2 Laufzeitaufwand und Entschlüsselung

Simon Singh: Geheime Botschaften

- Passwort knacken
  Brute-Force-Methode
  4 Stellen (26 Zeichen): 456976 Möglichkeiten
  leistungsstarker PC: 1 Milliarde Angriffe pro Minute
  geknackt in ca. 0,5 ms
  Profis: ca. 2 Billionen sekündlich
  8 Stellen (96 Zeichen): $7{,}2 \cdot 10^{15}$ Möglichkeiten
  geknackt in ca. 42 Tagen
  Aber:
  Passwortknacker verwenden Wörterlisten mit häufigen Passwörtern.
  Oder: Umgekehrter Angriff
  Checke, welcher Benutzer das Passwort 12345 hat.

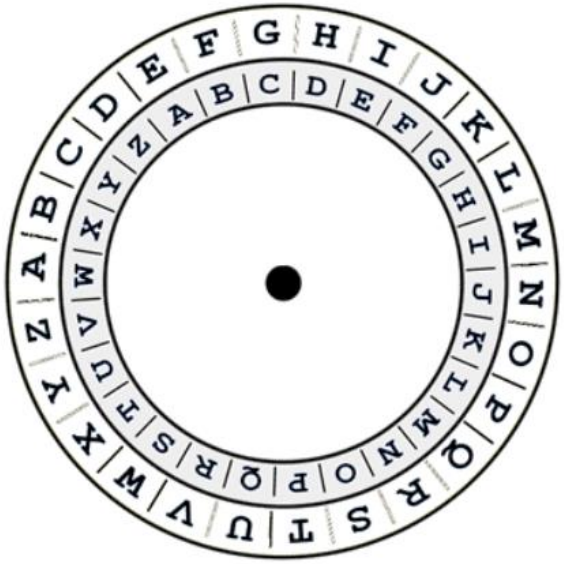
- Skytale:
  Papierstreifen wird auf Stab mit bestimmtem Durchmesser gewickelt und beschrieben. Nebeneinander liegende Zeichen sind in der verschlüsselten Botschaft um eine bestimmte Anzahl von Zeichen verschoben.
  Schlüssel: Stab

(Könnt ihr auch selber machen:
dünnen Papierstreifen um Stift wickeln, leicht versetzt, so dass Papier einlagig nebeneinander, dann zeilenweise beschreiben und wieder abwickeln.)

Text (ungefähr) um Stabilo gewickelt:

HIER GEHT ES LOS BIN GESPANNT OB ES NACH
KOPIEREN ZU LESEN IST KW

- **Caesar-Verschlüsselung**
  A → W
  INFORMATIK → EJBKNIWPEG
  26 Schlüssel möglich



  Variante:
  beliebige Permutationen des Alphabets zulassen
  $26! \approx 4 \cdot 10^{26}$ Schlüssel

  Monoalphabetische Verschlüsselung:
  Jedes Zeichen wird durch ein bestimmtes Geheimzeichen verschlüsselt
  → Häufigkeitsanalyse

- **Vigenère-Verschlüsselung**
  Polyalphabetische Verschlüsselung
  S. 138/3 a)
  VG RYKH YXA ZNZ YXA GOPKS GJO
  Häufigkeitsanalyse führt nicht zum Ziel.