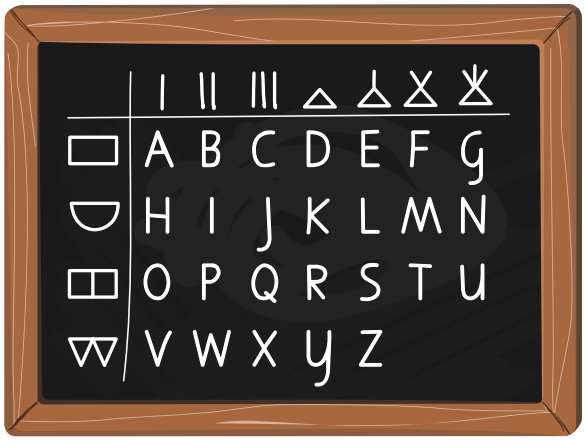
Lösung

Die richtige Antwort ist A), der Klartext lautet: INFORMATIK IST TOLL.

Hier ist die vollständige Geheimschrift-Tabelle:



Man kann die Tabelle einfach rekonstruieren. Die Buchstaben des lateinischen Alphabets sind zeilenweise in der Reihe von links nach rechts gesetzt. Man bemerkt, dass neue Zeichen so zusammengesetzt sind, dass die Zeilenbezeichnung den unteren Teil und die Spaltenbezeichnung den oberen Teil ausmachen. Der einzige fehlende untere Teil, der im Geheimtext vorkommt, ist das ▭. Somit ist dieses Zeichen die Bezeichnung der ersten Zeile. Genauso schnell kann man die drei fehlenden Zeichen für die Spalten ermitteln.

Es ist aber nicht notwendig die Tabelle vollständig wiederherzustellen. Man kann die Buchstaben einsetzen, die man von der beschädigten Tabelle direkt ablesen kann. So erhält man den folgenden Lückentext:

I N _ O _ _ _ _ I _ I S _ _ O L L

Mit diesem Lückentext kann man alle Lösungen ausser A) ausschliessen: B) beginnt mit «MA», C) endet mit «EIM», D) endet mit «IER».

Ein anderer Lösungsansatz ist der, dass man erkennt, dass der Geheimtext mit zwei gleichen Zeichen endet. Somit kommen nur noch A) und B) in Frage. Das erste Zeichen kann man in der beschädigten Tabelle eindeutig als «I» identifizieren, womit klar ist, dass die richtige Lösung A) ist.

Dies ist Informatik!

Informationen geheim zu halten oder Daten zu schützen ist eine 4000 Jahre alte Aufgabe. Unzählige Geheimsprachen wurden zu diesem Zweck entwickelt und benutzt. Heute ist Datensicherheit eines der Kernthemen der Informatik. Eine der Methoden, Daten vor unbefugtem Lesen zu schützen, ist sie zu *chiffrieren*. Das Chiffrieren verwandelt einen *Klartext* in einen *Geheimtext*. Das Rekonstruieren des Klartextes aus dem Geheimtext nennt man *Dechiffrieren*. Die Lehre der Geheimschriften nennt man *Kryptologie*.

Die antiken Kulturen verwendeten meistens Geheimschriften, die durch Codierung von Buchstaben mit anderen Buchstaben oder ganz neuen Zeichen erzeugt worden sind. Die Geheimschrift hier ist speziell für den Informatik-Biber entwickelt worden, basiert aber auf einem Konzept aus dem antiken Palästina. Die damalige Sicherheitsregel war, dass nur Geheimschriften verwendet worden sind, die man leicht auswendig lernen kann. Eine schriftliche Beschreibung der Geheimschrift aufzubewahren, betrachtete man als zu grosses Risiko. Eine Tabelle, wie sie hier verwendet wird, kann man gut auswendig lernen. Die berühmte Geheimschrift der Freimaurer basiert auf diesem Prinzip.

Stichwörter und Webseiten

- Kryptologie: `https://de.wikipedia.org/wiki/Kryptologie`
- Geheimschrift
- Chiffrieren
- Dechiffrieren