**Das Verschlüsselungsverfahren nach Polybios**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **1** | **2** | **3** | **4** | **5** |
| **1** | A | B | C | D | E |
| **2** | F | G | H | I/J | K |
| **3** | L | M | N | O | P |
| **4** | Q | R | S | T | U |
| **5** | V | W | X | Y | Z |

Der griechische Geschichtsschreiber Polybius (etwa 200 v. Chr.) erwähnte einen Code, der die Buchstaben des Alphabets durch **zweistellige Zahlen** ersetzt. Die Buchstaben des Alphabetes werden dazu in eine Matrix aus 5 Zeilen und 5 Spalten eingetragen. Da das Alphabet aus 26 Buchstaben besteht, besetzen die Buchstaben "I" und "J" denselben Platz.

1. Beschreibe das Prinzip des Verfahrens, indem du 24 33 21 34 42 32 11 44 24 25 24 43 44 44 34 31 31 entschlüsselst.
2. Verschlüssele Kryptografie mit Polybios.

Um die Entschlüsselung zu erschweren kann ein Schlüsselwort verwendet werden, welches die ersten Buchstaben ersetzt.

1. Erstelle und verschlüssele ein Quadrat mit dem Schlüsselwort Informatiklehrer.

**Playfair**

Die Playfair-Verschlüsselung wurde 1854 von Charles Wheatstone entwickelt und nach seinem Freund Lord Lyon Playfair benannt, der die Nutzung dem britischen Militär empfahl, wo sie bis zum Ende des 1. Weltkrieges eingesetzt wurde.

Zunächst wird der Klartext zunächst in Buchstabenpaare eingeteilt. Durch die besondere Art der Verschlüsselung ist es erforderlich, dass die Paare aus keinem doppelten Buchstaben bestehen. Sollte dies im Klartext vorkommen, so wird ein "X" eingefügt und dann weiter eingeteilt. Falls der Klartext (gegebenenfalls durch zusätzlich eingefügte Buchstaben "X") aus einer ungeraden Anzahl von Buchstaben besteht, wird als letzter Buchstabe ein weiteres "X" angehängt.

**Beispiel**:

Klartext : Beispielklartext 🡪 BE IS PI EL KL AR TE XT  
Geheimtext: 🡪 CA HT OK AP FP BQ UD YS

1. Ermittle die Verschlüsselungsregeln für Playfair. Unterteile in die Fälle A) beide Buchstaben stehen in der gleichen Zeile, B) beide Buchstaben stehen in der gleichen Spalte, C) die Buchstaben stehen in unterschiedlichen Zeilen und Spalten.
2. Entschlüssele EI FE AQ CE EB mit dem Geheimwort Fortbildung.