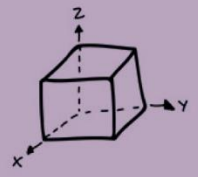
ALPEN-ADRIA UNIVERSITÄT
FAKULTÄT FÜR TECHNISCHE WISSENSCHAFTEN

Herzlich Willkommen zum

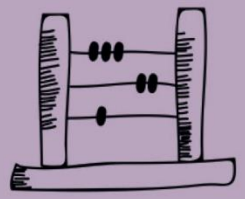
# KOMMMIT - TAG




## der Mathematik und Informatik

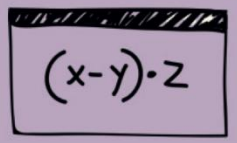
**27. September 2019**

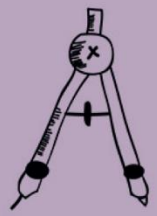
**Alpen-Adria-Universität Klagenfurt**



I06
Alexandra Webernig

a + b



</>

www.aau.at/komm-mit

# I06
# Der Krieg der Kryptologen auf der Suche nach dem „x“

Informatik

Sek 1 / Sek 2

*Alexandra Webernig*

# Wo im Alltag versteckt sich Verschlüsselung?

Wir benutzen Verschlüsselung täglich:

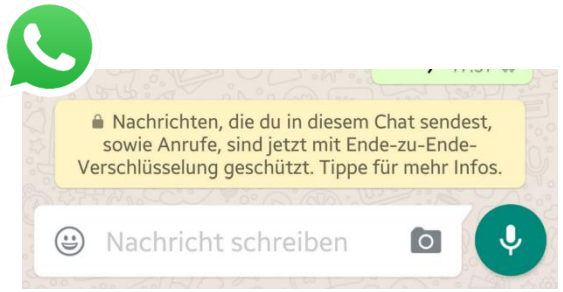
- W-LAN Anmeldung
- Bezahlen mit der Bankomatkarte
- E-Mails schreiben
- Onlinebanking

# Lernziele

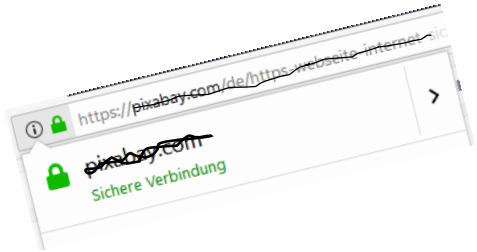
- Verschlüsselung ist in Computernetzen sinnvoll und notwendig
- Verschiedene Techniken möglich
- Unterschiede der einzelnen Techniken wissen

# Allgemeine Informationen: Kryptographie

- Wofür wird verschlüsselt?




- Anknüpfungspunkte für den Unterricht



# Entwicklung der Verschlüsselung

- Skytale
- Caesar-Verschlüsselung
- Vigenere-Verschlüsselung
- Enigma
- Moderne Methoden

# Funktionsweise der Verfahren

**Symmetrisches Verfahren**

**Asymmetrisches Verfahren**

# Funktionsweise der Verfahren

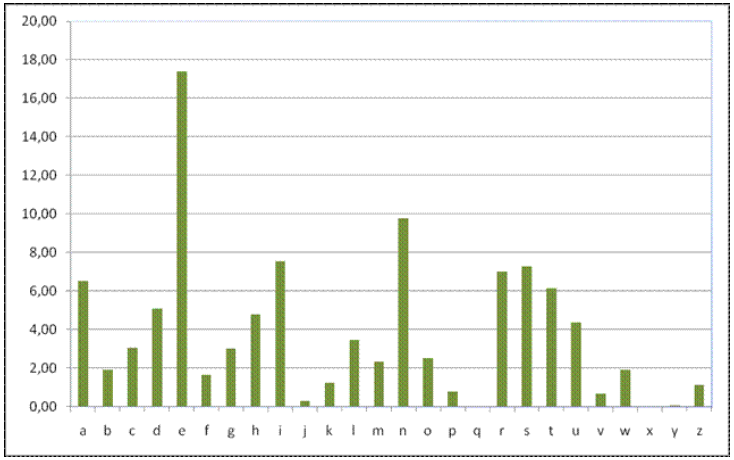
**Symmetrisches Verfahren**

# Caesar Verschlüsselung

Der römische Feldherr Julius Caesar verschlüsselte seine geheimen Nachrichten, indem er jeden Buchstaben durch einen anderen ersetzte. Dabei wurde der Buchstabe immer durch den um eine bestimmte Anzahl von Stellen im Alphabet verschobenen Buchstaben ersetzt.

# Caesar Verschlüsselung knacken

- 25 Möglichkeiten probieren
- Häufigkeitstabelle



# Skytale

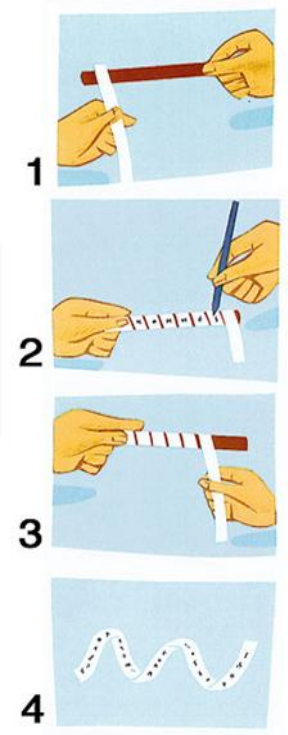
Die Spartaner benutzten eine so genannte

„Skytale“, um geheime Befehle an das

Militär zu verschlüsseln.

Die Skytale bestand aus einem

Holzstab und einem Lederstreifen.



# Skytale knacken

- Stäbe mit verschiedener Dicke und Länge ausprobieren
- Zählen aus wie vielen Buchstaben der Geheimtext besteht. Den Geheimtext spaltenweise untereinander anordnen. Anzahl der Spalten ist wichtig.

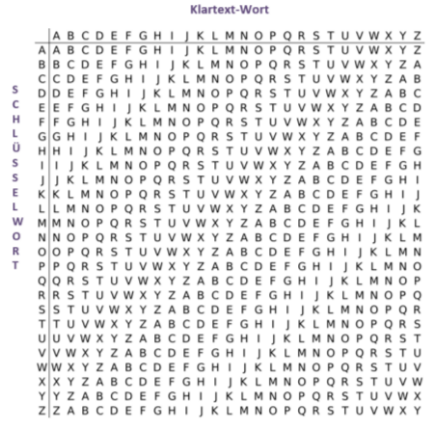
# Vigenère-Verschlüsselung

Die Vigenère-Verschlüsselung stammt vom französischen Diplomat Blaise de Vigenère. Die Anzahl der verwendeten Alphabete hängt vom Schlüsselwort ab.

Zum Verschlüsseln muss man sich ein

beliebiges Schlüsselwort ausdenken.

HALLO
⇩ „MIT“
TIEXW



# Die Vigenère Verschlüsselung knacken

- Der Geheimtext wird nach Buchstabenfolgen durchsucht, die mehrmals vorkommen
- Die Länge des Schlüsselwortes muss ermittelt werden
- Das Schlüsselwort wird bestimmt

# Funktionsweise der Verfahren

**Asymmetrisches Verfahren**

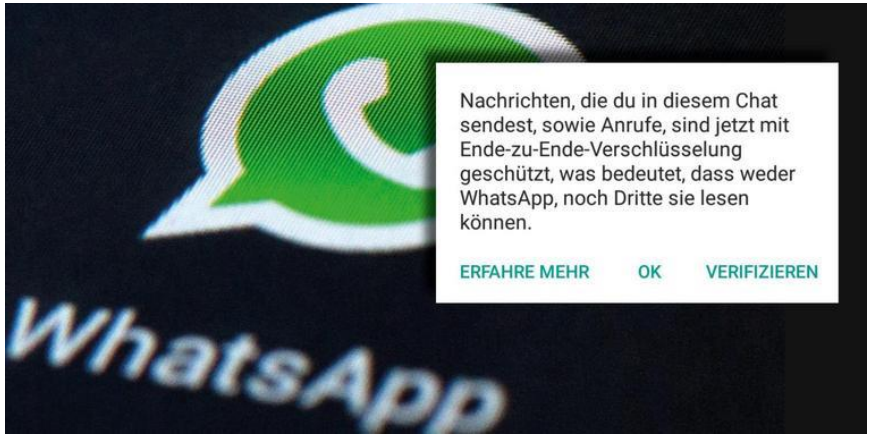
# Enigma

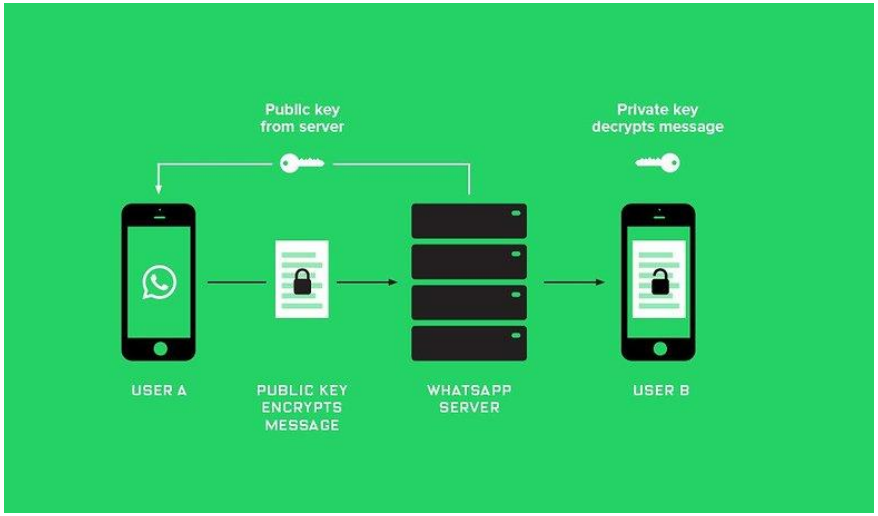
- Wurde von den Deutschen im Zweiten Weltkrieg verwendet
- Jeder Buchstabe hat eine eigene Verschiebung
- Große Anzahl an Kombinationsmöglichkeiten
- Statistische Verfahren, wie eine Häufigkeitsanalyse sind (beinahe) wirkungslos
    - Jeder Buchstabe kommt annähernd gleich oft vor

# Moderne Methoden

- Sicherheit durch riesigen Schlüsselraum und damit extremen Zeit-/Rechenaufwand beim Durchprobieren
- Brechen der Verschlüsselung durch Probieren
  - Sofern Passwort „zufällig“
- Verfahren sind allgemein bekannt, basieren auf mathematischen Problemen

# Ende zu Ende Verschlüsselung



# Komm MIT

## Tag der Mathematik und Informatik

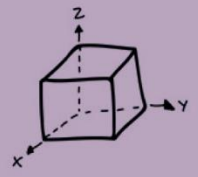
# Quellen


- https://www.planet-wissen.de/natur/forschung/kryptologie_die_lehre_des_verborgenen/pwiekryptologieimalltag100.html
- https://www.kryptowissen.de
- http://www.geo.de/GEOlino/kreativ/basteln/wer-knackt-den-code-278.html?p=2
- https://www.youtube.com/watch?v=OP5kpVIKoRk

ALPEN-ADRIA UNIVERSITÄT
FAKULTÄT FÜR TECHNISCHE WISSENSCHAFTEN

Herzlich Willkommen zum

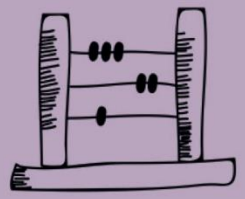
# KOMMMIT - TAG




## der Mathematik und Informatik

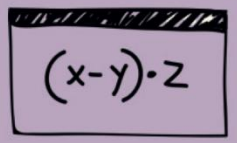
**27. September 2019**

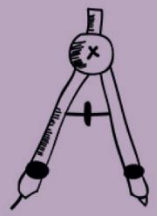
**Alpen-Adria-Universität Klagenfurt**



I06
Alexandra Webernig

a + b



</>

www.aau.at/komm-mit