# Die Verschlüsselungsverfahren von Polybios und Playfair

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **** | **** | **** | **** | **** |
| **** |  |  |  |  |  |
| **** |  |  |  |  |  |
| **** |  |  |  |  |  |
| **** |  |  |  |  |  |
| **** |  |  |  |  |  |

## Polybios

Archäologen fanden bei Ausgrabungen verschiedenen Papyrusrollen des Griechen Polybios (\* 200 v. Chr.; † 120 v. Chr.). Diese enthielten unter anderem das nebenstehende Quadrat als auch den Geheimtext . Ihnen war schnell klar, dass es sich um ein Verschlüsselungsverfahren handeln muss.

1. Versuche den **griechischen** Klartext zu bestimmen.
2. Beschreibe das Verschlüsselungsverfahren.
3. Übertrage das Verfahren ins Deutsche. Nutze als Tabellenkopf die Zahlen 1 bis 5.
4. Verschlüssle den aus dem Griechischen stammende Ausspruch „Arzt, heil dich selbst“.

Um eine Entschlüsselung zu erschweren, kann man die Reihenfolge der Buchstaben durch ein Schlüsselwort verändern.

1. Einige Dich mit deinem Nachbarn auf ein Schlüsselwort, füge es in das deutsche Polybios-Quadrat ein und fülle mit den verbliebenen Buchstaben systematisch auf.
2. Sendet Euch nun verschlüsselte Nachrichten mit der Angabe zu den geplanten Wochenendaktivitäten.

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

## Playfair

Fast 2000 Jahr nach Polybios entwickelt der englische Physiker Charles Wheatstone das nach seinem Bekannten, Baron Playfair von St. Andrews, benannte Playfair-Verfahren. Wheatstone ordnet die Buchstaben ebenfalls in einem Quadrat, ggf. mit Schlüsselwort an. Der Klartext wird in Zweierbuchstabenpaare zerlegt. Dabei müssen Paare mit gleichen Buchstaben oder übrig gebliebene Buchstaben mit Füllzeichen verändert werden. Anschließend kann die paarweise Verschlüsselung beginnen.

**Beispiel:**

Klartext: TREFFPUNKT GASSE 🡪 TR EF FP UN KT GA SX SE

Geheimtext: US AK KL SP IU FB XC UC

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. Entschlüssle den Geheimtext PB UG YM SU CA PS UY CP und erläutere die Bedeutung des Klartextes.

## Lösung

### Polybios

1. ΠΥΘΑΓOΡΑΣ 🡪 Pythagoras
2. Ein Buchstabe wird verschlüsselt, indem er durch seine Zeilen- und Spaltenbezeichnung ersetzt wird.
3. siehe Tabelle.

Hinweis: In einigen Quellen werden die Buchstaben U/V zusammenfassen. Dadurch erhält man ebenfalls 24 Buchstaben und ein Leerzeichen

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **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 |

1. 11 42 55 44 23 15 24 31 14 24 13 23 43 15 31 12 43 44
2. Schlüsselwort UNIVERSITÄT ROSTOCK ergibt das Polybios-Quadrat:

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

1. –

### Playfair

1. A) Die Buchstaben werden jeweils zyklisch durch den rechts stehenden ersetzt.  
   B) Die Buchstaben werden jeweils zyklisch durch den darüber stehenden ersetzt.  
   C) Vom ersten Klartextbuchstaben ausgehend wird nach links oder rechts gegangen, bis man in der gleichen Spalte wie der zweite Klartextbuchstabe ist. Die gefunden Zelle ist der erste Geheimtextbuchstabe. Für den zweiten Buchstabe verfährt man analog und sucht ausgehend vom zweiten Klartextbuchstaben durch horizontales Wechseln der Spalte jene auf, die auch die Spalte des ersten Klartextbuchstaben ist. Die gefunden Zelle markiert den zweiten Geheimtextbuchstaben.
2. Klartext: MERKWORTBENUTZEN

Wie bei Polybios kann man die Reihenfolge der Buchstaben im Quadrat durch den Einsatz eines Merkwortes verändern.