Versteckte Botschaften für schlaue Biber

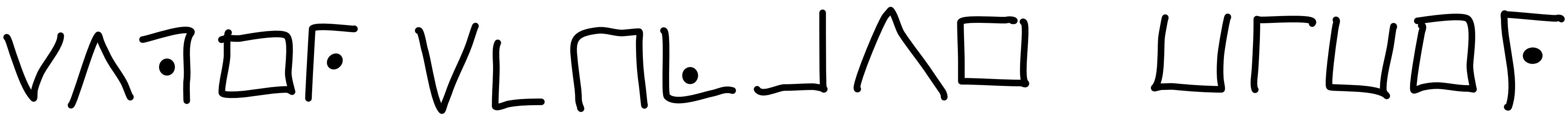
STIU-Workshop am 21. Juni 2023

Herzlich Willkommen!

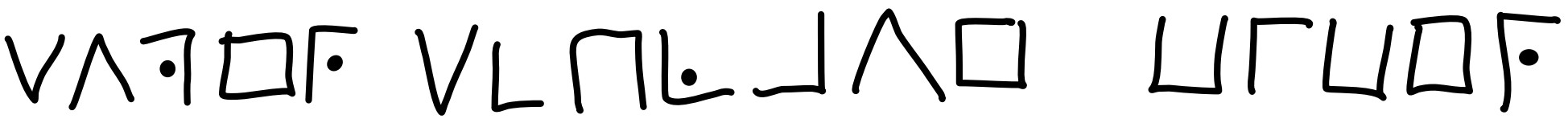
von Susanne Datzko-Thut und Nora Anna Escherle

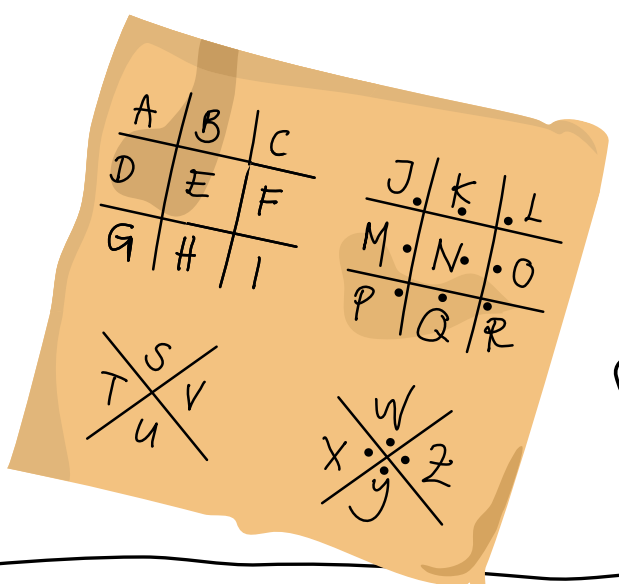
Informatikbiber-Wettbewerb Schweiz

Geheime Botschaft!



Geheime Botschaft!





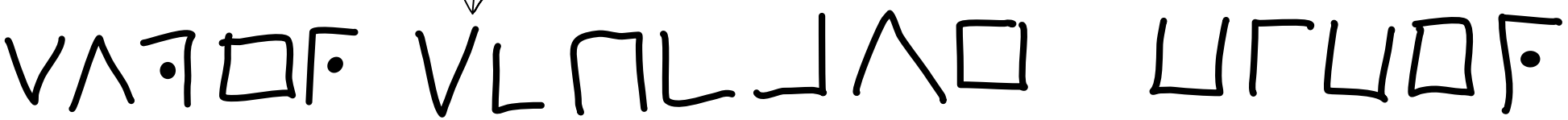
Lösung:

SUPER SCHLAUE BIBER

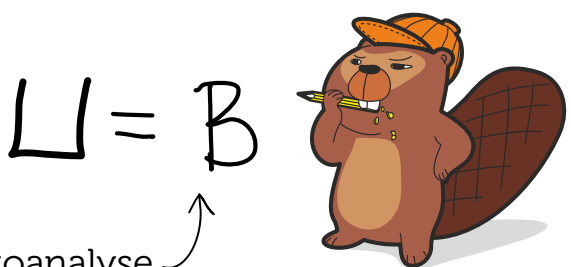
Begriffe - Kryptographie

altgriechisch für «Verborgen»

(verschlüsselter) Geheimtext

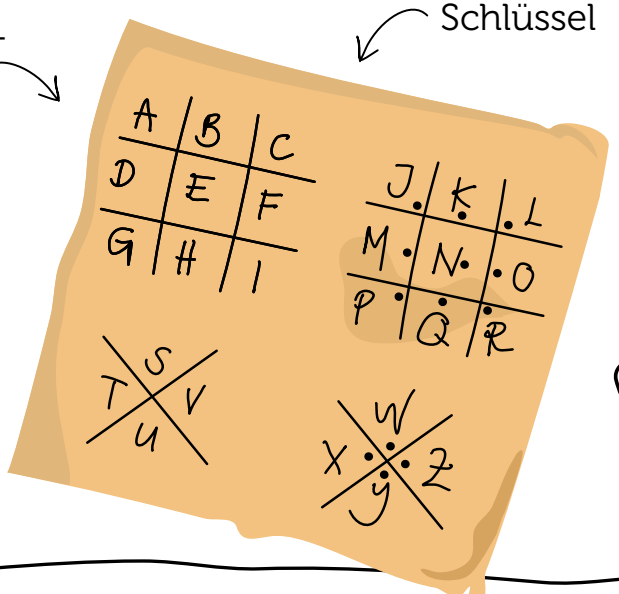


Kryptoanalyse



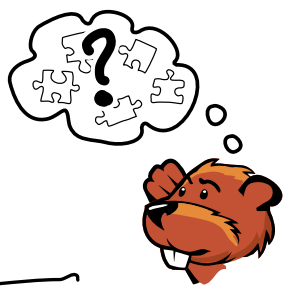
Freimaurer-Alphabet

Schlüssel

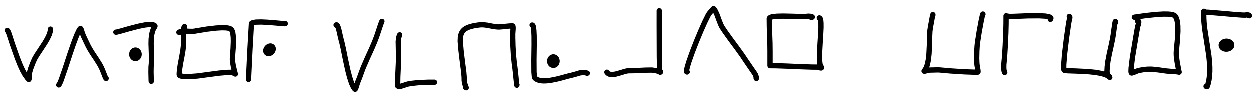


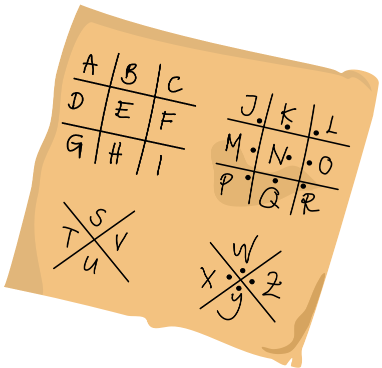
SUPER SCHLAUE BIBER

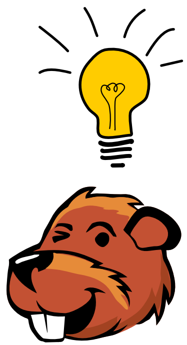
(entschlüsselter) Klartext



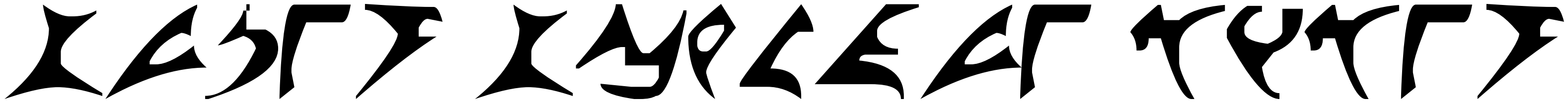
Begriffe - Kryptographie

- Klartext: **SUPER SCHLAUE BIBER**
- Geheimtext: 
- "geheimer" Schlüssel:
  Buchstaben und geometrische Formen
- "geheimes Verfahren":
  Buchstaben leiten sich aus den geometrischen Formen ab.





Noch ein Geheimtext?



Noch ein Geheimtext?

klingonische Schrift

Klingonische Zeichentabelle

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

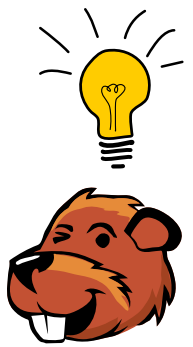
Unterschied zwischen Codierung und Verschlüsselung

Codierung

- “öffentliche” Zeichentabelle
- jeder Buchstabe hat eine genaue Zuordnung zu einem anderen Zeichen

Verschlüsselung

- “geheimer” Schlüssel
- Klartext oder Geheimschrift wird durch ein “geheimes” Verfahren verändert

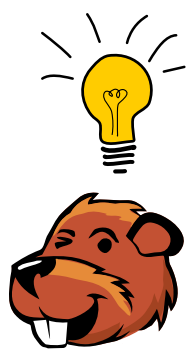


Monoalphabetische Substitution festes Schlüsselalphabet

- Freimaurer-Alphabet
  → Monoalphabetische Substitution
- für jeden Buchstaben ein einziges Zeichen
- nicht sicheres Verschlüsselungsverfahren, weil Buchstaben sind unterschiedlich häufig:
  Sieben super schlaue Biber stauen mit ihrem Biberbau, den Fluss so dass ein tiefer See entsteht.
  → einfach zum Entschlüsseln

Weiterentwicklung der Verschlüsselung

- polyalphabetische Verschlüsselungsverfahren:
  → jeder Buchstabe einen anderen Schlüssel
- Rotormaschinen:
  mechanische Verschlüsselungsmaschinen (z.B. Enigma)
- symmetrische Verschlüsselungsverfahren:
  Wörter/Blöcke von Zeichnen in mehreren Runden verändern (z.B. Buchstaben verschieben, umdrehen)
  – gleiche Schlüssel für Ver- und Entschlüsseln
- asymmetrische Verschlüsselungsverfahren:
  – je ein Schlüssel zum Ver- und Entschlüsseln, die Schlüssel hängen mathematisch zusammen.



Dein Plakat

Inhalt:

- Geheimtext (Überschrift: “super schlaue Biber”)
- Schlüssel
- Verschlüsselungsverfahren
- weitere Aufgaben*
- interessante Facts*

Quellenverzeichnis/Links

Weiterführende Links

- Informatik-Biber Schweiz: https://www.informatik-biber.ch/, https://wettbewerb.informatik-biber.ch/
- CrypTool: https://www.cryptool.org/