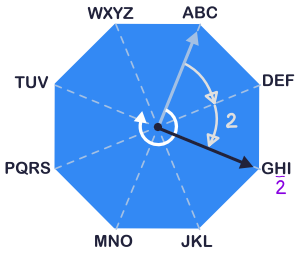
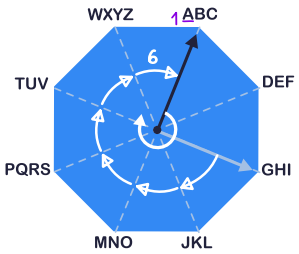
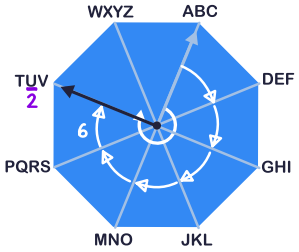
Lösung



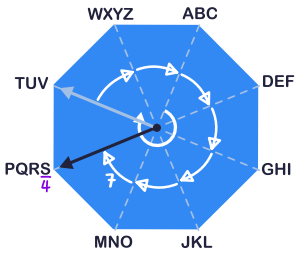
22 bedeutet, dass der Zeiger vom Block «ABC» zum Block «GHI» gedreht wird (erste Ziffer 2), und dass der zweite Buchstabe «H» genommen wird (zweite Ziffer 2).



61 bedeutet, dass der Zeiger nun vom Block «GHI» zum Block «ABC» gedreht wird (erste Ziffer 6), und dass der zweite Buchstabe «A» genommen wird (zweite Ziffer 1).



62 bedeutet, dass der Zeiger nun vom Block «ABC» zum Block «TUV» gedreht wird (erste Ziffer 6), und dass der zweite Buchstabe «U» genommen wird (zweite Ziffer 2).



74 bedeutet, dass der Zeiger nun vom Block «TUV» zum Block «PQRS» gedreht wird (erste Ziffer 7), und dass der vierte Buchstabe «S» genommen wird (zweite Ziffer 4).

Damit ist die Antwort B) «HAUS» korrekt.

Man hätte auch schneller auf diese Lösung kommen können: Die Antwort C) HALLO kann gar nicht in Frage kommen, da sie aus fünf Buchstaben besteht, der Geheimtext aber nur vier Buchstaben repräsentiert. Da der letzte Buchstabe mit einer 4 als zweiter Ziffer verschlüsselt ist, kann er nur «S» oder «Z» sein. Nur die Antworten A), B) und D) erfüllen dies. Der Buchstabe davor ist muss aus dem Buchstabenblock sieben Drehungen gegen den Uhrzeigersinn sein, also aus dem Block «TUV». Damit kann es nur noch die Antwort B) «HAUS» sein.

Dies ist Informatik!

Seit tausenden von Jahren versucht der Mensch, Informationen so zu verstecken, dass nur die Empfänger sie entziffern können. Was mit Papierstreifen, die um einen Stab gewickelt wurden, anfing («Skytale»), entwickelte sich über Transpositionschiffrem wie dem «Caesar-Code» und *polyalphabetischen Verschlüsselungsverfahren* (wie dem «Vigenére-Verfahren») zur modernen *Public-Key-Kryptographie* (wie zum Beispiel «GnuPG», das unter anderem das «RSA-Verfahren» nutzt).

Das Verschlüsselungsverfahren aus dieser Aufgabe ist ein polyalphabetisches Verschlüsselungsverfahren, denn derselbe Buchstabe wird nicht notwendigerweise mit demselben Geheimtext verschlüsselt: der Buchstabe «A» im Beispiel wird am Anfang als 31, aber am Ende als 81 verschlüsselt. Prinzipiell sind diese Verschlüsselungsverfahren heute alle mit Hilfe von Computern schnell und einfach zu entziffern.

In diesem Fall ist das Entziffern jedoch denkbar einfach: es gibt nur genau einen Schlüssel, um einen Text zu verschlüsseln. Selbst wenn man die Startposition des Zeigers nicht bei ABC sondern bei irgendeinem Block starten lassen könnte, hätte man nur acht verschiedene Schlüssel ... da ist selbst der Caesar-Code, der über 2000 Jahre alt ist, «sicherer». Nun kann man noch argumentieren, dass das Geheime gar nicht der Schlüssel sondern das Verschlüsselungsverfahren ist. Aber das *Kerckhoffs'sche Prinzip*, das Auguste Kerckhoffs (1835 bis 1903) 1883 formuliert hat, und das bis heute gilt, macht deutlich, dass die Sicherheit eines *Kryptosystems* nicht auf dem Geheimhalten eines Verschlüsselungsverfahrens beruhen darf, denn dies könnte zu leicht anderen bekannt werden.

Stichwörter und Webseiten

- Caesar-Code: `https://de.wikipedia.org/wiki/Caesar-Verschlüsselung`
- Polyalphabetische Substitution: `https://de.wikipedia.org/wiki/Polyalphabetische_Substitution`
- Verschlüsselungsverfahren: `https://de.wikipedia.org/wiki/Verschlüsselungsverfahren`
- Vigenére-Verfahren: `https://de.wikipedia.org/wiki/Vigenère-Chiffre`
- Public-Key-Kryptographie: `https://de.wikipedia.org/wiki/Asymmetrisches_Kryptosystem`
- GnuPG: `https://de.wikipedia.org/wiki/GNU_Privacy_Guard`
- RSA-Verfahren: `https://de.wikipedia.org/wiki/RSA-Kryptosystem`
- Kerckhoffs'sche Prinzip: `https://de.wikipedia.org/wiki/Kerckhoffs'_Prinzip`
- Auguste Kerckhoffs: `https://de.wikipedia.org/wiki/Auguste_Kerckhoffs`
- Kryptosystems: `https://de.wikipedia.org/wiki/Kryptosystem`
- Kryptographie: `https://de.wikipedia.org/wiki/Kryptographie`