Leibniz Gemeinschaft

IPN
Leibniz-Institut für die Pädagogik der Naturwissenschaften und Mathematik

Die Skytale

Historisches

- Älteste militärische Verschlüsselung, die man kennt
- Spartaner, ca. 400v Chr.

Die Skytale

Voraussetzung:

- Buchstaben aus dem lateinischen Alphabet
- Sender und Empfänger haben gleichen Schlüssel

Vorgehen:

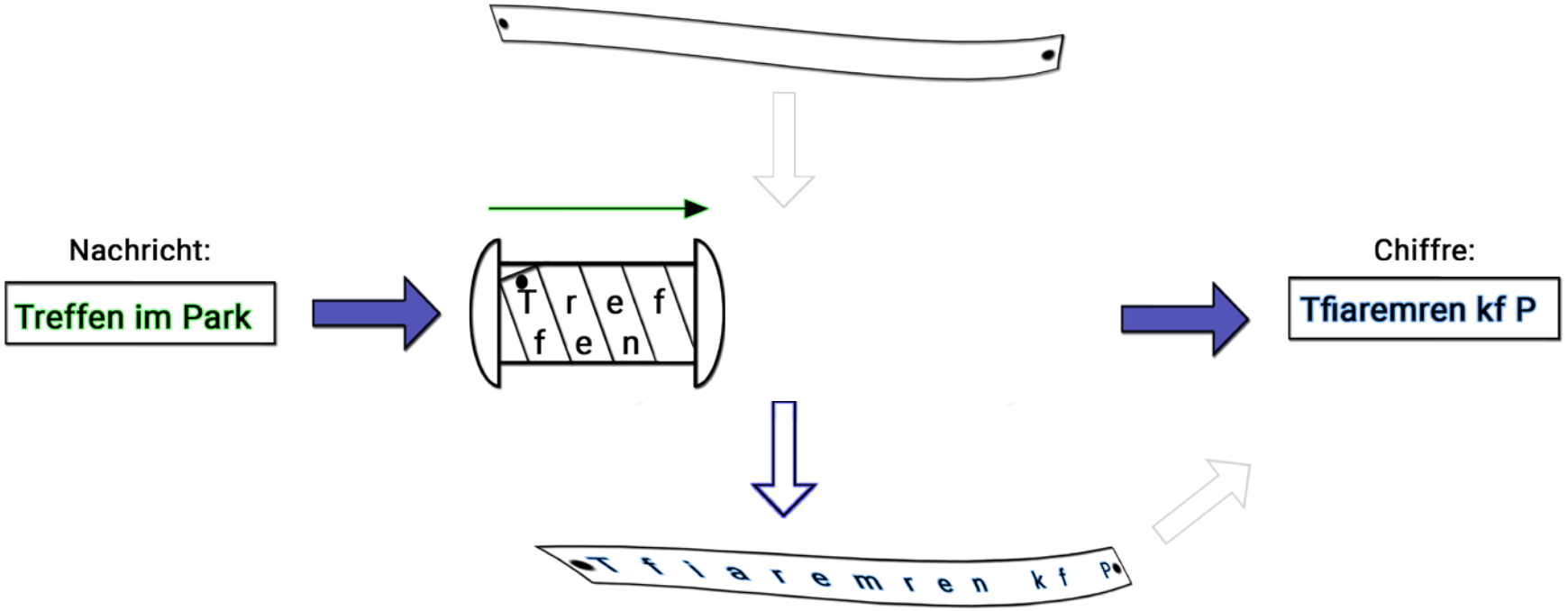
- Die Buchstaben werden untereinander Vertauscht.
- Nach welchem Schema bestimmt der Schlüssel.

Die Skytale

Wie verschlüsseln wir mit der Skytale?

- Leeren Papierstreifen um Zylinder wickeln
- Papierstreifen horizontal (→) beschreiben
- Papierstreifen abwickeln
- Buchstaben sind in vertauschter Reihenfolge

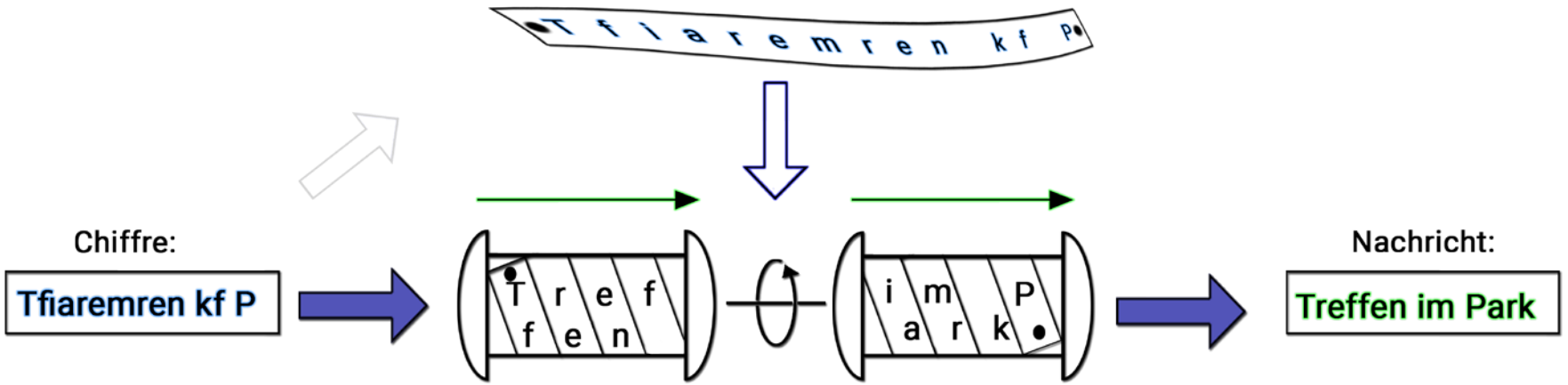
Wie verschlüsseln wir mit der Skytale?



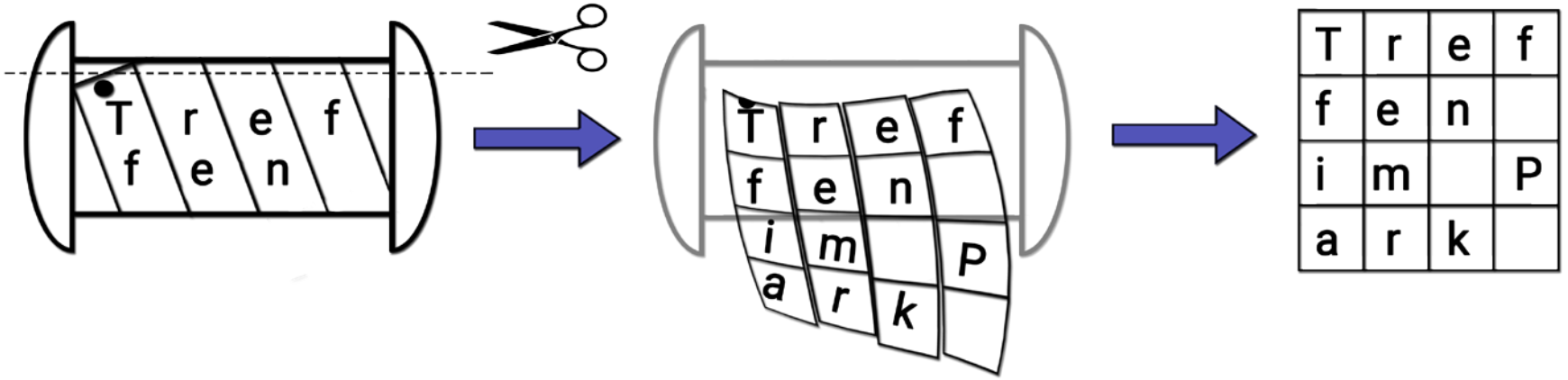
Entschlüsseln mit der Skytale

- Papierstreifen mit verschlüsselter Nachricht um den Zylinder wickeln
- Papierstreifen horizontal (→) ablesen

Entschlüsseln mit der Skytale



Die Skytale systematisieren



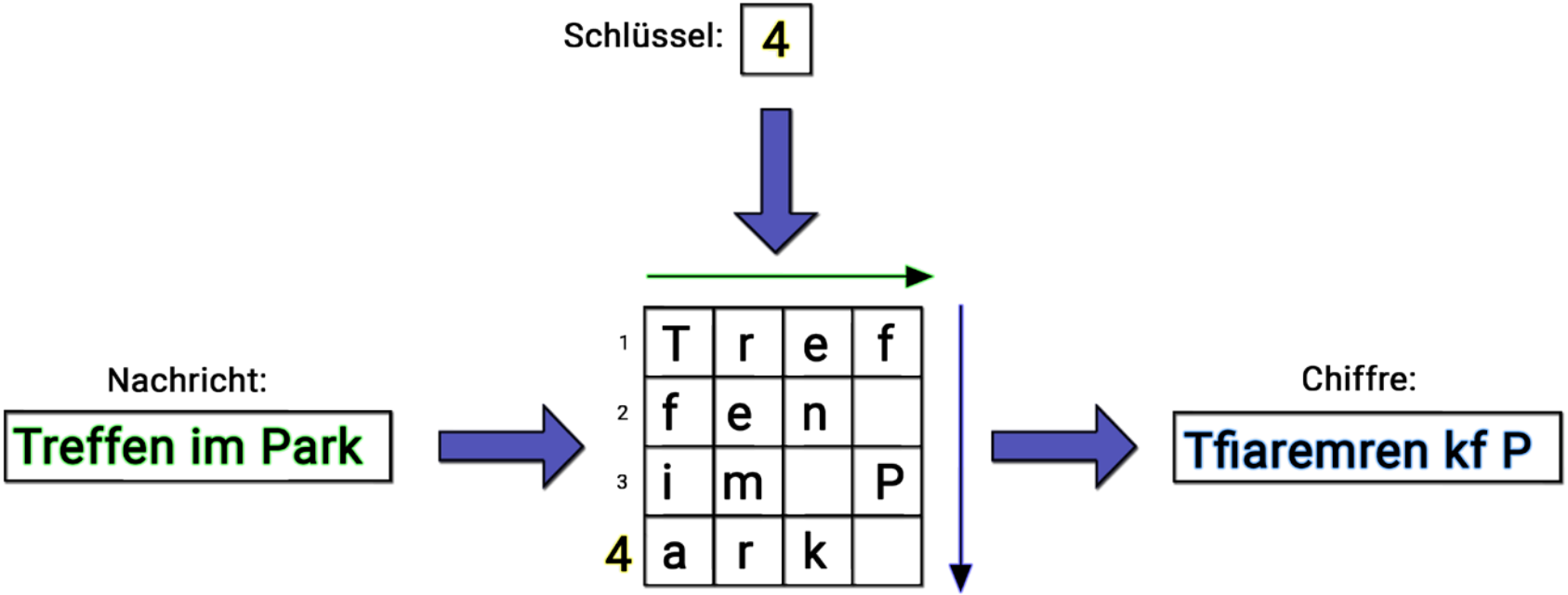
Dicke & Länge der Skytale gibt Anzahl der Zeilen und Spalten vor

Die Skytale systematisieren

- Skytale umwickeln & beschriften = Tabelle zeilenweise auffüllen (→)
- Skytale abwickeln = Tabelle spaltenweise auslesen (↓)

- Schlüssel: Anzahl der Zeilen

Verschlüsseln systematisieren



Der Schlüssel

- Wie viele Spalten hat die Tabelle?
- ‚Treffen im Park‘ hat 15 Zeichen
  (inkl. Leerzeichen)
- 15 Zeichen auf 4 Zeilen verteilen
- Dann müssen in jeder Zeile __ Zeichen stehen

Der Schlüssel

- Wie viele Spalten hat die Tabelle?
- ‚Treffen im Park‘ hat 15 Zeichen
  (incl. Leerzeichen)
- 15 Zeichen auf 4 Zeilen verteilen
- Dann müssen in jeder Zeile 4 Zeichen stehen
- Anzahl der Spalten:

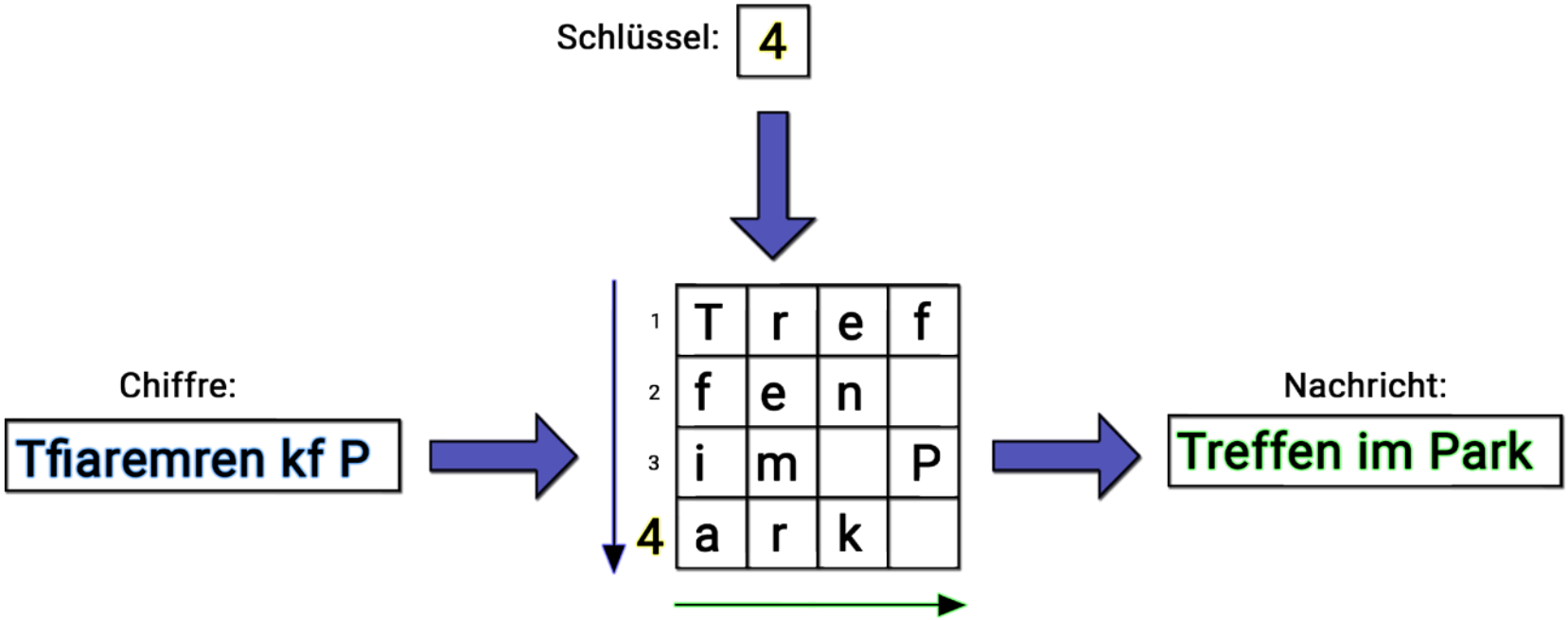
Der Schlüssel

- Wie viele Spalten hat die Tabelle?
- ‚Treffen im Park‘ hat 15 Zeichen
  (incl. Leerzeichen)
- 15 Zeichen auf 4 Zeilen verteilen
- Dann müssen in jeder Zeile 4 Zeichen stehen
- Anzahl der Spalten: 4 = 15 : 4 (aufgerundet)

Entschlüsseln systematisieren

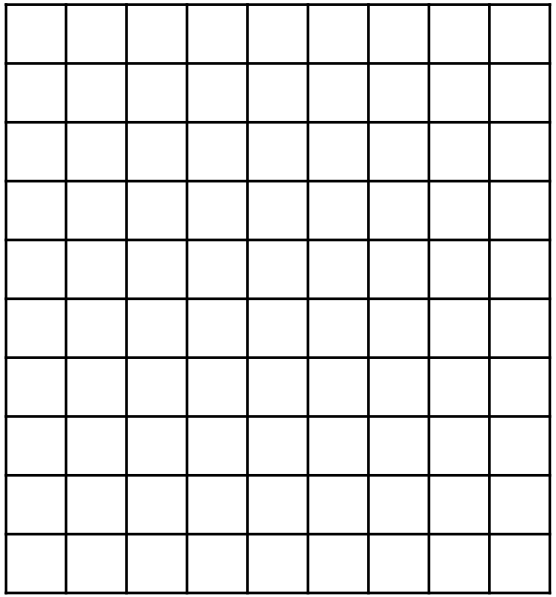
- Skytale umwickeln = Tabelle spaltenweise befüllen (↓)
- Skytale ablesen = Tabelle zeilenweise auslesen (→)

Entschlüsseln systematisieren



Die Skytale mit einer Tabelle

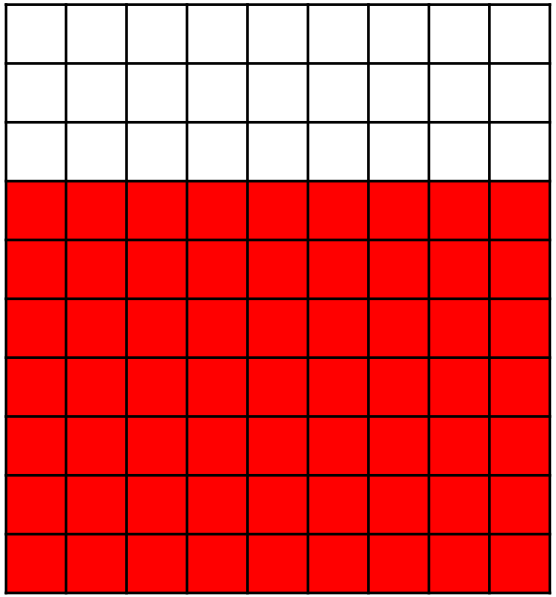
- Schlüssel: 3
- Länge der Nachricht: 20



Die Skytale mit einer Tabelle

- Schlüssel: 3
- Länge der Nachricht: 20

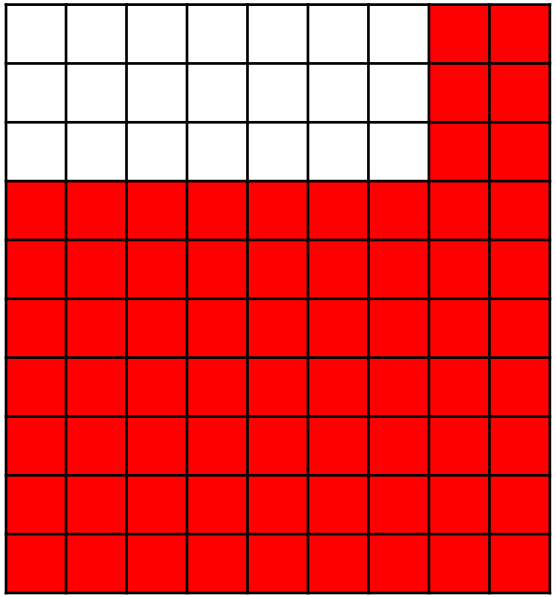
- Spalten: 7 (20 passt in 3 * 7)



Die Skytale mit einer Tabelle

- Schlüssel: 3
- Länge der Nachricht: 20

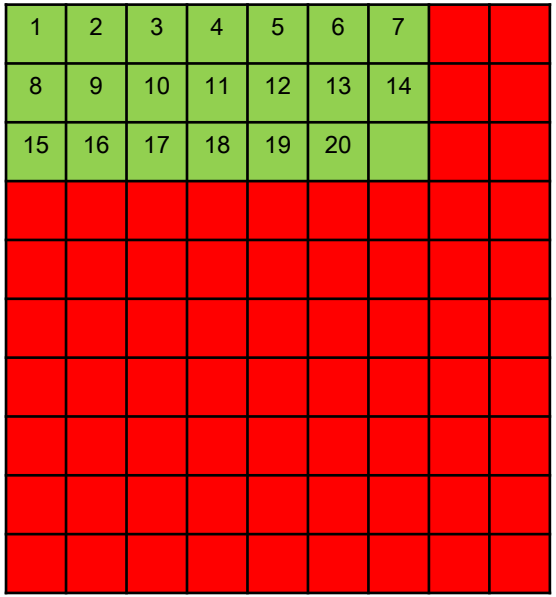
- Spalten: 7 (20 passt in 3 * 7)



Die Skytale mit einer Tabelle

- Schlüssel: 3
- Länge der Nachricht: 20

- Spalten: 7 (20 passt in 3 * 7)



Auftrag Nr. 2

- Entschlüssele die **Nachricht**: „“
- ‚Mttciurhtnol gfeV fceeehrintsn,!pg äes‘

- Schlüssel: 4
- Klartext: ‚Mit Verspätung eingetroffen, schlecht!‘

Sicherheit der Skytale

Wie kann ein Angreifer aus einer Chiffre den Klartext erhalten, ohne den Schlüssel zu kennen?

- Alle Schlüssel ausprobieren
- Häufigkeitsanalyse

Alle Schlüssel ausprobieren

- Entschlüssele die Chiffre mit jedem möglichen Schlüssel.
- Unter den Ergebnissen befindet sich der Klartext.
- Wie viele Versuche braucht man?
- Hängt von der Länge der Nachricht ab.
- Weniger als die Nachricht Stellen hat.

Sicherheit der Skytale

Wie kann ein Angreifer aus einer Chiffre den Klartext erhalten, ohne den Schlüssel zu kennen?

- Alle Schlüssel ausprobieren
- Häufigkeitsanalyse

Häufigkeitsanalyse

- Skytale ändert nur die Reihenfolge
- Häufigkeit in der Chiffre = Häufigkeit im Klartext

Hast du eine Frage, einen Fehler gefunden oder sonstige Anregungen? Melde dich bei uns!

Unter karrasch@leibniz-ipn.de oder info@panama-project.eu