- Wenn ein Schlüssel übers Computernetz übertragen wird, dann kann er abgehört werden. Mehr dazu im Kapitel über das Schlüsselaustausch-Problem (Kapitel 10).
- Es ist wesentlich schwieriger, als man denkt, große Mengen an Zufallszahlen herzustellen, die wirklich zufällig sind. Mehr dazu im Kapitel über Zufallszahlen (Kapitel 14).

Die genannten Nachteile sind so gravierend, dass der One-Time-Pad in der Praxis nicht eingesetzt wird. Es gibt jedoch sehr viele Verfahren, die die dahinter stehende Idee ausnutzen, indem sie aus einem kurzen Schlüssel einen langen generieren, der dann wie im One-Time-Pad eingesetzt wird. Eine gewisse Bedeutung hat der One-Time-Pad zudem im Geheimdienst- und im Militärbereich. Ist beispielsweise Bob als Spion im Auftrag des Geheimdiensts von Kryptoland unterwegs, dann trägt er stets einen versiegelten Umschlag mit sich, der eine längere Folge von zufälligen Buchstaben enthält. Diese Buchstabenfolge kann Bob in Notfällen als One-Time-Pad-Schlüssel verwenden, um eine Nachricht an die Einsatzzentrale zu schicken. Ein solches Verschlüsselungsverfahren ist sehr sicher und obendrein einfach zu handhaben. Selbst ein Laie kann damit eine Nachricht zuverlässig verschlüsseln und braucht dazu nur Stift und Papier.

4.4 Permutationschiffren

Neben den Substitutionschiffren gibt es eine weitere einfache Klasse von Verschlüsselungsverfahren: die **Permutationschiffren**. Bei einer Permutationschiffre werden die Buchstaben des Klartexts nicht durch andere ersetzt, sondern in ihrer Reihenfolge vertauscht. Betrachtet man beispielsweise jeweils fünf Klartextbuchstaben auf einmal, dann ist durch folgende Vorschrift eine Permutationschiffre gegeben:

> Buchstabe 4 kommt auf Position 1, 1 auf 2, 2 auf 3, 5 auf 4 und 3 auf 5. Der Schlüssel ist hierbei (in Kurzform): (4, 1, 2, 5, 3).

Der Klartext

ESGIBTZWEIARTENVONLEUTEN:SOLCHE,DIEZUENDEBRINGEN,WASSIEANFANGEN.

wird durch diese Chiffrierung zum Geheimtext:

IESBGETZIWEARNTLVOENNUTS:EHOLEC,ZDIUEEENBDGRIENS,NWSANIEFAEANNG.

Eine solche Verschlüsselung können Alice und Bob auch mit einem Passwort als Schlüssel durchführen, das leichter zu merken ist als eine Folge von Zahlen. Die Vertauschungsvorschrift erhalten sie, indem sie die Buchstaben dieses Worts alphabetisch sortieren. Beispielsweise ergibt sich aus dem Passwort ALICE die alphabetisch sortierte Folge ACEIL, was (1, 4, 5, 3, 2) entspricht. Am einfachsten

können Alice und Bob dieses Verfahren nutzen, wenn Absenderin Alice den Klartext unter dem Schlüsselwort zeilenweise aufschreibt und dann die Spalten umsortiert:

```
ALICE      ACEIL
_____      _____
ESGIB      EIBGS
TZWEI      TEIWZ
ARTEN      AENTR
VONLE      VLENO
UTENS      UNSET
OLCHE  =>  OHECL
DIEZU      DZUEI
ENDEB      EEBDN
RINGE      RGENI
NWASS      NSSAW
IEANF      INFAE
ANGEN      AENGN
```

Der Geheimtext lautet also EIBGSTEIWZA... Eine in dieser Form verwendete Permutationschiffre wird auch als **Würfel** bezeichnet. Führt Alice den Würfel zweimal hintereinander mit unterschiedlichen Passwörtern aus, dann spricht man von einem **Doppelwürfel**.

Die Kryptoanalyse einer Permutationschiffre ist oft einfacher, als man zunächst vermutet. Mallory stehen für diesen Zweck Verfahren zur Verfügung, die Häufigkeiten von Buchstabenpaaren (Bigrammen) und Buchstabendreiergruppen (Trigrammen) ausnutzen. Im Deutschen kommen beispielsweise die Bigramme EN, ER und CH sowie die Trigramme ICH, EIN und UND am häufigsten vor. Mallorys Kryptoanalyse läuft daher darauf hinaus, die Buchstaben des Texts auf unterschiedliche Weise umzugruppieren, um danach jeweils die Anzahl der Bigramme und Trigramme zu untersuchen. Bei einer Schlüssellänge von fünf (wie in den beiden Beispielen) ist dies durchaus zu schaffen. Mit zunehmender Schlüssellänge wird die Aufgabe für Mallory jedoch immer schwieriger.

Besonders schwer zu knacken ist ein Doppelwürfel. Wenn Alice und Bob dieses Verfahren richtig verwenden (mit zwei langen Wörtern, deren Länge keine gemeinsamen Teiler haben), dann ist die Kryptoanalyse selbst mit Computerunterstützung schwierig bis unslösbar. Der Doppelwürfel zählt daher zu den besten Verfahren, die sich ohne Computerunterstützung praktikabel nutzen lassen. Im Kalten Krieg war der Doppelwürfel deshalb ein beliebtes Verfahren für Spione, die verschlüsselte Nachrichten an ihre Agentenführer verschickten. Da ein Spion im Feindesland nicht mit einer One-Time-Pad-Liste oder gar einer Ver-