Franziska Plank und Patrick Wiesner

WER BIN ICH?

DOSB DEUTSCHE OLYMPISCHE AKADEMIE

EINFÜHRUNG IN DIE KRYPTOLOGIE

Kryptologie – Was ist das? Wofür wird sie gebraucht?

- **Codierung:** Bei einer Codierung werden Informationen von einer Darstellung in eine andere übersetzt.
- **Kryptologie:** Kryptologie ist ein Teilbereich der Codierung. Sie meint die Wissenschaft des Verschlüsselns (Kryptografie) und Entschlüsselns (Kryptoanalyse) von Nachrichten. Das Ziel: Botschaften sollen von einem Sender zu einem Empfänger übermittelt werden, ohne dass eine andere Person die Nachricht verstehen kann.

Kryptografie – Methoden im Laufe der Zeit

5. Jhd. v. Chr.

Steganografie

Steganografie ist keine klassische Ver- und Entschlüsselung einer Nachricht, sondern das Verstecken von Botschaften. So wurden z. B. Tafeln mit eingeritzten Nachrichten mit Wachs übergossen und in dieser Form transportiert.

5. Jhd. v. Chr.

Skytale

Bei dieser Methode einigen sich Sender und Empfänger vorab auf den Durchmesser eines Stabs, der für alle anderen unbekannt ist. Der Sender umwickelt den Stab mit einem Papierstreifen und beschreibt diesen mit der Nachricht. Anschließend wickelt er diesen ab und sendet ihn an den Empfänger. Die Nachricht kann nur entschlüsselt werden, wenn der Empfänger einen Stab mit dem gleichen Durchmesser verwendet.

2. Jhd. v. Chr.

Polybius-Chiffre

Diese Methode geht auf den griechischen Geschichtsschreiber Polybios (ca. 200 – 120 v. Chr.) zurück. Hierbei werden die Buchstaben in eine rechteckige Tafel in zufälliger Reihenfolge geschrieben. Diese Reihenfolge kennen nur Sender und Empfänger der Nachricht. Der Sender verschlüsselt seinen Text, indem er anstelle eines Buchstabens dessen Position in der Tabelle angibt. Der Empfänger kann die Nachricht mithilfe der Tabelle entschlüsseln. Später wurde die Methode auch inGefängnissen verwendet, z. B. als Klopfcode unter Gefangenen.

M 2
Video zur Erklärung

Beispiel:
Der Ausdruck „PARIS“ wird bei nebenstehender Tafel zu:
„43 – 11 – 45 – 13 – 24“

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

Mittel der Kryptoanalyse
Um Nachrichten, die mit dieser Methode verschlüsselt wurden, zu entschlüsseln, ist es hilfreich zu wissen, wie häufig im Schnitt ein Buchstabe im Text vorkommt. Damit kannst du Rückschlüsse auf die Buchstaben ziehen. So ist die häufigste Positionsangabe meist ein „E“ oder „N“:

Folgende Tabelle hilft dir dabei:

E	N	I	S	R	A	T	D	H	U	L	C	G
17,40 %	9,78 %	7,55 %	7,27 %	7,00 %	6,51 %	6,15 %	5,08 %	4,76 %	4,35 %	3,44 %	3,06 %	3,01 %

M	O	B/W	F	K	Z	P	V	ß	J	Y	X	Q
2,53 %	2,51 %	1,89 %	1,66 %	1,21 %	1,13 %	0,79 %	0,67%	0,31 %	0,27 %	0,04 %	0,03 %	0,02 %

ca. 50 v. Chr.

Cäsar-Verschlüsselung

Wie der Name erkennen lässt, wurde die Methode von dem römischen Feldherrn Gaius Julius Cäsar (100 – 44 v. Chr.) erfunden. Dabei werden die Buchstaben des Alphabets um eine bestimmte Zahl nach links oder rechts verschoben. Sender und Empfänger der Nachricht müssen sich im Vorfeld auf Richtung und Anzahl der zu verschiebenden Stellen einigen.

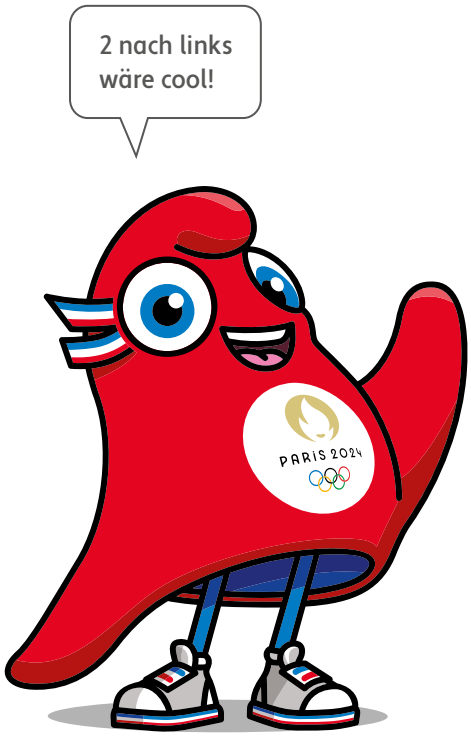
Beispiel:
Der Ausdruck „OLYMPIA“ soll mit unten stehender Tafel verschlüsselt werden (Verschiebung um 3 nach rechts)

M3 Video zur Erklärung

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

Es ergibt: „LIVJMFX“

Mittel der Kryptoanalyse
Um einen nach der Cäsar-Methode verschlüsselten Text zu entschlüsseln, müssen Richtung und Anzahl der Verschiebung herausgefunden werden. Dies kann – ähnlich wie bei der Polybius-Chiffre – systematisch geschehen. Hier hilft dir auch die obige Tafel. Meist lohnt sich die Konzentration auf die Verschiebung des „E“ – der Rest geht häufig schnell.



16. Jhd.

Vignère-Chiffre

Diese Methode kann als Erweiterung der Cäsar-Verschlüsselung gesehen werden. Hier nutzen Sender und Empfänger eine Tafel, die aus jeder Möglichkeit der Cäsar-Verschlüsselung besteht. Außerdem einigen sie sich vorher auf ein Schlüsselwort. Nun wird das Schlüsselwort fortlaufend über jeden einzelnen Buchstaben der zu codierenden Botschaft geschrieben. Der Buchstabe des Schlüsselworts gibt an, welche Zeile in der Verschlüsselungstafel verwendet werden muss.

Beispiel:
„OLYMPIA“ soll mit dem Schlüsselwort „PARIS“ verschlüsselt werden →

P	A	R	I	S	P	A
O	L	Y	M	P	I	A

„O“ in Zeile P nachschauen

„P“ in Zeile S nachschauen →

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

→

Z	L	H	E	X	T	A

aus „O“ wurde in Zeile P „Z“

aus „P“ wurde in Zeile S „X“

20. + 21. Jhd.

Enigma

Enigma ist eine Maschine, die von Deutschland im Zweiten Weltkrieg für die Verschlüsselung von Funksprüchen eingesetzt wurde. Die Maschine nutzt die Ideen der Cäsar- und Vignère-Chiffre in einer komplizierten Form. Die Methode konnte von dem britischen Mathematiker Alan Turing und seinem Team „geknackt“ werden.

RSA-Verfahren

Diese Methode nutzt Primzahlen, um Botschaften zu verschlüsseln. Besonders ist, dass sich Sender und Empfänger nicht vorher auf einen gemeinsamen Code einigen müssen.

Blockchain

Diese Methode wird aktuell für die Verschlüsselung von Inhalten im Internet verwendet, z. B. bei Kryptowährung. Zur Verschlüsselung werden „Hash-Funktionen“ genutzt.

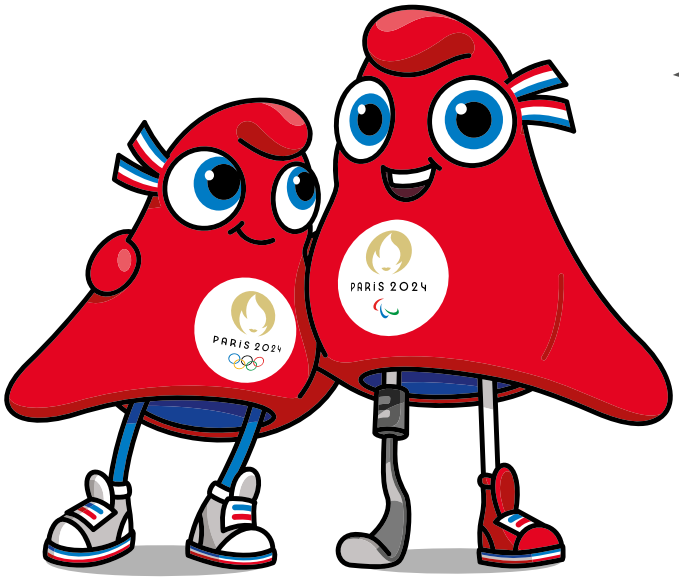
WER BIN ICH?

Sportler*innen mithilfe von Kryptografie erkennen

Finde heraus, wer hinter den anonymen Personen auf den nächsten Seiten steckt. Zwei der insgesamt sieben Athlet*innen warten darauf, entlarvt zu werden.

Was ist zu tun?

- Eigne dir zunächst Wissen zum Themengebiet der Kryptologie mithilfe von M1 an. Schaue die beiden Videos zu den ausgewählten Verschlüsselungsverfahren, die du mit den QR-Codes aufrufen kannst.
- Wende dein Wissen an, indem du die Interviews der Phrygen mit den anonymen Personen entschlüsselst. Dadurch erfährst du, welche Athlet*innen mit den Maskottchen gesprochen haben.



1. Was war dein beeindruckendster Fair-Play-Moment?
2. Was ist die entscheidende Eigenschaft für deine Sportart?
3. Was ist deine wichtigste Trainingsausrüstung?

Damit du die Antworten in den Sprechblasen entschlüsseln kannst, musst du entweder die **Polybius-Chiffre** oder die **Cäsar-Verschlüsselung** knacken. Mit einem scharfen Blick und einigen Hinweisen in den Aufgaben erkennst du, wie du die beiden Entschlüsselungsverfahren auf der nächsten Seite anwenden musst. Die QR-Codes verraten dir anschließend, ob du die Aufgabe richtig gelöst hast.

© Joachim Sielski+DBS

Boccia:
Boris Nicolai


© Lisa Unruh

Bogenschießen:
Lisa Unruh


© Oliver Kremer+DBS

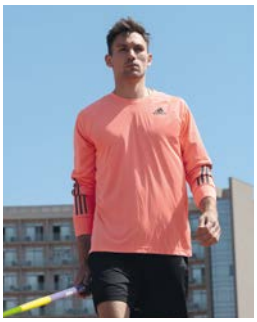
Para Radsport:
Denise Schindler


© DTV

Breaking:
Thomas Stark


© Nadine Harms

Reiten:
Jessica von Bredow-Werndl und Stute Dalera


© Niklas Kaul

Zehnkampf:
Niklas Kaul


© Danny-Ralph Cäsar

Rollstuhlbasketball:
Mareike Miller

Aufgabe 1: Polybius

Mit welcher Polybius-Tafel sind die Antworten in der ersten Sprechblase verschlüsselt? Kreuze die richtige Option an.

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

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

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

1. 1552 1342 52141542415315421
2. 43144541535311512315251545523415551542
3. 2444132215241

Ich bin: _____

Aufgabe 2: Cäsar

Wird ein Text mit dieser Methode verschlüsselt, musst du u.a. wissen, um welche Zahl die Buchstaben des Alphabets verschoben wurden. Wenn du M1 genauer ins Auge nimmst, wirst du in der zweiten Sprechblase schnell die richtige „Verschiebungszahl“ ***nach links*** *herausfinden.*

Verschiebungszahl: ☐

1. VTQUV XQP GKPGT IGIPGTKP
2. BCGJPG BWUCOOGPDGKUUGP
3. JGNO WPF HCJTTCF

Ich bin: _____

Early finisher task: Teamarbeit

Beschreibe eine*n weitere*n Sportler*in mit einem Schlagwort und verschlüssle dieses mit einer der beiden Methoden. Dein*e Partner*in kann nun deinen Code knacken.

WER BIN ICH?

Sportler*innen mithilfe von Kryptografie erkennen

Lösungen

Aufgabe 1: Polybius

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

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

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

Aufgabe 2: Cäsar

Verschiebungszahl: 2 (nach links)

Aufgabe 3: Wer bin ich?

Sprechblase 2: Polybius-Chiffre

1. EM in Muenchen
2. Durchhaltevermoegen
3. Spikes

Ich bin: Niklas Kaul

Sprechblase 3: Cäsar-Verschlüsselung

1. Trost von einer Gegnerin
2. Zaehne zusammenbeissen
3. Helm und Fahrrad

Ich bin: Denise Schindler