



Die Buchstaben bleiben, **was** sie sind, aber nicht, **wo** sie sind.
Solche Verschlüsselungen heißen **Transposition**. (Das Wort *Transposition* ist abgeleitet vom lateinischen Wort *transponere* = verschieben.)

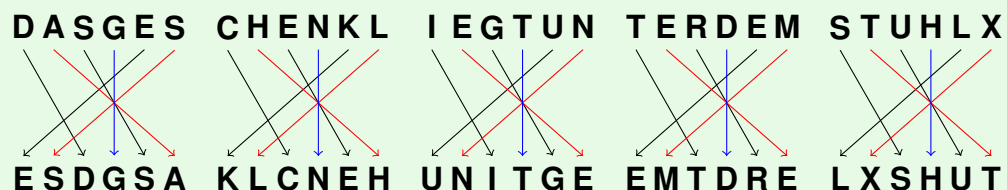
Bei einer Blockverschlüsselung wird eine Nachricht ohne Leerzeichen in Blöcke einer festen Länge unterteilt. Ist die Nachricht zu kurz, werden Füllbuchstaben ans Ende gesetzt. Es gibt verschiedene Möglichkeiten, die Blöcke zu verschlüsseln. Wir betrachten den Modus *Elektronic Code Book (ECB)*, bei dem jeder Block von den anderen unabhängig verschlüsselt wird. Dafür benutzen wir als Schlüssel Permutationen. Eine Permutation vertauscht die Buchstaben eines Textes auf eine vorgegebene Weise. Dabei schreiben wir die Permutation auf, indem wir die neuen Stellen der Buchstaben unter die alten Stellen schreiben.

Beispiel Für die Blocklänge 6 und die Permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 5 & 4 & 1 & 2 \end{pmatrix}$$

schreiben wir den ersten Buchstaben auf die dritte Stelle, den zweiten Buchstaben auf die sechste Stelle, den dritten Buchstaben auf die fünfte Stelle, den fünften Buchstaben auf die erste Stelle und den sechsten Buchstaben auf die zweite Stelle. Der vierte Buchstabe bleibt dabei einfach stehen.

Also wird die Nachricht **DAS GESCHENK LIEGT UNTER DEM STUHL** verschlüsselt zu **ESDGS AKLCNEHUNITGEEMTDRELXSHUT**. Dies sieht man besser, wenn man die Nachricht in Blöcke einteilt und mit Pfeilen zeigt, welche Buchstaben an welche Stellen geschoben werden:



Die Anordnung der Pfeile einer Permutation bleibt bei jedem Block gleich. Deswegen können wir die Permutationshilfen nutzen, um Nachrichten schneller und korrekt zu verschlüsseln. Dabei ist es wichtig, dass du die Buchstaben nicht zu nah aneinander schreibst. Nutze dafür die Vorlage für Texte und schreibe in jedes Kästchen genau einen Buchstaben. Lege dann die Permutationshilfe der richtigen Blocklänge mit dem oberen Fenster auf den Block des Klartextes und schreibe die Buchstaben dann entsprechend der Pfeile in das untere Fenster.