Stefan Jansen

Technische Hochschule Augsburg

Weihnachtsvorlesung

Was hat Wichteln mit Klausuraufgaben und seltsamen Maschinen zu tun?

11.12.2025

Was erwartet Euch?

Teil 1:
Autobiographisch: *Worüber mache ich mir beim Korrigieren von Klausuren Gedanken (oder wie lenke ich mich gekonnt von der Arbeit ab...)?*

Teil 2:
Gesellschaft: *Wichteln, aber richtig!*

Teil 3:
Geschichte: *Wie Mathematiker die Welt retten.*

Was erwartet Euch?

Teil 1:
Autobiographisch: *Worüber mache ich mir beim Korrigieren von Klausuren Gedanken (oder wie lenke ich mich gekonnt von der Arbeit ab...)?*

Teil 2:
Gesellschaft: *Wichteln, aber richtig!*

Teil 3:
Geschichte: *Wie Mathematiker die Welt retten.*

Warnung:

Was erwartet Euch?

Teil 1:
Autobiographisch: *Worüber mache ich mir beim Korrigieren von Klausuren Gedanken (oder wie lenke ich mich gekonnt von der Arbeit ab...)?*

Teil 2:
Gesellschaft: *Wichteln, aber richtig!*

Teil 3:
Geschichte: *Wie Mathematiker die Welt retten.*

Warnung:

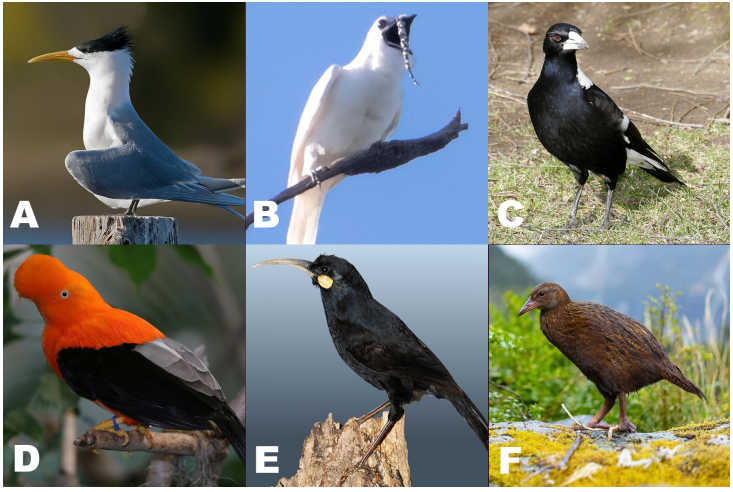
Der Vortrag enthält Mathematik!

Es begab sich zu einer Zeit ...

Es begab sich zu einer Zeit ...

... als Klausuren korrigiert werden mussten!

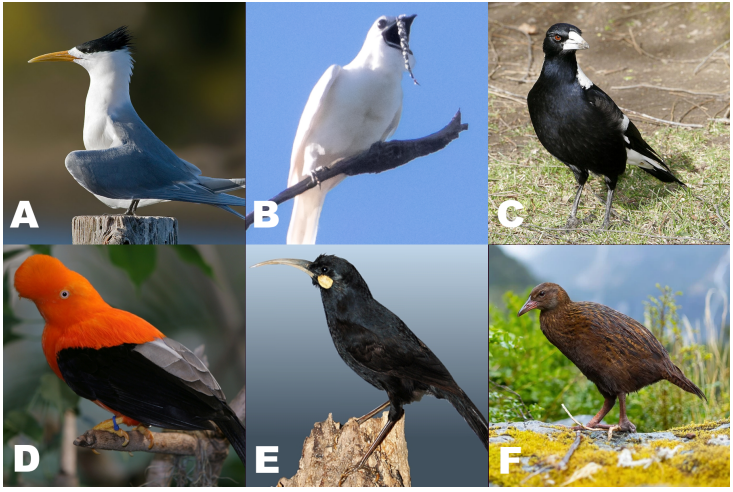
Klausuraufgabe



Aufgabe:
Ordne die Vögeln zu. Für jede richtige Antwort gibt es 1 Punkt, für jede falsche 0 Punkte.

[ ] Einlappenkotinga
[ ] Huia
[ ] Eilseeschwalbe
[ ] Flötenkrähenstar
[ ] Andenklippenvogel
[ ] Wekaralle

Klausuraufgabe



Aufgabe:
Ordne die Vögeln zu. Für jede richtige Antwort gibt es 1 Punkt, für jede falsche 0 Punkte.

[B] Einlappenkotinga
[E] Huia
[A] Eilseeschwalbe
[C] Flötenkrähenstar
[D] Andenklippenvogel
[F] Wekaralle

Klausuraufgabe

Beobachtungen:

- Erstaunlich viele haben bei der Aufgabe genau 0 oder genau 1 Punkt!

Fragen:

- Wie viele verschiendene Antwortmöglichkeiten hat der Student Paul Planlos, der von der Klausur überrascht wurde, leider nicht lernen konnte und deshalb raten muss?
- Bei wie vielen der Möglichkeiten hat Paul keinen Punkt geholt?
- Wie viele Punkte erreichen ratende Studenten durchschnittlich? (Erwartungswert)

Klausuraufgabe

Beobachtungen:

- Erstaunlich viele haben bei der Aufgabe genau 0 oder genau 1 Punkt!

Fragen:

- Wie viele verschiendene Antwortmöglichkeiten hat der Student Paul Planlos, der von der Klausur überrascht wurde, leider nicht lernen konnte und deshalb raten muss?
- Bei wie vielen der Möglichkeiten hat Paul keinen Punkt geholt?
- Wie viele Punkte erreichen ratende Studenten durchschnittlich? (Erwartungswert)

Antworten:

- $6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 6! = 720$ Möglichkeiten (Permutationen)
- Bei zweiter und dritter Frage ist (ohne Vorwissen) nicht sofort klar.

Untersuche Problem

Frage: Wie wahrscheinlich ist es keinen Punkt zu holen? (Fixpunktfreie Permutationen)

Ausprobieren: Schwierig mit $n = 6$ Antworten. Aber mit $n = 1$, $n = 2$, $n = 3$ und $n = 4$.

A B C D	B A C D	C A B D	D A B C
A B D C	B A D C	C A D B	D A C B
A C B D	B C A D	C B A D	D B A C
A C D B	B C D A	C B D A	D B C A
A D B C	B D A C	C D A B	D C A B
A D C B	B D C A	C D B A	D C B A

$n \backslash k$	0	1	2	3	4	Perm.
1	0	1				1
2	1	0	1			2
3	2	3	0	1		6
4	9	8	6	0	1	24

Untersuche Problem

Frage: Wie wahrscheinlich ist es keinen Punkt zu holen? (Fixpunktfreie Permutationen)

Ausprobieren: Schwierig mit $n = 6$ Antworten. Aber mit $n = 1$, $n = 2$, $n = 3$ und $n = 4$.

A B C D	B A C D	C A B D	D A B C
A B D C	B A D C	C A D B	D A C B
A C B D	B C A D	C B A D	D B A C
A C D B	B C D A	C B D A	D B C A
A D B C	B D A C	C D A B	D C A B
A D C B	B D C A	C D B A	D C B A

$n \backslash k$	0	1	2	3	4	Perm.
1	0	1				1
2	1	0	1			2
3	2	3	0	1		6
4	9	8	6	0	1	24

Simulieren für $n = 6$**:**

```
## $`Anzahl Simulationen`
## [1] 100000
##
## $`Anzahl Punkte`
## y
##     0     1     2     3     4     6
## 36779 36637 18775  5614  2050   145
```

```
## $`Prozent Punkte`
## y
##      0      1      2      3      4      6
## 0.3678 0.3664 0.1878 0.0561 0.0205 0.0014
##
## $`Mittelwert Punkte`
## [1] 1.00099
```

Untersuche Problem: Fixpunktfreie Permutationen

n	#Permutationen	#fixpunktfreier Perm.	rel. Anteil fixpunktfr. Perm.
1	1	0	0
2	2	1	0.5
3	6	2	$0.\overline{3}$
4	24	9	0.375
5	120	44	$0.3\overline{6}$
6	720	265	$0.3680\overline{5}$
7	5 040	1 854	0.36785714...
8	40 320	14 833	0.36788194...
9	363 880	133 496	0.36787918...
10	3 628 800	1 334 961	0.36787946...

Anzahl der fixpunktfreien Permutationen (Derangements):

$$!n = n! \cdot \sum_{k=0}^{n} \frac{(-1)^k}{k!} = n! \cdot \left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + \frac{(-1)^n}{n!}\right) \qquad \lim_{n \to \infty} \frac{!n}{n!} = \frac{1}{\mathrm{e}}$$

$!n$ heißt **Subfakultät** und entspricht der Anzahl der fixpunktfreien Permutationen.

Rencontres-Zahlen (franz.: *Begegnungen*)

$n \backslash k$	0	1	2	3	4	5	6	7	8	Summe
0	1									1
1	0	1								1
2	1	0	1							2
3	2	3	0	1						6
4	9	8	6	0	1					24
5	44	45	20	10	0	1				120
6	265	264	135	40	15	0	1			720
7	1 854	1 855	924	315	70	21	0	1		5 040
8	14 833	14 832	7 420	2 464	630	112	28	0	1	40 320

- Die Zahlen mit $k = 0$ sind die fixpunktfreien Permutationen oder Derangements.
- Die Rencontres-Zahlen können direkt berechnet werden: $D_{n,k} = !(n-k)\binom{n}{k} = \frac{n!}{k!}\sum_{j=0}^{n-k}\frac{(-1)^j}{j!}$.
- Der Erwartungswert der 'Punkte' beim Raten in der Klausur ist unabhängig von n immer 1.

Alles verstanden?

Spielregeln:

- Spieler 1 und Spieler 2 bekommen jeweils ein Kartenspiel mit 52 verschiedenen, sehr gut gemischten Karten. Die Kartenspiele sind identisch.
- Beide Spieler drehen immer gemeinsam die oberste Karte um.
- Spieler 1 gewinnt genau dann, wenn zu einem beliebigen Zeitpunkt die jeweils obersten Karten gleich sind, Spieler 2 genau dann, wenn das bis zum Ende nicht eintritt.

Alles verstanden?

Spielregeln:

- Spieler 1 und Spieler 2 bekommen jeweils ein Kartenspiel mit 52 verschiedenen, sehr gut gemischten Karten. Die Kartenspiele sind identisch.
- Beide Spieler drehen immer gemeinsam die oberste Karte um.
- Spieler 1 gewinnt genau dann, wenn zu einem beliebigen Zeitpunkt die jeweils obersten Karten gleich sind, Spieler 2 genau dann, wenn das bis zum Ende nicht eintritt.

Fragen:

- Welcher Spieler hat die höhere Gewinnwahrscheinlichkeit?

[A] Spieler 1 **[B]** Spieler 2 **[C]** Ist bei beiden gleich.

Alles verstanden?

Spielregeln:

- Spieler 1 und Spieler 2 bekommen jeweils ein Kartenspiel mit 52 verschiedenen, sehr gut gemischten Karten. Die Kartenspiele sind identisch.
- Beide Spieler drehen immer gemeinsam die oberste Karte um.
- Spieler 1 gewinnt genau dann, wenn zu einem beliebigen Zeitpunkt die jeweils obersten Karten gleich sind, Spieler 2 genau dann, wenn das bis zum Ende nicht eintritt.

Fragen:

- Welcher Spieler hat die höhere Gewinnwahrscheinlichkeit?

  [A] Spieler 1 **[B]** Spieler 2 **[C]** Ist bei beiden gleich.

- Wenn die Spieler nun ein Kartenspiel mit 32 Blatt nehmen, verbessert das die Gewinnwahrscheinlichkeit (messbar)?

  [A] für Spieler 1 **[B]** für Spieler 2 **[C]** für keinen der Spieler

Alles verstanden?

Spielregeln:

- Spieler 1 und Spieler 2 bekommen jeweils ein Kartenspiel mit 52 verschiedenen, sehr gut gemischten Karten. Die Kartenspiele sind identisch.
- Beide Spieler drehen immer gemeinsam die oberste Karte um.
- Spieler 1 gewinnt genau dann, wenn zu einem beliebigen Zeitpunkt die jeweils obersten Karten gleich sind, Spieler 2 genau dann, wenn das bis zum Ende nicht eintritt.

Fragen:

- Welcher Spieler hat die höhere Gewinnwahrscheinlichkeit?

  [A] Spieler 1 **[B]** Spieler 2 **[C]** Ist bei beiden gleich.

- Wenn die Spieler nun ein Kartenspiel mit 32 Blatt nehmen, verbessert das die Gewinnwahrscheinlichkeit (messbar)?

  [A] für Spieler 1 **[B]** für Spieler 2 **[C]** für keinen der Spieler

Lösungen: [A] und **[C]** (es sei denn sie spielen öfter als 10^{20} mal pro Sekunde – seit dem Urknall)

Wichteln (engl.: Secret Santa)

Spielregeln / Idee:

- Jeder Teilnehmer verschenkt genau ein Geschenk.
- Jeder Teilnehmer bekommt genau ein Geschenk.
- Keiner darf sich selbst beschenken.
- Anonymität: Der Beschenkte sollte nicht wissen von wem er das Geschenk bekommt.
- Fairness: Jede Konstellation sollte gleich wahrscheinlich sein.

Methode 1: naive Vorgehensweise

Theorie:

- Jeder schreibt seinen Namen auf einen kleinen Zetteln.
- Alle Zettel werden Nikolausmütze gesammelt.
- Jeder zieht einen Zettel aus der Mütze und der Person auf der Person muss man ein Geschenk machen.
- Aber: sobald einer sich selbst zieht, werden alle Zettel wieder eingesammelt und alle ziehen erneut.
- Sobald eine fixpunktfreie Permutation der Spieler zustande gekommen ist kann gewichtelt werden.

Methode 1: naive Vorgehensweise

Theorie:

- Jeder schreibt seinen Namen auf einen kleinen Zetteln.
- Alle Zettel werden Nikolausmütze gesammelt.
- Jeder zieht einen Zettel aus der Mütze und der Person auf der Person muss man ein Geschenk machen.
- Aber: sobald einer sich selbst zieht, werden alle Zettel wieder eingesammelt und alle ziehen erneut.
- Sobald eine fixpunktfreie Permutation der Spieler zustande gekommen ist kann gewichtelt werden.

Praxis / Problem:

- Methode ist anonym und fair.
- In ca. 63.2% der Fälle (ab 4 Spieler) zieht einer der Beteiligten sich selbst! Führt ggf. zu verringertem Wichtelspaß.

Erfolgswahrscheinlichkeit:

Versuche	1	2	3	4	5	6	7	8	9	10
Erfolg [%]	36.8	60.0	74.7	84.0	89.9	93.6	96.0	97.5	98.4	99.0

Methode 2: naive Vorgehensweise mit Zurücklegen

Theorie:

- wie Methode 1, aber
- zieht jemand sich selbst: zurücklegen und einen anderen Zettel ziehen

Methode 2: naive Vorgehensweise mit Zurücklegen

Theorie:

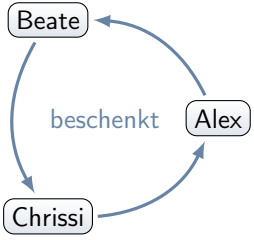
- wie Methode 1, aber
- zieht jemand sich selbst: zurücklegen und einen anderen Zettel ziehen

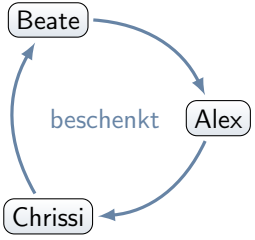
Praxis / Problem:

- Weder fair, noch anonym (siehe Beispiel!)
- Im schlechtesten Fall zieht sich der letzte selbst und alle müssen von vorne anfangen

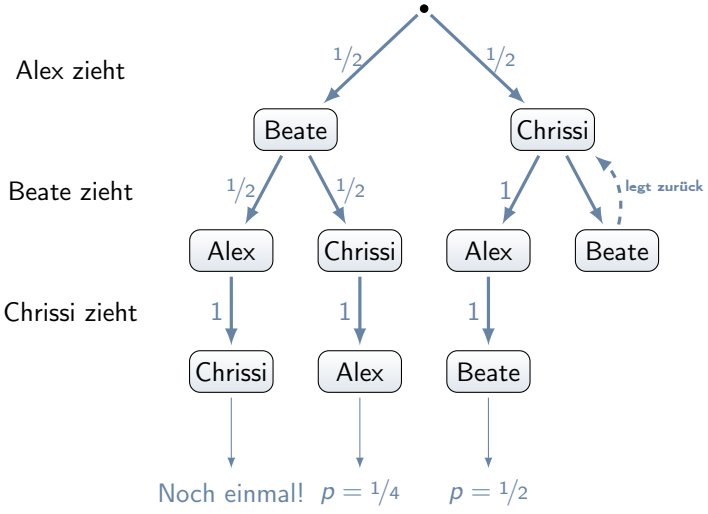
Methode 2: Beispiel 3 Spieler

Alex	Beate	Chrissi	ok?	
Alex	Beate	Chrissi	✗	
Alex	Chrissi	Beate	✗	
Beate	Alex	Chrissi	✗	
Beate	Chrissi	Alex	✓	(linkes Bild)
Chrissi	Alex	Beate	✓	(rechtes Bild)
Chrissi	Beate	Alex	✗	

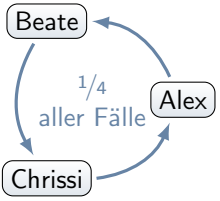


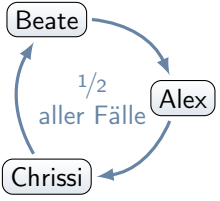


Methode 2: Fairness / Anonymität



- Anonymität: Gibt es bei 3 Spielern noch nicht!





und in $1/4$ aller Fälle wiederholen.

Methode 2: 4 Spieler (Wiederholung bei 4.)

A	B	C	D	p
B	A	D	C	$1/9$
B	C	D	A	$1/18$
B	D	A	C	$1/9$
C	A	D	B	$1/12$
C	D	A	B	$1/12$
C	D	B	A	$1/12$
D	A	B	C	$1/6$
D	C	A	B	$1/12$
D	C	B	A	$1/12$
				$31/36 \approx 0.86$

Wahrscheinlichkeiten:

gibt\nimmt	A	B	C	D
A		$\frac{10}{36}$	$\frac{9}{36}$	$\frac{12}{36}$
B	$\frac{13}{36}$		$\frac{8}{36}$	$\frac{10}{36}$
C	$\frac{10}{36}$	$\frac{12}{36}$		$\frac{9}{36}$
D	$\frac{8}{36}$	$\frac{9}{36}$	$\frac{14}{36}$	$(\frac{5}{36})$

- In $\frac{5}{36} \approx 14\%$ der Fälle zieht der Letzte sich selbst, und es muss noch einmal ausgelost werden.

- Es wird der Reihe nach A, B, C dann D gezogen, nur wenn der letzte (hier D) sich selbst zieht wird wiederholt.
- keine Anonymität: Zieht z.B. C (vorletzter) sich selbst, so weiß er danach alles! Zieht B (zweiter) sich selbst, so kann er auf 2 mögliche Konstellationen schließen.

Methode 2: 4 Spieler (Wiederholung bei 3. und 4.)

A	B	C	D	p
B	A	D	C	$1/9$
B	C	D	A	$1/18$
B	D	A	C	$1/18$
C	A	D	B	$1/12$
C	D	A	B	$1/12$
C	D	B	A	$1/12$
D	A	B	C	$1/12$
D	C	A	B	$1/12$
D	C	B	A	$1/12$
				$13/18 \approx 0.72$

Wahrscheinlichkeiten

gibt\nimmt	A	B	C	D
A		$\frac{8}{36}$	$\frac{9}{36}$	$\frac{9}{36}$
B	$\frac{10}{36}$		$\frac{8}{36}$	$\frac{8}{36}$
C	$\frac{8}{36}$	$\frac{9}{36}$		$\frac{9}{36}$
D	$\frac{8}{36}$	$\frac{9}{36}$	$\frac{9}{36}$	

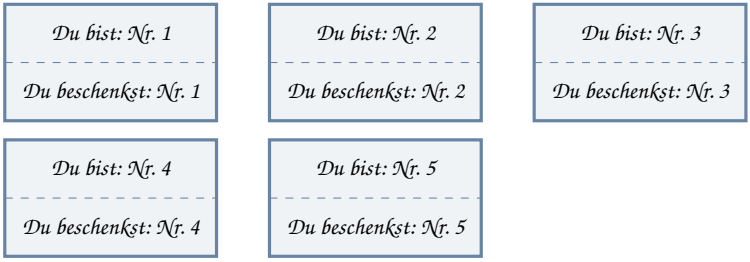
- In etwa $\frac{10}{36} \approx 28\%$ der Fälle zieht sich der Vorletzte oder der Letzte selbst und es muss nocheinmal ausgelost werden.

- Neu ziehen, wenn der vorletzte oder der letzte Spieler (hier C und D) sich selbst zieht, ziehen A und B sich selbst wird zurückgelegt.
- Anonymität: Besser als im vorherigen Fall, da nie eindeutig auf Konstellation zurückgeschlossen werden kann beim Zurücklegen.

Methode 3: Wichteln für Fortgeschrittene

Idee: Erzeugt zuerst eine fixpunktfreie Permutation, dann verteilt die Kärtchen.

1. Man nimmt bei n Personen n gleiche, rechteckige Zettel, knickt sie in der Mitte und beschriftet sie wie abgebildet (jeweils mit den Nummern 1 bis n).

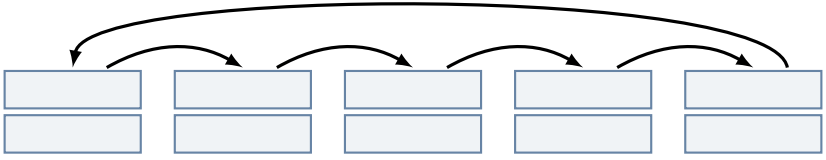


2. Dann dreht die Kärtchen so hin, dass die Zahlen nicht gesehen werden können.

Methode 3: Wichteln für Fortgeschrittene

- Nun schneidet man alle Kärtchen durch ...

- ... und verschiebt oberen und unteren Teil um eins gegeneinander
  $\Longrightarrow$ so ist die Fixpunktfreiheit sichergestellt!



Methode 3: Wichteln für Fortgeschrittene

5. Auf diese Art entsteht eine fixpunktfreie Permutation:

Du bist: Nr. 3	*Du bist: Nr. 5*	*Du bist: Nr. 2*	*Du bist: Nr. 1*	*Du bist: Nr. 4*
Du beschenkst: Nr. 4	*Du beschenkst: Nr. 3*	*Du beschenkst: Nr. 1*	*Du beschenkst: Nr. 5*	*Du beschenkst: Nr. 2*

6. Die so entstandenen (allen unbekannten) Kombinationen werden gemischt und an alle Teilnehmer verteilt.
7. Am Ende muss es noch eine Liste mit allen Namen geben in die sich jeder einträgt (siehe rechts)

Wichteln

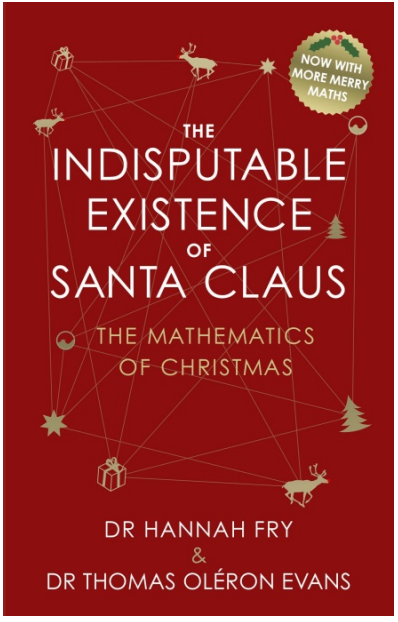
Bitte tragt Euren Namen hinter Eurer Zahl ein:

1. *Frank N. Stein*
2. *Marie Huana*
3. *Hugo Slawien*
4. *Johannes Bär*
5. *Polly Zist*

Bemerkung:

- Nicht jede fixpunktfreie Permutation ist möglich: es kann z.B. nicht passieren, dass zwei Leute sich gegenseitig beschenken.
- Ggf. (falls gewollt) künstlich einfügbar.

Buchtipp

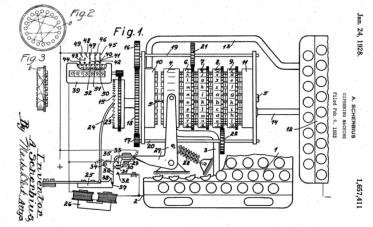


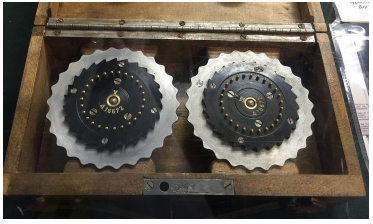
CONTENTS

Rätsel: Was ist das?

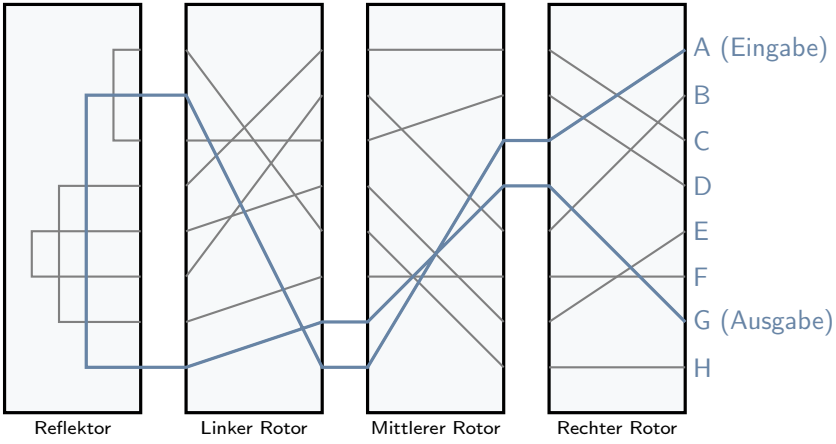
Historisches:

- Rotor-Schlüsselmaschine zur Verschlüsselung von Nachrichten
- entwickelt zuerst 1915, dann 1918 patentiert
- insbesondere während des zweiten Weltkriegs von den Deutschen zur Verschlüsselung von Nachrichten verwendet
- enthält ursprünglich drei später fünf Walzen, die jeweils mit 26 Kontakten auf beiden Seiten ausgestattet sind
- keine monoalphabetische Verschlüsselung (z.B. MOMO wird zu GLGL), sondern durch die Rotoren 'dynamisch'
- $\Longrightarrow$ galt deshalb als unknackbar, da bis dahin verwendete Dechiffrierverfahren nicht mehr funktionierten
- Polnischer Mathematiker Marian Rejewski knackte Code (bis 1938), danach französisch, britische und polnische Mathematiker mit bis zu 14 000 Menschen und 'Turing Bombe' (Maschine).

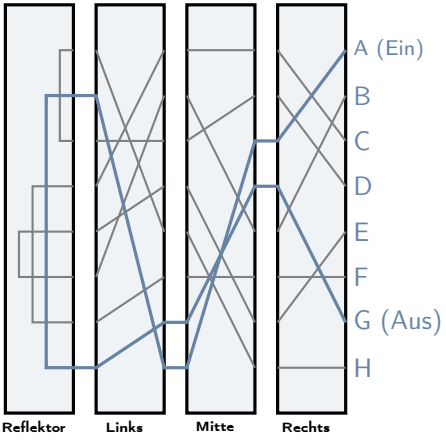


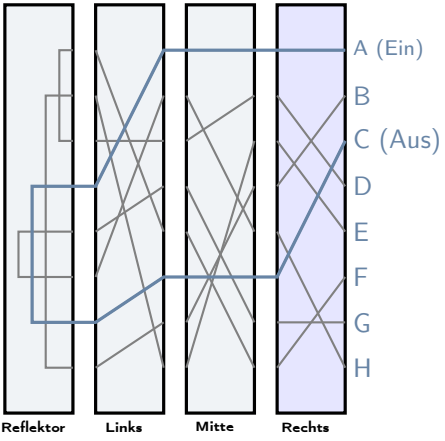


ENIGMA: Wie funktioniert's?



ENIGMA: Wie funktioniert's?





- Die rechte Rolle im rechten Bild wird um eine Einheit weitergedreht

Wie gut ist die Verschlüsselung?

- Schlüsselraum setzt sich aus 4 Teilen zusammen:
  - Lage der Rotoren: (3 aus 5) macht 60 Möglichkeiten
  - Ringstellungen: 01 bis 26 bei zwei relevanten Ringen macht $26^2 = 676$ Möglichkeiten
  - Die Rotorenstellung zueinander: $26 \cdot 25 \cdot 26 = 16\,900$ Walzenstellungen
  - Steckerverbindungen: bis zu 13 Verbindungen bei 26 Buchsen (10 wurden de facto verwendet) machen nochmal 150 738 274 937 250 Möglichkeiten.

- Selbst heute mit *brute force* kaum zu machen.
- Aber: In Wirklichkeit kleinerer Raum den man durchsuchen musste, nur ca. 1 Million Möglichkeiten (Im wesentlichen sind es nur nur Rotoren und die Walzenstellungen, da Rest fix bleibt).
- Eigentliche Schwäche ist Umkehrwalze!

Wie gut ist die Verschlüsselung?

- Schlüsselraum setzt sich aus 4 Teilen zusammen:
  - Lage der Rotoren: (3 aus 5) macht 60 Möglichkeiten
  - Ringstellungen: 01 bis 26 bei zwei relevanten Ringen macht $26^2 = 676$ Möglichkeiten
  - Die Rotorenstellung zueinander: $26 \cdot 25 \cdot 26 = 16\,900$ Walzenstellungen
  - Steckerverbindungen: bis zu 13 Verbindungen bei 26 Buchsen (10 wurden de facto verwendet) machen nochmal 150 738 274 937 250 Möglichkeiten.

- Selbst heute mit *brute force* kaum zu machen.
- Aber: In Wirklichkeit kleinerer Raum den man durchsuchen musste, nur ca. 1 Million Möglichkeiten (Im wesentlichen sind es nur nur Rotoren und die Walzenstellungen, da Rest fix bleibt).
- Eigentliche Schwäche ist Umkehrwalze!

Wie gut ist die Verschlüsselung?

- Schlüsselraum setzt sich aus 4 Teilen zusammen:
  - Lage der Rotoren: (3 aus 5) macht 60 Möglichkeiten
  - Ringstellungen: 01 bis 26 bei zwei relevanten Ringen macht $26^2 = 676$ Möglichkeiten
  - Die Rotorenstellung zueinander: $26 \cdot 25 \cdot 26 = 16\,900$ Walzenstellungen
  - Steckerverbindungen: bis zu 13 Verbindungen bei 26 Buchsen (10 wurden de facto verwendet) machen nochmal 150 738 274 937 250 Möglichkeiten.

- Selbst heute mit *brute force* kaum zu machen.
- Aber: In Wirklichkeit kleinerer Raum den man durchsuchen musste, nur ca. 1 Million Möglichkeiten (Im wesentlichen sind es nur nur Rotoren und die Walzenstellungen, da Rest fix bleibt).
- Eigentliche Schwäche ist Umkehrwalze!

Wie gut ist die Verschlüsselung?

- Schlüsselraum setzt sich aus 4 Teilen zusammen:
  - Lage der Rotoren: (3 aus 5) macht 60 Möglichkeiten
  - Ringstellungen: 01 bis 26 bei zwei relevanten Ringen macht $26^2 = 676$ Möglichkeiten
  - Die Rotorenstellung zueinander: $26 \cdot 25 \cdot 26 = 16\,900$ Walzenstellungen
  - Steckerverbindungen: bis zu 13 Verbindungen bei 26 Buchsen (10 wurden de facto verwendet) machen nochmal 150 738 274 937 250 Möglichkeiten.

- Selbst heute mit *brute force* kaum zu machen.
- Aber: In Wirklichkeit kleinerer Raum den man durchsuchen musste, nur ca. 1 Million Möglichkeiten (Im wesentlichen sind es nur nur Rotoren und die Walzenstellungen, da Rest fix bleibt).
- Eigentliche Schwäche ist Umkehrwalze!

Wie gut ist die Verschlüsselung?

- Schlüsselraum setzt sich aus 4 Teilen zusammen:
  - Lage der Rotoren: (3 aus 5) macht 60 Möglichkeiten
  - Ringstellungen: 01 bis 26 bei zwei relevanten Ringen macht $26^2 = 676$ Möglichkeiten
  - Die Rotorenstellung zueinander: $26 \cdot 25 \cdot 26 = 16\,900$ Walzenstellungen
  - Steckerverbindungen: bis zu 13 Verbindungen bei 26 Buchsen (10 wurden de facto verwendet) machen nochmal $150\,738\,274\,937\,250$ Möglichkeiten.

  Das sind dann etwa 10^{23} Möglichkeiten, also etwa 76 bit.
- Selbst heute mit *brute force* kaum zu machen.
- Aber: In Wirklichkeit kleinerer Raum den man durchsuchen musste, nur ca. 1 Million Möglichkeiten (Im wesentlichen sind es nur nur Rotoren und die Walzenstellungen, da Rest fix bleibt).
- Eigentliche Schwäche ist Umkehrwalze!

Knacken des Codes: Schwäche Umkehrwalze

Umkehrwalze erzeugt nur selbstinverse fixpunktfreie Permutationen.

Beispiel:

ABCD	ABDC	ACBD	ACDB	ADBC	ADCB
BACD	BADC	BCAD	BCDA	BDAC	BDCA
CABD	CADB	CBAD	CBDA	CDAB	CDBA
DABC	DACB	DBAC	DBCA	DCAB	DCBA

- Von den $4! = 24$ Permutationen, der 4 Buchstaben A, B, C und D sind nur 9 fixpunktfrei, und davon sind nur 3 selbstinvers.
- Nur diese kommen in der Enigma vor, da man nicht nur z.B. von A zu C chiffriert, sondern auch von C wieder zu A dechiffrieren muss!
  $\Longrightarrow$ Deutliche Reduktion der möglichen Permutationen von etwa $4 \cdot 10^{26}$ auf nur $5 \cdot 10^{13}$.
- Noch schlimmer: Fixpunktfreiheit hilft bei der suche nach Wörtern (siehe nächste Folie).

```
  BHNCXSEQKOBIIODWFBTZGCYEHQQJEWOYNBDXHQBALHTSSDPWGW
1 OBERKOMMANDODERWEHRMACHT
 2 OBERKOMMANDODERWEHRMACHT
  3 OBERKOMMANDODERWEHRMACHT
   4 OBERKOMMANDODERWEHRMACHT
    5 OBERKOMMANDODERWEHRMACHT
     6 OBERKOMMANDODERWEHRMACHT
      7 OBERKOMMANDODERWEHRMACHT
       8 OBERKOMMANDODERWEHRMACHT
        9 OBERKOMMANDODERWEHRMACHT
        10 OBERKOMMANDODERWEHRMACHT
         11 OBERKOMMANDODERWEHRMACHT
          12 OBERKOMMANDODERWEHRMACHT
           13 OBERKOMMANDODERWEHRMACHT
            14 OBERKOMMANDODERWEHRMACHT
             15 OBERKOMMANDODERWEHRMACHT
              16 OBERKOMMANDODERWEHRMACHT
               17 OBERKOMMANDODERWEHRMACHT
                18 OBERKOMMANDODERWEHRMACHT
                 19 OBERKOMMANDODERWEHRMACHT
                  20 OBERKOMMANDODERWEHRMACHT
                   21 OBERKOMMANDODERWEHRMACHT
                    22 OBERKOMMANDODERWEHRMACHT
                     23 OBERKOMMANDODERWEHRMACHT
                      24 OBERKOMMANDODERWEHRMACHT
                       25 OBERKOMMANDODERWEHRMACHT
                        26 OBERKOMMANDODERWEHRMACHT
                         27 OBERKOMMANDODERWEHRMACHT
  BHNCXSEQKOBIIODWFBTZGCYEHQQJEWOYNBDXHQBALHTSSDPWGW
```

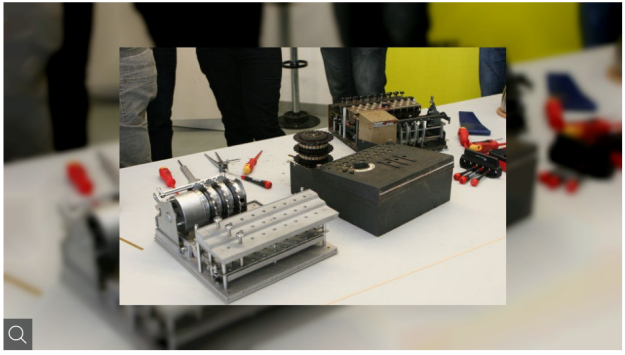
- Beim Suchen nach bestimmten Wörtern oder Satzteilen (solche, die wahrscheinlich sind und häufig vorkommen) können die Möglichkeiten ausgeschlossen werden bei denen Buchstanben übereinstimmen.
- Im Beispiel links sind das die roten Buchstaben.
- Von den 27 Möglichkeiten bleiben im linken Beispiel nur 8 übrig.

Anekdote

- Professor Dr. Wolfgang Ertel Informatiker / Kryptologie der Hochschule Ravensburg-Weingarten hat mit Studenten in einem Projekt die Enigma nachgebaut.
- Das war der lokalen Presse ein Artikel wert, die daraufhin titelte:

Studenten bauen deutsche Kriegs-Maschine nach

LESEDAUER: 7 MIN



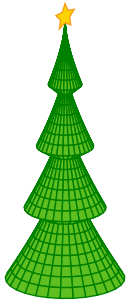
Alt und neu: Rechts eine historische Enigma, links der Nachbau, der jedoch noch nicht ganz fertig ist.

(Schwäbische / Weingarten am 03.05.2010)

Videos:

- Wie knackt man die Enigma?
  - How Enigma works (Numberphile):
    `https://www.youtube.com/watch?v=G2_Q9FoD-oQ`
  - Flaw in the Enigma Code (Numberphile):
    `https://www.youtube.com/watch?v=V4V2bpZlqx8`
  - Video zur Enigma: (Algorithmen Verstehen)
    `https://www.youtube.com/watch?v=GQCD0xV6IzQ`
  - Filmtipp: *The Imitation Game*
- Welches Toilettenhäuschen benutzt man bei einem Festivalbesuch?
  - Mathematical Way to Choose a Toilet (Numberphile):
    `https://www.youtube.com/watch?v=ZWib5olGbQ0`
- Wievele Menschen muss man daten um den Partner fürs Leben zu finden?
  - Hannah Fry - The Mathematics of Love (TEDx):
    `https://www.youtube.com/watch?v=yFVXsjVdvmY`

Danke für Ihre Aufmerksamkeit



... und Frohes Fest