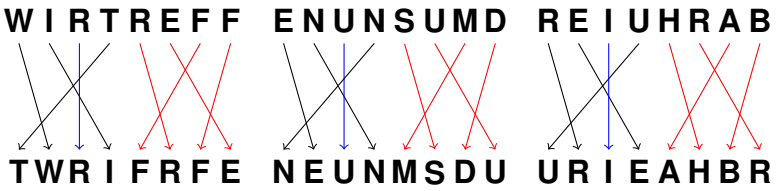
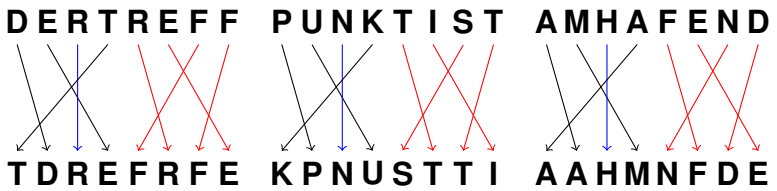
Lösung 1 Durch verschiedene Füllbuchstaben kann der letzte Block variieren. Die Lösung kann zum Beispiel so aussehen:



Lösung 2 Das Verfahren ist umgekehrt zum Verschlüsselungsvorgang. Man teilt die Nachricht in Blöcke der bekannten Länge und wendet den Schlüssel (= Permutation) umgekehrt an. Das bedeutet, die Permutation wird von unten nach oben gelesen. Bei der Permutationshilfe legt man das untere Fenster auf die Nachricht und schreibt die Buchstaben dann entsprechend gegen die Pfeilrichtung in das obere Fenster.

Lösung 3 Die entschlüsselte Nachricht lautet **DER TREFFPUNKT IST AM HAFEN**.



Lösung 4 Zu dieser Aufgabe gibt es keine allgemeine Lösung.

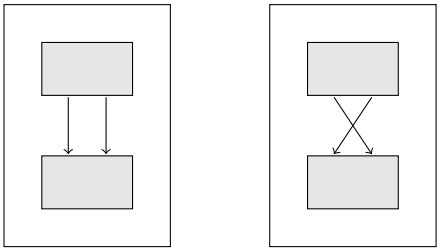
Lösung 5 Zu dieser Aufgabe gibt es keine allgemeine Lösung.

CC BY NC SA

Version vom 2019-08-06

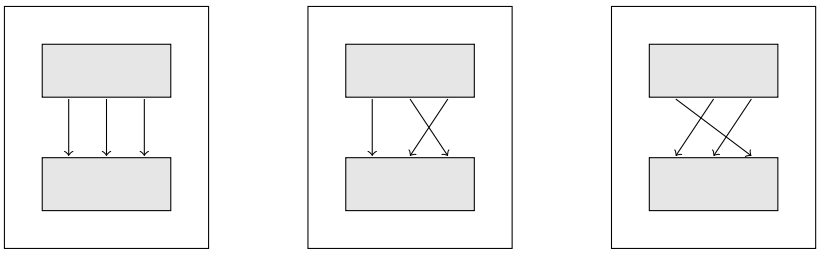
Lösung 6 Für die Blocklänge 2 gibt es zwei Schlüssel (Permutation), aber nur eine davon ist für eine Verschlüsslung sinnvoll. Die beiden Buchstaben werden dabei einfach vertauscht. Die Permutationen sehen so aus:

$$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

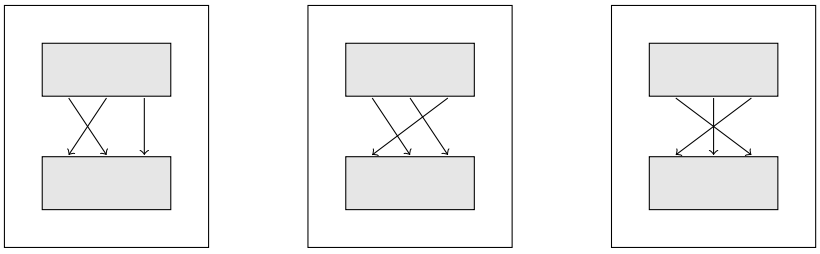


Für die Blocklänge 3 gibt es 6 mögliche Schlüssel (Permutationen). Dabei ist wieder eine nicht sinnvoll:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$



$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$



Version vom 2019-08-06