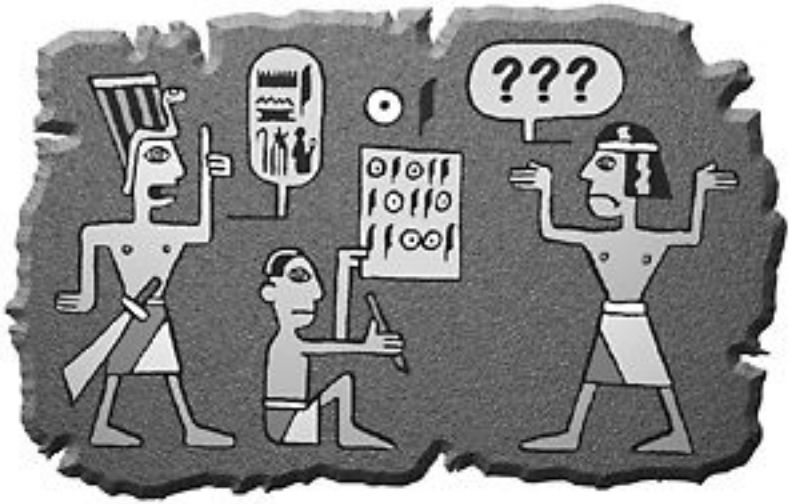
Kryptographische Grundbegriffe



Technisches Seminar SS 2012

Nam Nguyen

Agenda

- **Einleitung**
- **Terminologie**
  - Kryptographie
  - Kryptoanalyse
  - Kryptologie
  - Kryptographischer Algorithmus
  - Kryptographische Verfahren
- **Ziele**
  - Vertraulichkeit
  - Integrität
  - Authentizität

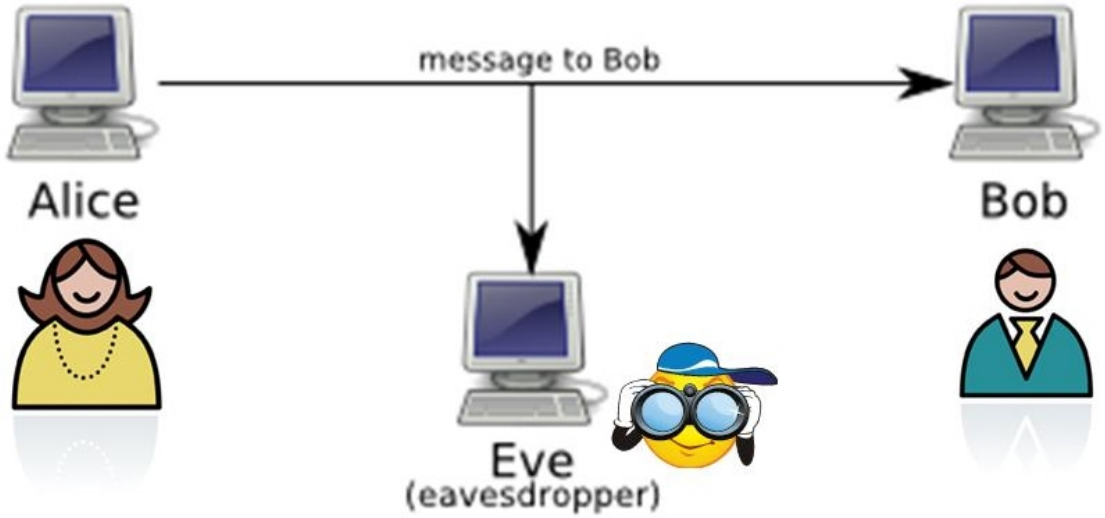
Agenda

- **Chiffrierungsmethoden**
  - Substitution
  - Transposition
- **Zusammenfassung**

Einleitung

Kommunikationsszenario

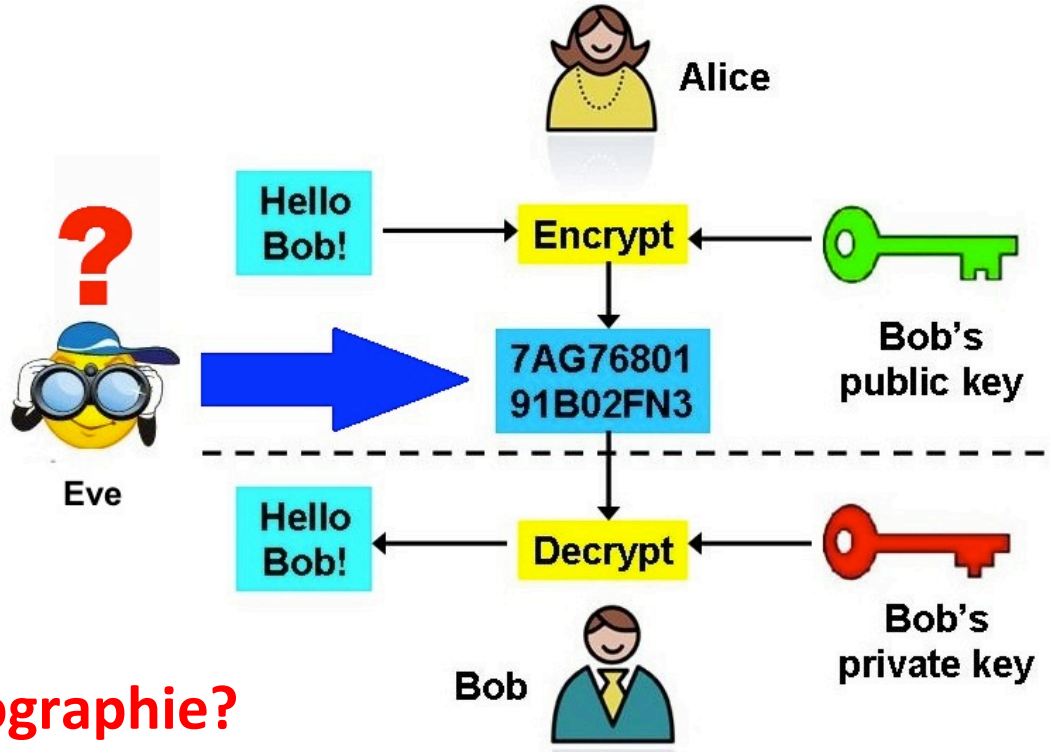
- Alice und Bob kommunizieren via E-Mail miteinander
  - Gesprächsinhalt soll geheim bleiben
- Eve hört die Leitung ab
  - **Unsichere Leitung**



Einleitung

Kommunikationsszenario

- Alice und Bob *verschlüsseln* Ihre Texte mithilfe eines *Schlüssels*
  - Eve versteht den Inhalt der Nachricht nicht
  - **Sichere Leitung**

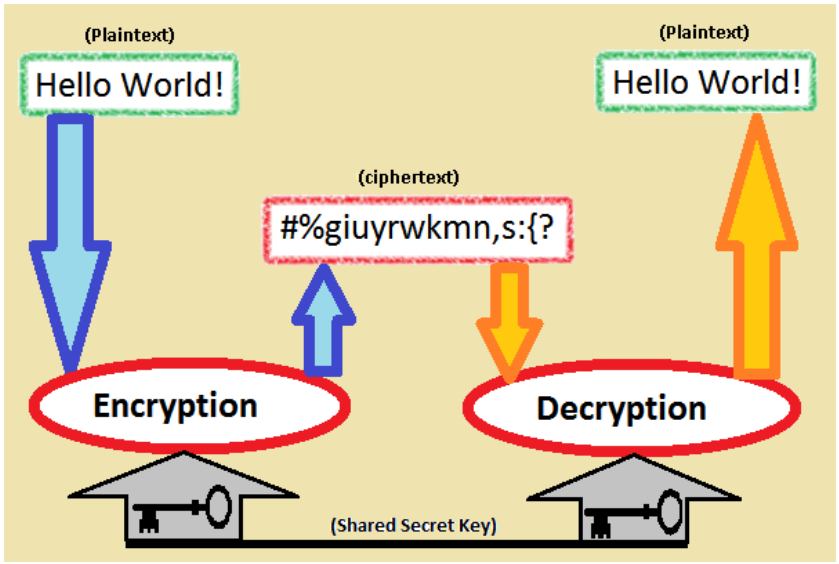


Was ist nun Kryptographie?

Terminologie

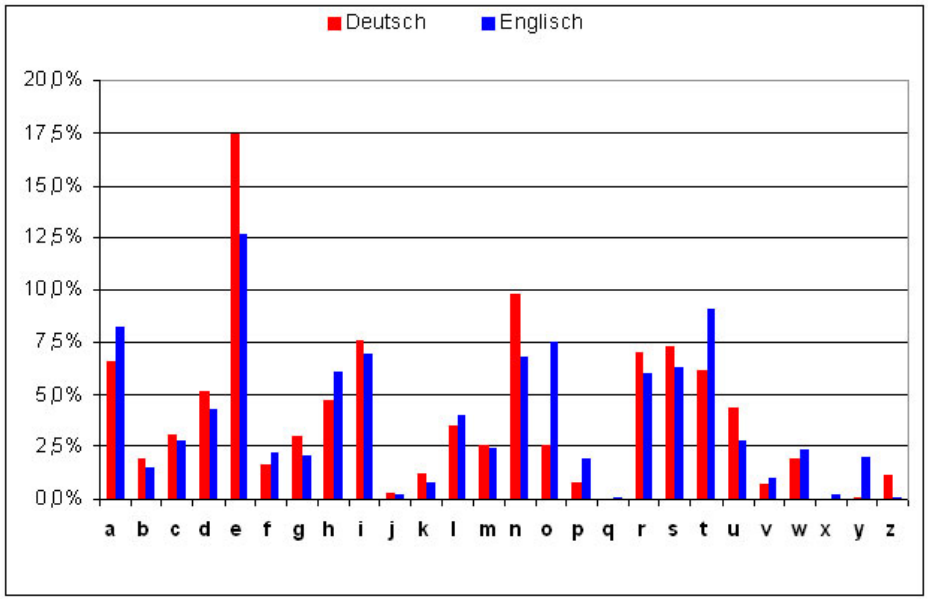
„Unter **Kryptographie** versteht man die Lehre von den Methoden der Verschlüsselung und der Entschlüsselung [von Nachrichten]“

- Sender und Empfänger
- Klartext (plaintext P)
- Verschlüsselung (encryption E)
- Chiffretext (ciphertext C)
- Entschlüsselung (decryption D)



Terminologie

„**Kryptoanalyse** ist die Wissenschaft vom Entschlüsseln von Nachrichten durch unauthorisierte Mithörer“



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
D	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

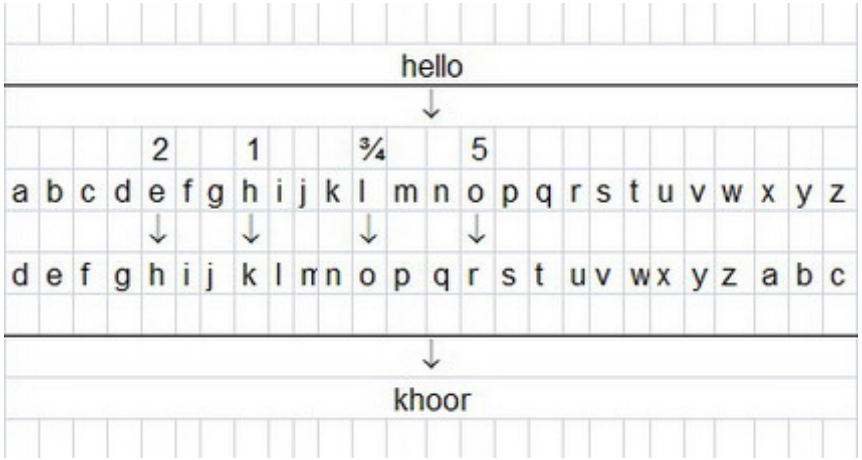
Terminologie

„Die **Kryptologie** schließlich fast die Disziplinen Kryptographie und Kryptoanalyse zusammen“

Terminologie

Kryptographischer Algorithmus

(Auch Chiffrierung) ist die mathematische Funktion, die zur Ver- und Entschlüsselung verwendet wird.



e = encryption (Verschlüsseln)

d = decryption (Entschlüsseln)

k = Schlüssel

k = 3

x = hello

Es muss immer gelten: $d_K(e_K(x)) = x$

e_3 (x = hello) = khoor

d_3 (khoor) = hello

Terminologie

Kryptographische Verfahren

- Codesystem
  - Ganze Wörter, Phrasen, Sätze werden mithilfe eines *Codebuchs* in entsprechenden Chiffretext verschlüsselt
  - Beispiel:

Dackel* = *Agriff in der Dämmerung

Terminologie

Kryptographische Verfahren

- Kryptosystem
  - Fünftupel mit folgenden Eigenschaften
    - P ist eine endliche Menge von Klartexten (‚*plaintext'*)
    - C ist eine endliche Menge von Chiffretexten (‚*ciphertext*')
    - K (‚*keyspace*') ist eine endliche Menge von Schlüsseln
    - E (‚*encryption*') sind die Verschlüsselungsfunktionen (je eine, e_K , pro Schlüssel $k \in K$)
    - D (‚*decryption*') sind die Entschlüsselungsfunktionen (je eine, d_K , pro Schlüssel $k \in K$)
    - Es muss gelten: $d_K (e_K (x)) = x$, für jeden Klartext x und Schlüssel k

Terminologie

Kryptographische Verfahren

- Kryptosystem
  - Beispiel (Caesar Codierung):
    - P = {a,b,...,z}
    - C = {A,B,...,Z}
    - K = {K | 0≤K≤25}
    - $e_{K=3}$ (s) = V
    - $d_{K=3}$ (V) = s

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
D	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

  - Symmetrische und asymmetrische Kryptosysteme

Ziele

Wie kann man Nachrichten vor Fremden geheim halten?

Wie kann man also Vertraulichkeit erreichen?

Wie kann man Texte und Daten vor unerlaubte Manipulation schützen?

Wie sichert man also die Integrität von Texten und Daten?

Wie kann man vermeiden, dass der Urheber einer Nachricht eine falsche Identität vorspiegelt?

Wie lässt sich also die Authentizität einer Nachricht sicherstellen?

Ziele

Vertraulichkeit

Wie kann Alice eine Mitteilung an Bob senden, ohne dass Eve sie liest?

Wie kann Bob seine Daten so aufbewahren, dass Eve auch nach vielen Jahren keinen Zugriff darauf erlangen kann?

Ziele

Integrität

Wie kann Alice Bob eine Nachricht so schicken, dass er sicher erkennen kann, ob sie von jemandem verändert worden ist?

Ziele

Authentizität

Wie kann Bob sicher sein, dass diese Botschaft wirklich von Alice stammt und nicht etwa von jemand anderem frei erfunden worden ist?

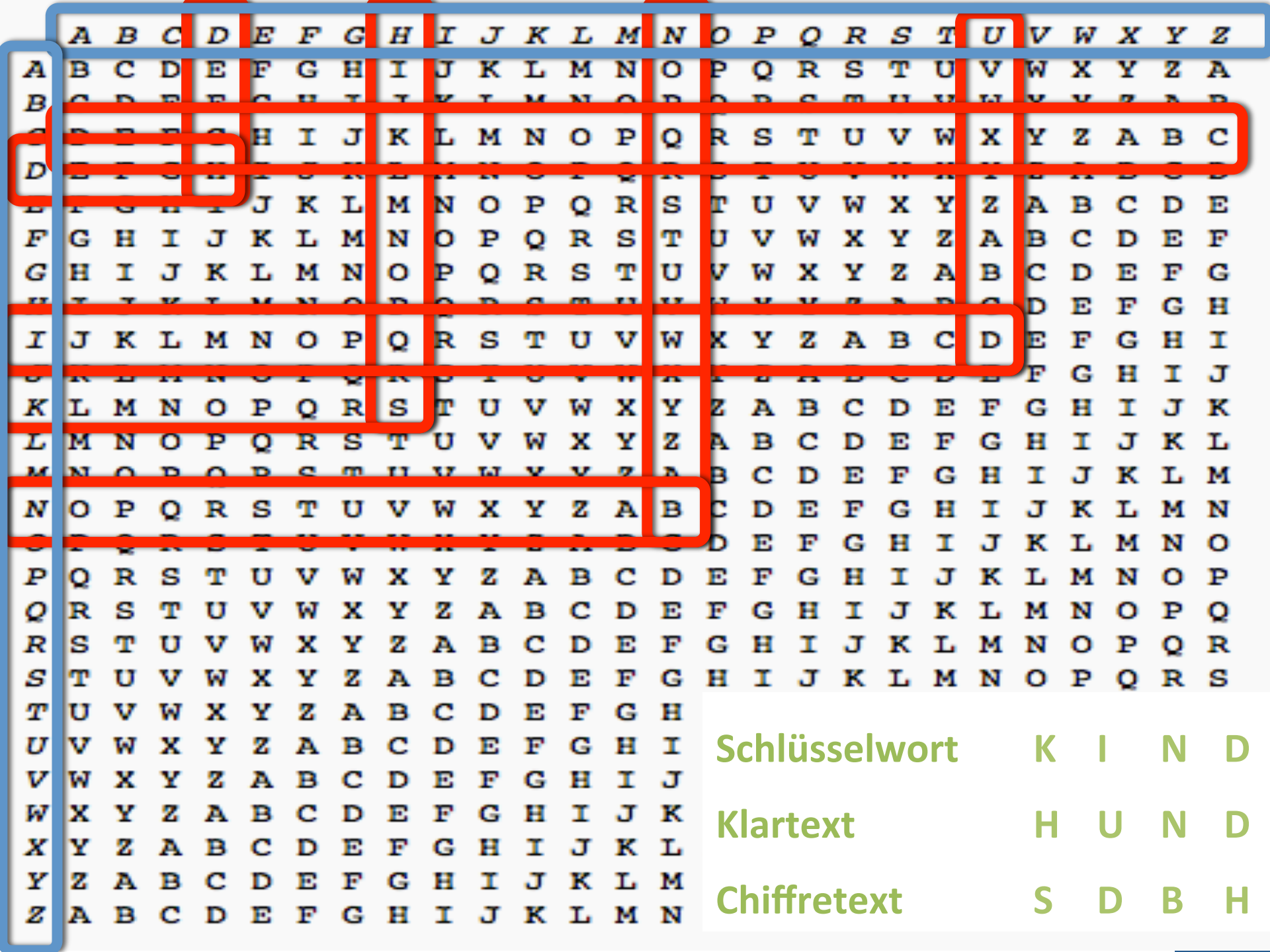
Wie kann Bob sicherstellen, dass Alice nicht später einmal leugnet, dass sie Bob diese Botschaft gesendet hat?

Chiffrierungsmethoden

Substitution

- Ersetzt jedes Zeichen des Klartextes einzeln durch ein fest zugeordnetes Zeichen des Chiffretextes

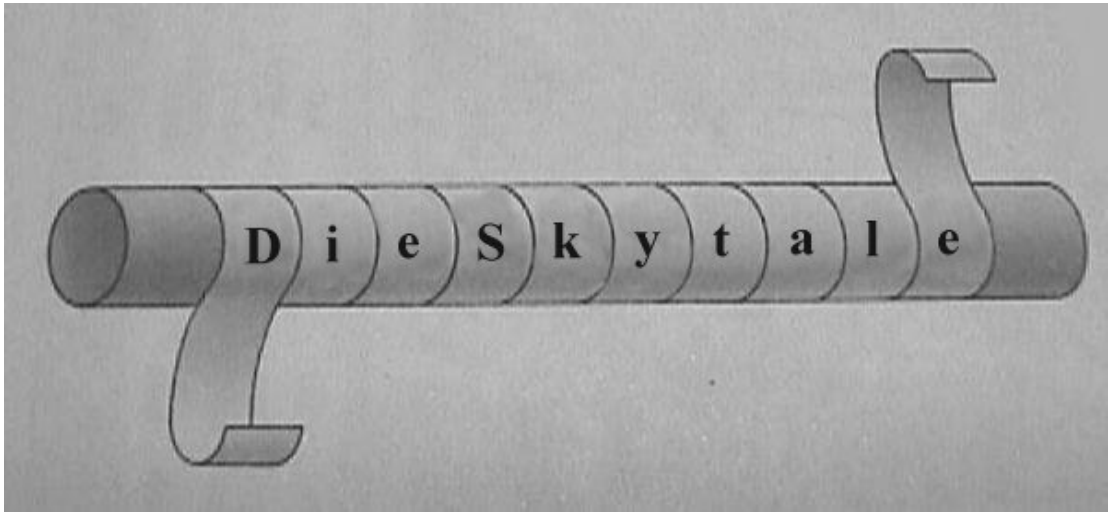
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C


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
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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 A B C D E F G H
U V W X Y Z A B C D E F G H I
V W X Y Z A B C D E F G H I J
W X Y Z A B C D E F G H I J K
X Y Z A B C D E F G H I J K L
Y Z A B C D E F G H I J K L M
Z A B C D E F G H I J K L M N
Schlüsselwort K I N D
Klartext H U N D
Chiffretext S D B H

Chiffrierungsmethoden

Transposition

- Änderung der Anordnung der Zeichen des Klartextes

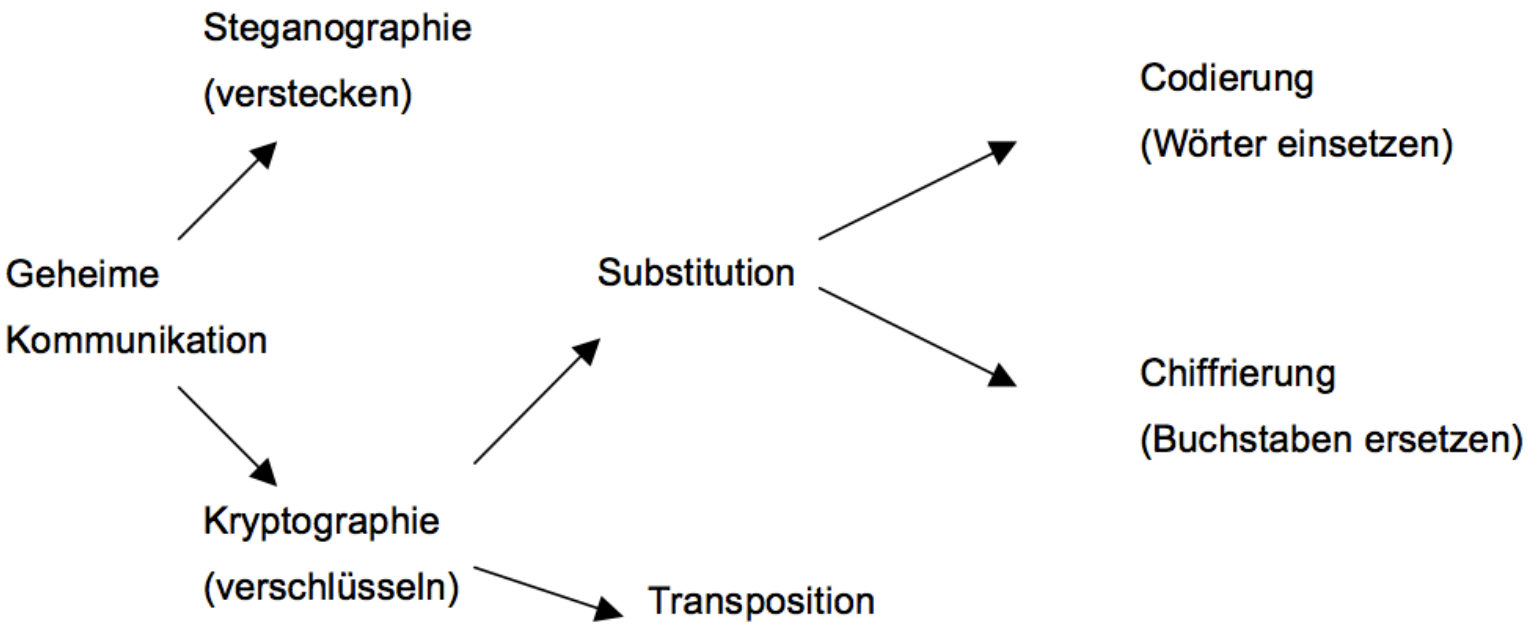


Klartext: ANGRIFF IM MORGENGRAUEN!

Schlüssel: 4 cm

Chiffretext: AIMGRENFMEANGFONU!RIRG

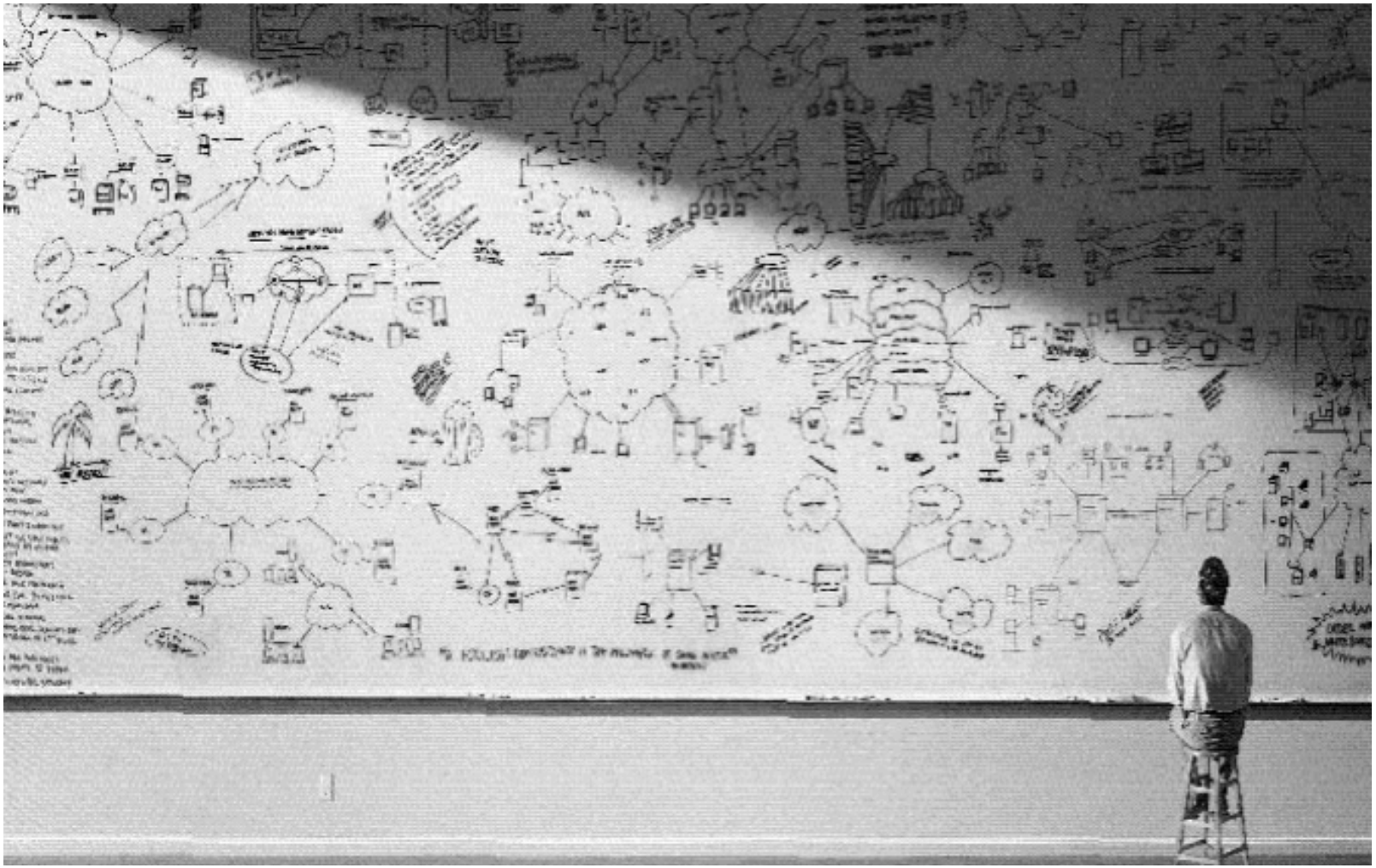
Zusammenfassung



Ziele:

1. Vertraulichkeit
2. Integrität
3. Authentizität

Fragen?



Vielen Dank für Ihre Aufmerksamkeit!