GEHEIMBOTSCHAFTEN

WIE MAN NACHRICHTEN VERSTECKT UND KNACKT

Prof. Dr. Max Horn · Kinder-Uni, 18. November 2026

RPTU
Rheinland-Pfälzische
Technische Universität
Kaiserslautern
Landau



GEHEIMBOTSCHAFT DES TAGES

HIV WGLPYIWWIP MWX HVIM YRH IMRW

GV EJVU FPGFNODDNFU

- Wer kann das lesen?
- Wer sie knackt, ist offiziell Codeknacker!

GEHEIME BOTSCHAFTEN

- Alia hat ein Geheimnis für Ben
- … mitten im Unterricht
- Zurufen? Hört jeder!
- Zettel? Kann abgefangen werden …
- Wie bleibt es geheim?



Illustration mit ChatGPT generiert

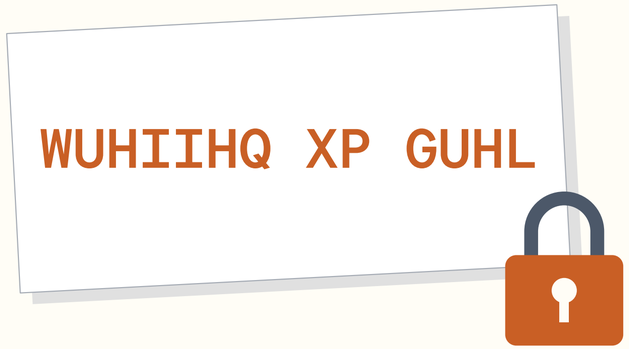
ZWEI TRICKS

VERSTECKEN



Unsichtbare Tinte

VERSCHLÜSSELN



Buchstabensalat

Verstecktes kann man finden. Verschlüsseltes muss man erst knacken!

TRICK 2: VERSCHLÜSSELN

Botschaft (Klartext)

Treffen wir uns nach der Schule?



Geheimbotschaft

WUHIIHQZLUXQVQDFK GHUVFKXOH

- Nur Ben soll die Geheimbotschaft entschlüsseln können
- Verschlüsselung ist ein Teil der Kryptografie

EINE URALTE IDEE

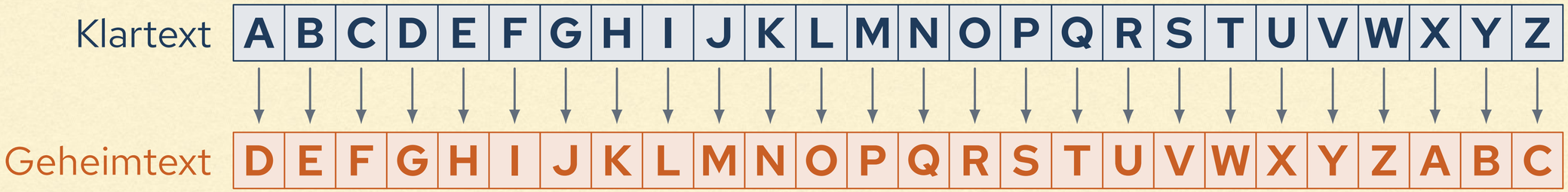
- Julius Caesar
- Feldherr im alten Rom
- vor über 2000 Jahren
- Seine Idee: Buchstaben verschieben



Illustration aus Wikipedia (Foto des „Caesar Tusculum“ von Ángel M. Felicísimo)

CAESARS TRICK

- Jeder Buchstabe rutscht 3 Plätze weiter
- Nach Z geht es wieder bei A los
- Entschlüsseln: einfach zurückschieben



DIE CAESAR-SCHEIBE

- Außen: **Klartext**
- Innen: **Geheimtext**
- Drehen, bis D unter A steht
- Das ist Schlüssel 3
- **HALLO → KDOOR**



JETZT IHR!

Agenten-Blatt · Aufgabe 1

- Wähle einen Schlüssel von 1 bis 6
- Verschlüssle deinen Vornamen
- Tausche das Blatt mit deinem Nachbarn
- Entschlüsselt eure Namen!



MAX → PDA

MINI-QUIZ

Agenten-Blatt · Aufgabe 2

- Was steht hier?
- Tipp: Der Schlüssel ist 3

NLQGHUXQL

KINDERUNI

ABGEFANGEN!

- Ein Lauscher fängt die Botschaft ab
- Er kennt sogar Caesars Trick
- Aber: Um wie viel wurde verschoben?
- Die Verschiebung ist der **geheime Schlüssel**
- Ohne Schlüssel kein Klartext – oder doch?



Illustration mit ChatGPT generiert

KNACKT DEN CODE!

Agenten-Blatt · Aufgabe 3

YWJKKUZSPY UFZXJSMTK IWJN ZMW

- Der Schlüssel ist unbekannt!
- Trick 1: einfach alle Schlüssel ausprobieren
- Es gibt ja nur 25 Stück
- Gruppe 1 testet Schlüssel 1, Gruppe 2 Schlüssel 2, …

TRICK 1: ALLE AUSPROBIEREN

```
Schlüssel 1:  XVIJJTYROX TEYWIRLSJ HVIM YLV
Schlüssel 2:  WUHIISXQNW SDXVHQKRI GUHL XKU
Schlüssel 3:  VTGHHRWPMV RCWUGPJQH FTGK WJT
Schlüssel 4:  USFGGQVOLU QBVTFOIPG ESFJ VIS
Schlüssel 5:  TREFFPUNKT PAUSENHOF DREI UHR
Schlüssel 6:  SQDEEOTMJS OZTRDMGNE CQDH TGQ
```

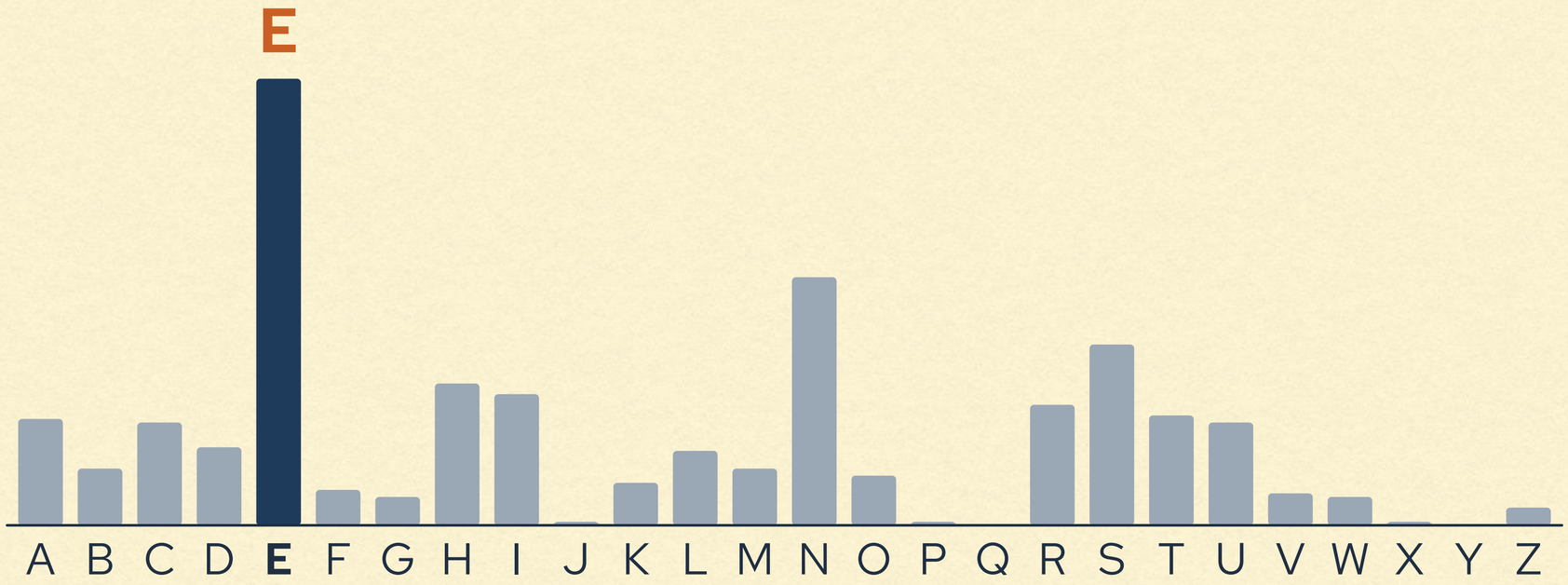
Nur Schlüssel 5 ergibt Sinn – geknackt!

TRICK 2: ZÄHLEN

- Welcher Buchstabe kommt in deutschen Texten am häufigsten vor?

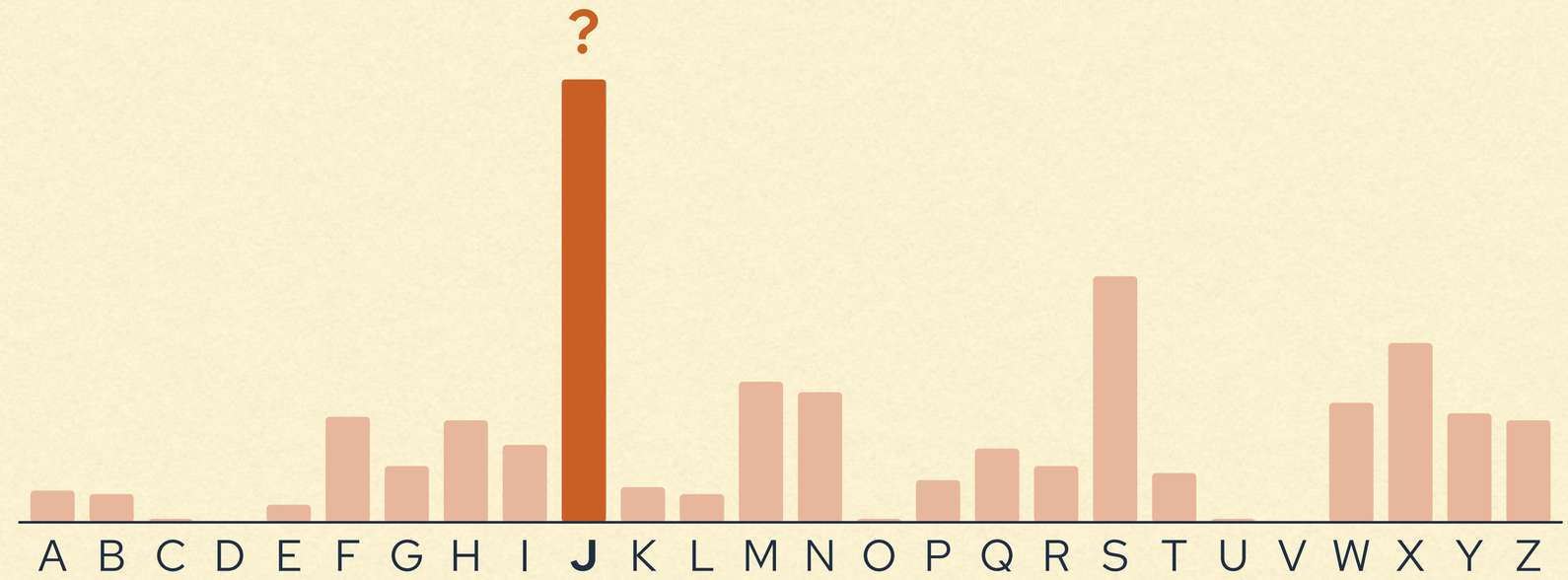


DAS E IST DER STAR



- In deutschen Texten ist etwa jeder sechste Buchstabe ein E

DAS VERKLEIDETE E



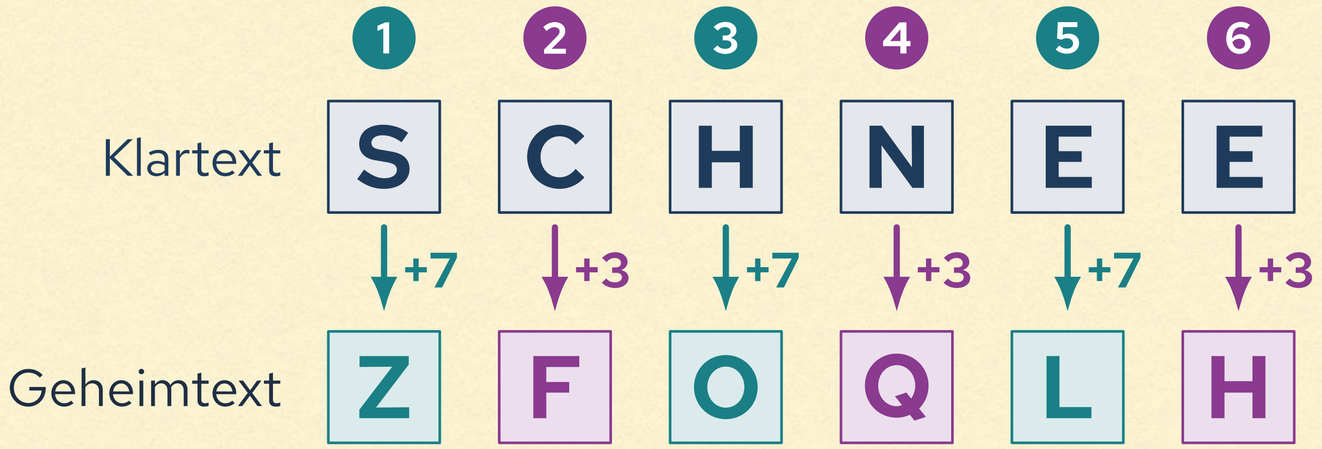
- Im Geheimtext ist **J** der häufigste Buchstabe
- **J** ist das verkleidete E – also Schlüssel 5

GUTE IDEE ≠ GUTE SICHERHEIT

Caesars Geheimschrift ist in Sekunden geknackt.

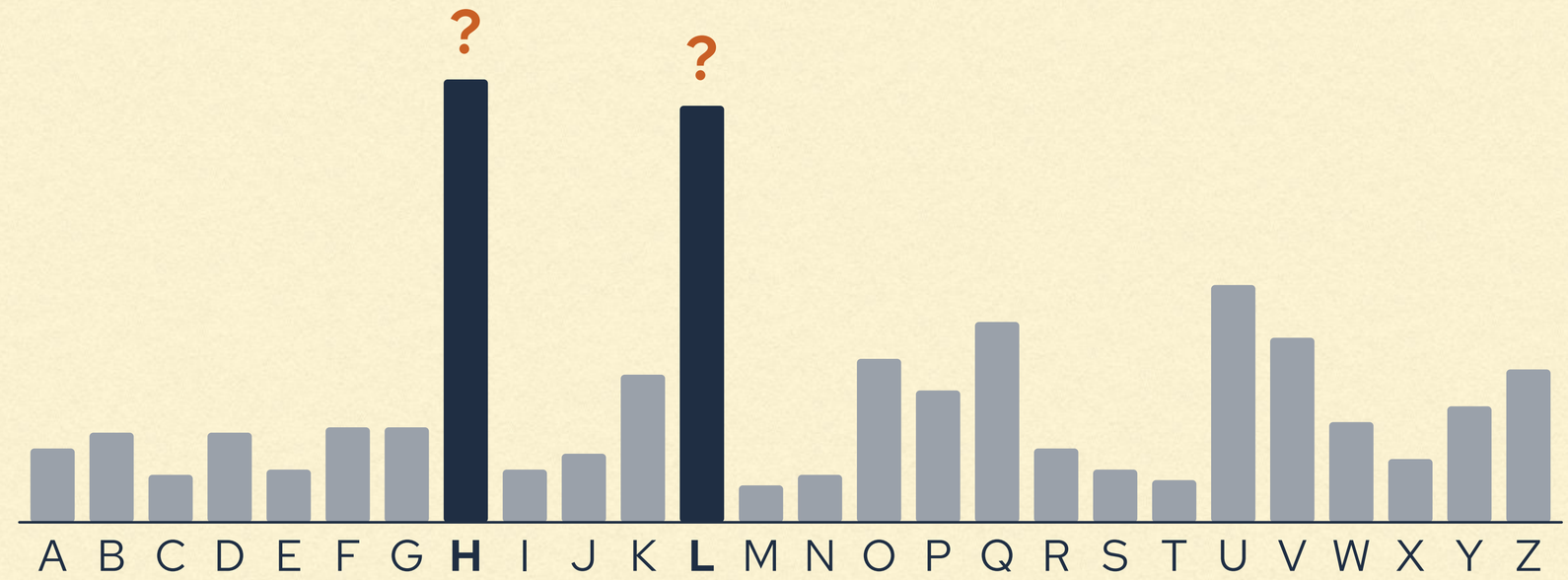
Wir brauchen eine bessere Idee!

ZWEI SCHLÜSSEL IM WECHSEL



- Buchstabe 1, 3, 5, …: **Schlüssel 7**
- Buchstabe 2, 4, 6, …: **Schlüssel 3**
- Aus E wird mal L und mal H!

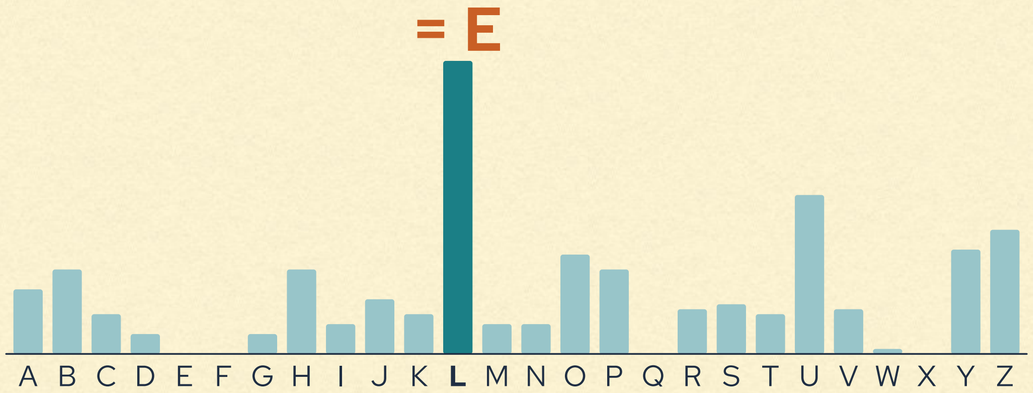
DER E-TRICK VERSAGT



- Zwei Türme: H und L – welcher ist das E?
- Keine Verschiebung macht den ganzen Text lesbar

IN ZWEI TEAMS ZÄHLEN

Team 1: Buchstabe 1, 3, 5, …



Team 2: Buchstabe 2, 4, 6, …



- **Team 1**: L ist das verkleidete E → Schlüssel 7
- **Team 2**: H ist das verkleidete E → Schlüssel 3
- Der E-Trick klappt wieder – in jedem Team einzeln!

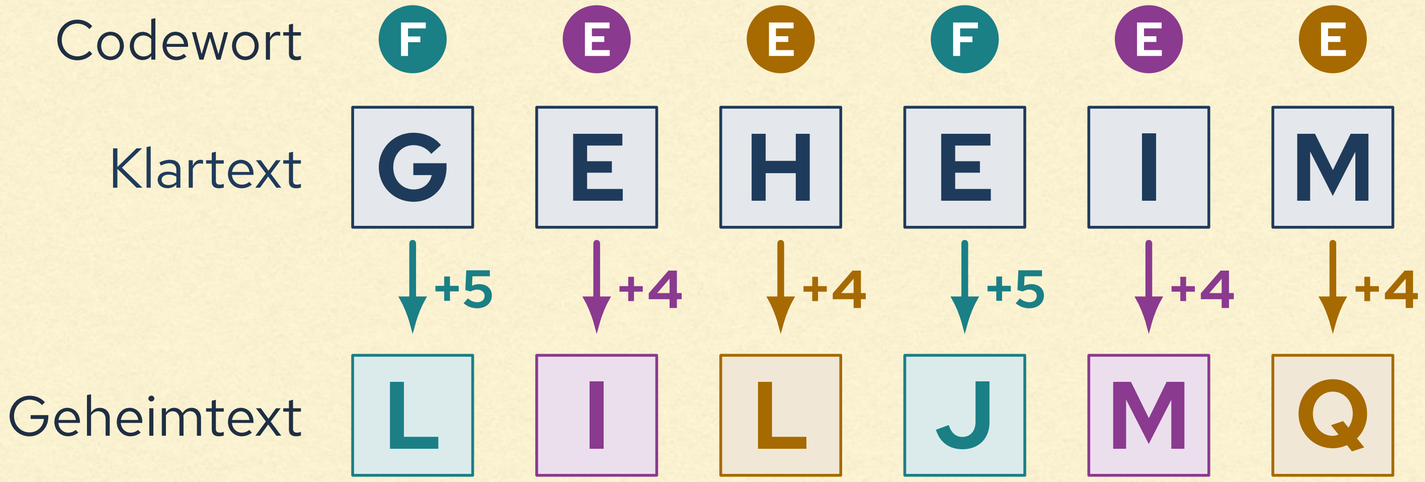
BUCHSTABEN ALS SCHLÜSSEL

- Mehr als zwei Schlüssel? Geht auch!
- Jeder Buchstabe steht für einen Schlüssel
- Ein Codewort ist dann eine ganze Schlüssel-Folge

Buchstabe	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
Schlüssel	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

FEE → 5, 4, 4

GEHEIMSCHRIFT MIT CODEWORT



- Das Codewort wird immer wiederholt
- Knacken? Team-Trick – mit 3 Teams
- Aber: Wie lang ist das Codewort?

CODEWORT-QUIZ

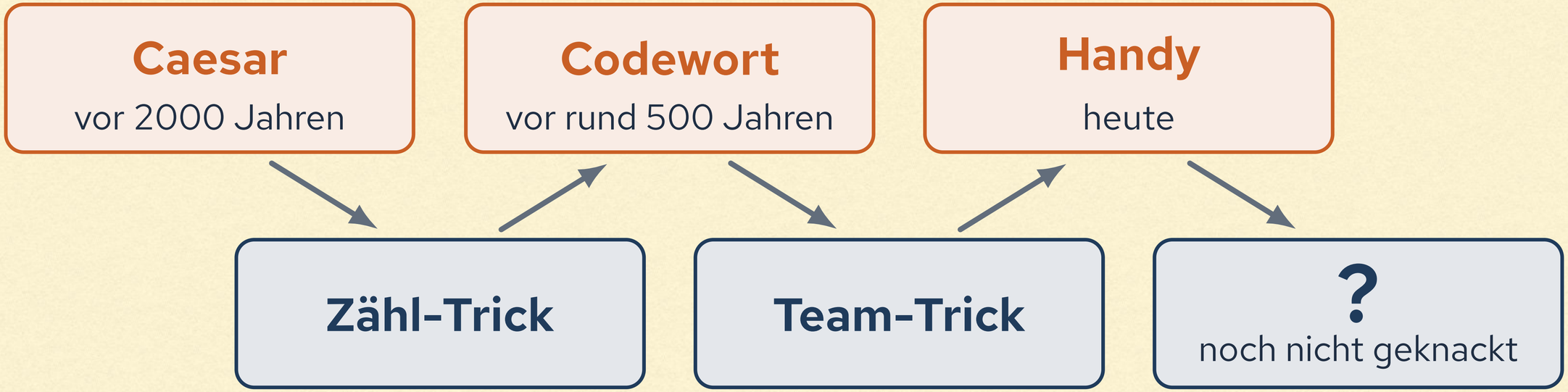
Agenten-Blatt · Aufgabe 4

- Was steht hier?
- Das Codewort ist FEE

XTMTR

SPION

DAS GROßE WETTRENNEN



Geheimschrift-Erfinder gegen **Codeknacker** – seit 2000 Jahren

VERSCHLÜSSELUNG IST ÜBERALL

- Chat-Nachrichten
- Webseiten
- WLAN
- Funk-Autoschlüssel
- …



Illustration mit ChatGPT generiert

WIE VIELE SCHLÜSSEL?

Caesar-Scheibe:

25

Alphabet wild durchmischen:

403 291 461 126 605 635 584 000 000

Verschlüsselung im Handy:

115 792 089 237 316 195 423 570 985 008 687 907 853
269 984 665 640 564 039 457 584 007 913 129 639 936

Alle ausprobieren? Dauert länger, als es das Universum gibt!

VIELE SCHLÜSSEL REICHEN NICHT

Funk-Autoschlüssel
KeeLoq
im Einsatz seit den 1990ern
GEKNACKT 2008

Handy-Netz
GSM · A5/1
im Einsatz seit den 1990ern
GEKNACKT 2009

Altes WLAN
WEP
im Einsatz 1997 bis nach 2010
GEKNACKT 2001

- Jedes hatte mehr als eine Billion Schlüssel
- Geknackt wurden sie trotzdem – durch clevere Tricks

HEUTE: AES UND RSA

AES

schützt WLAN, Chats, Festplatten

im Einsatz seit 2001

GILT ALS SICHER

RSA

rechnet mit riesigen Primzahlen

im Einsatz seit 1977

GILT ALS SICHER

- An beiden beißen sich Codeknacker seit Jahrzehnten die Zähne aus
- Sie gelten als sicher … **im Moment**

DAHINTER STECKT MATHEMATIK

- Wer erfindet neue Geheimschriften?
- Und wer prüft, ob sie halten?
- **Mathematikerinnen und Mathematiker!**
- Mathematik kann man studieren
- … zum Beispiel an der RPTU 😉



GEHEIMBOTSCHAFT DES TAGES

HIV WGLPYIWWIP MWX HVIM YRH IMRW

DER SCHLUESSEL IST DREI UND EINS

GV EJVU FPGFNODDNFU

DU BIST CODEKNACKER

- **Blaue Box**: einfache Verschiebung – welcher Schlüssel?
- **Rote Box**: Die Schlüssel verrät die **blaue Box**

DANKE!

VIEL SPAß BEIM VERSCHLÜSSELN UND KNACKEN

Für zu Hause: eure Caesar-Scheibe und das Rätselblatt

RPTU Rheinland-Pfälzische Technische Universität Kaiserslautern Landau

