

# IT-Sicherheit

- Sicherheit vernetzter Systeme -

## Kapitel 4: Grundlagen der Kryptologie

# Inhalt

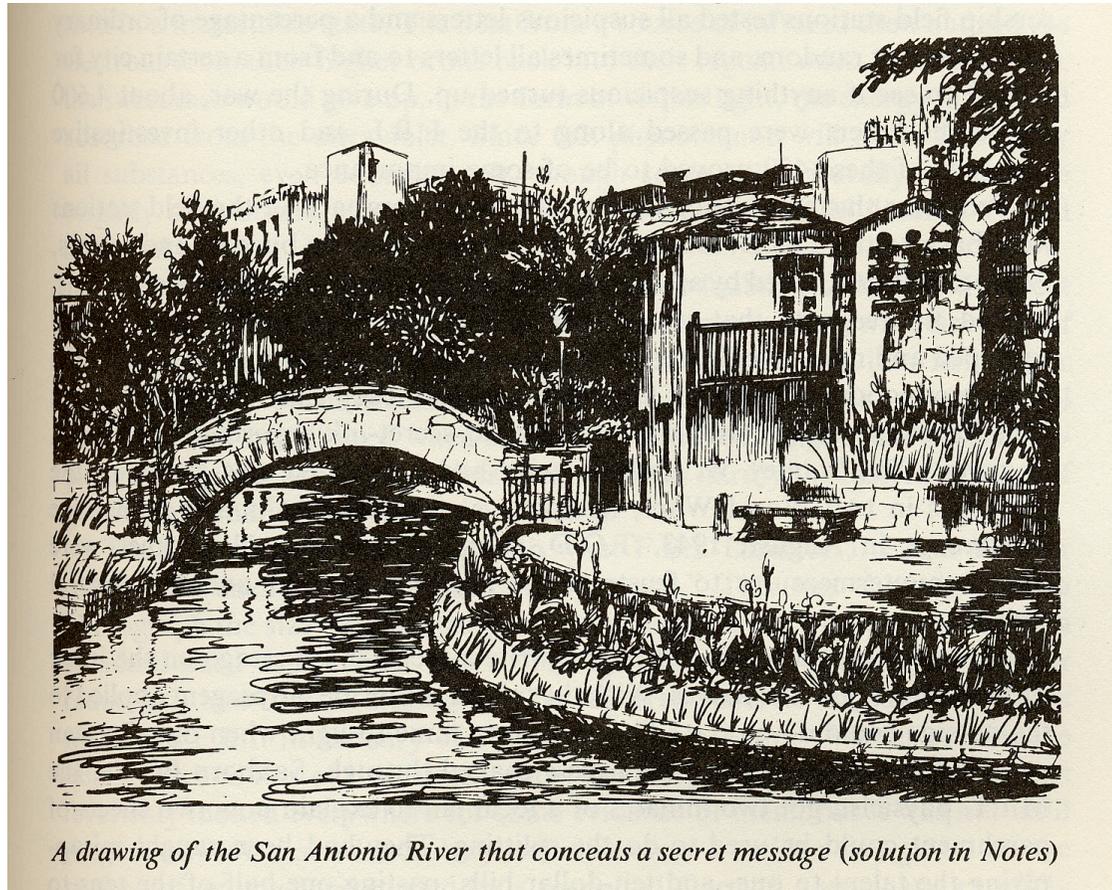
1. Kryptologie: Begriffe, Klassifikation
2. Steganographie
3. Kryptographie, Begriffe und Definitionen
  - Kryptosystem
  - Substitution
  - Permutation
  - Symmetrische versus asymmetrische Kryptosysteme
  - Kryptoanalyse
  - Abschätzung Brute-Force Angriff

# Kryptologie: Begriffe, Klassifikation

- **Kryptographie:** Lehre von den Methoden zur Ver- und Entschlüsselung von Nachrichten
- **Kryptoanalyse, Kryptanalyse:** Wissenschaft von den Methoden zur Entschlüsselung ohne im Besitz den Schlüssels zu sein (Angriffe auf Kryptographische Verfahren)
- **Kryptologie** = Kryptographie + Kryptoanalyse
- **Kryptographische Protokolle:** Protokolle, die kryptographische Techniken verwenden, um z.B. Schlüssel auszutauschen, Kommunikationspartner zu authentisieren, ....
- **Steganographie** (verdecktes Schreiben): Methoden die bereits die Existenz der geheimen Nachricht verbergen (geheime Nachricht in anderen nicht geheimen „Nachrichten“ verbergen)  
Unterscheidung in **linguistische** und **technische** Steganographie

# Linguistische Steganographie

- **Semagramme:** Nachrichten, die in **Details** von Schriften oder Bildern verborgen sind.
- Bsp. aus David Kahn: *The Codebreakers*, Scribner, 1996



- Wo verbirgt sich die Nachricht?
- Wie lautet diese?

# Linguistische Steganographie (Forts.)

## ■ Maskierung (Open Code):

Nachricht verborgen in offen übertragener, unverfänglicher Nachricht

(z.B. Husten in „Wer wird Millionär“)

- **Stichworte:** Begriff, Satzteil oder Satz mit vorher vereinbarter Bedeutung;  
z.B. *HIGASHI NO KAZE AME* („Ostwind, Regen“) im japanischen Wetterbericht - zwei mal wiederholt - sollte „Krieg mit USA“ bedeuten

## ■ Jargon, Millieu Code:

Sondersprachen oder Sonderzeichen beruflicher oder gesellschaftlicher Art

- Bettler, Vagabunden und Gauner:  
Rotwelsch (Deutschland), Argot (Frankreich), ...  
z.B. „Schnee“ für Kokain; „Kies“ für Geld; „abstauben“ ,.....

Für Zensoren durch „gestelzte“ Sprache relativ leicht erkennbar

# Technische Steganographie

- Herodot (490 v.Chr.): Nachricht auf den rasierten Schädel eines Sklaven tätowiert
- Alle Arten von „Geheimtinten“
- Steganographie in digitalen Bildern; Beispiele mit `outguess`

Original



Steganographie



# Steganographie in Bildern

- **Cover** = Bild in das die Nachricht eingebettet wird
- Finde redundante Bits im Cover
  - Least Significant Bits
  - „Rauschen“
  - Nahe zusammenliegende Farben
- Kodieren der Nachricht in diesen redundanten Bits
  
- Steganographie führt zu “sehr geringen Veränderungen” im Bild

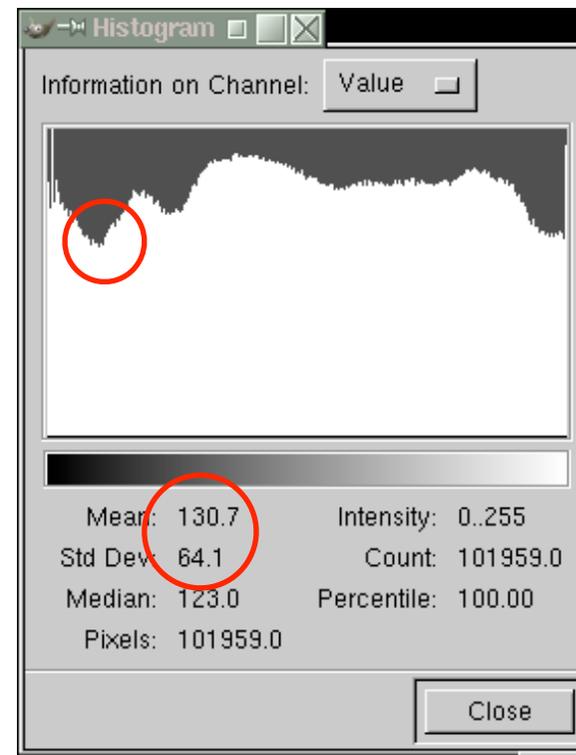
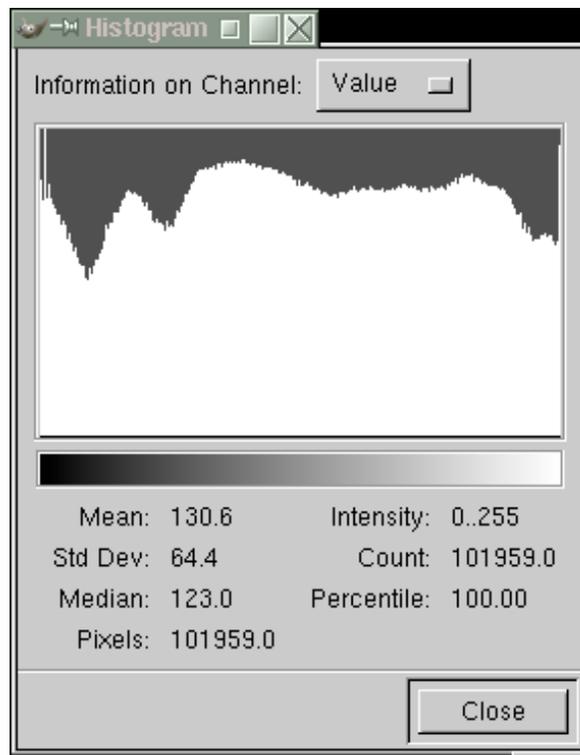
# Steganographie; Veränderungen im Bild

## ■ Histogramm:

Original



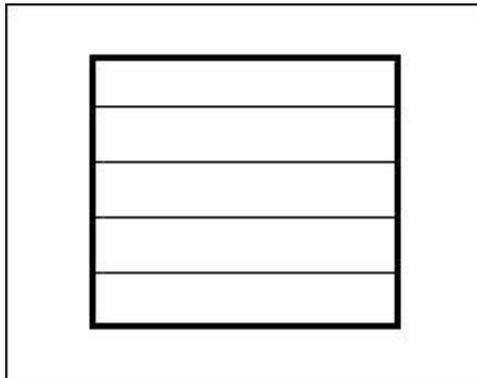
Steganographie



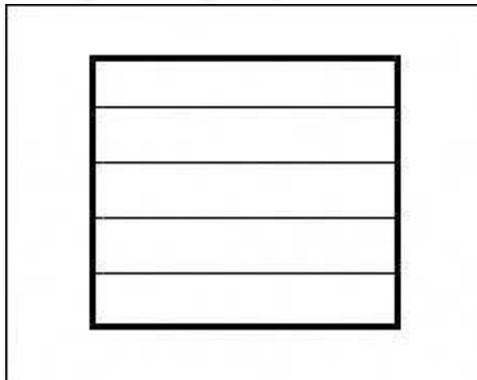
# Steganographie; Merkmale

- Unterschiede bei “sehr strukturierten Bildern” mit hohem versteckten Datenvolumen evtl. erkennbar

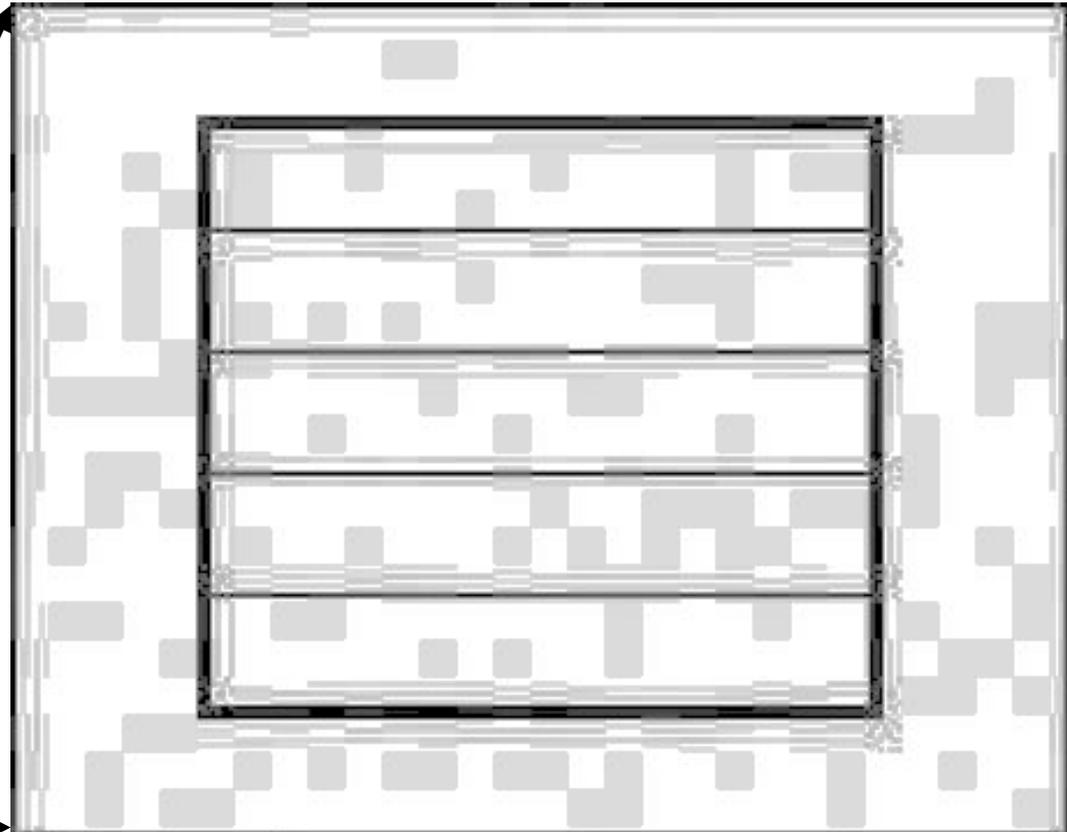
Original



Steganographie



Vergrößerung + (starke) Kontrasterhöhung



# Inhalt

1. Kryptologie: Begriffe, Klassifikation
2. Steganographie
3. Kryptographie, Begriffe und Definitionen
  - Kryptosystem
  - Substitution
  - Permutation
  - Symmetrische versus asymmetrische Kryptosysteme
  - Kryptoanalyse
  - Abschätzung Brute-Force Angriff

# Kryptographie, Begriffe

- **Klartext (Plaintext):** die zu verschlüsselnde Nachricht
- **Geheimtext (Ciphertext):** verschlüsselte Nachricht
- **Verschlüsselung, Chiffrierung (Encryption):** Vorgang der Klar- in Geheimtext überführt
- **Entschlüsselung, Dechiffrierung (Decryption):** Überführung von Geheim- in Klartext
- **Chiffriersystem (Cryptographic Algorithm, Cipher):** Algorithmisches Verfahren zur Ver- bzw. Entschlüsselung
- Benötigen **Schlüssel (Key)**



# Kryptographisches System (Def.)

- Geg. zwei endliche Zeichenvorräte (Alphabete)  $A_1$  und  $A_2$
- Ein Kryptosystem (KS) ist gegeben durch ein Tupel

$$KS = (M, C, EK, DK, E, D)$$

1. Nicht leere endliche Menge von Klartexten  $M \subseteq A_1^*$  mit  $A_1^*$  Menge aller Worte über dem Alphabet  $A_1$
2. nicht leere endliche Menge von Krypto- bzw. Chiffrentexten  $C \subseteq A_2^*$
3. der nicht leeren Menge von Verschlüsselungsschlüsseln  $EK$
4. der nicht leeren Menge von Entschlüsselungsschlüsseln  $DK$  sowie einer Bijektion  $f: EK \rightarrow DK$  Diese assoziiert zu jedem Verschlüsselungsschlüssel  $K_E \in EK$  einen dazu passenden Entschlüsselungsschlüssel  $K_D \in DK$ , d.h.  $f(K_E) = K_D$

# Kryptographisches System (Def.); Forts.

## ■ Kryptosystem (KS)

$$KS = (M, C, EK, DK, E, D)$$

5. Dem injektiven Verschlüsselungsverfahren

$$E : M \times EK \rightarrow C$$

6. Dem Entschlüsselungsverfahren

$$D : C \times DK \rightarrow M$$

mit der Eigenschaft, dass für zwei Schlüssel  $K_E \in EK$  und  $K_D \in DK$  mit  $f(K_E) = K_D$  gilt:

$$\forall m \in M : D(E(m, K_e), K_d) = m$$

D.h. ein bel. Klartext  $m$  der mit einem Verschlüsselungsschlüssel verschlüsselt wurde, kann mit dem passenden Entschlüsselungsschlüssel wieder entschlüsselt werden

# Kryptosystem, Bsp.: Substitution

- **Substitution:**  $f : A_1^n \rightarrow A_2^m$
- **Alphabete:**  $A_1 = \{a, b, \dots, z\} (= Z_{25})$ ;  $A_2 = \{1, 2, 3, 4, 5\}$
- **Verschlüsselungsverfahren:**  $E : A_1^1 \rightarrow A_2^2$
- **Schlüssel**  $K_E = K_D$

	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

- **Bsp.:**  
421142133243543451 = `iailhouse` (Jailhouse)

# Kryptosystem, Bsp.: Permutation

- **Permutation** als Spezialfall der Substitution:  $f : A^n \rightarrow A^n$   
gleiche Wortlänge; gleiche Alphabete  $A_1 = A_2 = \{a, b, \dots, z\}$
- $K_E = K_D$  (NEWYORK, 1) (+ Alg. zur Anwendung)  
(Zur besseren Lesbarkeit, werden Chiffrentexte trotzdem oft in Großbuchstaben dargestellt.)

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

## Zyklenschreibweise:

(a,n,h) (b,e,o,i) (c,w,u,s,p,j) (d,y,x,v,t,q,l,f,r,m,g,k)

- Bsp.:  
QAOWI YOEMO NDOMP = thecodebreakers  
Chiffrentext wird in Blöcken übertragen  
Leer- und Satzzeichen werden nicht kodiert (Leerzeichen noch häufiger als „e“)

# Kryptosystem: Symmetrische Verfahren

- Ver- und Entschlüsselungsschlüssel gleich, oder leicht voneinander ableitbar
- Kommunikationspartner teilen **gemeinsamen, geheimen Schlüssel (symmetrisch)**
- Setzt vorherige Verständigung (**Schlüsselaustausch**) voraus

- Protokoll:

1. Alice und Bob vereinbaren („**out of band**“) gemeinsamen Schlüssel:

$$K_E = K_D = K_{A,B}$$

2. Alice verschlüsselt  $m$ :  $C = E(m, K_{A,B})$  und sendet  $C$  an Bob

3. Bob entschlüsselt  $C$ :

$$m = D(C, K_{A,B}) = D(E(m, K_{A,B}), K_{A,B})$$

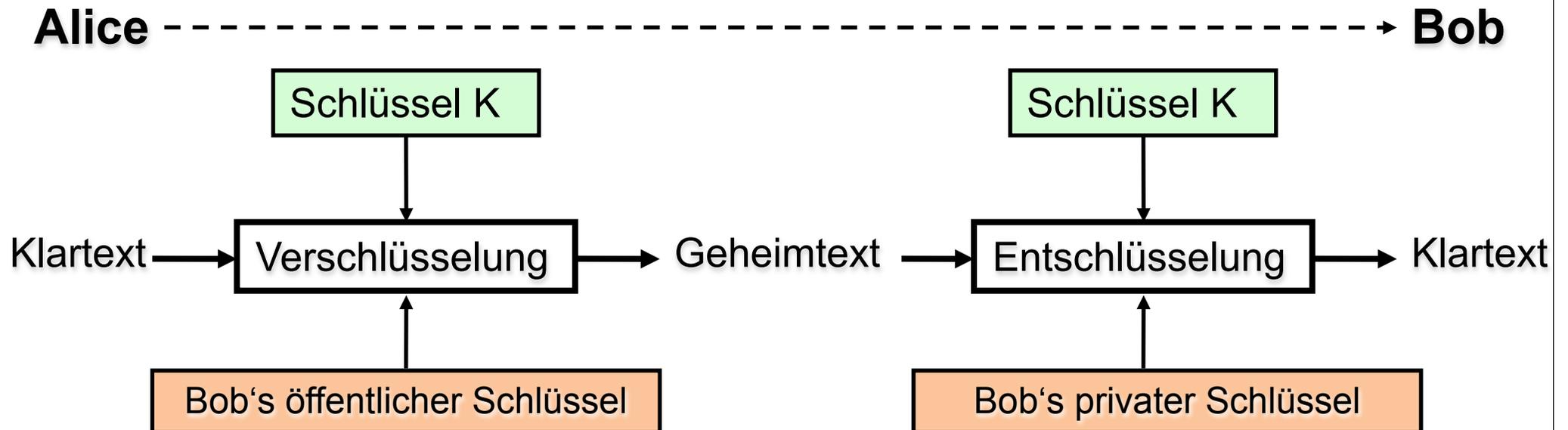
- Beispiele: DES, AES, IDEA,.....

# Kryptosystem: Asymmetrische Verfahren

- Jeder Partner besitzt **Schlüsselpaar** aus
  - persönlichem, **geheim** zu haltendem **Schlüssel** (*private key*)  
(wird NIE übertragen)
  - und **öffentlich** bekannt zu gebendem **Schlüssel** (*public key*)  
(kann über unsichere und öffentliche Kanäle übertragen werden)
- Protokoll:
  1. Alice und Bob erzeugen sich Schlüsselpaare:
$$(K_E^A, K_D^A); (K_E^B, K_D^B)$$
  2. Öffentliche Schlüssel werden öffentlich zugänglich gemacht
  3. Alice will  $m$  an Bob senden; dazu benutzt sie B's öffentlichen Schlüssel
$$C = E(m, K_E^B)$$
  4. Bob entschlüsselt die Nachricht mit seinem privaten Schlüssel:
$$m = D(C, K_D^B) = D(E(m, K_E^B), K_D^B)$$
- Bsp.: RSA, ElGamal,...

# Vergleich Symmetrische / Asymmetrische Verfahren

	Symmetrisch	Asymmetrisch
Schlüsselaustausch	Sicherer Kanal erforderlich	öffentlich
Schlüssellänge	128 bis 256 Bit	1024 bis 4096 Bit
Geschwindigkeit		Faktor 100 bis 1000 langsamer



# Kryptoanalyse

- Wissenschaft von Methoden zur Entschlüsselung **ohne** Schlüssel
- Klassen kryptographischer Angriffe:
  - **Brute force; exhaustive search:** vollständiges Durchsuchen des Schlüsselraumes
  - **Klartext Angriff (ciphertext-only):** Dem Analytiker stehen mehrere Chiffren zur Verfügung. Ziel: Schlüssel und/oder Klartext berechnen
  - **Bekannter Klartext (known-plaintext):** Analytiker kennt Klartext-/Chiffren-Kombinationen die mit selbem Schlüssel verschlüsselt wurden. Ziel: Schlüssel brechen oder Algorithmus der jede mit dem Schlüssel verschlüsselte Nachricht entschlüsseln kann
  - **Gewählter Klartext (chosen-plaintext):** Analytiker kann selber Klartexte wählen und diese verschlüsseln lassen.
  - **Gewählte Chiffre (known-ciphertext):** Angreifer kann sich zu ausgewählten Chiffren, den Klartext berechnen lassen
- Weitere Informationen: Vgl. F.L. Bauer: Entzifferte Geheimnisse

# Einschub: Abschätzung Brute-Force Angriff

- Der Schlüssellänge sei 128 Bit
- Ihr Rechner ist in der Lage 50.000 Verschlüsselungsoperationen pro Sekunde durchzuführen
- Wie viele Jahre dauert ein Brute-Force-Angriff?
- Schlüsselraum  $S = 2^{128} \approx 3,4 \cdot 10^{38}$   
340.282.366.920.938.463.463.374.607.431.768.211.456
- 1 Jahr hat rund 31.536.000 Sekunden
- $(S / 50.000) / 31.536.000$  Sekunden  $\approx 2 \cdot 10^{27}$   
215.805.661.416.120.283.779.410.583,099802 Jahre
- Wieviele Schlüssel müssen Sie pro Sek. berechnen um „nur“ 100 Jahre zu brauchen?
- $\sim 107.902.830.708.060.141.889.705.291.549,901$   
 $\approx 1,1 \cdot 10^{30}$