KRYPTOGRAFIE

WIE MATHEMATIK BEIM VERSTECKEN HILFT

Prof. Dr. Max Horn

RPTU
Rheinland-Pfälzische
Technische Universität
Kaiserslautern
Landau



GEHEIME BOTSCHAFTEN

- Alia möchte Ben etwas Geheimes mitteilen
- im Unterricht...
- Zurufen? Hört jeder → *öffentlicher Kanal*
- Zettel unter der Bank? 😉
- Problem: kann abgefangen werden…



Illustration mit ChatGPT generiert

LÖSUNG: VERSCHLÜSSELN

Botschaft (Klartext)

Treffen wir uns nach der Schule?



Geheimbotschaft

WUHIIHQZLUXQV QDFKGHUVFKXOH

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

VERSCHLÜSSELUNG IST ÜBERALL

- Webseiten
- Chat
- Funk-Autoschlüssel
- WLAN
- ...



Illustration mit ChatGPT generiert

EINE URALTE IDEE

- Julius Caesar
- 1. Jahrhundert vor Christus
- also vor über 2000 Jahren
- Kernidee: „Buchstaben verschieben“



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

DER CAESAR-CHIFFRE

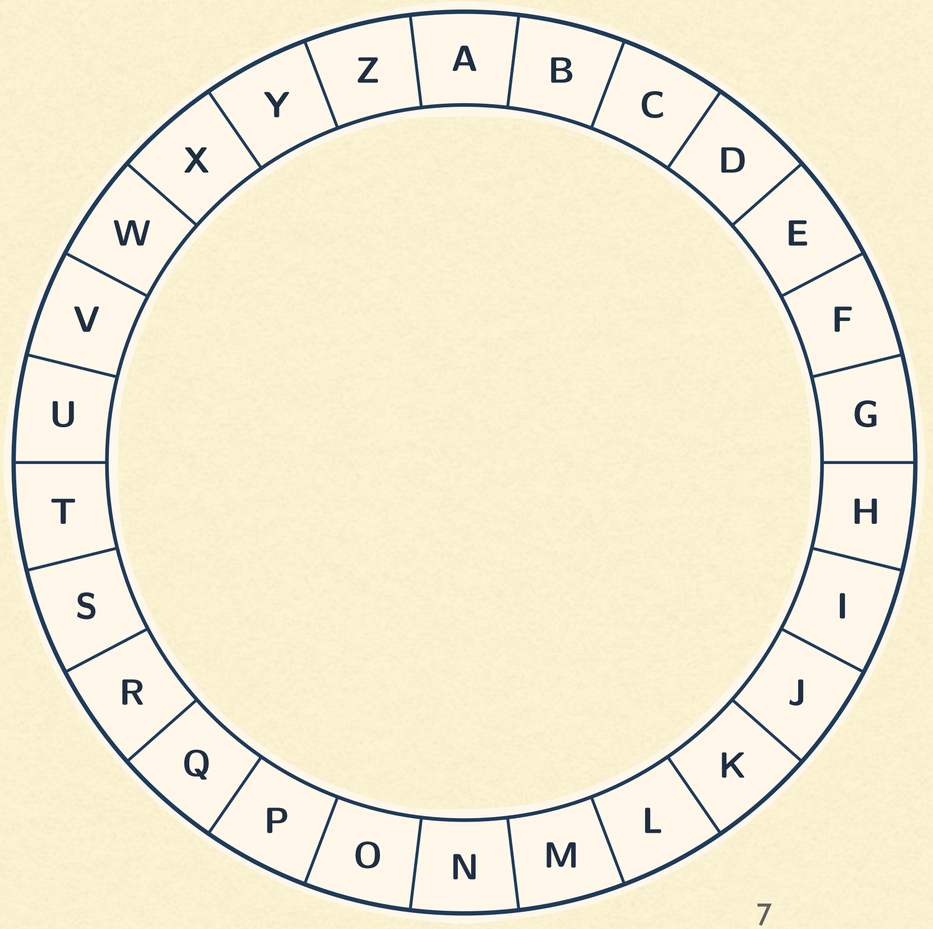
- Verschlüsseln: jeden Buchstabe durch einen anderen ersetzen
- z. B. Alphabet „drei Schritte weit verschieben“
- A B C D E F G ⋯ W X Y Z
  ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓
  D E F G H I J ⋯ Z A B C
- Entschlüsseln: zurückschieben



Illustration: Foto eines „Decoder Rings“ aus dem amerikanischen Bürgerkrieg; Foto Copyright (C) Chris Daniels 2017

BEISPIEL CAESAR

- Geheimbotschaft: HALLO
- Verschlüsselt: KDOOR
- Zum entschlüsseln: einfach umgekehrt verschieben



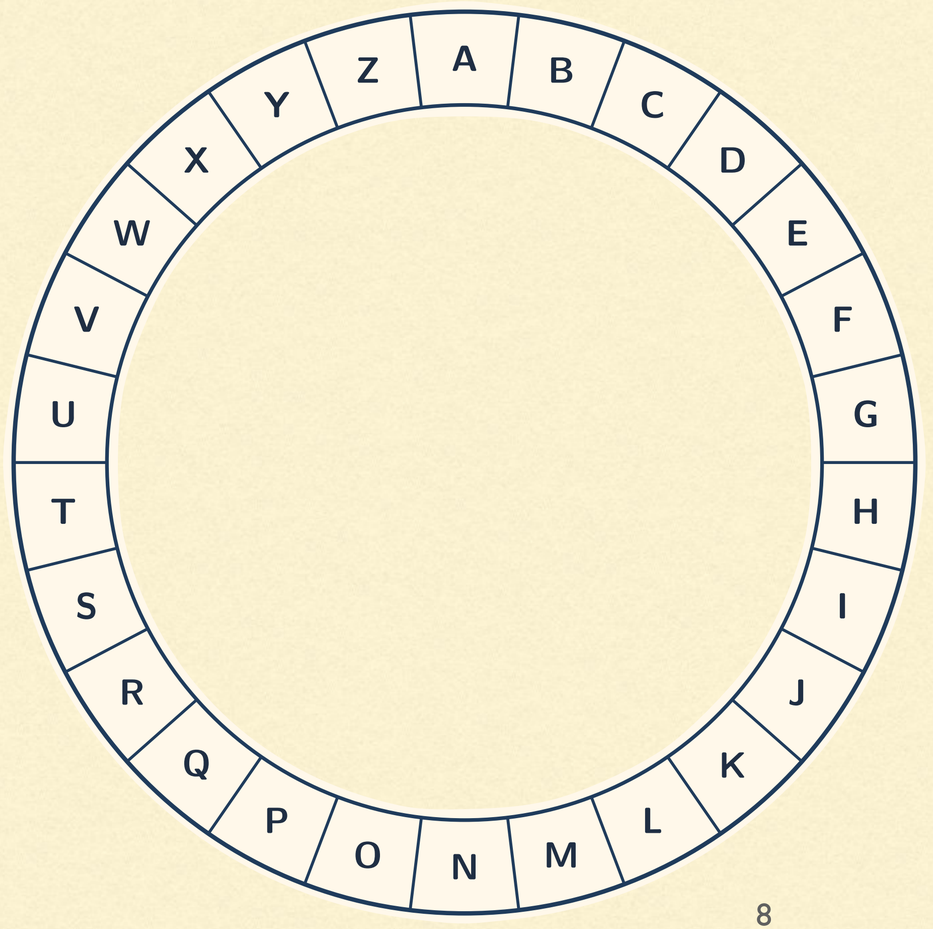
Illustrationen selbst mit LaTeX und TiKZ erstellt

MINI-QUIZ

Was bedeutet das hier wohl:
PDWKHPDWLN

Wer bekommt es raus?

MATHEMATIK



Illustrationen selbst mit LaTeX und TiKZ erstellt

WIE SICHER IST DAS?

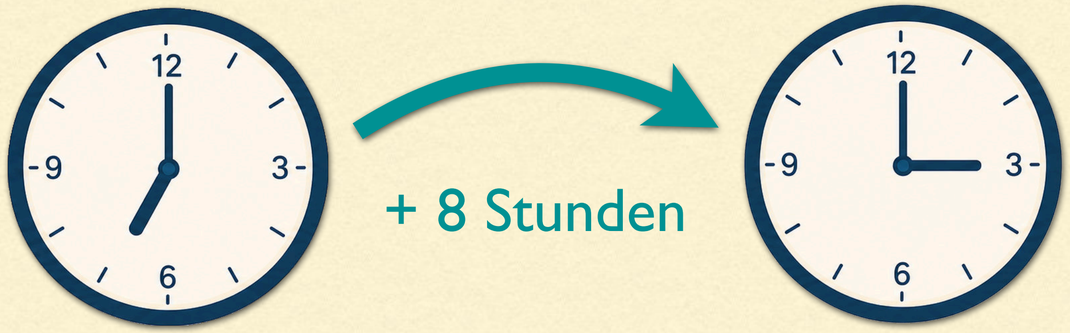
- Geheimbotschaft wird abgehört – was nun?
- Lauscher kennt Caesar-Chiffre *nicht*: vorerst sicher
- Lauscher kennt Caesar-Chiffre: komplett unsicher
- Idee: andere Verschiebung wählen (etwa 8 statt 3)
- Gewählt Verschiebung ist *geheimer Schlüssel*
- Problem: nur 25 sinnvolle Schlüssel ⇝ kann man durchprobieren



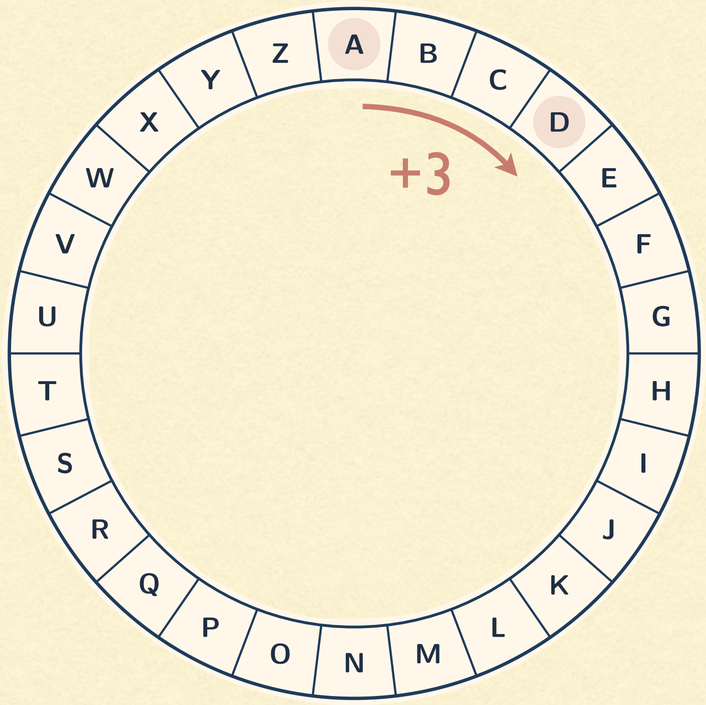
Illustration mit ChatGPT generiert

RECHNEN IM KREIS

- „Es ist jetzt 7 Uhr. In 8 Stunden treffen wir uns. Dann ist es 3 Uhr.“



- Bei Caesar machen wir fast dasselbe...
- statt 12 Stunden eben 26 Buchstaben
- Wir „addieren im Kreis“ statt auf einem Zahlenstrahl



Illustrationen mit ChatGPT generiert

EXKURS: MODULO-RECHNEN

- „Es ist jetzt 7 Uhr. In 8 Stunden treffen wir uns. Dann ist es 3 Uhr.“
- Jetzt mal mit Mathe ...
- Wähle eine natürliche Zahl N, den *Modulus* (z. B. 12 oder 26)
- Für ganze Zahl x sei $x \bmod N$ der Rest von x nach Division durch N
- Beispiel: $(7 + 8) \bmod 12 = 15 \bmod 12 = 3$
- Mini-Quiz: Was ist $(18 + 13) \bmod 26 = ?$ $= 31 \bmod 26 = 5$

CAESAR UND MODULO

- Sei nun $N = 26$
- Identifiziere Buchstaben mit Zahlen:
- A B C D E F G ⋯ W X Y Z
  ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓
  0 1 2 3 4 5 6 ⋯ 22 23 24 25
- Caesar-Chiffre verschlüsselt x zu $(x + 3) \bmod 26$
- Idee: Identifiziere nun den „Schlüssel“ 3 mit dem Buchstaben D

VIGENÈRE-CHIFFRE

- Vigenère-Chiffre: Geheim-Schlüssel ist ein Wort
- Beispiel: Botschaft „MATHEMATIK“, Schlüssel „PSST“
- Schreibe übereinander, wiederhole Schlüssel wenn nötig:

MATHEMATIK		12	0	19	7	4	12	0	19	8	10
PSSTPSSTPS	+	15	18	18	19	15	18	18	19	15	18
BSLATESMXC		1	18	11	0	19	4	18	12	23	2

Geheimbotschaft

- Entschlüsseln: durch Subtraktion $\mod 26$

MODERNE VERFAHREN

- Caesar und Vigènere sind mit Computern leicht zu knacken
  - jedenfalls wenn die Botschaften lang genug sind
- Moderne Chiffren sind z. B. AES, DES, RSA, ECDSA, NTRU, ...
- Bei allen spielt Modulo-Rechnung eine Rolle
- ... und noch mehr Mathematik

GEHEIMNIS-AUSTAUSCH

- Alia und Ben einigen sich öffentlich auf Primzahl $p := 29$ sowie *Erzeuger* $g := 2$
- Alia wählt geheimes $a \in \{2,\ldots,p-1\}$, veröffentlicht $A := g^a \bmod p$
  - z. B. $a := 5, \quad A := 2^5 \bmod 29 = 32 \bmod 29 = 3$
- Ben wählt geheimes $b \in \{2,\ldots,p-1\}$, veröffentlicht $B := g^b \bmod p$
  - z. B. $b := 8, \quad B := 2^8 \bmod 29 = 256 \bmod 29 = 24$
- Alle kennen $p = 29,\ g = 2,\ A = 3,\ B = 24$; nur Alia kennt a, nur Ben kennt b
- p groß $\rightsquigarrow$ schwer, a, b aus A, B zu berechnen $\rightsquigarrow$ *diskreter-Logarithmus-Problem*

GEHEIMNIS-AUSTAUSCH, TEIL 2

- Alle in der Klasse kennen jetzt $p = 29,\ g = 2,\ A = 3,\ B = 24$
- nur Alia kennt a, nur Ben kennt b
- Alia berechnet $B^a \bmod p = 24^5 \bmod 29 = 7$
- Ben berechnet $A^b \bmod p = 3^8 \bmod 29 = 7$
- Zweimal der gleiche Wert – Zufall?! Nein: $A^b = (g^a)^b = g^{ab} = (g^b)^a = B^a$
- Alia und Ben kennen nun beide den Geheimwert 7, sonst niemand
- Dies ist der *Diffie-Hellman-Schlüsselaustausch*

SICHERE KOMMUNIKATION

- ... braucht heute ganz viel Mathematik
  - z. B. *Modulo-Rechnung, Faktorisieren, diskrete Logarithmen*
  - aber auch algebraische Strukturen (*Gruppen, Ringe, Körper*)
  - und vieles mehr
- Daran und damit wird bis heute weiter geforscht

TAG DER MATHEMATIK 2026



- Am 13. Juni 2026, 9:30-15:30 Uhr
- An der RPTU in Kaiserslautern
- Vorträge, Workshops, Ausstellungen...
- und Kryptografie zum Anfassen 😉
- Mehr unter math.rptu.de/tdm