









## Lösung

Das erste Zeichen besteht aus den Formen  und . Es ist also in der dritten Zeile und in der ersten Spalte zu finden: dort steht der Buchstabe S. Damit können nur noch die Antworten A) oder C) richtig sein.

Der zweite, dritte und vierte Buchstabe ist bei den Antworten A) und C) gleich. Die Zeichen entsprechen auch den Buchstaben A, V und E. Beim fünften Buchstaben aber unterscheiden sich die beiden Antworten wieder. Dieses Zeichen besteht aus den Formen  und . Das entspricht dem Buchstaben W. Damit ist die Antwort A) richtig. Auch die letzten vier Zeichen entsprechen den Buchstaben A, T, E und R.

Es gibt eine Abkürzung, wie man die Aufgabe lösen kann. Wenn man anstelle des ersten Zeichens das letzte Zeichen anschaut, sieht man, dass sich alle Antworten im letzten Buchstaben unterscheiden. Die Formen  und  des letzten Zeichens entsprechen dem Buchstaben R und nur die Antwort A) hat diesen Buchstaben am Ende.

## Dies ist Informatik!

Datensicherheit ist heutzutage eine wichtige gesellschaftliche Aufgabe. Eine der Methoden, Daten vor unbefugtem Lesen zu schützen, ist sie zu chiffrieren. Die Wissenschaft des Verschlüsseln von Informationen (die *Kryptographie*) ist schon mindestens 3500 Jahre alt. Eine der ältesten bekannten Methoden der Verschlüsselung basiert auf dem Ersetzen von Buchstaben durch andere Buchstaben oder Zeichen. Beim *Verschlüsseln* (manchmal auch *Chiffrieren*) wird ein *Klartext* mit Hilfe eines *Schlüssels* in einen *Geheimtext* verschlüsselt. Das Rekonstruieren des Klartextes aus dem Geheimtext mit Hilfe des Schlüssels nennt man *Entschlüsseln* (manchmal auch *Dechiffrieren*). Wenn man den Klartext eines Geheimtextes ohne Kenntnis des Schlüssels herausfindet, nennt man das *Entziffern*. Das Verschlüsselungsverfahren dieser Aufgabe ist eine sogenannte *monoalphabetische Verschlüsselung*. Bei diesen Verfahren wird für jeden Buchstaben genau ein neues Zeichen ausgewählt. Häufig werden dazu Systeme verwendet, die man sich leicht merken kann. Das System aus dieser Aufgabe ähnelt dem Freimaurer-Alphabet. Kryptoanalytiker, die solche Texte entziffern, würden spezielle Techniken wie Häufigkeitsanalysen oder *n*-Gramme im Geheimtext benutzen, um die Zeichen den richtig entschlüsselten Buchstaben zuzuordnen. Dass dies bei monoalphabetischen Verschlüsselungen generell möglich ist, hat Edgar Allen Poe in seiner 1843 veröffentlichten Kurzgeschichte "The Gold-Bug" gezeigt.

Was hätte Dara machen können, wenn sie die Tabelle nicht gehabt hätte, aber die vier möglichen Bedeutungen gekannt hätte? Sie hätte feststellen können, dass das zweite und sechste sowie das vierte und achte Zeichen gleich sind. Wenn sie von einer monoalphabetischen Verschlüsselung ausgeht, müsste sie nur noch den Text finden, dessen zweiter und sechster sowie vierter und achter Buchstabe gleich sind, und das wäre nur die Antwort A).

## Stichwörter und Webseiten

Kryptographie, Monoalphabetische Verschlüsselung

- <https://de.wikipedia.org/wiki/Kryptographie>
- [https://de.wikipedia.org/wiki/Monoalphabetische\\_Substitution](https://de.wikipedia.org/wiki/Monoalphabetische_Substitution)
- <https://de.wikipedia.org/wiki/Freimaurer-Alphabet>
- <https://de.wikipedia.org/wiki/H%C3%A4ufigkeitsanalyse>