Einführung Decentralized Security

Prof. Dr. Hagen Lauer

Agenda

- Einführung Decentralized Security
- Kryptografie für dezentralisierte Sicherheit
- Distributed Ledger Technologies
- Dezentrale Authentifizierung und Zugriffskontrolle
- Dezentrale Sicherheit in der Praxis
- Ausblick
- Zusammenfassung

Centralized Systems

Alle Nutzer sind an zentralen „Knoten“ angebunden, mit zahlreichen Vorteilen:

Entscheidungsprozesse

Verfügbarkeit

Verwaltung

Standardisierung

Skaleneffekte

https://www.fz-juelich.de/en/news/archive/press-release/2022/first-european-exascale-supercomputer-coming-to-julich

Centralized Systems - Pro

Alle Nutzer sind an zentralen „Knoten“ angebunden, mit zahlreichen Vorteilen:

Überwachung

Koordination

Sicherheitsstandards und Richtlinien

Security Management

Skaleneffekte

https://www.fz-juelich.de/en/news/archive/press-release/2022/first-european-exascale-supercomputer-coming-to-julich

Centralized Systems - Kontra

Alle Nutzer sind an zentralen „Knoten“ angebunden, mit zahlreichen Nachteilen:

Single Point of Failure (SPOF)

Vertrauen u. Datenschutz

Kommunikation

Skalierbarkeit

„Perimetersicherheit“

https://www.fz-juelich.de/en/news/archive/press-release/2022/first-european-exascale-supercomputer-coming-to-julich

Zentrale und zentralisierte Systeme/Anwendungen

Recherchieren Sie ca. 10 Minuten:

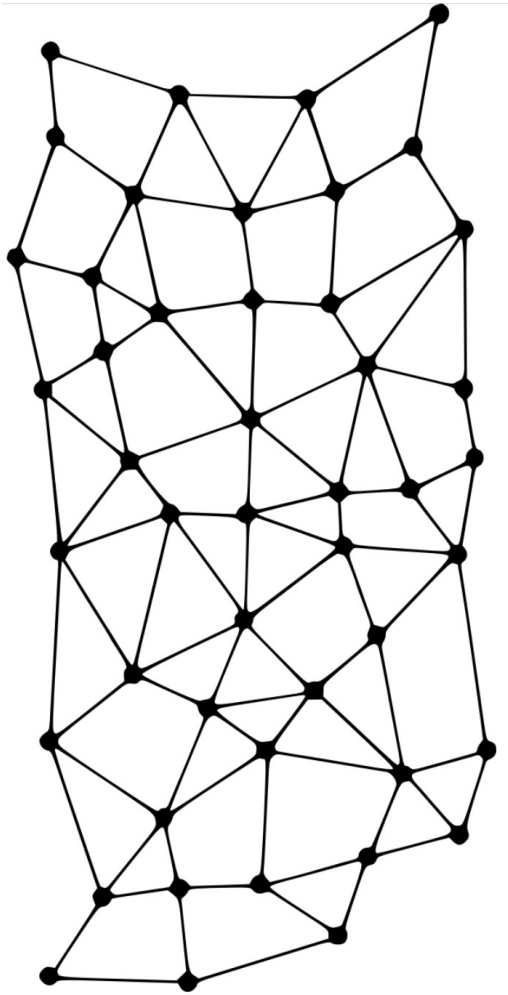
Betrachten Sie besonders die **Anreize** zum Betrieb im zentralisierten Modus.

Geben sie ggf. bekannte Nachteile des zentralen Betriebs an.

Gibt es Hürden, die ein anderes Modell untersagen?

Verteilte Systeme – Distributed Systems

- **Unabhängige** Knoten (typischerweise Computer), die zu einem bestimmten Zweck zusammenarbeiten
- Kommunikation über verschiedene **Kanäle** (channels)
  - Lokale Netzwerke, Drahtlosnetze, Internet
- Topologie:
  - „Architektur“ des Systems bestehend aus Knoten und Verbindungen
  - “Veritces and Edges“ $G = (V, E)$, zu Deutsch *Knoten* und *Kanten*
    - V beschreibt eine *Menge* von *Knoten* (Vertex, Vertices)
    - E beschreibt Kanten in der Form $\{x, y\} \in E$, mit x und $y \in V$ (Knoten)
    - *Hypergraphen* und *Hyperkanten*



DISTRIBUTED
(C)

Verteilte Systeme – Distributed Systems - Pro

Unabhängige Knoten (typischerweise Computer), die zu einem bestimmten Zweck zusammenarbeiten.

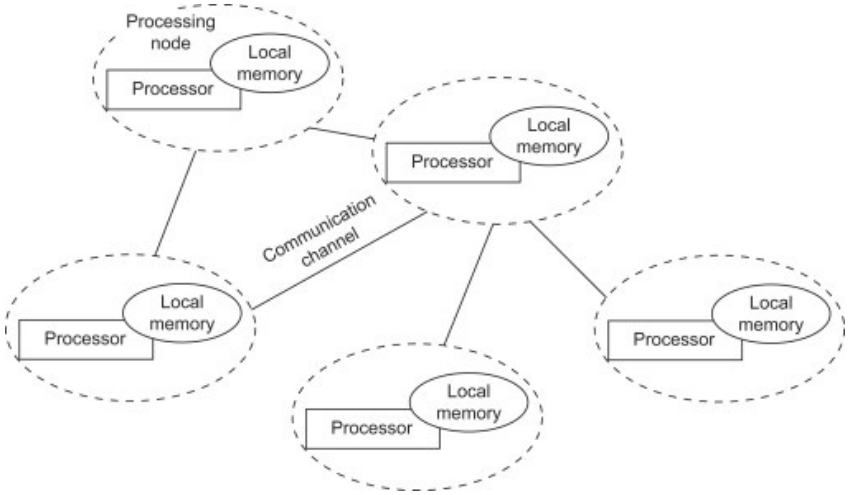
Betrachten Sie folgende Szenarien:

I. “link destruction“ (Kante(n) wird/werden entfernt)

II. „node destruction“ (Knoten wird/werden entfernt)

Welchen Effekt haben die o.g. Szenarien in einem verteilten System?

Welchen Effekt haben die o.g. Szenarien in einem zentralisierten System?

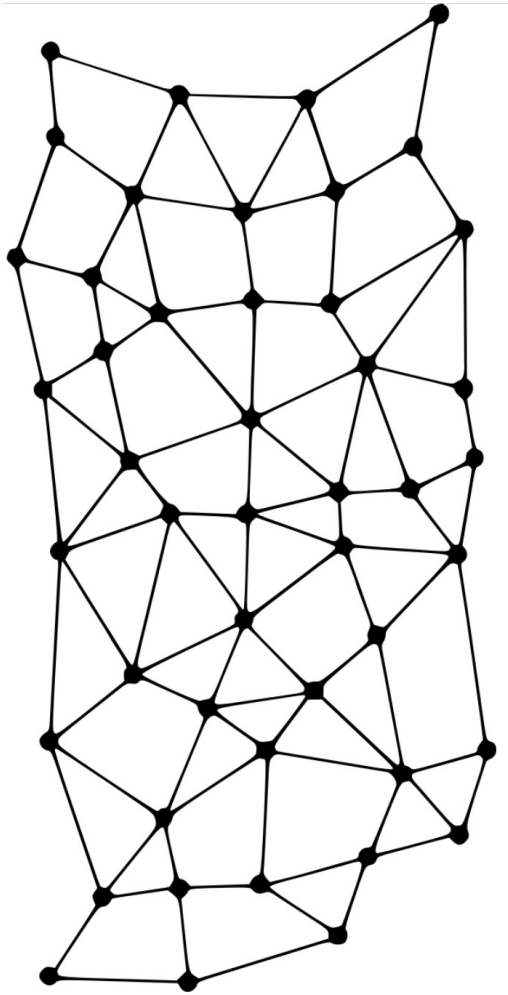


Source: ToDo. Sorry, future me.

Verteilte Systeme – Distributed Systems - Kontra

Unabhängige Knoten (typischerweise Computer), die zu einem bestimmten Zweck zusammenarbeiten.

- Komplexität
- Sicherheit & Vertrauenswürdigkeit […]
- Konsistenz
  - Unterschiedliche Versionen von Daten
- Latenz
- Management u. Kontrolle



DISTRIBUTED
(C)

Verteilte Systeme / Anwendungen

Recherchieren Sie ca. 10 Minuten:

Betrachten Sie besonders die **Anreize** zum Betrieb im verteilten Modus.

Geben sie ggf. bekannte Nachteile des verteilten Betriebs an.

Gibt es Hürden, die ein anderes Modell untersagen?

Dezentrale Systeme

Begriff populär durch *Rummel* um Bitcoin

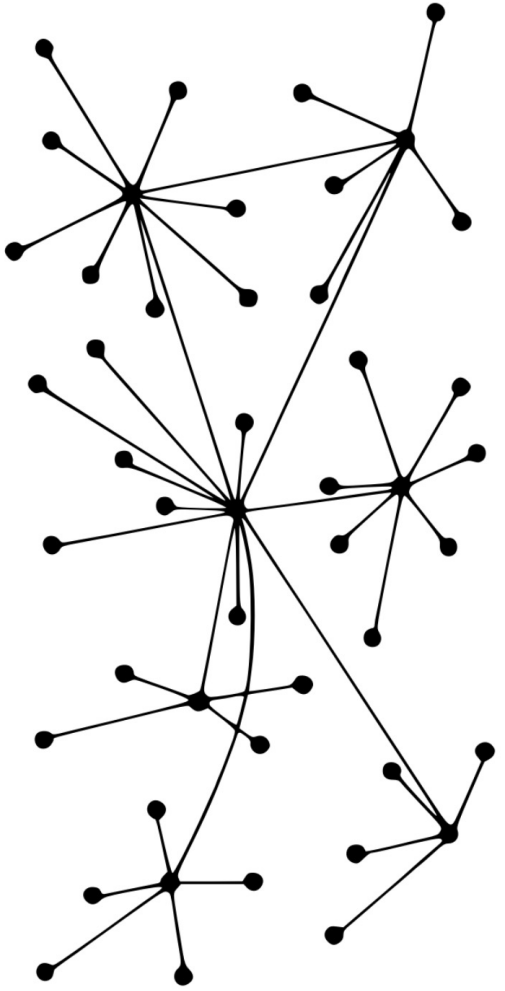
- Dezentrale Systeme sind **Untermenge** und **Teilgebiet** der verteilten Systeme
- Relevant ist die Idee: Weg von zentralisierten Systemen in gewissen Aspekten – *Security, Trust, Control, …*

Jeder Knoten (*i.e., Computer*) ist unabhängig

Keine *einzelne* Steuereinheit (Erinnerung an „Clocks“)

Mehrere „zentrale“ Einheiten (Nodes, mehrere Sever)

Nur *teilweise* fehlertolerant bei Ausfall bestimmter Knoten und Server



DECENTRALIZED
(B)

Dezentrale Systeme - Pro

Begriff populär durch *Rummel* um Bitcoin

- Dezentrale Systeme sind **Untermenge** und **Teilgebiet** der verteilten Systeme
- Relevant ist die Idee: Weg von zentralisierten Systemen in gewissen Aspekten – *Security, Trust, Control, …*

Skalierbarkeit (vertikal und horizontal)

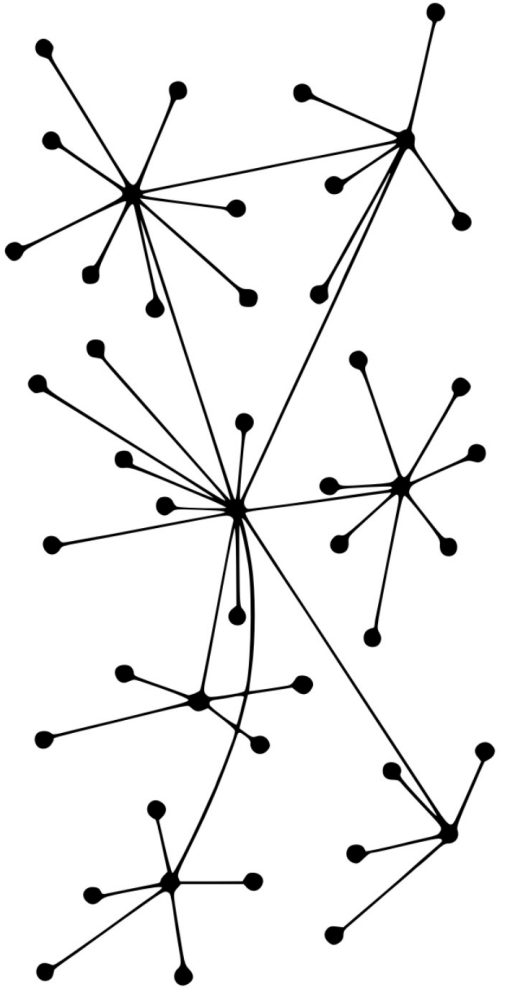
Resilienz, Fehlertoleranz, Flexibilität

Performanz u. Effizienz

Transparenz

Räumliche Verteilung

Können sicherer sein



DECENTRALIZED
(B)

Dezentrale Systeme - Kontra

Begriff populär durch *Rummel* um Bitcoin

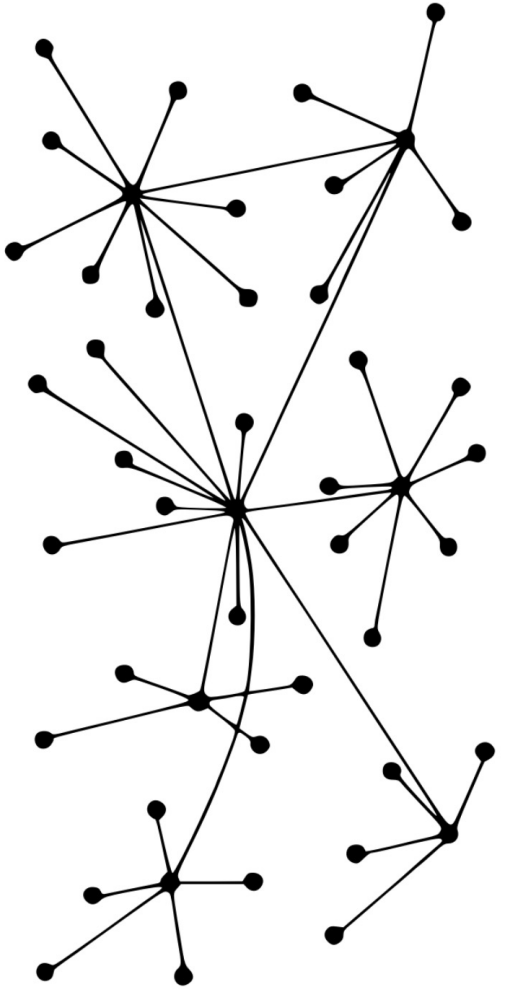
- Dezentrale Systeme sind **Untermenge** und **Teilgebiet** der verteilten Systeme
- Relevant ist die Idee: Weg von zentralisierten Systemen in gewissen Aspekten – *Security, Trust, Control, …*

Komplexität

Entscheidungsprozesse

Vertraulichkeit und Privatsphäre

Management, Konsistenz, Enforcement



DECENTRALIZED
(B)

Dezentrale Systeme / Anwendungen

Recherchieren Sie ca. 10 Minuten:

Betrachten Sie besonders die **Anreize** zum Betrieb im verteilten Modus.

Geben sie ggf. bekannte Nachteile des verteilten Betriebs an.

Gibt es Hürden, die ein anderes Modell untersagen?

Zentralisiert / Dezentralisiert / Verteilt

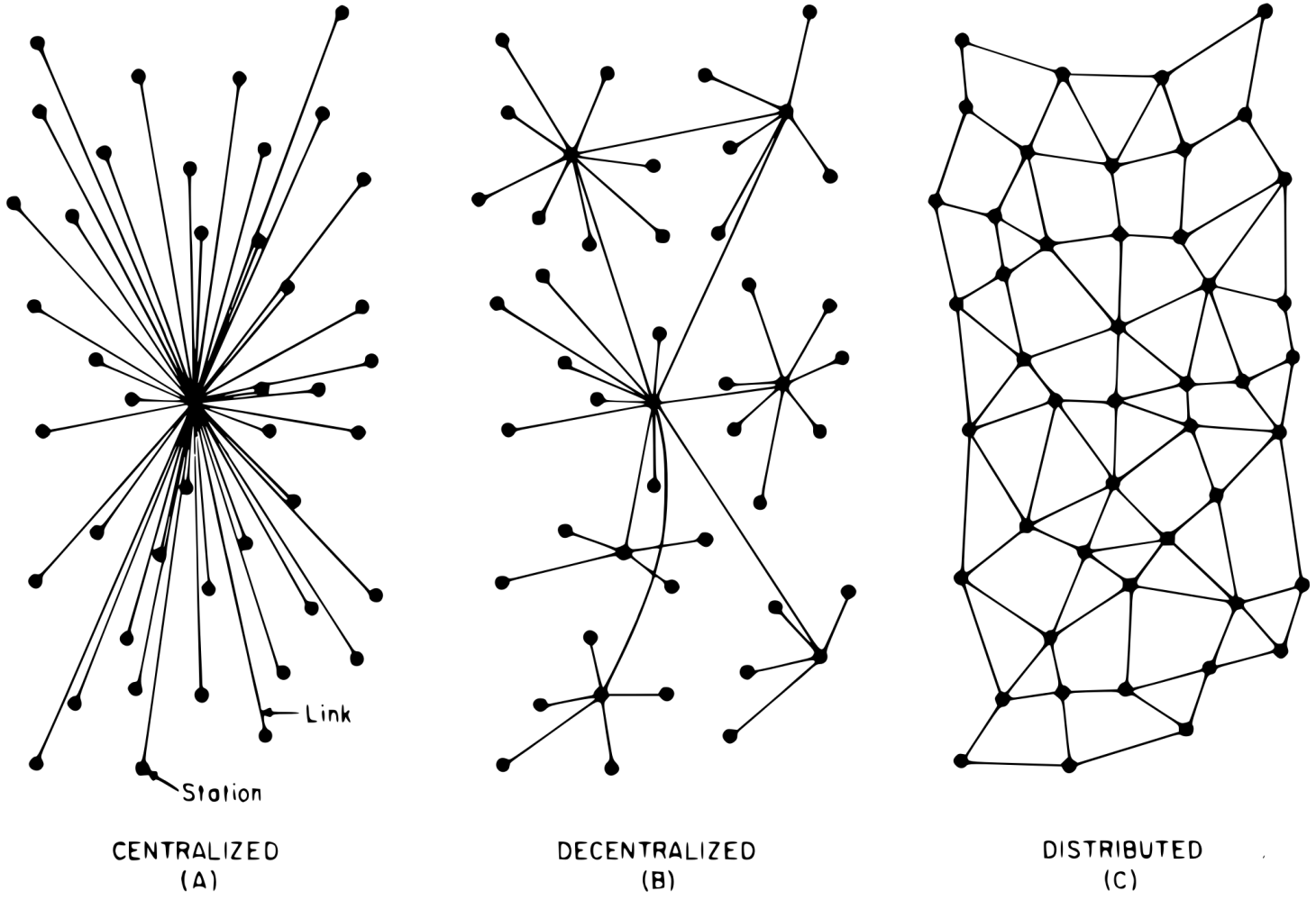


FIG. 1 — Centralized, Decentralized and Distributed Networks

Baran, P. (1964). On Distributed Communications, Memorandum RM-3420-PR. (Link)

Top 5 Anwendungen – Zentrale Systeme

- Bankenwesen
- Verkauf und Vertrieb
- Social Media
- Transport und Logistik
- Gesundheitswesen

(Governance)

(Bildung)

Top 5 Anwendungen – Verteilte Systeme

- Cloud / Edge - Computing
- Content-Delivery, File Sharing und Streaming
- Verteilte Datenbanken
- Internet-of-Things
- Seit 2010: Blockchain(s) für alles Mögliche

Top 5 Anwendungen – Dezentrale Systeme

- Kryptowährungen
- File-Sharing
- Soziale Netzwerke (e.g. Mastodon, Diaspora)
- Supply Chain Integrity, Transparency and Trust (e.g. SBOM, IETF RFC SCITT)
- Identity Management

EWD117 – Trust & Quality of Results

University of Texas at Austin

Edsger W Dijkstra: Programming Considered as a Human Activity

https://www.cs.utexas.edu/~EWD/transcriptions/EWD01xx/EWD117.html

E. Dijkstra. 1979. Programming considered as a human activity. Classics in software engineering. Yourdon Press, USA, 1–9.

Q: Welche Aufgaben ergeben sich für „Security“ im Kontext verteilter Systeme?

Abschluss VL - 28.04.

- Seminar:
  - Erarbeiten von Review Folien
  - Selektion von Paper für Anwendungen/Security verteilter und dezentraler Systeme
  - Fokus auf „bahnbrechende“ Papiere
- Nächste Woche:
  - Erster Versuch ***Reading Group***

Kryptografie für Dezentrale Sicherheit

Kryptographie

Dictionary

Definitions from Oxford Languages · Learn more

cryptography

noun

noun: **cryptography**

the art of writing or solving codes.

Use over time for: cryptography

See translations in 100+ languages

Translate to German

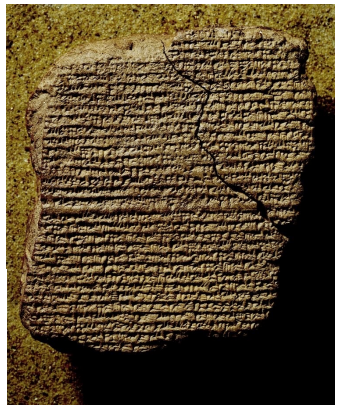
noun

1. Geheimschrift

See more →

Geschichte der Kryptografie (Antike)

- Antike:
  - Skytala („Stock“) Chiffre der Spartaner
  - Hieroglyphen in Grabkammern von Pyramiden (1900 v.Chr.)
  - Mesopotamische Tontafeln, die z.B. Rezepte enthielten (1500 v.Chr.)
  - Verschlüsselung des hebräischen Alphabets Atbash Chiffre (600 v.Chr)
  - Polybius Chiffre

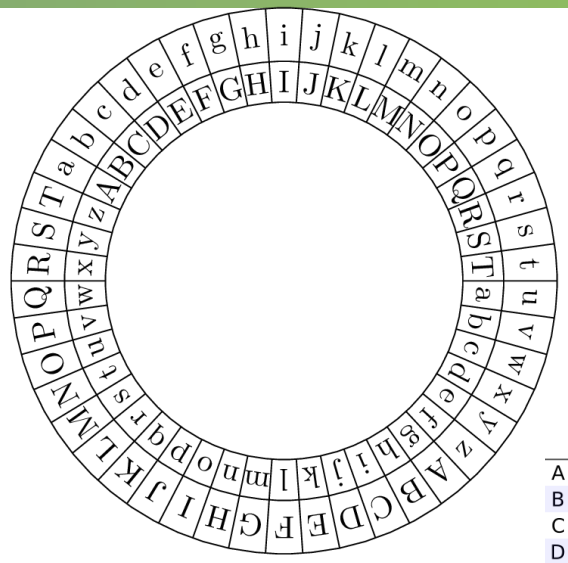


	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Source: Wikipedia – Polybius square

Geschichte der Kryptografie (Mittelalter)

- Al-Khalil (ca. 750) „Book of Cryptographic Messages“ - Permutationen
- Ahmad al-Qalqashandi (ca. 1400) – ***homophonische*** Substitution und Transposition
- Leon Battista Alberti (ca. 1467) „Vater der westlichen Kryptografie“ – polyalphabetische Substitution
- Vigenère Chiffre, von Giovan Battista Bellaso (1553) brachte *praktisches* System (bis 1863!)



Wikipedia: Cäsar Chiffre

Wikipedia: Vigenère Chiffre

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

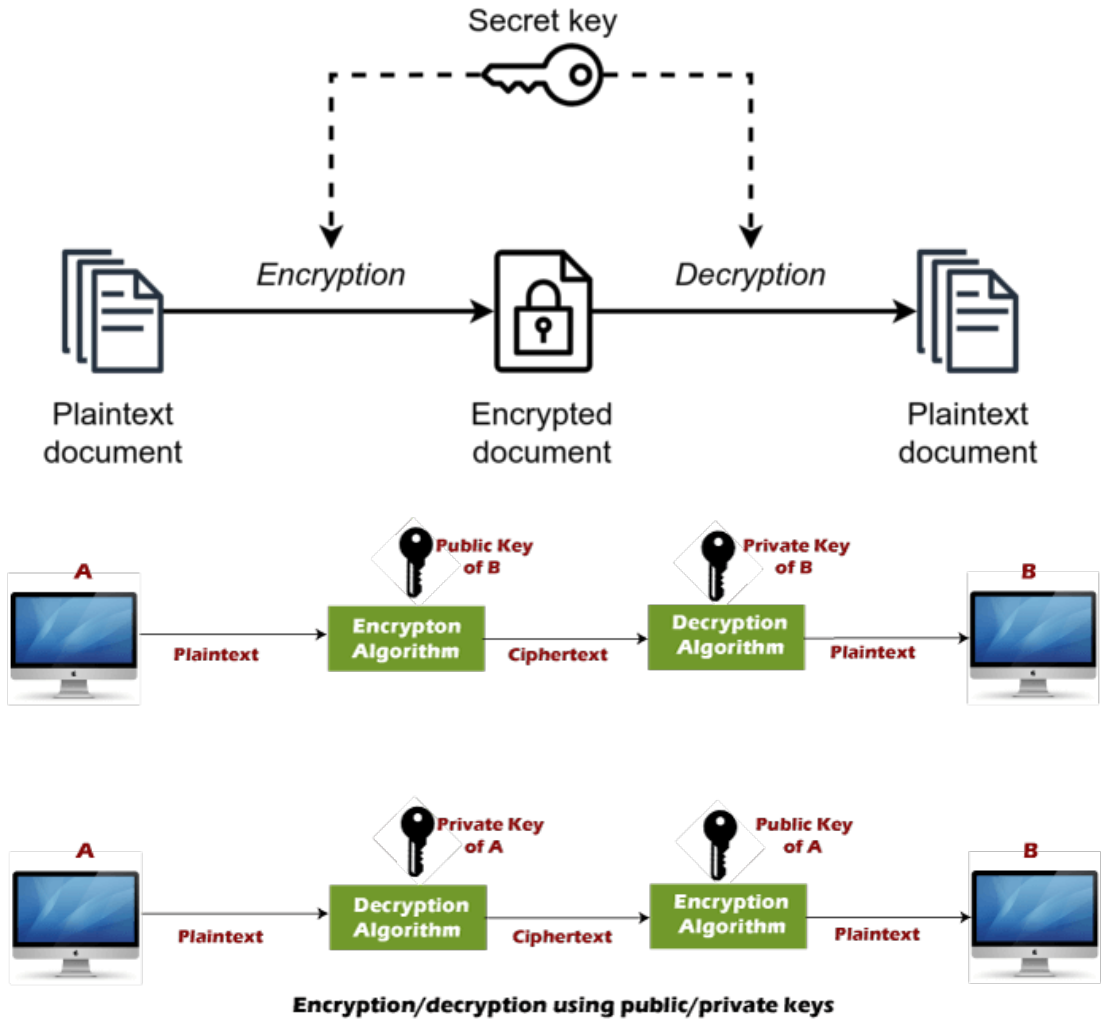
Geschichte der Kryptografie (Neuzeit)

- One Time Pad, Frank Miller 1882, Gilbert Vernam, 1917 (U.S. Pat.)
- Enigma-Apparat von Arthur Scherbius (ca. 1920) beruhte auf „Spruchschlüsseln“ für jede Nachricht aus „Schlüsseltafeln“
- Teilweise gebrochen 1932 durch Marian Rejewski
- Bletchley Park und „Ultra“ nutzen Erkenntnisse über Funktion, kryptografische Schwächen und gefundene Schlüsseltafeln gegen Enigma

A	B	XOR
0	0	0
0	1	1
1	0	1
1	1	0

Moderne Kryptografie

- Moderne symmetrische Chiffren von DES, 3DES, bis zu AES (1975 – heute)
- Public-Key, bzw. asymmetrische, Chiffren (RSA, 1977*)
  - ***Verschiedene Schlüssel zur Ver- und Entschlüsselung***
- Kryptografische Prüfsummen, aka. Hashes, Hashfunktionen oder „Digests“ (1979 - heute)
  - Rabin, Yuval, Merkle*
    - Definition: Birthday Paradox, Collision Resistance, Second Preimage Resistance, Preimage Resistance



https://www.esat.kuleuven.be/cosic/publications/article-1532.pdf

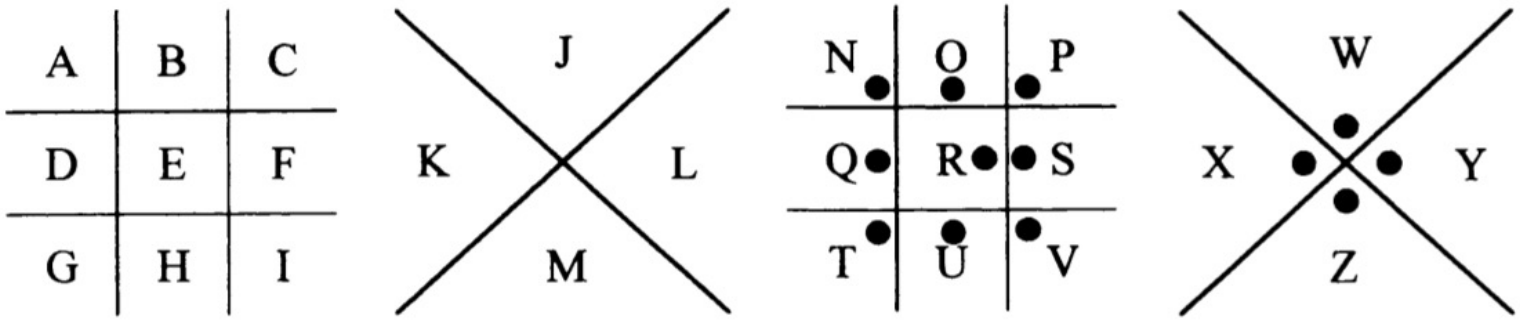
Begriffe

- Kryptologie: Geheimhaltung von Informationen durch Veränderung der Daten
- Kryptografie: Wissenschaft des Ver- und Entschlüsselns von Daten
- Kryptoanalysis: Entschlüsselung, Gewinnung des Schlüssels, Gewinnung von Informationen, Brechen oder Verbessern von Systemen

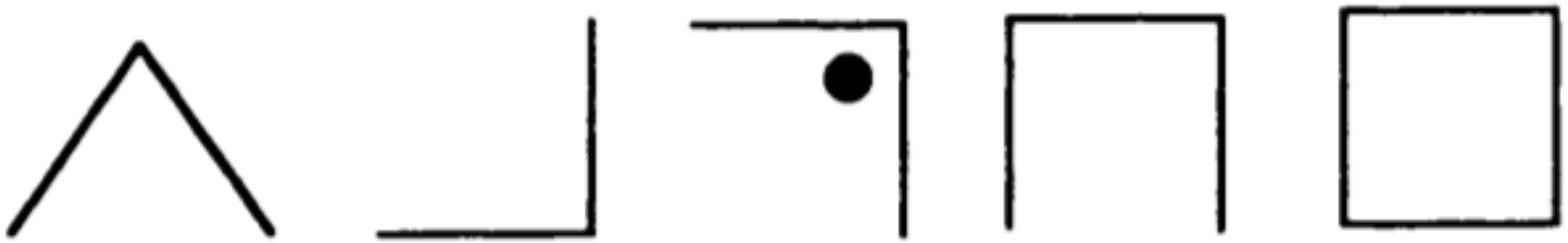
Begriffe

- **Chiffre** (cipher): System oder Verfahren zur Transformation von Daten
- **Schlüssel** (key): Element für einzigartige* und eindeutige* Abbildung von Klartext (plain text) zu Chiffretext (ciphertext)
- **Verschlüsseln** oder chiffrieren (encipher, encrypt): „Lesbare“ in „unlesbare“ Daten transformieren
- **Entschlüsseln** oder dechiffrieren (decyper, decrypt): „Unlesbare“ in „lesbare“ Daten transformieren
- **Brechen**: Chiffre wird „entziffert“ durch Angreifer oder Kryptoanalyst

Freimaurer Chiffre



- Verschlüsselung von MATHE ergibt:

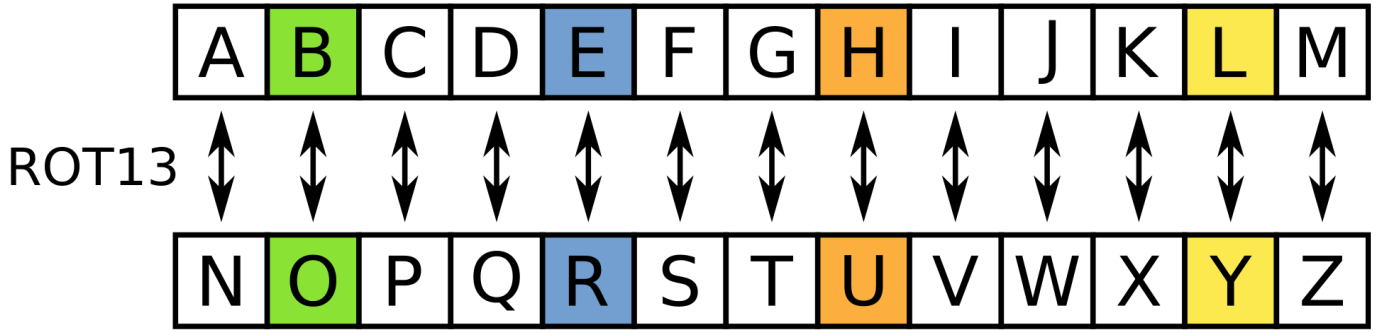


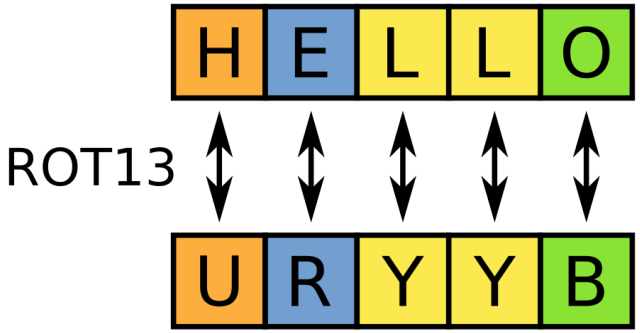
Beispiel ROT13

Caesar Chiffre mit festem „k“=13

- Willkommen:
  - Jvyxxbzzra
  - Jvyyxbzzra
  - Jvyyxbbzra

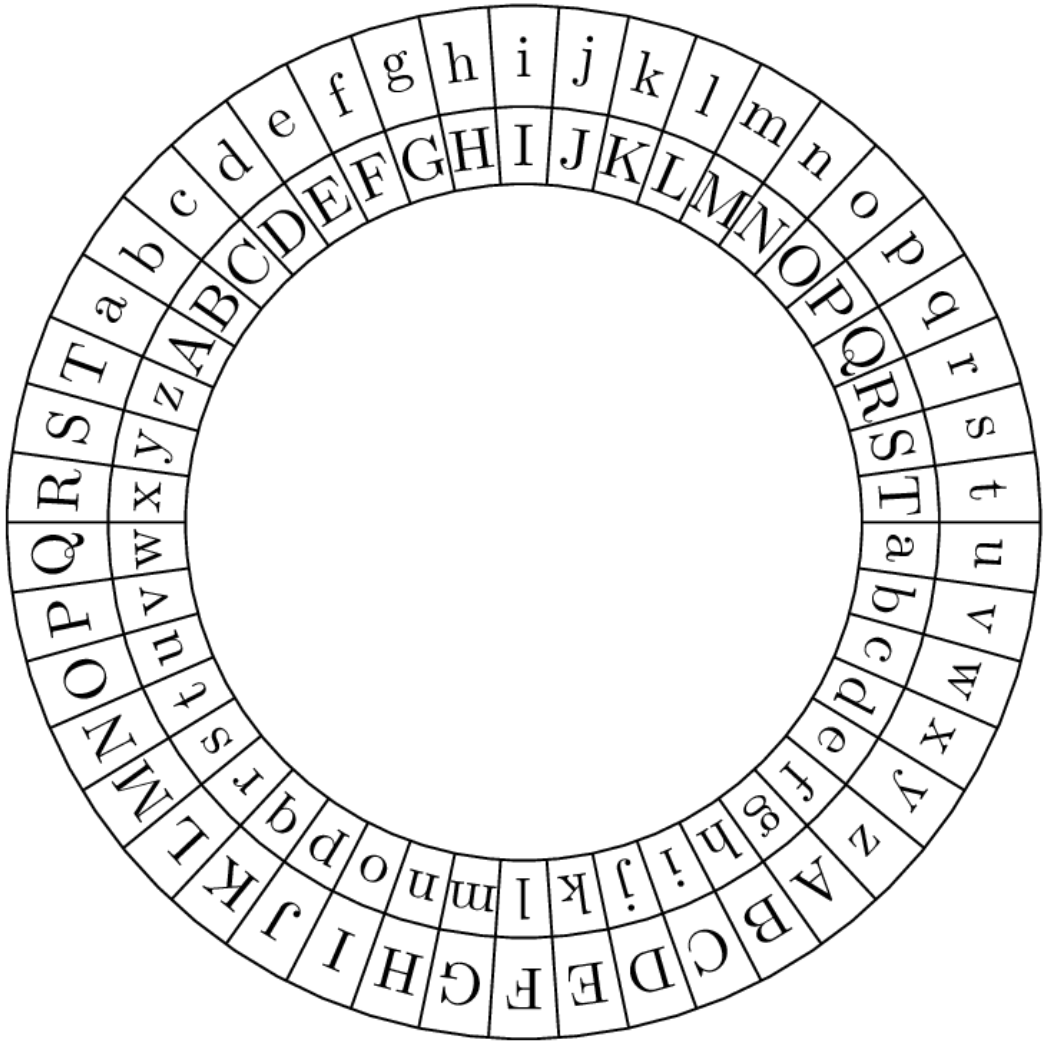
Was muss hier die richtige Verschlüsselung sein?





Caesar mit Schlüsseln

- Wie viele Schlüssel gibt es?
- Wie würden Sie die Chiffre „brechen“?
- Wie könnte das System verbessert werden?

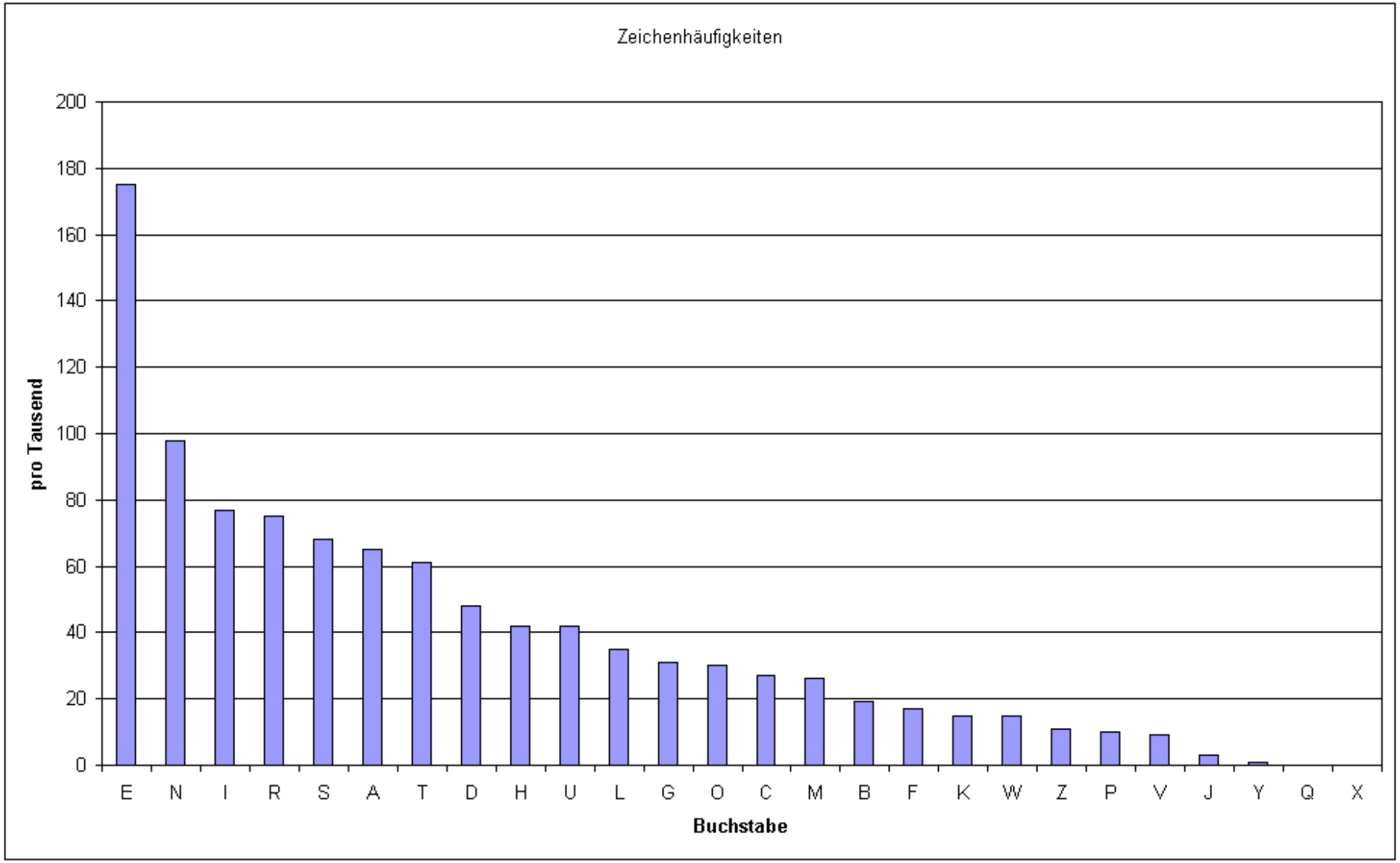


Verbesserte Caesar Chiffre

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

- Permutationen:
  - 26! = 403 291 461 126605 635 584000 000
- Wie würden Sie die modifizierte Caesar Chiffre brechen?

Buchstabenhäufigkeit – Letter Frequency



Kryptoanalyse: Wie sicher ist das Verfahren?

- 26! ?

- Recherchieren Sie, wie man die Stärke von kryptographischen Verfahren bestimmt.

Vigenère

Schlüsselwort:	D	A	C	H	D	A	C	H	D	A	C	H	D	A	C	H										
Klartext:	P	O	L	Y	A	L	P	H	A	B	E	T	I	S	C	H										
Geheimtext:	S	O	N	F	D	L	R	O	D	B	G	A	L	S	E	O										

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

Ihre Präsentationen

- Ziel (u.a.) Sammlung an wichtigen Kryptographischen Primitiven

Relevante Konzepte

- Symmetrische Verschlüsselung
- Asymmetrische Verschlüsselung
- Digitale Signaturen
- Hash-Funktionen