Hochschule Düsseldorf
University of Applied Sciences

HSD

# Kryptographie

**Modul D3.2**

Referent: Dr. Jörg Cosfeld

Evaluation

http://fh-duesseldorf.evasys.de/evasys/online.php?p=28Y47

Hochschule Düsseldorf
University of Applied Sciences

HSD

# Kryptographie

**Modul D3.2**

Referent: Dr. Jörg Cosfeld

Evaluation

http://fh-duesseldorf.evasys.de/evasys/online.php?p=28Y47

# Kryptographie

Was lernen wir in dieser Vorlesung?

Gutes Verständnis für **kryptographische Verfahren** und ihre Anwendungen.

# Kryptographie

Was lernen wir in dieser Vorlesung?

Gutes Verständnis für **kryptographische Verfahren** und ihre Anwendungen.

Erlangen der Kenntnisse über den **Aufbau**, die **Prinzipien**, die **Architektur** und die **Funktionsweise** von kryptographischen Verfahren.

# Kryptographie

Was lernen wir in dieser Vorlesung?

Gutes Verständnis für **kryptographische Verfahren** und ihre Anwendungen.

Erlangen der Kenntnisse über den **Aufbau**, die **Prinzipien**, die **Architektur** und die **Funktionsweise** von kryptographischen Verfahren.

Einen guten **Überblick** über die aktuellen **kryptographische Verfahren**.

# Kryptographie

**Was ist der Wunsch nach Vertraulichkeit?**

# Kryptographie

**Was ist der Wunsch nach Vertraulichkeit?**

Transformation einer
**verständlichen Informationsdarstellung**

# Kryptographie

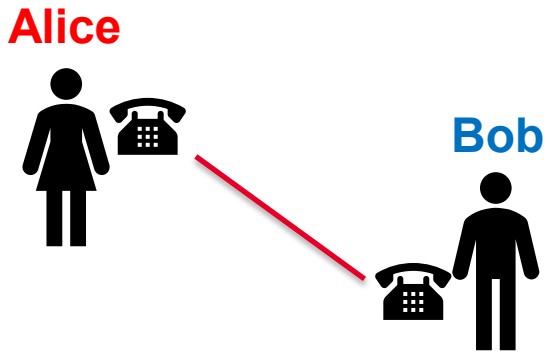
**Was ist der Wunsch nach Vertraulichkeit?**

Transformation einer
**verständlichen Informationsdarstellung**

in eine
**nicht verständliche Informationsdarstellung**

# Kryptographie

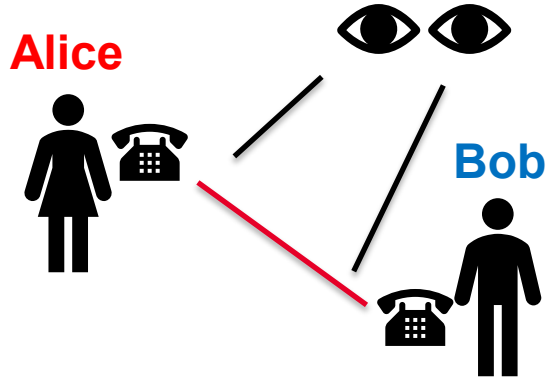
**Was ist der Wunsch nach Vertraulichkeit?**




Transformation einer
**verständlichen Informationsdarstellung**

in eine
**nicht verständliche Informationsdarstellung**

# Kryptographie

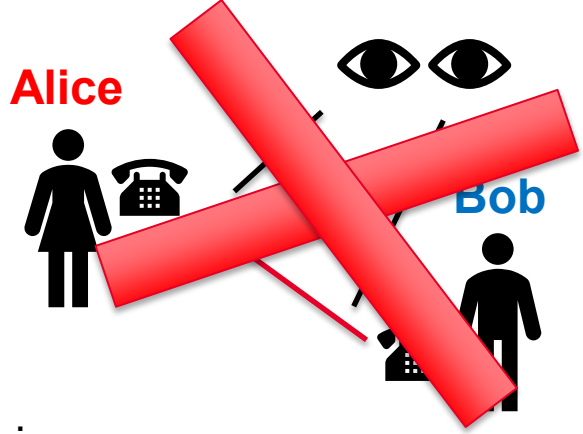



**Was ist der Wunsch nach Vertraulichkeit?**

Transformation einer
**verständlichen Informationsdarstellung**

in eine
**nicht verständliche Informationsdarstellung**

# Kryptographie




**Was ist der Wunsch nach Vertraulichkeit?**

Transformation einer
**verständlichen Informationsdarstellung**

in eine
**nicht verständliche Informationsdarstellung**

# Kryptographie

**Was ist der Wunsch nach Vertraulichkeit?**

seit 6000 Jahren gibt es Schrift

# Kryptographie

**Was ist der Wunsch nach Vertraulichkeit?**

seit 6000 Jahren gibt es Schrift

seit rund 3000 Jahren Verschlüsselung

# Kryptographie

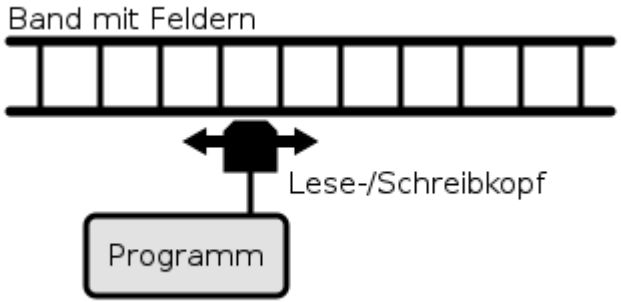
**Was ist der Wunsch nach Vertraulichkeit?**

Alan Turing

* 23. Juni 1912 in London; † 7. Juni 1954 in Wilmslow, Cheshire

# Kryptographie

**Was ist der Wunsch nach Vertraulichkeit?**

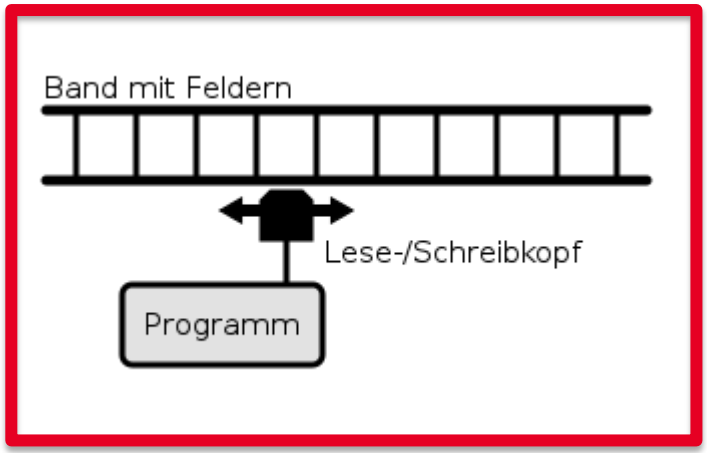



Alan Turing

* 23. Juni 1912 in London; † 7. Juni 1954 in Wilmslow, Cheshire

# Kryptographie

**Was ist der Wunsch nach Vertraulichkeit?**



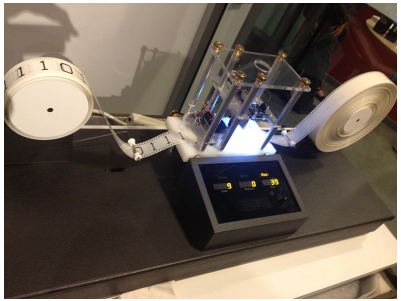

Turing Maschine

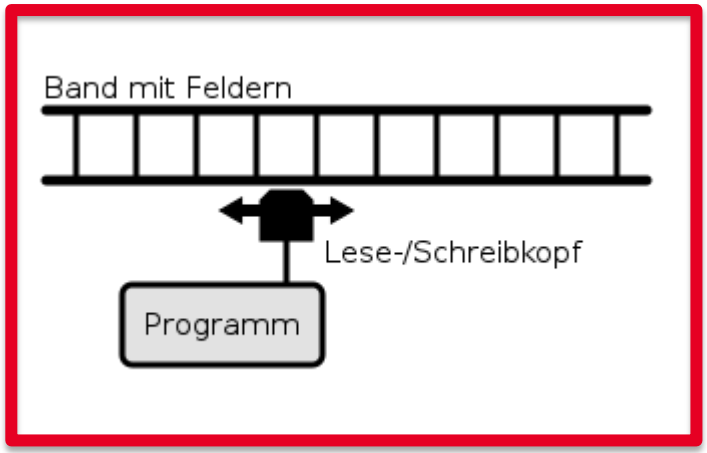
Alan Turing

* 23. Juni 1912 in London; † 7. Juni 1954 in Wilmslow, Cheshire

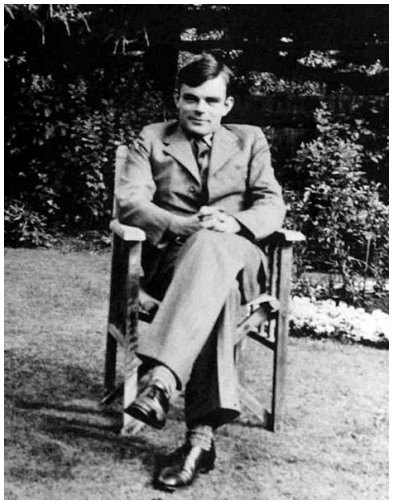
# Kryptographie

**Was ist der Wunsch nach Vertraulichkeit?**






Turing Maschine

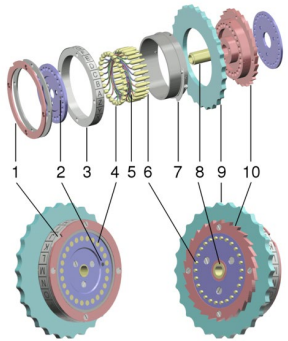


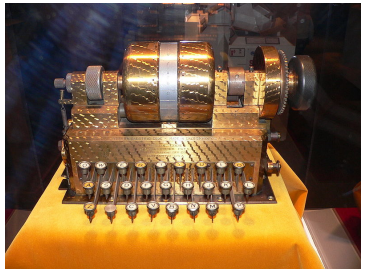
Alan Turing

* 23. Juni 1912 in London; † 7. Juni 1954 in Wilmslow, Cheshire

# Kryptographie

**Was ist der Wunsch nach Vertraulichkeit?**



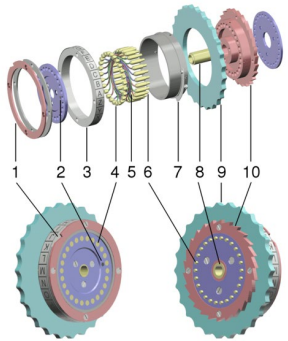



Alan Turing

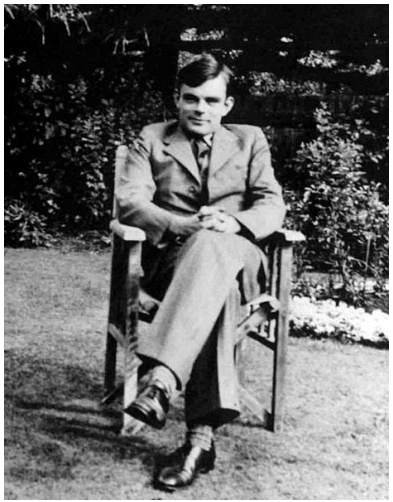
* 23. Juni 1912 in London; † 7. Juni 1954 in Wilmslow, Cheshire

# Kryptographie

**Was ist der Wunsch nach Vertraulichkeit?**




Rotor-Chiffriermaschine
verwendet von Nazi Deutschland



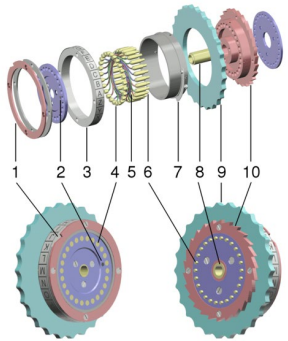
Alan Turing

* 23. Juni 1912 in London; † 7. Juni 1954 in Wilmslow, Cheshire

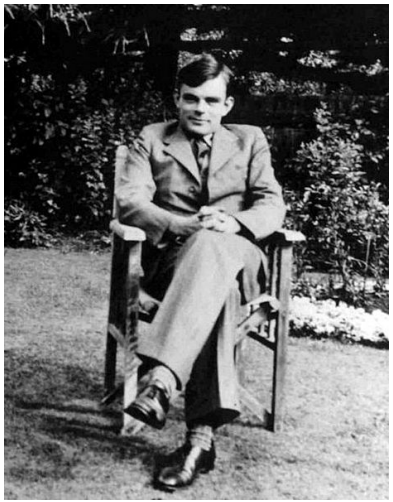
# Kryptographie

Aber wie?

**Was ist der Wunsch nach Vertraulichkeit?**




Rotor-Chiffriermaschine
verwendet von Nazi Deutschland



Alan Turing

* 23. Juni 1912 in London; † 7. Juni 1954 in Wilmslow, Cheshire

# Kryptographie

Aber wie?

**Was ist der Wunsch nach Vertraulichkeit?**


https://www.youtube.com/watch?v=G2_Q9FoD-oQ

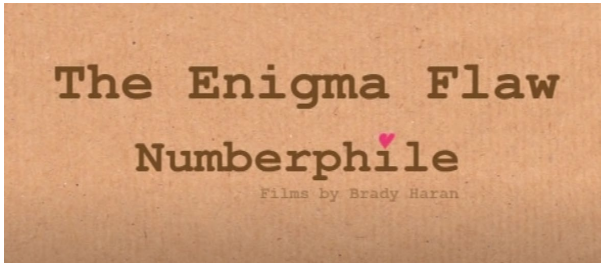
Alan Turing

* 23. Juni 1912 in London; † 7. Juni 1954 in Wilmslow, Cheshire

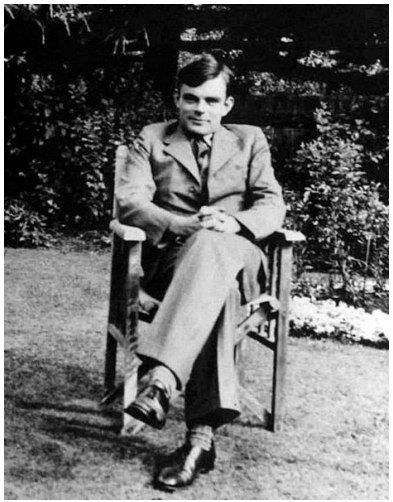
# Kryptographie

Aber wie?

**Was ist der Wunsch nach Vertraulichkeit?**




https://www.youtube.com/watch?v=V4V2bpZlqx8



Alan Turing

* 23. Juni 1912 in London; † 7. Juni 1954 in Wilmslow, Cheshire

# Kryptographie

https://www.youtube.com/watch?v=6178TGqHkH0

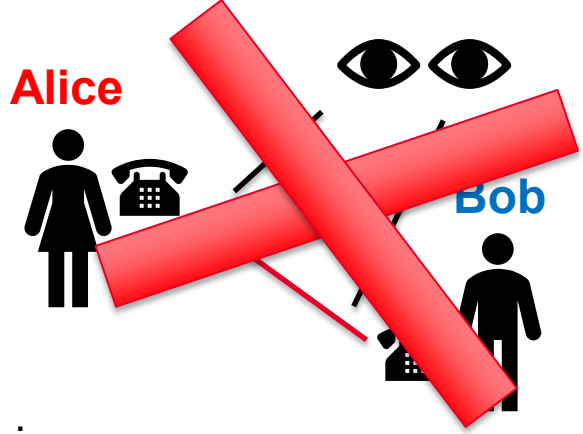
Alan Turing

* 23. Juni 1912 in London; † 7. Juni 1954 in Wilmslow, Cheshire

# Kryptographie

1942 heuerte die **US-Armee Navajo-Indianer** an, um **kriegsrelevante Botschaften** zu **ver-** und **entschlüsseln**. Die Sprache **war außerhalb der Indianer-Population** nahezu **unbekannt** und Außenstehenden unverständlich.

# Kryptographie




**Was ist der Wunsch nach Vertraulichkeit?**

Transformation einer
**verständlichen Informationsdarstellung**

in eine
**nicht verständliche Informationsdarstellung**

# Kryptographie

**Was ist der Wunsch nach Vertraulichkeit?**

Transformation einer
**verständlichen Informationsdarstellung**

in eine
**nicht verständliche Informationsdarstellung**

Grundlagen der IT-Sicherheit → fvy33b9/8YR/uJlk96T6TbfZjYBFZc680GC AOs8fNFTzmA1zxLHZEXHc+LJ99xfYopN BTPnuU6VPlByc+3QeKjQ+pWulyFCkqU PzSluIn0a5x81rAMQ5fxhLJ7G32qp

# Kryptographie

**Wann begegnen wir Kryptographie im Alltag?**

- Telefonkarten
- Mobilfunk
- Nummerncodierung in der Banknote

# Kryptographie

**Wann begegnen wir Kryptographie im Alltag?**

- Telefonkarten
- Mobilfunk
- Nummerncodierung in der Banknote
- Geldautomaten
- Wegfahrsperre im Auto
- Bitcoin etc.

# Kryptographie

**Wann begegnen wir Kryptographie im Alltag?**

Klassifizierung als 6er Tupel

M = Menge der Klartext-Nachrichten m (messages, plain text)
z.B. M = {0, 1}, also die Menge der endlichen 0,1-Folgen

# Kryptographie

**Wann begegnen wir Kryptographie im Alltag?**

Klassifizierung als 6er Tupel

M = Menge der Klartext-Nachrichten m (messages, plain text)
z.B. M = {0, 1}, also die Menge der endlichen 0,1-Folgen

C = Menge der Kryptogramme c (verschlüsselte Nachrichten, cipher text)
z.B. C = {0, 1}

# Kryptographie

**Wann begegnen wir Kryptographie im Alltag?**

Klassifizierung als 6er Tupel

M = Menge der Klartext-Nachrichten m (messages, plain text)
z.B. M = {0, 1}, also die Menge der endlichen 0,1-Folgen

C = Menge der Kryptogramme c (verschlüsselte Nachrichten, cipher text)
z.B. C = {0, 1}

KE = endliche, nicht-leere Menge der Verschlüsselungs-Schlüssel
z.B. KE = {0, 1}256 (256 Bit)

# Kryptographie

**Wann begegnen wir Kryptographie im Alltag?**

Klassifizierung als 6er Tupel

KD = endliche, nicht-leere Menge der Entschlüsselungs-Schlüssel
mit: kd = f(ke)

# Kryptographie

**Wann begegnen wir Kryptographie im Alltag?**

Klassifizierung als 6er Tupel

KD = endliche, nicht-leere Menge der Entschlüsselungs-Schlüssel
mit: kd = f(ke)

E = Verschlüsselungsverfahren E

D = Entschlüsselungsverfahren D

# Kryptographie

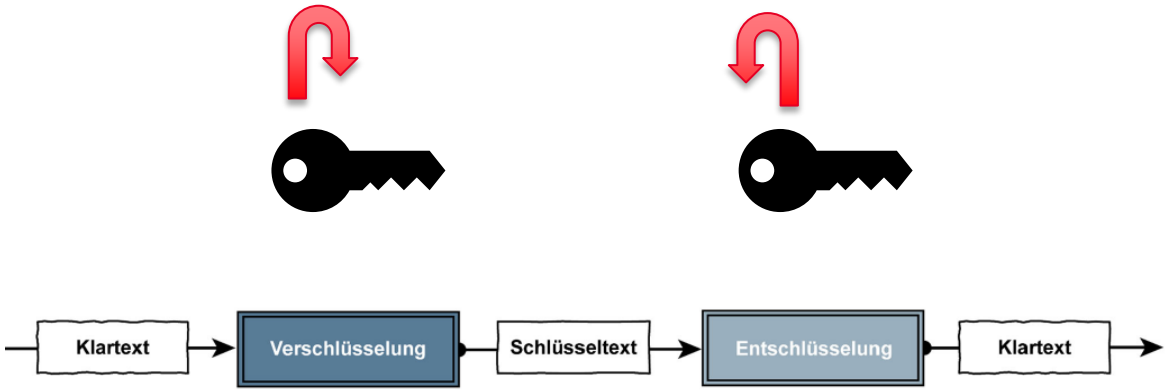
**Wann begegnen wir Kryptographie im Alltag?**

Klassifizierung als 6er Tupel

# Kryptographie

**Wann begegnen wir Kryptographie im Alltag?**

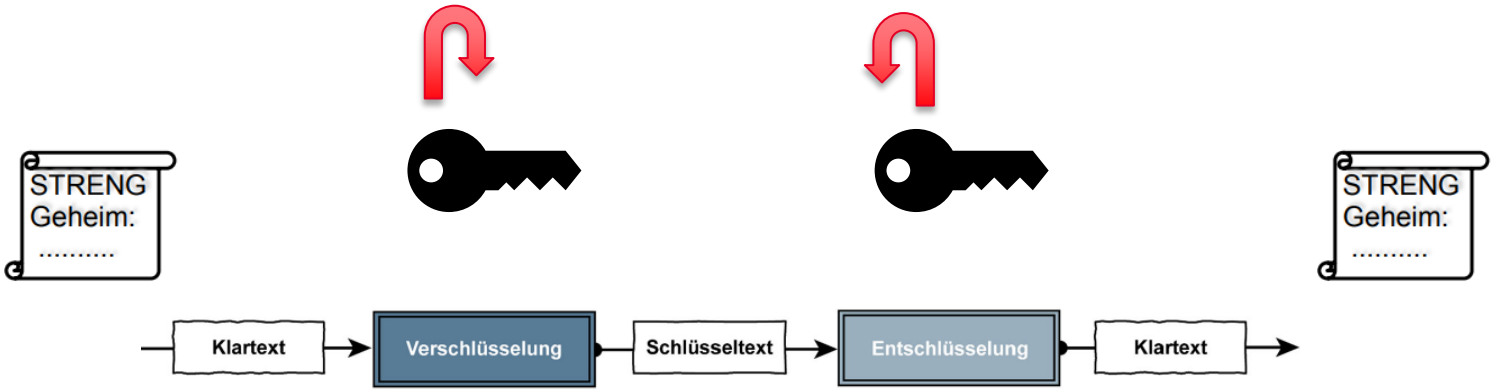
Klassifizierung als 6er Tupel



# Kryptographie

**Wann begegnen wir Kryptographie im Alltag?**

Klassifizierung als 6er Tupel



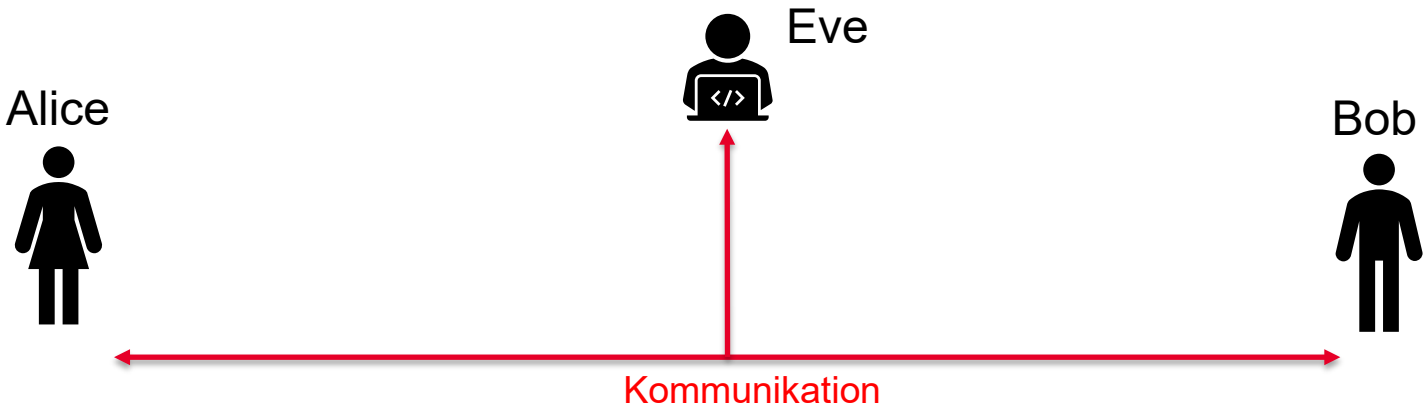
# Kryptographie

**Wer sind Alice und Bob?**


# Kryptographie

Eve kann passiv mithören.

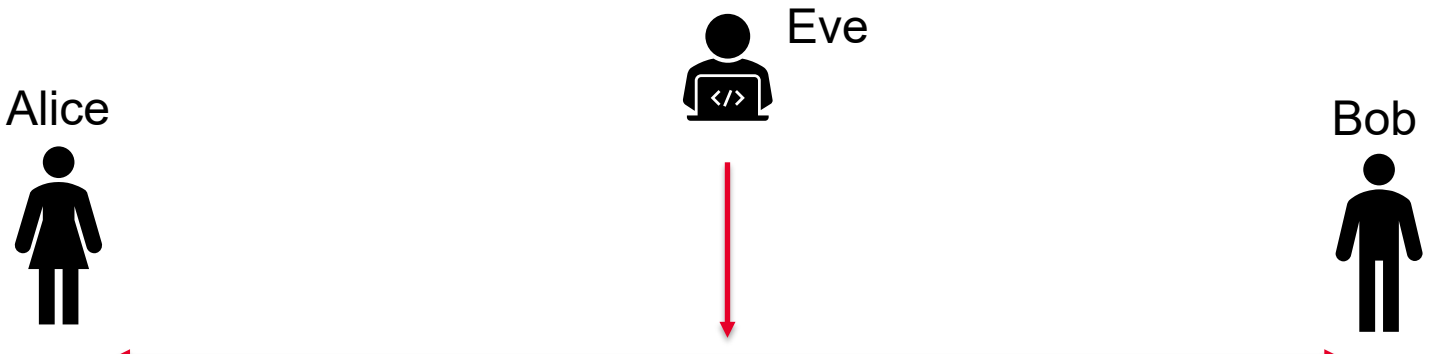
**Wer sind Alice und Bob?**




# Kryptographie

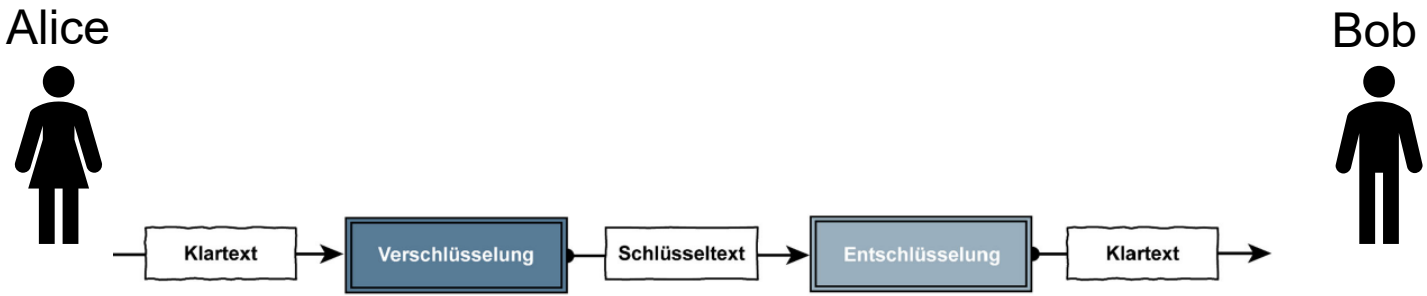
Eve kann aktiv manipulieren.

**Wer sind Alice und Bob?**



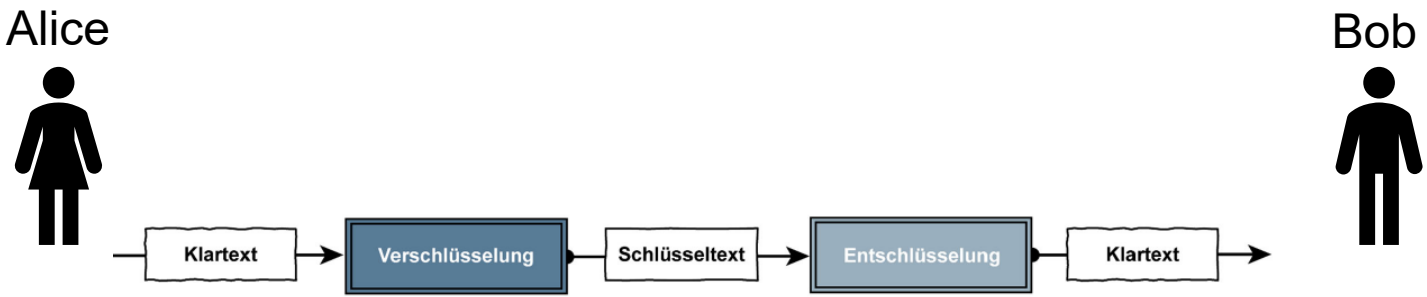

# Kryptographie

**Substitution:**



# Kryptographie

**Substitution:** $f : A_1^n \rightarrow A_2^m$

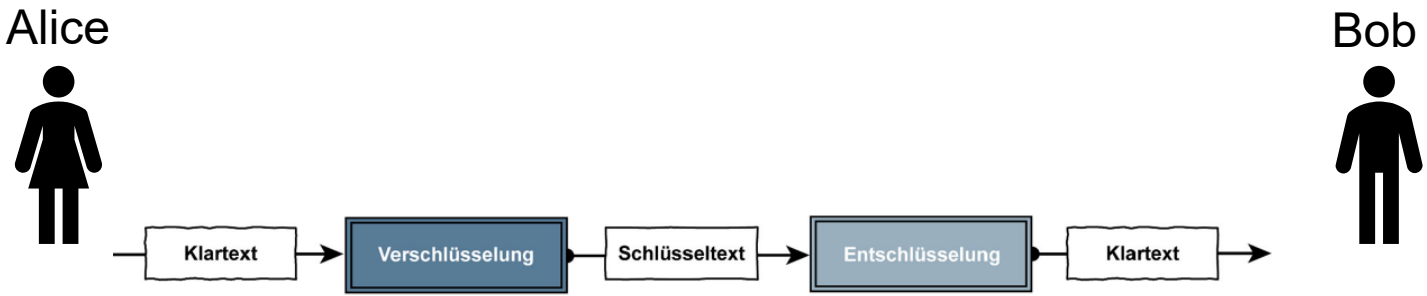


# Kryptographie

**Substitution:** $f : A_1^n \rightarrow A_2^m$

$$A_1 = \{a, b, \ldots, z\} \qquad A_2 = \{1,2,3,4,5\}$$

Unsere Wahl:



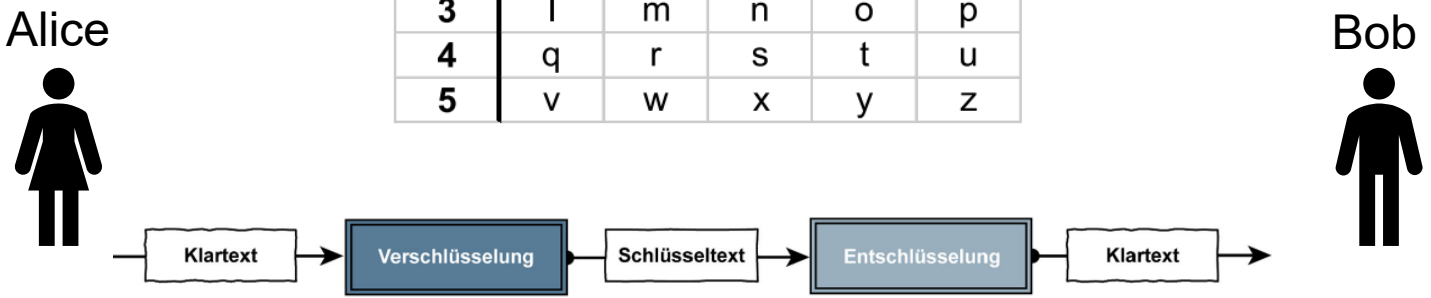
# Kryptographie

**Substitution:** $f : A_1^n \rightarrow A_2^m$ $\quad A_1 = \{a, b, \ldots, z\}$ $\quad A_2 = \{1,2,3,4,5\}$

Unsere Wahl:

$$E : A_1^1 \rightarrow A_2^2$$

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| **1** | a | b | c | d | e |
| **2** | f | g | h | i | k |
| **3** | l | m | n | o | p |
| **4** | q | r | s | t | u |
| **5** | v | w | x | y | z |

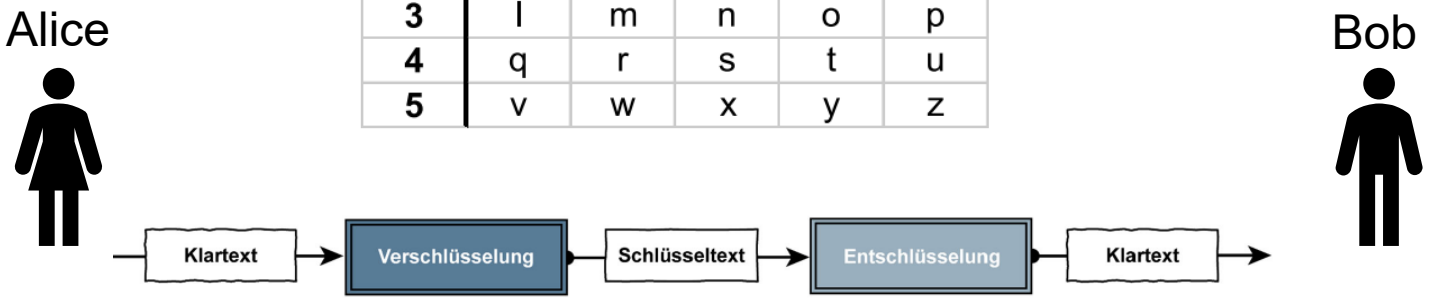


# Kryptographie

**Substitution:** vorlesung

$$E : A_1^1 \rightarrow A_2^2$$

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 1 | a | b | c | d | e |
| 2 | f | g | h | i | k |
| 3 | l | m | n | o | p |
| 4 | q | r | s | t | u |
| 5 | v | w | x | y | z |

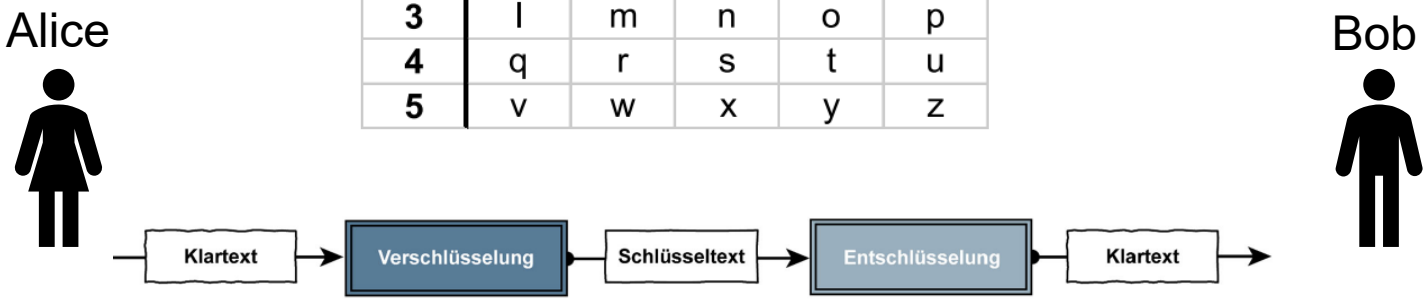


# Kryptographie

**Substitution:** vorlesung → 51

$$E : A_1^1 \rightarrow A_2^2$$

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| **1** | a | b | c | d | e |
| **2** | f | g | h | i | k |
| **3** | l | m | n | o | p |
| **4** | q | r | s | t | u |
| **5** | v | w | x | y | z |

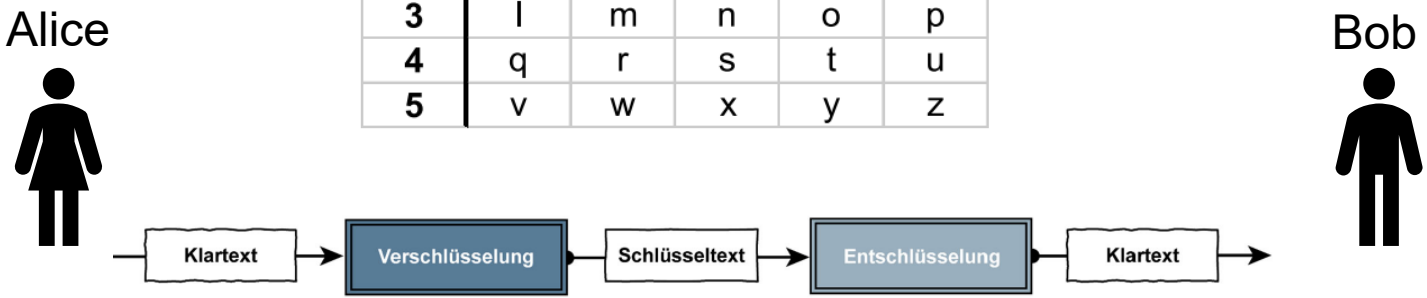


# Kryptographie

**Substitution:** vorlesung → 51

$$E : A_1^1 \rightarrow A_2^2$$

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 1 | a | b | c | d | e |
| 2 | f | g | h | i | k |
| 3 | l | m | n | o | p |
| 4 | q | r | s | t | u |
| 5 | v | w | x | y | z |

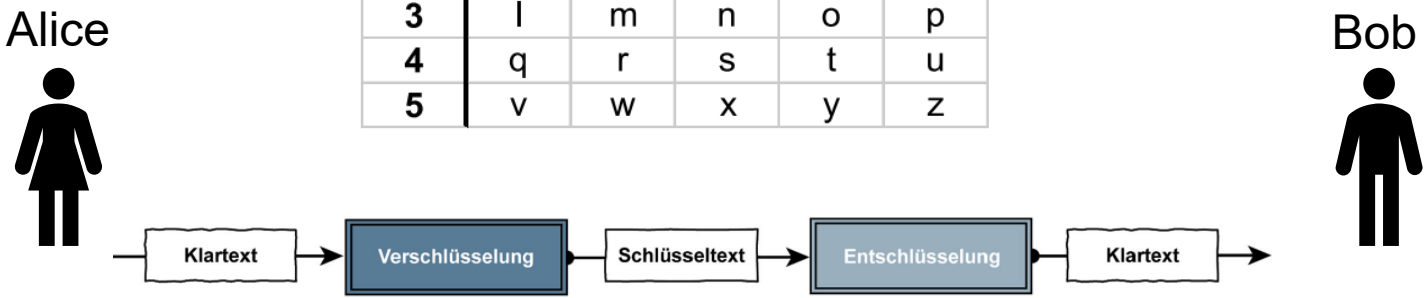


# Kryptographie

**Substitution:** vorlesung → 5134

$$E : A_1^1 \rightarrow A_2^2$$

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 1 | a | b | c | d | e |
| 2 | f | g | h | i | k |
| 3 | l | m | n | o | p |
| 4 | q | r | s | t | u |
| 5 | v | w | x | y | z |

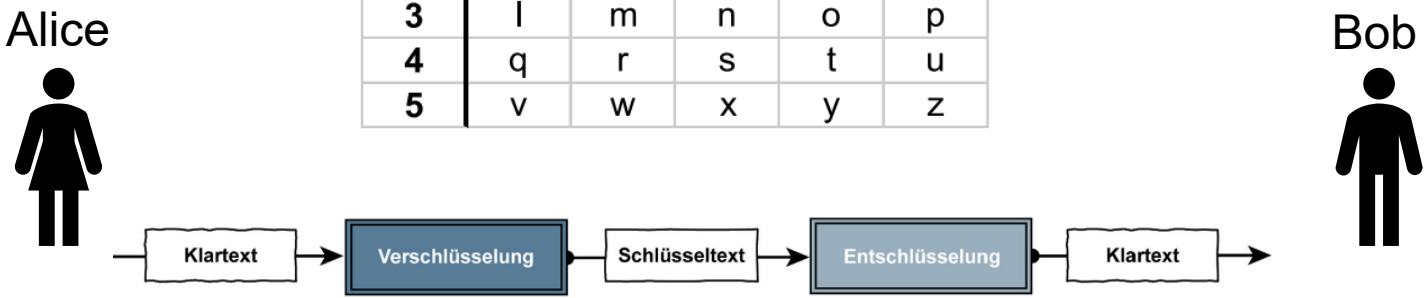


# Kryptographie

**Substitution:** vorlesung → 5134423115434533322

$$E : A_1^1 \rightarrow A_2^2$$

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 1 | a | b | c | d | e |
| 2 | f | g | h | i | k |
| 3 | l | m | n | o | p |
| 4 | q | r | s | t | u |
| 5 | v | w | x | y | z |



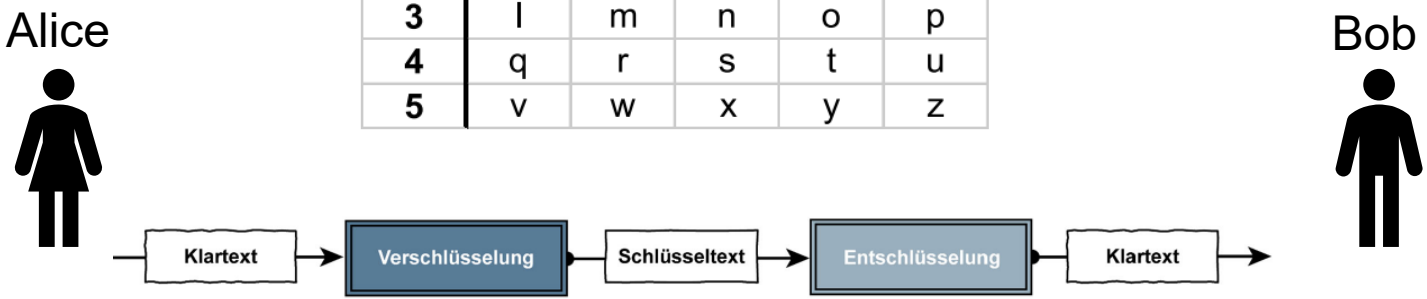
# Kryptographie

**Substitution:** vorlesung → 5134423115434533322

$$E : A_1^1 \rightarrow A_2^2$$

**Was ist der Schlüssel?**

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| **1** | a | b | c | d | e |
| **2** | f | g | h | i | k |
| **3** | l | m | n | o | p |
| **4** | q | r | s | t | u |
| **5** | v | w | x | y | z |



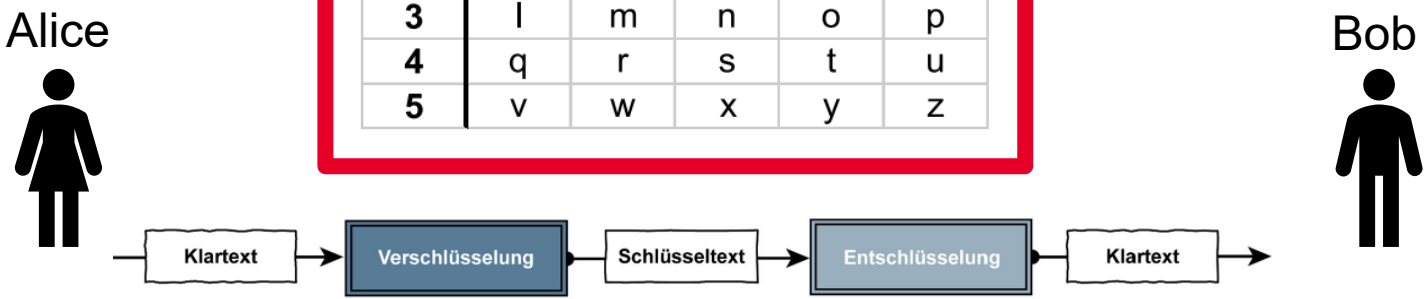
# Kryptographie

**Substitution:** vorlesung → 5134423115434533322

**Was ist der Schlüssel?**

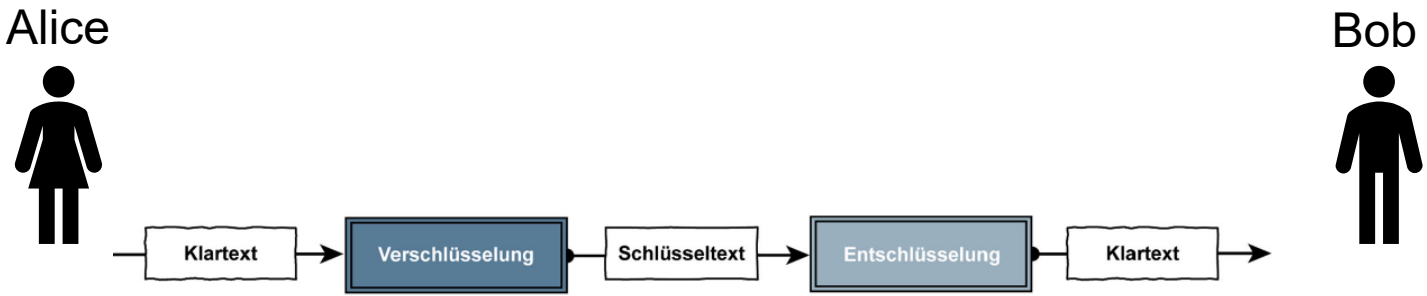
$$E : A_1^1 \rightarrow A_2^2$$

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 1 | a | b | c | d | e |
| 2 | f | g | h | i | k |
| 3 | l | m | n | o | p |
| 4 | q | r | s | t | u |
| 5 | v | w | x | y | z |



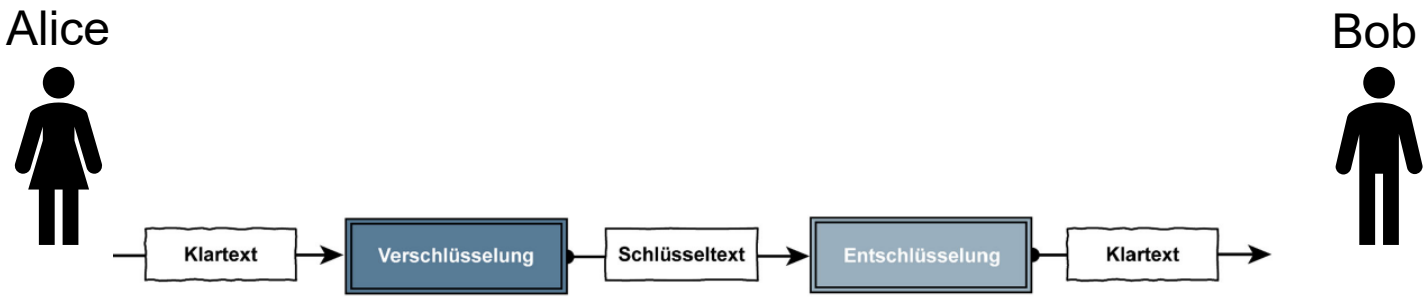
# Kryptographie

**Permutation:** $f : A^n \rightarrow A^n$



# Kryptographie

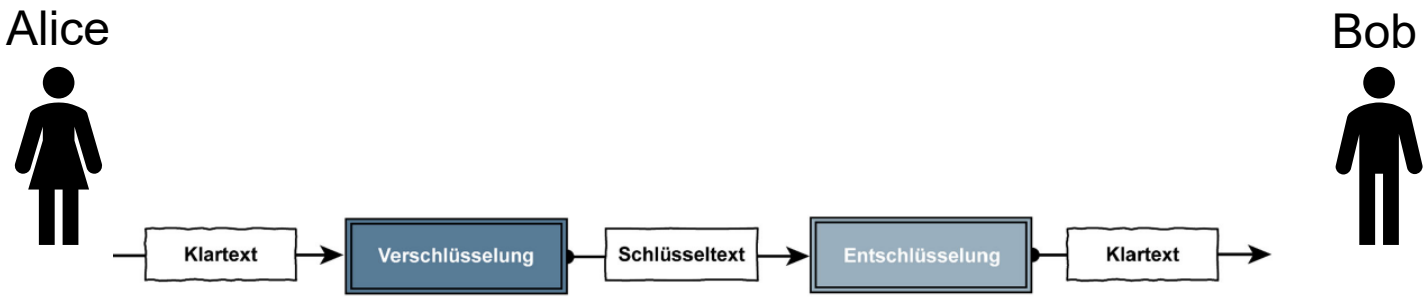
**Permutation:** $f : A^n \rightarrow A^n$ $\quad\quad$ $\mathrm{A}_1 = A_2 = \{a, b, \ldots, z\}$



# Kryptographie

**Permutation:** $f : A^n \rightarrow A^n$ $\quad A_1 = A_2 = \{a, b, \ldots, z\}$

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



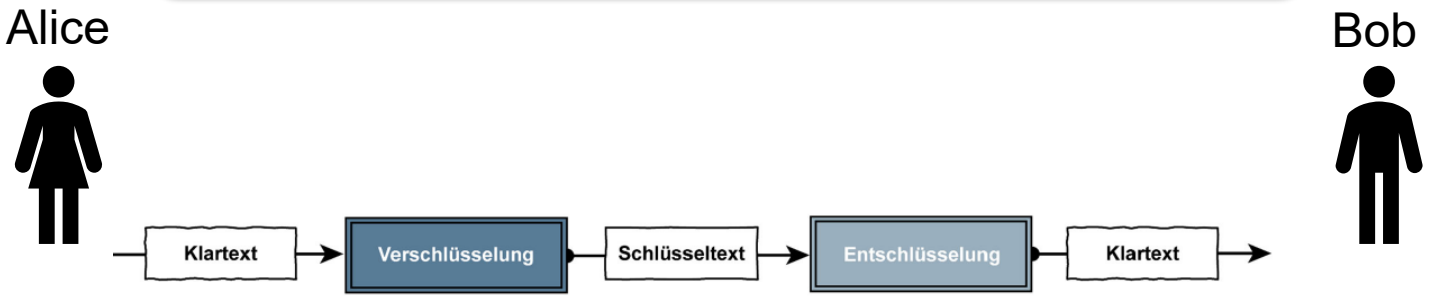
# Kryptographie

**Permutation:** $f : A^n \rightarrow A^n$ $\quad A_1 = A_2 = \{a, b, \ldots, z\}$

**Was ist der Schlüssel?**

TIMFOPSHKBQPBWAOMAOBQ = vorlesung it sicherheit

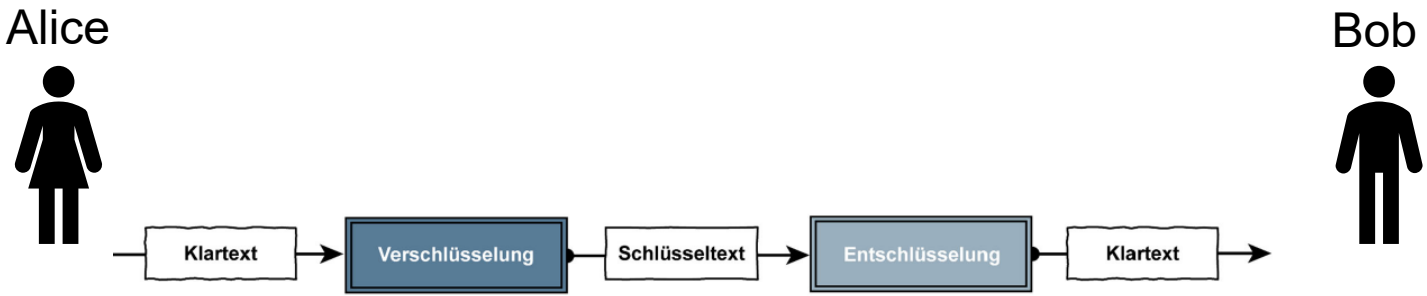
| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| N | E | W | Y | O | R | K | A | B | C | D | F | G | H | I | J | L | M | P | Q | S | T | U | V | X | Z |



# Kryptographie

**Beispielrechnung:**

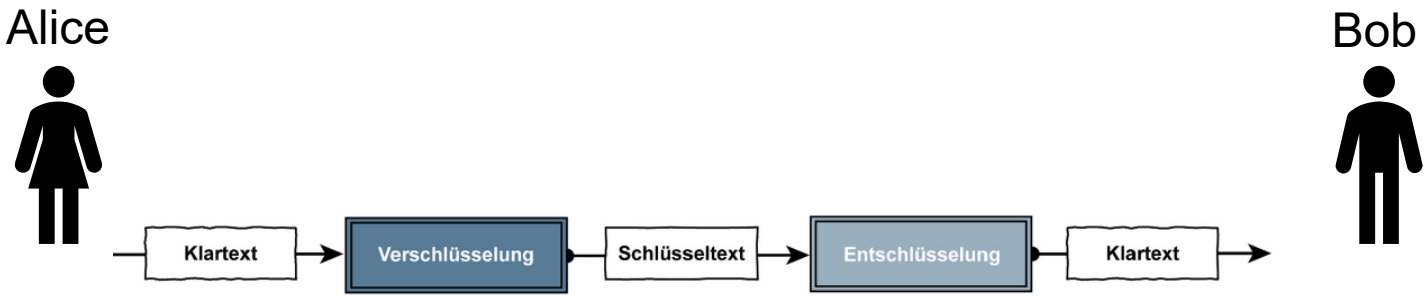
- Schlüssellänge 128 Bit
- Rechner des Angreifers schafft 3mio Schlüsselversuche



# Kryptographie

**Beispielrechnung:**

- Schlüssellänge 128 Bit
- Rechner des Angreifers schafft 3mio Schlüsselversuche
- 1000 Rechner stehen dem Angreifer zur Verfügung
- Schlüsselraum $S = 2^{128} \approx 3{,}4 \cdot 10^{38}$

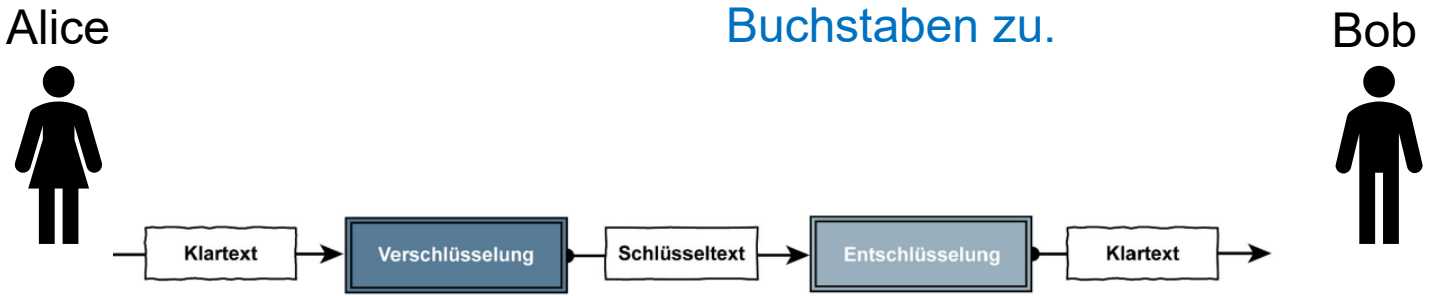


# Kryptographie

**Beispielrechnung:**

- Schlüssellänge 128 Bit
- Rechner des Angreifers schafft 3mio Schlüsselversuche
- 1000 Rechner stehen dem Angreifer zur Verfügung
- Schlüsselraum $S = 2^{128} \approx 3{,}4 \cdot 10^{38}$

Wir lassen 2 Buchstaben zu.



# Kryptographie

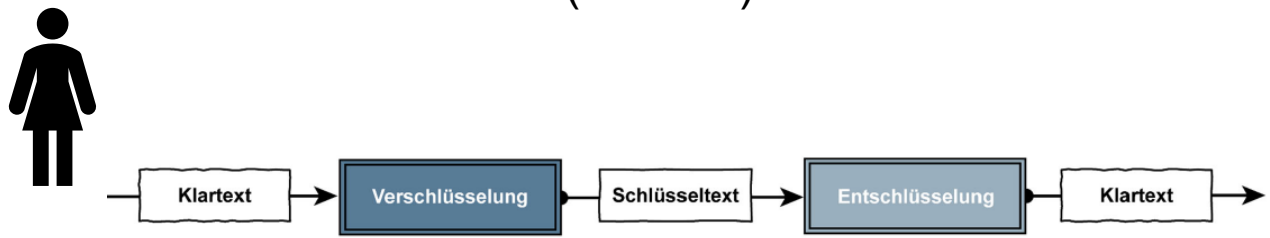
**Beispielrechnung:**

- Schlüssellänge 128 Bit
- Rechner des Angreifers schafft 3mio Schlüsselversuche *a*
- 1000 Rechner stehen dem Angreifer zur Verfügung *b*
- Schlüsselraum $S = 2^{128} \approx 3{,}4 \cdot 10^{38}$
- Ein Jahr hat 31.557.600 Sekunden *c*

Alice

Dauer= S / (a · b · c)

Bob



# Kryptographie

Alan Turing

* 23. Juni 1912 in London; † 7. Juni 1954 in Wilmslow, Cheshire

**Beispielrechnung:**

- Schlüssellänge 128 Bit
- Rechner des Angreifers schafft 3mio Schlüsselversuche *a*
- 1000 Rechner stehen dem Angreifer zur Verfügung *b*
- Schlüsselraum $S = 2^{128} \approx 3{,}4 \cdot 10^{38}$
- Ein Jahr hat 31.557.600 Sekunden *c*

Alice

Dauer= S / (a · b · c)

$3{,}6 \cdot 10^{18}$ Jahre

Bob

# Kryptographie

Alan Turing

* 23. Juni 1912 in London; † 7. Juni 1954 in Wilmslow, Cheshire

**Beispielrechnung:**

- Schlüssellänge 128 Bit
- Rechner des Angreifers schafft 3mio Schlüsselversuche *a*
- 1000 Rechner stehen dem Angreifer zur Verfügung *b*
- Schlüsselraum $S = 2^{128} \approx 3{,}4 \cdot 10^{38}$
- Ein Jahr hat 31.557.600 Sekunden *c*