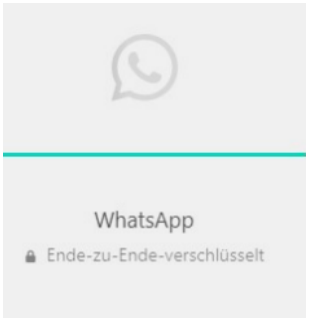
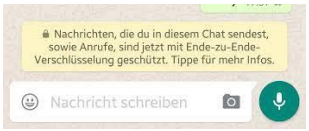
# Kryptosystem BenKo

Benedict Grupp & Kosta Kyriases

## Relevanz




Botschaften in der Art zu übermitteln, sodass sie ausschliesslich vom Empfänger gelesen werden können, ist seit alters ein Wunsch der Menschen. Daher gab es schon Jahrhunderte, bevor es Computer gab, Geheimschriften und Verschlüsselungen. Dennoch wird die Verschlüsselung in unseren heutigen Informationssystemen immer bedeutsamer: Der Schutz des Datenverkehrs wird zunehmend wichtiger, zum einen wegen des stetig wachsenden Umfangs der Vernetzung, zum anderen wegen der stetigen Entwicklung neuer Angriffsmöglichkeiten. Die Kenntnis der Vor- und Nachteile der gängigsten Verschlüsselungsverfahren hat somit nicht nur theoretischen Wert. Basisüberlegungen zu Sicherheitsaspekten und das Abwägen der Vor- und Nachteile von Verschlüsselungsverfahren sind somit auch im Alltag hilfreich.[1]

## Zielsetzung und Motivation

Die Lernenden sehen anhand des BenKo-Kryptosystems, wie man Transpositions-techniken verbinden kann, um neue Kryptosysteme zu entwickeln. Sie prüfen mit Hilfe der Kombinatorik die mögliche Anzahl Schlüssel der Verschlüsselung und können somit eine Aussage über die Sicherheit der Verschlüsselung machen.

Die Lernenden...

- ❑ verstehen das Verschlüsselungsmodell BenKo und wenden es an.
- ❑ erklären die Funktionsweise der Verschlüsselung.
- ❑ Bestimmen die mögliche Anzahl Schlüssel der Verschlüsselung.
- ❑ reflektieren, wie sich die Anzahl der Schlüssel ändert, wenn man die Parameter der Verschlüsselung ändert.
- ❑ begründen die Veränderung der Schlüssel anhand der Veränderung der Parameter der Verschlüsselung mathematisch.
- ❑ erstellen ausgehend von dieser Verschlüsselung ein eigenes Verschlüsselungsmodell.

## Vorwissen

Die Lernenden haben sich in der Unterrichtseinheit Kryptographie bereits folgende Inhalte angeeignet:

1. Motivation und historischen Überblick zur Kryptographie
2. Transposition mit dem Anwendungsbeispiel Skytale
3. Substitution mit dem Anwendungsbeispiel der Caesar-Verschlüsselung

[1] http://informatik-erleben.uni-klu.ac.at/einheiten/v/ , abgerufen am 7.12.2021

Parallel hierzu wurde im Mathematikunterricht die Kombinatorik betrachtet. Sollte dies zu einem früheren Zeitpunkt im Mathematikunterricht stattgefunden haben, fand ein Exkurs nach der Motivation und dem historischen Überblick im Informatikunterricht statt. Sowohl bei der Betrachtung der Transposition als auch der Substitution wurde die Kombinatorik zur Einschätzung des Möglichkeitsumfangs der Verschlüsselungen hinzugezogen.

# Einstiegsaufgabe

*Der Chefverschlüssler eines Geheimdienstes kommt spät am Abend von einem langen Arbeitstag nach Hause.*
*Anstelle eines Abendessens findet er auf dem Küchentisch nur eine Scheibe, die aus drei Ringen besteht, und einen Zettel, auf dem „451“ steht.*
*Die Ringe lassen sich unabhängig voneinander drehen. Der innerste Kreis mit dem roten Kreissektor ist nicht drehbar.*
*Er überlegt kurz. Dann lacht er. Er weiss genau, wo sich sein Abendessen befindet.*
*Kannst auch du es finden?*


## Erklärung:

Die Verschlüsselungsmethode basiert auf **Transpositionen**, d.h. auf Änderungen der Positionen der Buchstaben im Klartext.

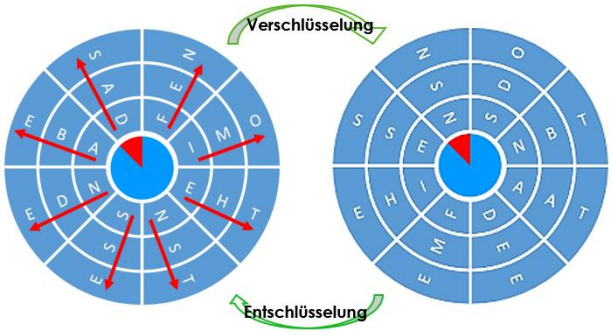
Verschlüsselung:

Man schreibt den Klartext Sektor für Sektor gegen den Uhrzeigersinn in die Scheibe von innen nach aussen, beginnend mit dem rot markierten Sektor.

Den Geheimtext erzeugt man, indem man die Ringe gegen den Uhrzeigersinn dreht.

Das Geheimnis der Geheimschrift ist lösbar durch die Drehung der einzelnen Ringe. Der *Schlüssel 451* gibt an, dass man den *inneren Ring um 4*, den *mittleren Ring um 5* und den *äusseren Ring um 1* Position gedreht hat.

Klartext:
DAS ABENDESSEN STEHT IM OFEN




Entschlüsselung:

Derselbe Schlüssel wird für das Entschlüsseln genutzt, nur dass diesmal im Uhrzeigersinn gedreht wird.

# Schüleraufgaben

Aufgabe 1:
Der nebenstehende Geheimtext wurde mit dem Kryptosystem BenKo mit dem Schlüssel 301 verschlüsselt. Entschlüssle den Geheimtext.

Aufgabe 2:

a) Wie viele unterschiedliche Möglichkeiten für die Verschlüsselung gibt es beim Eingangsbeispiel?

b) Angenommen das Einstiegsbeispiel hätte einen weiteren Ring mit ebenfalls 8 Sektoren, wie viele Möglichkeiten würde es nun geben?

c) Ist es effizienter, Ringe hinzuzufügen, oder die vorhandenen Ringe in mehr Sektoren zu unterteilen, um mehr Möglichkeiten zu generieren? Argumentiere!

d) Wie viele unterschiedlichen Möglichkeiten für die Verschlüsselung gibt es bei n Ringen und b Sektoren?

e) Nehmen wir an, ein Computer kann pro Sekunde 100 Kombinationen prüfen.

   (1) Wie viele Ringe bedarf es bei einer festen Anzahl von 8 Sektoren, damit ein Computer mehr als 1 Stunde für alle möglichen Kombinationen benötigt.
   (2) Wie viele Sektoren bedarf es bei einer festen Anzahl von 4 Ringen, damit ein Computer mehr als 1 Stunde für alle möglichen Kombinationen benötigt.

Aufgabe 3:
Wie verändert sich die Anzahl der Möglichkeiten, wenn man sowohl in als auch gegen den Uhrzeigersinn drehen kann?

Aufgabe 4:
Gibt es eine weitere Möglichkeit das Kryptosystem BenKo zu optimieren?

Aufgabe 5:
Entwickle einen eigenen Verschlüsselungsmechanismus, der auf einem ähnlichen Prinzip beruht. Nutze beim Erstellen deine Erkenntnisse aus Aufgabe 4.

# Lösung der Aufgaben

**Gewichtet mit Schwierigkeitsgrad (SG) 1 bis 5**

Aufgabe 1: (SG 1)

Der innere Ring muss um 3, der mittlere um 0 und der äussere Ring um 1 im Uhrzeigersinn gedreht werden. Auf diese Weise kann man den Klartext, beginnend am rot markierten Sektor, von innen nach aussen und gegen den Uhrzeigersinn auslesen. Der Klartext lautet dann: KRYPTOLOGIEV. Die Nachricht ist KRYPTOLOGIE, das V dient nur als Füllsymbol (ähnlich wie bei Skytale).


Aufgabe 2:

a) (SG 2)

In jedem Ring gibt es so viele Möglichkeiten wie Felder.
Da es zu jedem Feld des innersten Rings 8 Möglichkeiten des mittleren Rings gibt, und wiederum zu jeder dieser möglichen Kombinationen erneut 8 Möglichkeiten des äusseren Rings hinzukommen, erhält man:

$8 \cdot 8 \cdot 8 = 8^3 = 512$ Möglichkeiten

b) (SG 2)

$8^4 = 4096$ Möglichkeiten

c) (SG 3)

Durch Probieren erkennt man, dass das Hinzufügen von Ringen viel schneller zu einer Erhöhung der Möglichkeiten führt als das Hinzufügen von Sektoren.

Folgende Tabelle veranschaulicht die unterschiedliche Zuwachsgeschwindigkeit:

| n Ringe / b Sektoren | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 2 | 4 | 8 | 16 | 32 | 64 | 128 |
| 3 | 3 | 9 | 27 | 81 | 243 | 729 | 2187 |
| 4 | 4 | 16 | 64 | 256 | 1024 | 4096 | 16384 |
| 5 | 5 | 25 | 125 | 625 | 3125 | 15625 | 78125 |
| 6 | 6 | 36 | 216 | 1296 | 7776 | 46656 | 279936 |
| 7 | 7 | 49 | 343 | 2401 | 16807 | 117649 | 823543 |
| 8 | 8 | 64 | **$8^3 = 512$** | **$8^4 = 4096$** | **$8^5 = 32768$** | **$8^6 = 262144$** | **$8^7 = 2097152$** |
| 9 | 9 | 81 | **$9^3 = 729$** | 6561 | 59049 | 531441 | 4782969 |
| 10 | 10 | 100 | **$10^3 = 1000$** | 10000 | 100000 | 1000000 | 10000000 |
| 11 | 11 | 121 | **$11^3 = 1331$** | 14641 | 161051 | 1771561 | 19487171 |
| 12 | 12 | 144 | **$12^3 = 1728$** | 20736 | 248832 | 2985984 | 35831808 |

Der Fall des Eingangsbeispiels (3 Ringe, 8 Sektoren) ist grün markiert. Der Zuwachs durch Hinzufügen von Ringen ist in der gelb markierten Zeile, der Zuwachs durch Hinzufügen von Sektoren ist in der blau markierten Spalte abzulesen.

Mathematische Erklärung:

- Erhöht man den Wert des Faktors b (bzw. der Basis b), so wächst die Anzahl der Möglichkeiten potenziell,
- erhöht man die Anzahl der Faktoren n (bzw. den Exponenten n), so wächst die Anzahl der Möglichkeiten exponentiell.

Das Hinzufügen von Ringen generiert also immer mehr Möglichkeiten als das Hinzufügen von Sektoren.

d) (SG 2)

Für n Ringe und b Sektoren ergeben sich $b^n$ Möglichkeiten.

e) (SG 4)

(1) $8^n = 360000 \rightarrow n = \log_8 360000 = 6.152$ Man benötigt mindestens 7 Ringe

(2) $b^4 = 360000 \rightarrow n = \sqrt[4]{360000} = 24.5$ Man benötigt mindestens 25 Sektoren

Aufgabe 3: (SG 4)

Die Anzahl der Möglichkeiten ändert sich nicht, da jede Drehung im Uhrzeigersinn einer Drehung gegen den Uhrzeigersinn entspricht.

Beispiel: Bei 8 Sektoren entspricht eine Drehung von fünf Stellen gegen den Uhrzeigersinn einer Drehung von 3 Stellen im Uhrzeigersinn.

Aufgabe 4: (SG 5)

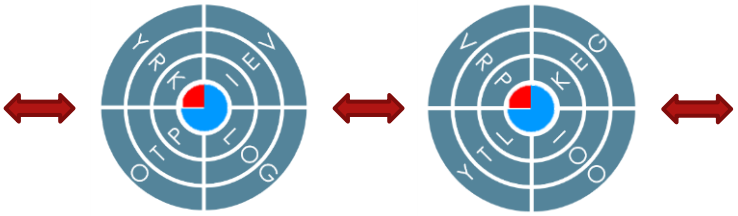
Es ist empfehlenswert, sich über die Ergebnisse dieser Aufgabe in der Klasse auszutauschen, um alle Lernenden auf Aufgabe 5 vorzubereiten.

**Lösungen von Lernenden könnten sein**:

- z.B. Durch das Ändern der Leserichtung
- z.B. durch Kombination mit einer Substitution
- …

Sofern sie nicht von den Lernenden selbst kommt, sollte folgende Optimierung thematisiert werden: Wenn man den Geheimtext aus der Scheibe herausschreibt, die Scheibe also nicht Teil der Botschaft ist, erhält man einen zweiten Schlüssel, welcher die Anzahl Ringe und die Anzahl Sektoren enthält:

*Nachricht im Klartext:*
**KRYPTOLOGIEV**



*Verschlüsselte Nachricht:*
**PRVLTYIOOKEG**

Schlüssel = 301 34

Aufgabe 5: (SG 5)

**Individuelle Lösung**