# Kryptografie

## Eine Einführung



# Kryptografie – Was ist das?

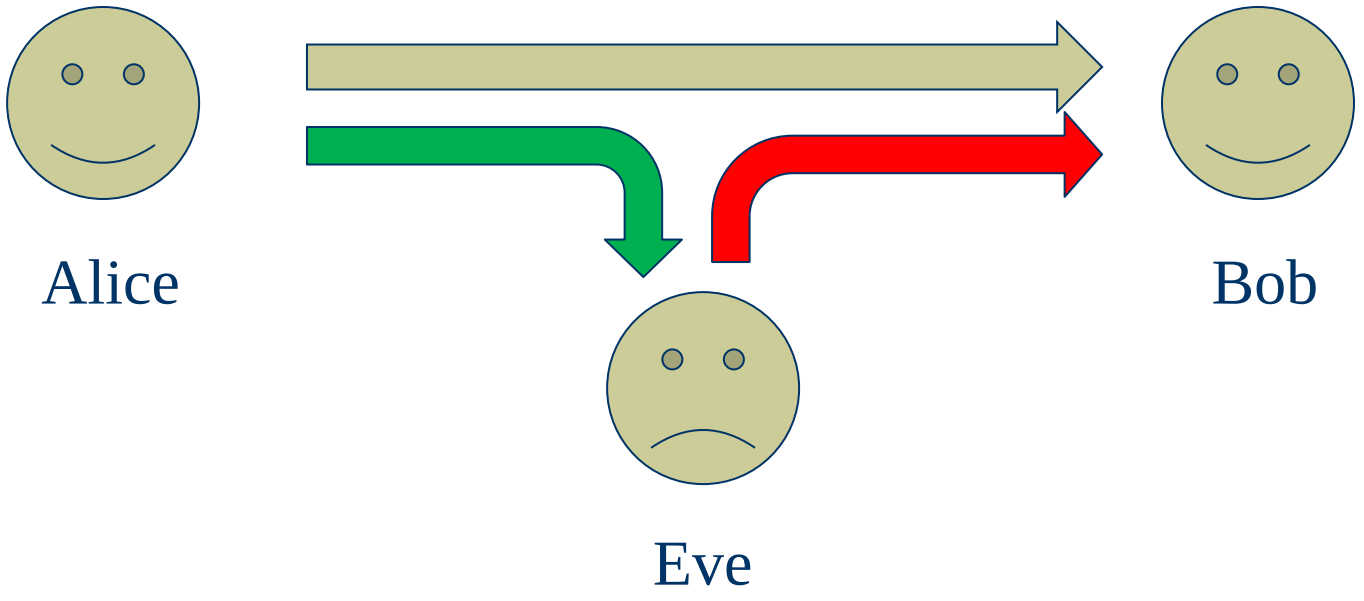
Das Wort Kryptographie stammt aus dem Griechischen und setzt sich aus den Worten *kryptos* (geheim, verborgen) und *graphein* (schreiben) zusammen. Somit ist Kryptographie die Kunst der Geheimschriften bzw. im modernen Sprachgebrauch der Verschlüsselung

# Wichtige Begriffe

- *Klartext*: unverschlüsselte Botschaft des Absenders an einen Empfänger
- *Geheimtext* (Chiffre): verschlüsselter Text

# Ziele der Kryptografie

## am Beispiel der „man in the middle attack“



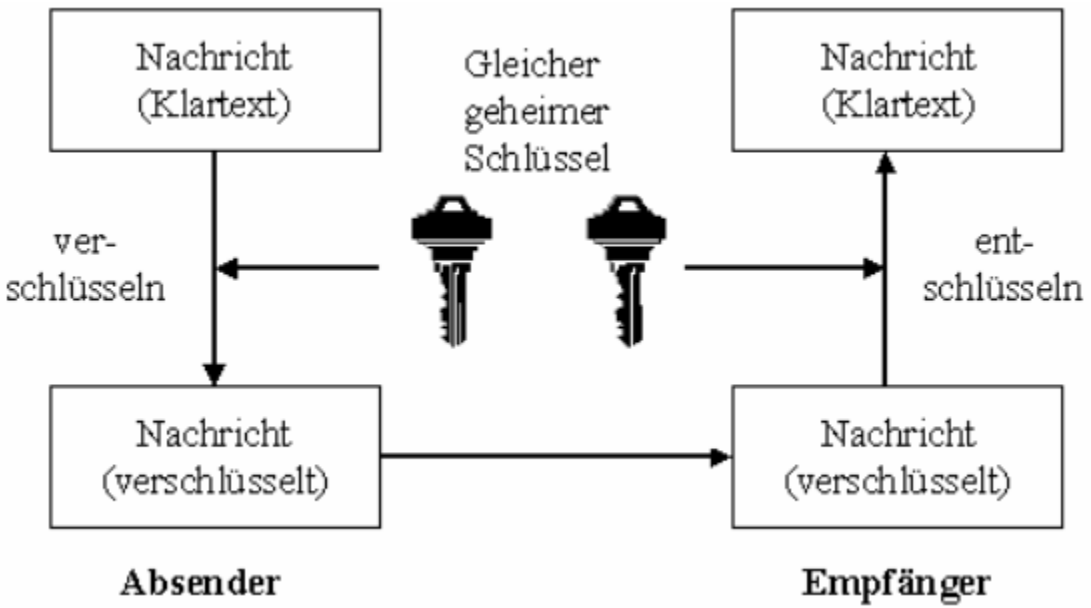

Vertraulichkeit, Integrität, Authentizität

# Ziele der Kryptografie

- **Vertraulichkeit**: Wie kann ich jemandem eine Nachricht übermitteln, ohne dass ein Unbefugter Kenntnis vom Inhalt der Nachricht erlangt?
  Lösung: Nachricht verschlüsseln.
- **Integrität**: Der Empfänger einer Nachricht muss sicher sein können, dass die empfangene Nachricht nicht verändert wurde. Falls es doch einem aktiven Angreifer gelingt, den Inhalt einer Nachricht zu verfälschen, so muss der Empfänger diese Manipulation sofort erkennen können.
  Lösung: Prüfsummen, Hashwerte verwenden
- **Authentizität**: Es geht hier um die Frage, ob die Nachricht auch wirklich vom angegebenen Absender stammt.
  Lösung: Digitale Signatur

# Verschlüsselungsverfahren I
# Symmetrische Verfahren

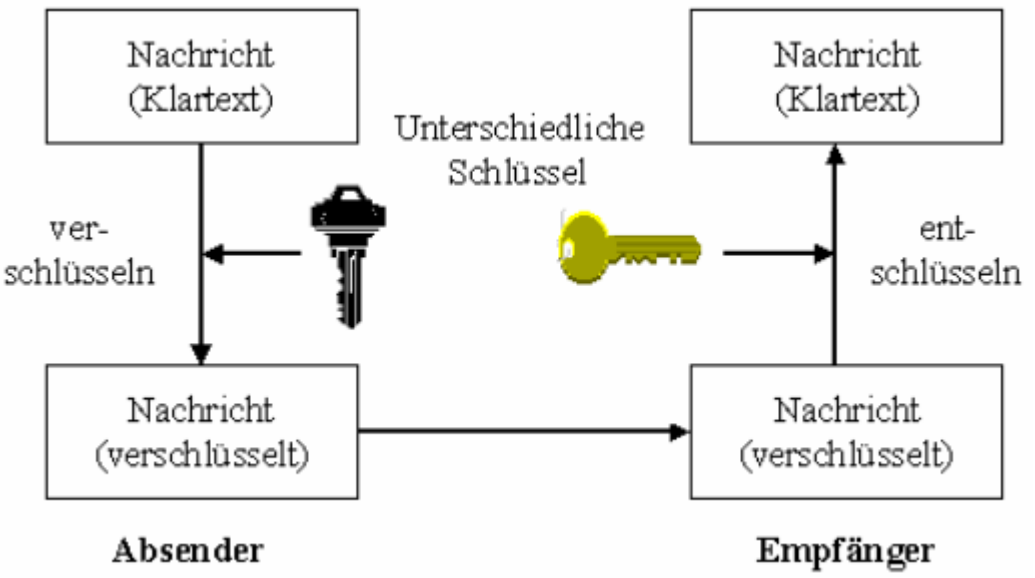
In symmetrischen Verschlüsselungsverfahren existiert ein Schlüssel, der gleichzeitig beim Absender zum Verschlüsseln und beim Empfänger zum Entschlüsseln einer Nachricht verwendet wird.




Probleme:
- Schlüsselaustausch
- Anzahl der Schlüssel

# Verschlüsselungsverfahren II
# Asymmetrische Verfahren

In asymmetrischen Verschlüsselungsverfahren existieren zwei verschiedene, gleichlange Schlüssel, die mathematisch miteinander zusammenhängen, der *Private-Key* und der *Public-Key:*



# Der Cäsar – Chiffre
## (monoalphabetischer Chiffre)



- monoalphabetische Substitution: Verfahren, bei dem jeder Buchstabe des Alphabets zu demselben Geheimtext-Buchstaben verschlüsselt wird.
- Beim Verschlüsseln mit dem Cäsar - Code notiert man unter dem Klartextalphabet (KTA) das Geheimtextalphabet (GTA). Das GTA ist eine Verschiebung des KTA um eine bestimmte Anzahl von Stellen. Sender und Empfänger müssen nur die "Verschiebungszahl" (Schlüssel) vereinbaren.

| KTA: | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| GTA: | 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 |

# Der Cäsar – Chiffre
## (Beispiel)

- Im folgenden Beispiel wurde das GTA um 4 Stellen gegenüber dem KTA verschoben (Schlüssel E).

| KTA: | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| GTA: | 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 |

- Die Verschlüsselung erfolgt nun vom KTA zum GTA. Man sucht den zu verschlüsselnden Buchstaben im KTA und notiert den darunter stehenden Buchstaben des GTA. Beim Entschlüsseln geht man den umgekehrten Weg. Beispiel:

| D | A | S | I | S | T | G | E | H | E | I | M |
|---|---|---|---|---|---|---|---|---|---|---|---|
| H | E | W | M | W | X | K | I | L | I | M | Q |

# Der Cäsar – Chiffre
## (Aufgaben)

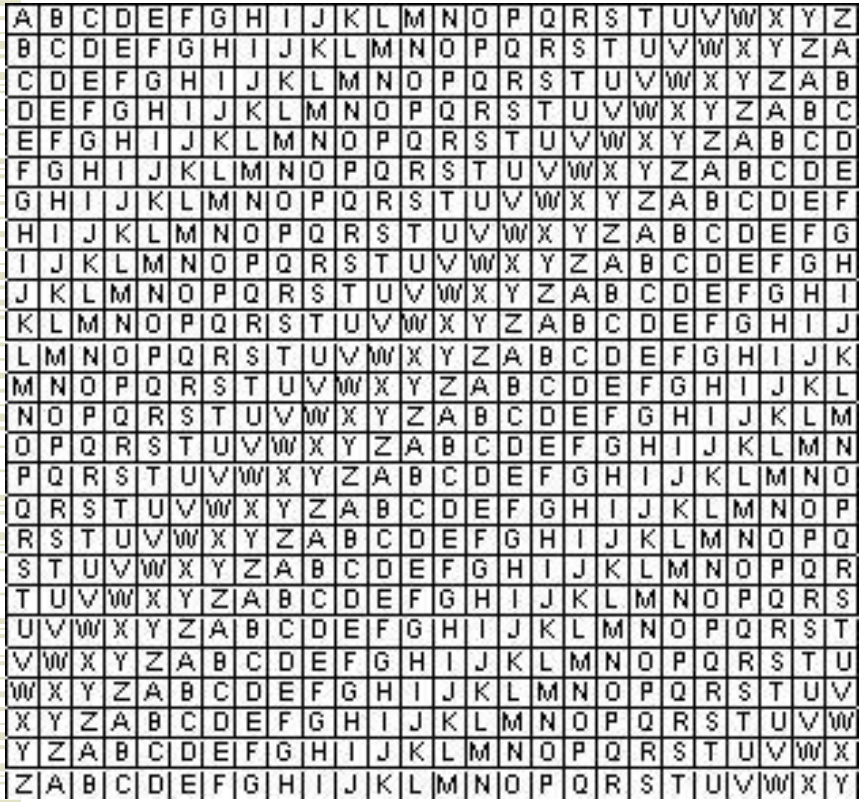
- Lösen Sie auf dem AB die Aufgaben 1 und 2 zum Thema „Cäsar-Verfahren“.
- Überprüfen Sie Ihre Lösungen mit dem Programm „krypto.exe“.

# Der Vigenère-Code
## (polyalphabetische Substitution)

- Bei der polyalphabetischen Substitution wird derselbe Klartextbuchstabe nicht stets mit demselben Geheimtextbuchstaben verschlüsselt.
- Bei der Verschlüsselung wird nicht nur ein Geheimtextalphabet, sondern verschiedene Alphabete benutzt; die sich wieder aus der Verschiebung des Klartextalphabetes (KTA) ergeben. Auf die verschiedenen GTA's wird durch einen festgelegten Schlüssel zugegriffen.



# Der Vigenère-Code
## (Beispiel)



Vigenere-Quadrat

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Schlüssel: | I | N | F | O | R | M | A | T | I | K | I | N | F | O | R | M | A | T |
| KTA: | D | A | S | I | S | T | S | T | R | E | N | G | G | E | H | E | I | M |
| GTA: | L | N | X | W | J | F | S | M | Z | O | V | T | L | S | Y | Q | I | F |

# Der Vigenère-Code
## (Aufgaben)

- Lösen Sie auf dem AB die Aufgaben 1 und 2 zum Thema „Vigenère-Verfahren“.
- Überprüfen Sie Ihre Lösungen mit dem Programm „krypto.exe“.

# Kryptoanalyse

- Wie schwierig ist es, einen Code zu knacken?
- Experimentieren Sie mit dem Programm „Cryptool“ und testen Sie wie schnell sich mit dem Cäsar- bzw. Vigenere-Verfahren verschlüsselte Texte knacken lassen.

# Kryptoanalyse mit einem Histogramm

| Buchstabe | Häufigkeit (in %) | Buchstabe | Häufigkeit (in %) |
|---|---|---|---|
| E | 17.40 | M | 2.53 |
| N | 9.78 | O | 2.51 |
| I | 7.55 | W | 1.89 |
| S | 7.27 | B | 1.89 |
| R | 7.00 | F | 1.66 |
| A | 6.51 | K | 1.21 |
| T | 6.15 | Z | 1.13 |
| D | 5.08 | P | 0.79 |
| H | 4.76 | V | 0.67 |
| U | 4.35 | J | 0.27 |
| L | 3.44 | Y | 0.04 |
| C | 3.06 | X | 0.03 |
| G | 3.01 | Q | 0.02 |

# Kryptoanalyse mit einem Histogramm

Oftmals können dann schon einige Wörter erraten werden, denn in der deutschen Sprache können Wörter schon erkannt werden, wenn die häufigsten Buchstaben bekannt sind.
Die –ehn haeu-i-sten –u-hsta-en i- deuts-hen –i-den –ereits drei –ierte- des –esa-tte-tes.

Häufigkeiten der Bigramme:

| *Buchstabenpaar* | *Häufigkeit (in %)* | *Buchstabenpaar* | *Häufigkeit (in %)* |
|---|---|---|---|
| en | 3.88 | nd | 1.99 |
| er | 3.75 | ei | 1.88 |
| ch | 2.75 | ie | 1.79 |
| te | 2.26 | in | 1.67 |
| de | 2.00 | es | 1.52 |