



# Kryptographie: Einführung

Symmetrische und asymmetrische Systeme  
Verschlüsselung und Authentikation  
Schlüsselverteilung und Schlüssellängen



Universität Hamburg  
DER FORSCHUNG | DER LEHRE | DER BILDUNG

## Kriterien zur Einteilung von Kryptosystemen

- Kryptographische Basisbausteine
  - Konzelationssysteme
  - Authentikationssysteme
  - Hashfunktionen
  - Pseudozufallszahlengeneratoren
- Schlüsselbeziehung Sender–Empfänger
  - Symmetrische Systeme
  - Asymmetrische Systeme
- Alphabet, auf dem die Chiffre operiert
  - Blockchiffre: Operiert auf Blöcken von Zeichen
  - Stromchiffren: Operiert auf einzelnen Zeichen
- Längentreue
- Erreichbare Sicherheit



## Anwendungsfall x Schlüsselbeziehung

	Konzelation (Verschlüsselung)	Authentikation
symmetrische	<i>One-time-pad, DES, Triple-DES, AES, IDEA, A5/1 (GSM), A5/2 (GSM) ...</i> <div> <div>GnuPG/PGP</div> <div>WPA2</div> <div>IPSec</div> <div>SSL/TLS</div> </div>	<i>Symmetrische Authentikationscodes, CCM, A3 (GSM), ...</i> <div> <div>SecurID</div> <div>WPA2</div> <div>IPSec</div> <div>SSL/TLS</div> </div>
asymmetrische	<i>RSA, ElGamal, McEliece, ...</i> <div> <div>GnuPG/PGP</div> <div>HBCI</div> <div>SSL/TLS</div> </div>	<i>RSA, ElGamal, DSA, GMR, ...</i> <div> <div>GnuPG/PGP</div> <div>HBCI</div> <div>SSL/TLS</div> </div>

*Algorithmus*

Anwendung

## Erreichbare Sicherheit

---

- Sicherheit

- (informations) theoretisch sicher
- kryptographisch stark (beweisbar)
  - gegen aktive Angriffe
  - gegen passive Angriffe
- wohluntersucht (praktisch sicher)
  - Chaos
  - Zahlentheorie
- geheim gehaltene

komplexitäts-  
theoretisch  
sicher

- Kerckhoffs-Prinzip

- Die Sicherheit eines kryptographischen Verfahrens soll von der Geheimhaltung des kryptographischen Schlüssels abhängen.
  - Geht zurück auf  
Auguste Kerckhoffs: La Cryptographie militaire, 1883

## Angriffsarten und Sicherheitskriterien

- Was kennt der Angreifer, was kann er wählen oder verändern?

### Ciphertext-only attack

Known  
Adaptively chosen

$$\left. \begin{array}{l} \text{Known} \\ \text{Adaptively chosen} \end{array} \right\} - \left\{ \begin{array}{l} \text{plaintext} \\ \text{ciphertext} \end{array} \right\} \text{ attack}$$

- Adaptively:
  - Der Angreifer kann in Abhängigkeit vorheriger gewählter Nachrichten neue Nachrichten wählen
- Non-adaptively:
  - Der Angreifer muss alle Nachrichten zu Beginn wählen, kann also nicht abhängig vom Verschlüsselungsergebnis, weitere Nachrichten wählen.

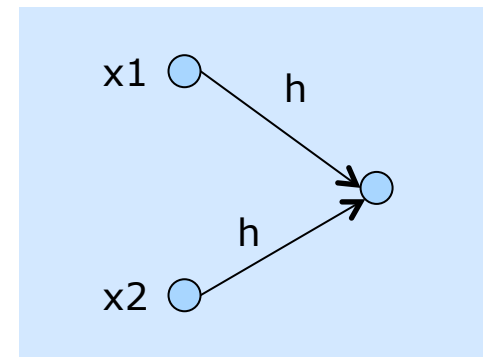
## Angriffsarten und Sicherheitskriterien

---

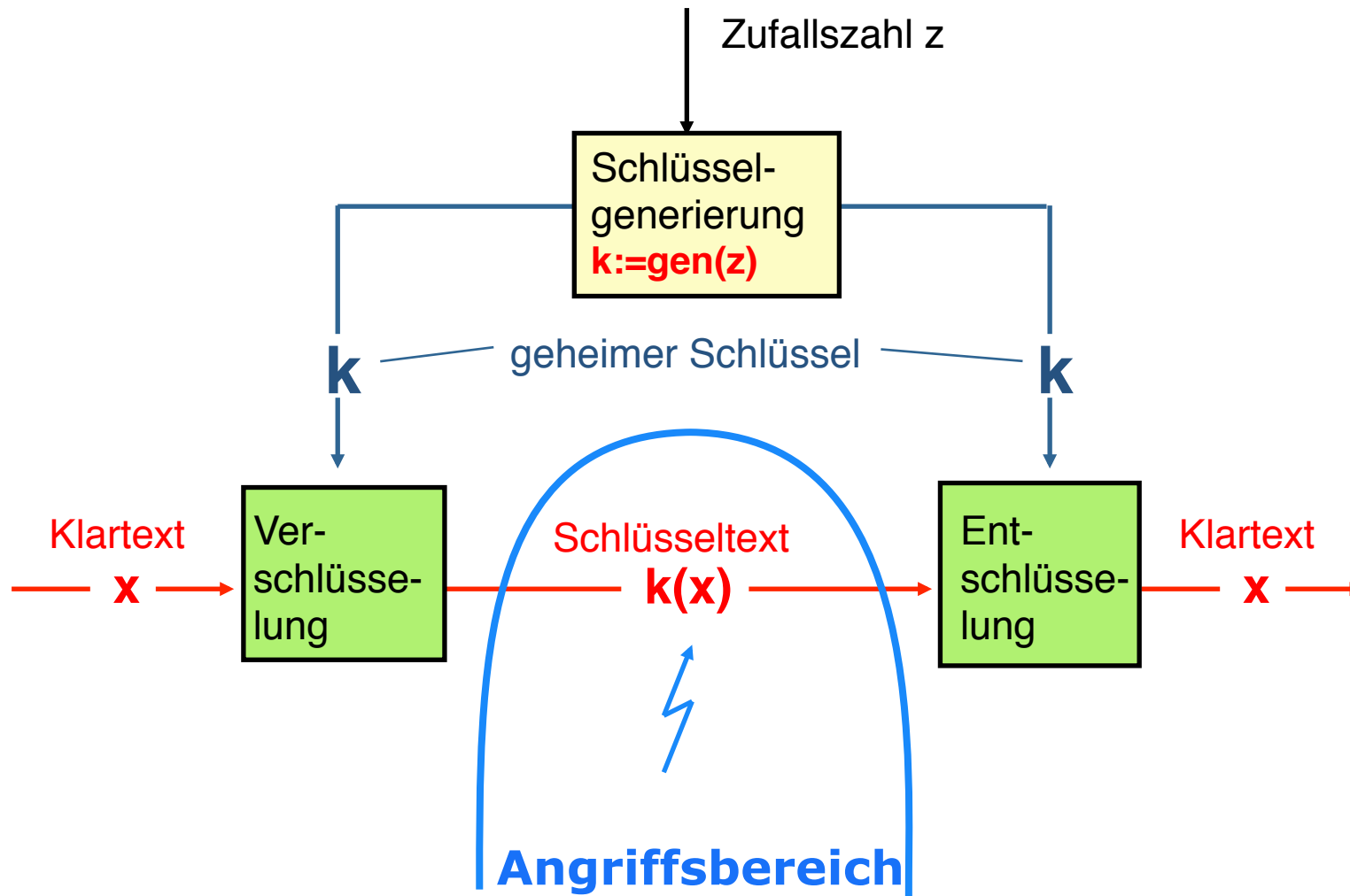
- Was wird durch den Angriff erreicht?  
oder: Brechen = Fälschen | Entschlüsseln
  - Vollständiges Brechen: Finden des Schlüssels
  - Universelles Brechen: Finden eines zum Schlüssel äquivalenten Verfahrens
  - Nachrichtenbezogenes Brechen: Brechen für einzelne Nachrichten, ohne den Schlüssel selbst in Erfahrung zu bringen
    - selektives Brechen: für einen bestimmten vom Angreifer abgefangene Nachricht
    - existenzielles Brechen: für irgendeine Nachricht
  - Aufwand/Kosten:
    - Einmalige Kosten, jeder Schlüssel effizient knackbar
    - Jeder Angriff verursacht Kosten beim Angreifer

## Hashfunktionen

- Abbildung  $h: X \rightarrow Y$ 
  - Einwegfunktion (auch: Falltürfunktion)
  - Umkehrfunktion nicht effizient berechenbar
  
- Hashfunktionen sind verkürzend:
  - Beliebige lange Inputs werden auf Output bestimmter Länge abgebildet (z.B. MD5: 128 Bit)
  
  - Kollision:
    - $h(x_1) = h(x_2)$  mit  $x_1 \neq x_2$



# Symmetrische Verschlüsselung

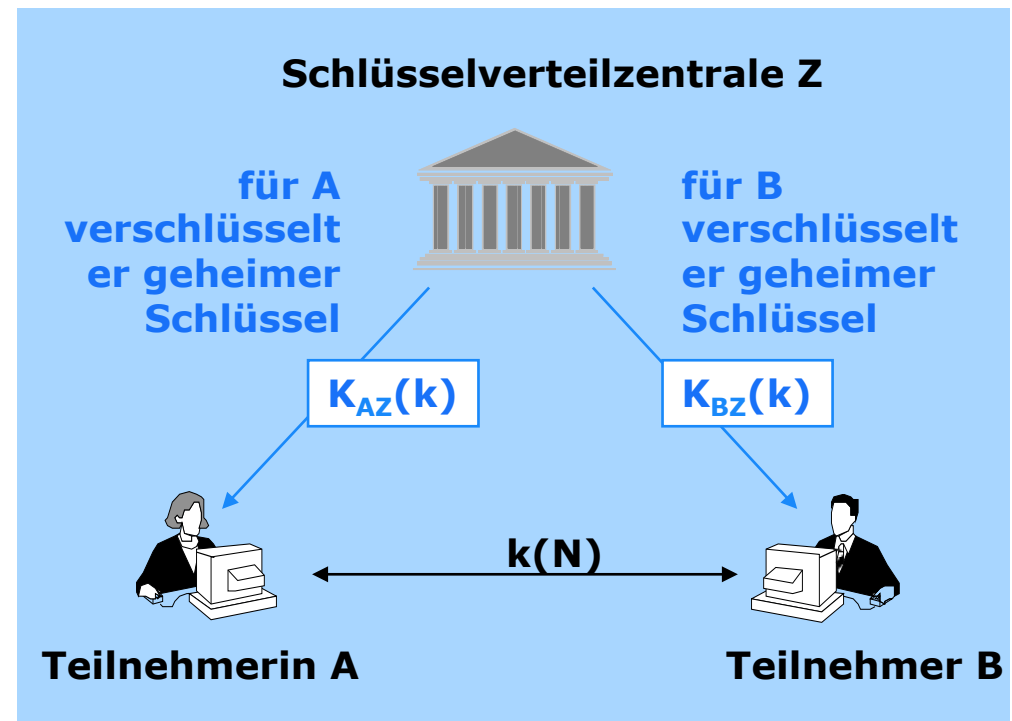


Undurchsichtiger Kasten mit Schloss. Es gibt zwei gleiche Schlüssel.



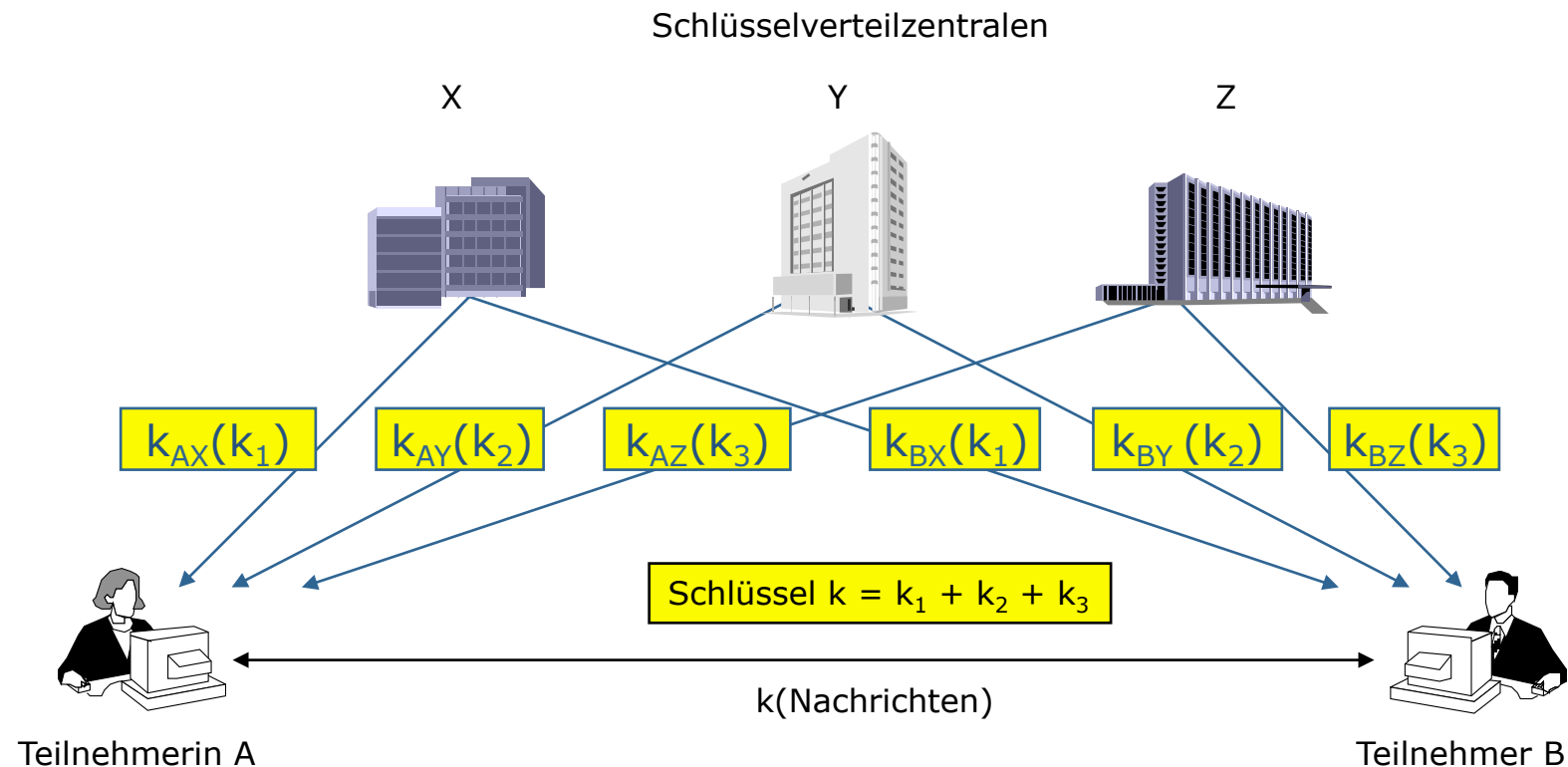
## Schlüsselverteilung für symmetrische Systeme

- Schlüsselaustausch:
  - A und B tauschen zunächst (offline) jeweils symmetrischen Schlüssel mit Z aus:
    - $K_{AZ}$  und  $K_{BZ}$
  - Z generiert auf Anforderung einen symmetrischen Kommunikationsschlüssel  $k$  und verschlüsselt diesen für A und B:
    - $K_{AZ}(k) \rightarrow A$
    - $K_{BZ}(k) \rightarrow B$
  - A und B entschlüsseln  $k$
- Kommunikation:
  - Sender verschlüsselt Nachricht  $N$  mit  $k$ :
    - $k(N)$

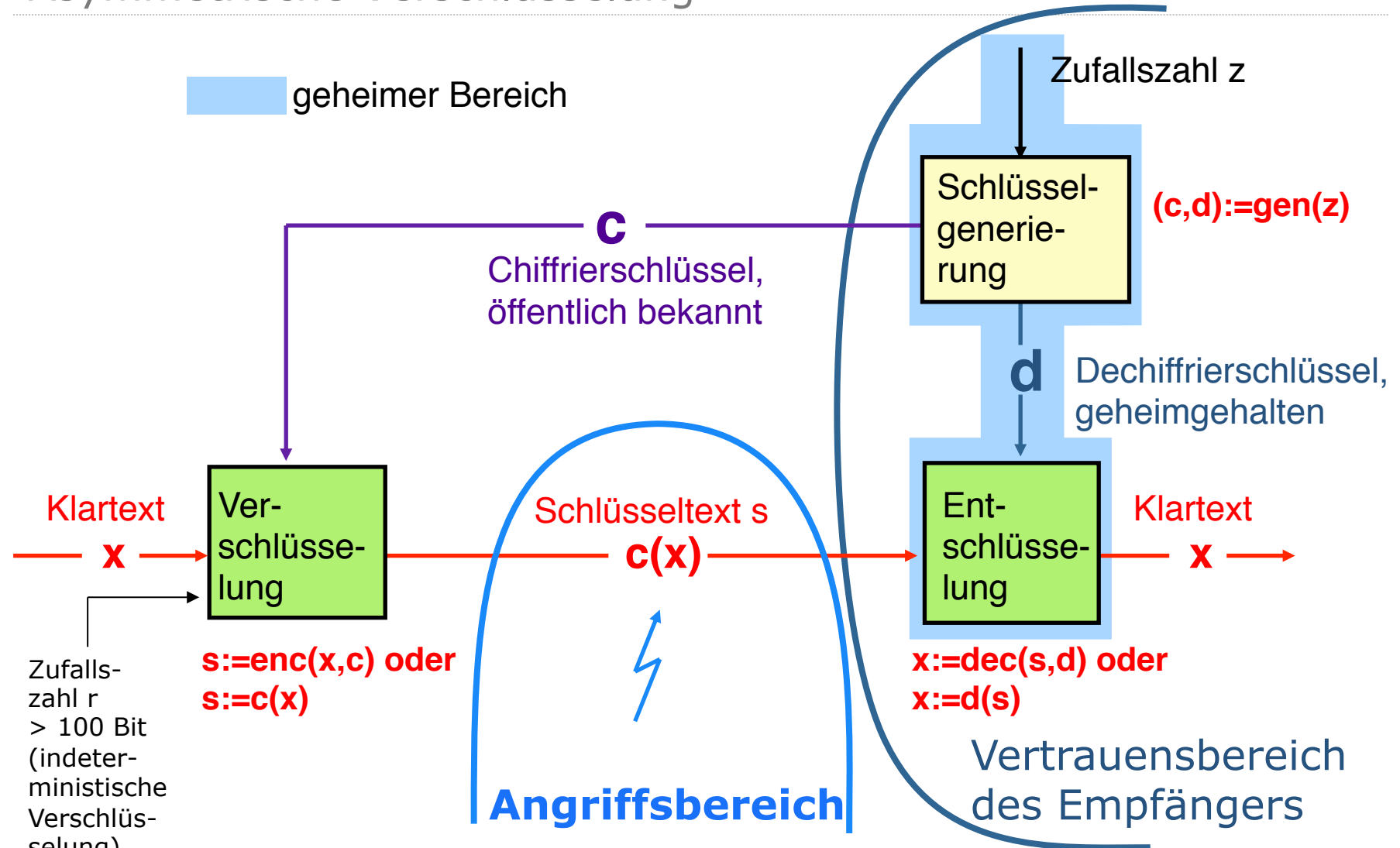


## Dezentralisierte Variante

- Dezentralisierte Schlüsselverteilung ist möglich
- Ziel: Alle beteiligten Schlüsselverteilzentralen müssen zusammen arbeiten, damit sie den Kommunikationsschlüssel  $k$  erfahren
- Überlagerung der Teilschlüssel z.B. mit XOR-Verknüpfung

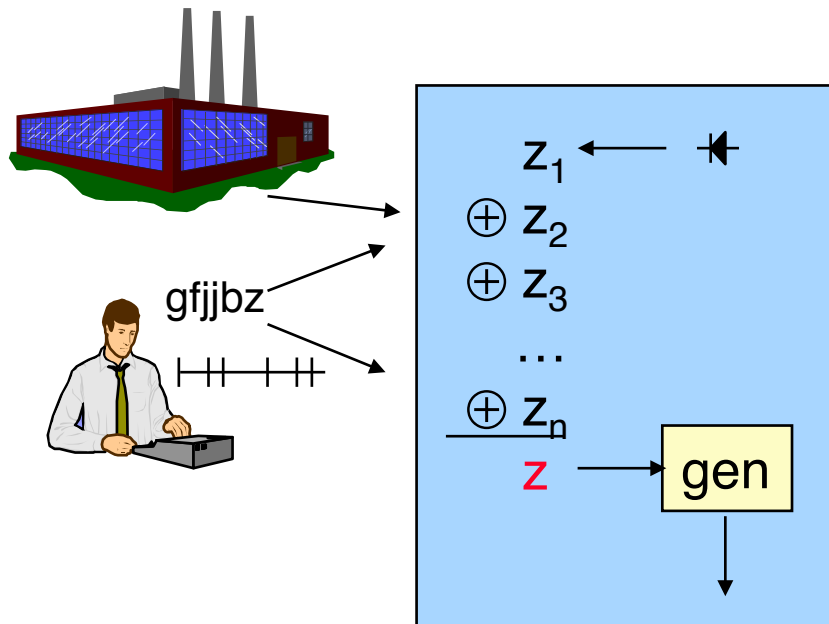


# Asymmetrische Verschlüsselung



Kasten mit Schnappschloss. Es gibt nur einen Schlüssel.

# Schlüsselgenerierung



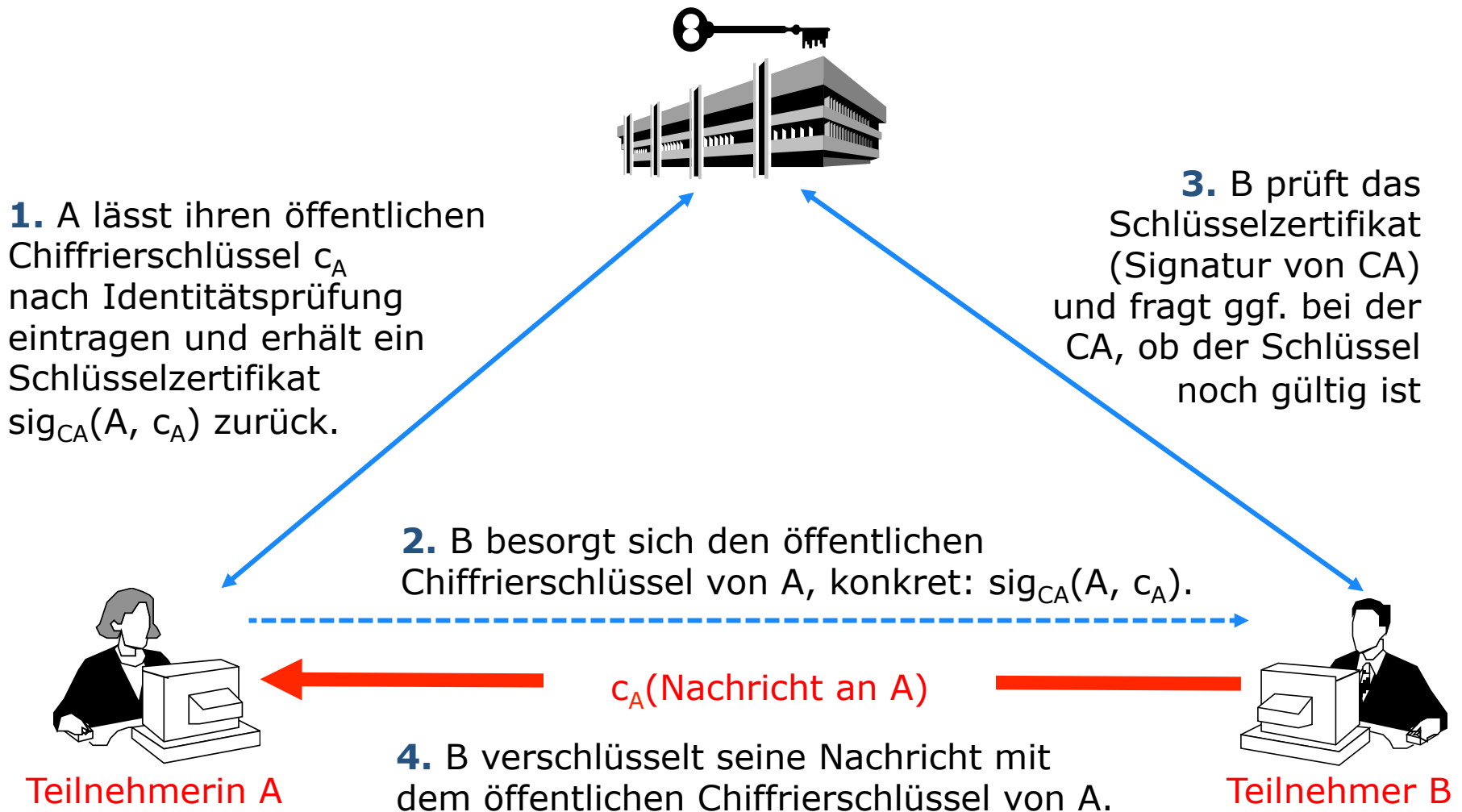
Erzeugung einer Zufallszahl  $z$  für die Schlüsselgenerierung:

XOR aus

- $z_1$ , einer im Gerät erzeugten,
- $z_2$ , einer vom Hersteller gelieferten,
- $z_3$ , einer vom Benutzer gelieferten,
- $z_n$ , einer aus Zeitabständen errechneten.

# Zertifizierung des öffentlichen Schlüssels

## Zertifizierungsstelle (Certification Authority) CA



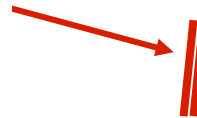
# Warum ist die Schlüsselbeglaubigung so wichtig?

## Alice hat Schlüsselpaar generiert und will ihn veröffentlichen

Alice <alice@abc.de>

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
mQGiBDQyJk0RBADVPjcdvmy0tqsZBt6z4/5M9MYDB
i+dYNnyisQEBXQcH/RGe2i30LRvRk4asX++JSTylku
8LM0lYorgW+lbmsVNxeQsdbSAUfd3d9bI/+fGwQcz
6W8lIw2zyQkfDaF7xPI7oVZUY1I7cqEfTvic003bgL
sUZygtg1nEfxqifxgukKj01066wVmqLnXcbi2XUebka
L0ViFDNkla2aw590ZW59gf5I0eUBevSmydIaliH9Pm
-----END PGP PUBLIC KEY BLOCK-----
```

$c_{\text{Alice}}$



### **Angreifer:**

- hält  $c_{\text{Alice}}$  zurück (blockiert Verteilung)
- generiert selbst Schlüsselpaar  $c_{\text{Mask}}, d_{\text{Mask}}$  unter falschem Namen
- schickt  $c_{\text{Mask}}$  an Bert

$c_{\text{Mask}}$



**Bert besitzt jetzt nicht authentischen Schlüssel von Alice**

Alice <alice@abc.de>

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
OTUAoLncfli6Yit0Kqgp/N9h37uopJHbiQCVAw
xBBPLRdmalP22ij0dARxbJL07u7XOrnyV3b4m0
l4ydpS/ruj9yaY62BwQNMEoGjAnZGA5t3MMGDF
7ZLp1dmFYVYPL4xRfOJ+MF5ifb8RXaDA1+lP8
CwMBAgAKCRDhQCBhSe8dh0YYAJseEURK2o+VsA
u64hb02wuFqlwwq1yb+JAD8DBRA00Ptk7V9cne
-----END PGP PUBLIC KEY BLOCK-----
```

## Maskerade-Angriff (2)

**Bert will Alice eine Nachricht  $N$  schicken**

$c_{\text{Mask}}(N)$

**Angreifer:**

- Weiterleitung verhindern
- entschlüsseln von  $c_{\text{Mask}}(N)$  mit  $d_{\text{Mask}}$
- verschlüsseln von  $N$  mit  $c_{\text{Alice}}$

$c_{\text{Alice}}(N)$

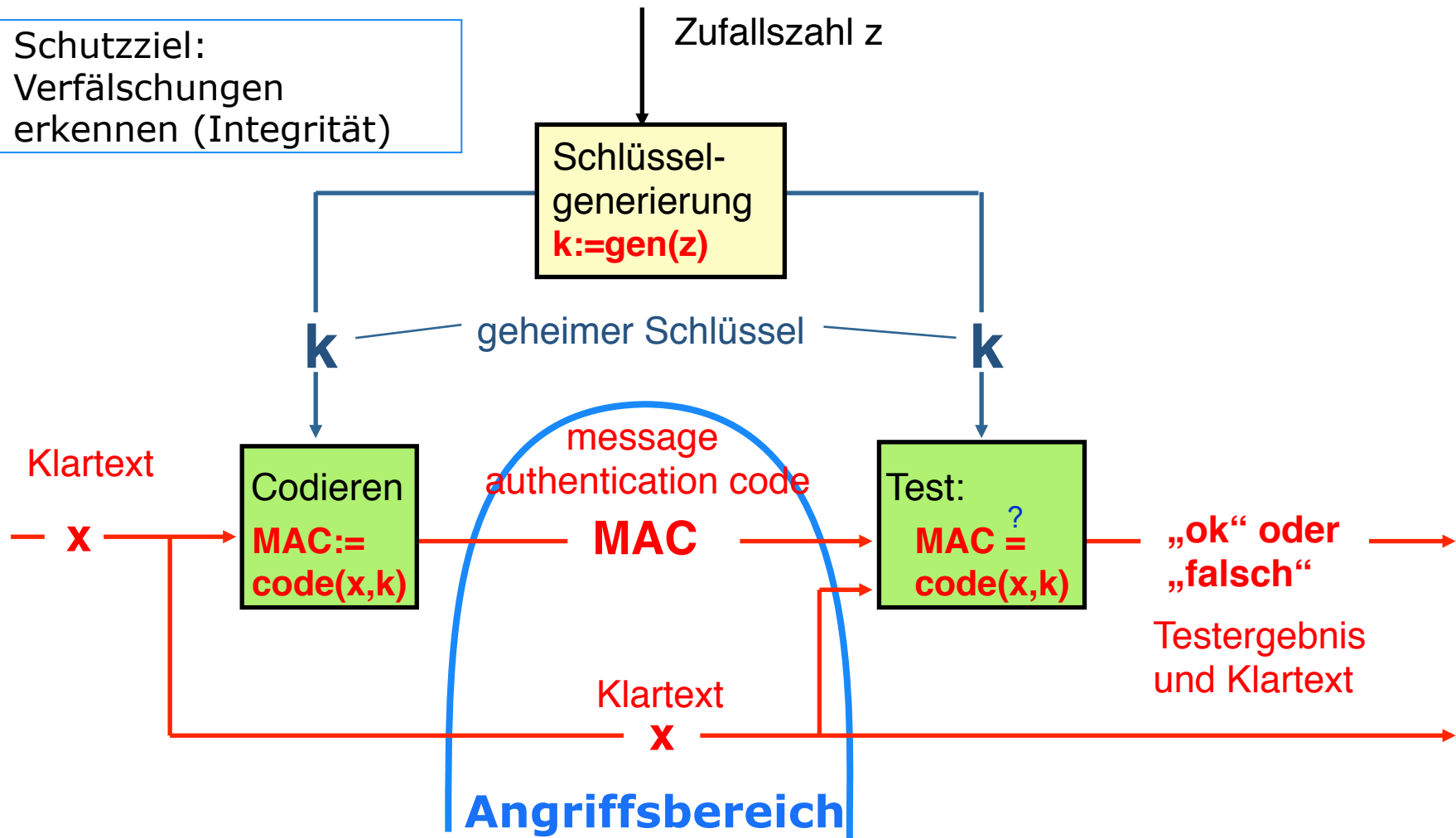
**Alice erhält Nachricht  $N$  verschlüsselt mit ihrem öff. Schlüssel**



- Ohne die Gewissheit über die Echtheit eines öffentlichen Schlüssels funktioniert keine sichere asymmetrische Kryptographie
- Deshalb: Schlüsselzertifizierung

# Symmetrische Authentikation

Schutzziel:  
Verfälschungen  
erkennen (Integrität)

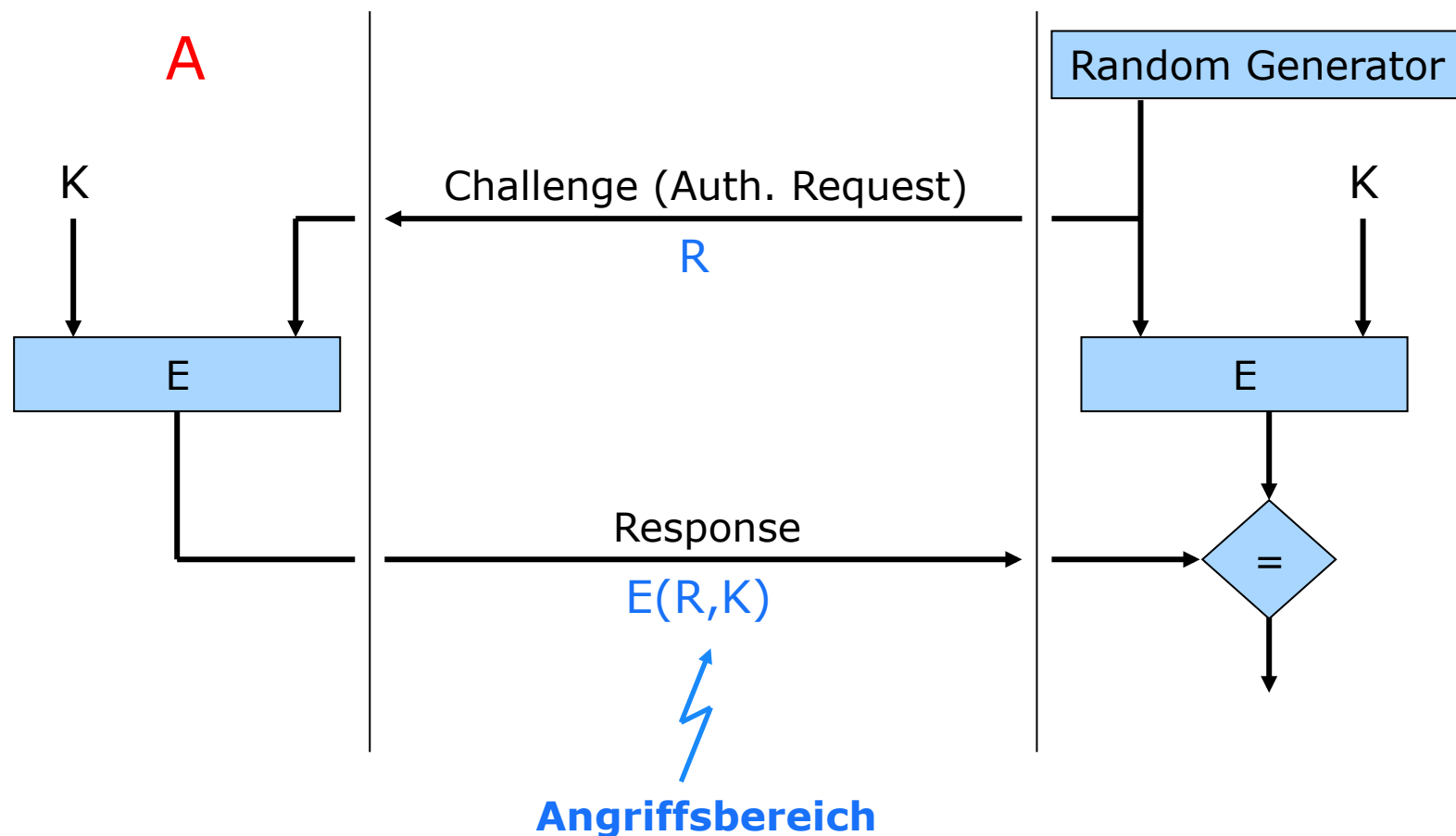


Glasvitrine mit Schloss. Es gibt zwei gleiche Schlüssel.

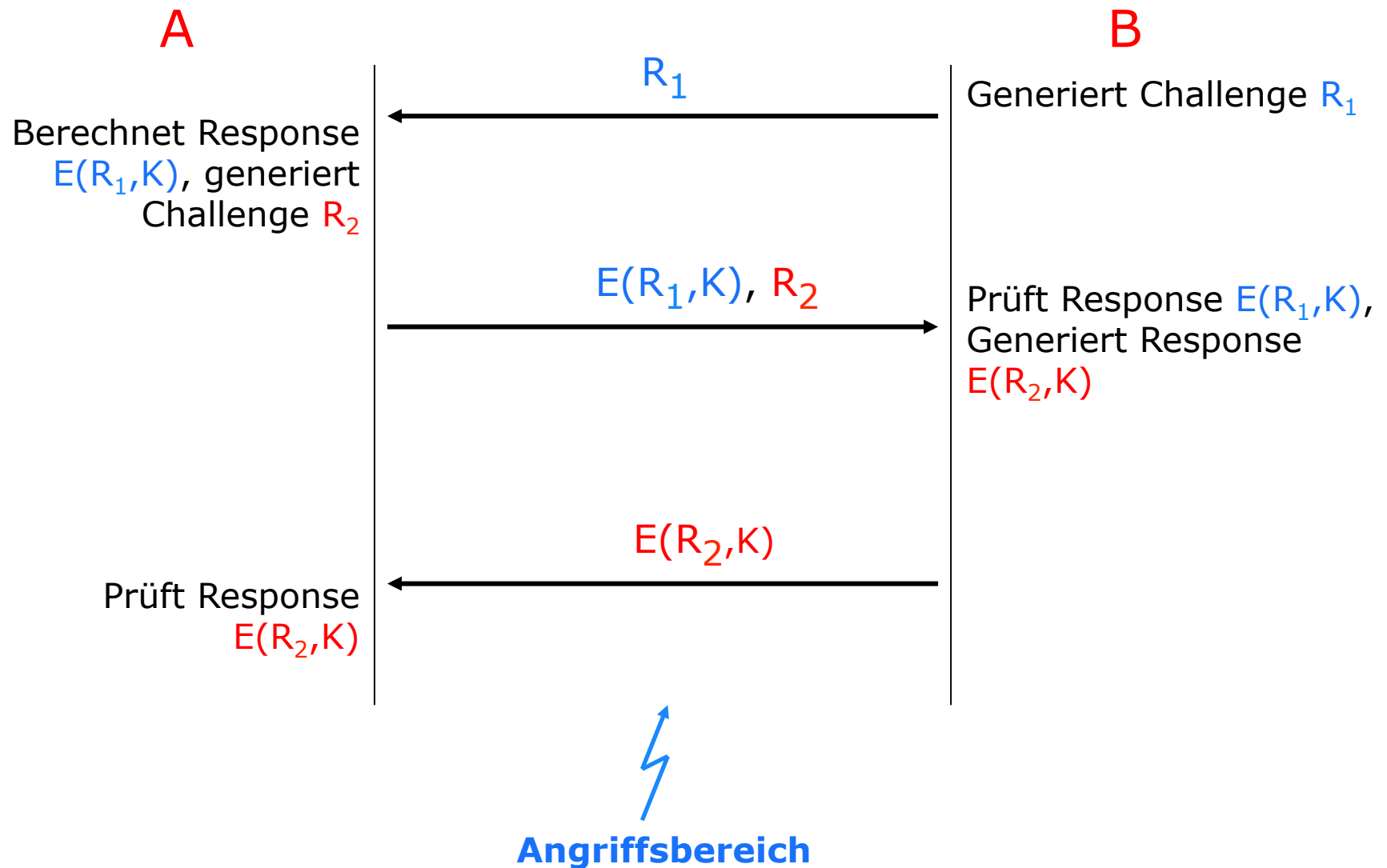


## Challenge-Response-Authentikation

- Frage-Antwort-Verfahren
  - meist basierend auf symmetrischem Authentikationssystem
  - A soll sich vor B authentisieren

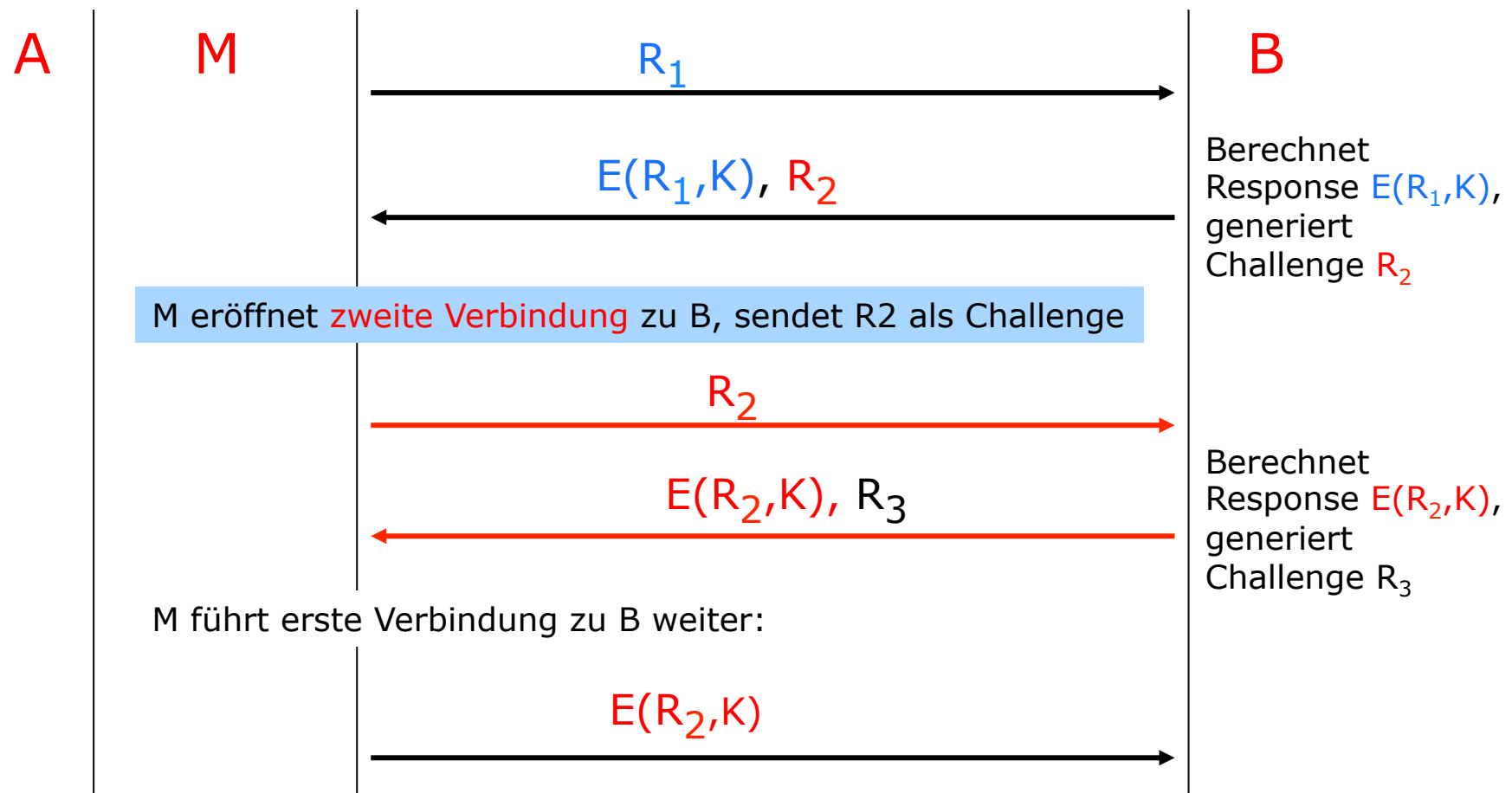


## Gegenseitige Authentikation



## Gegenseitige Authentikation

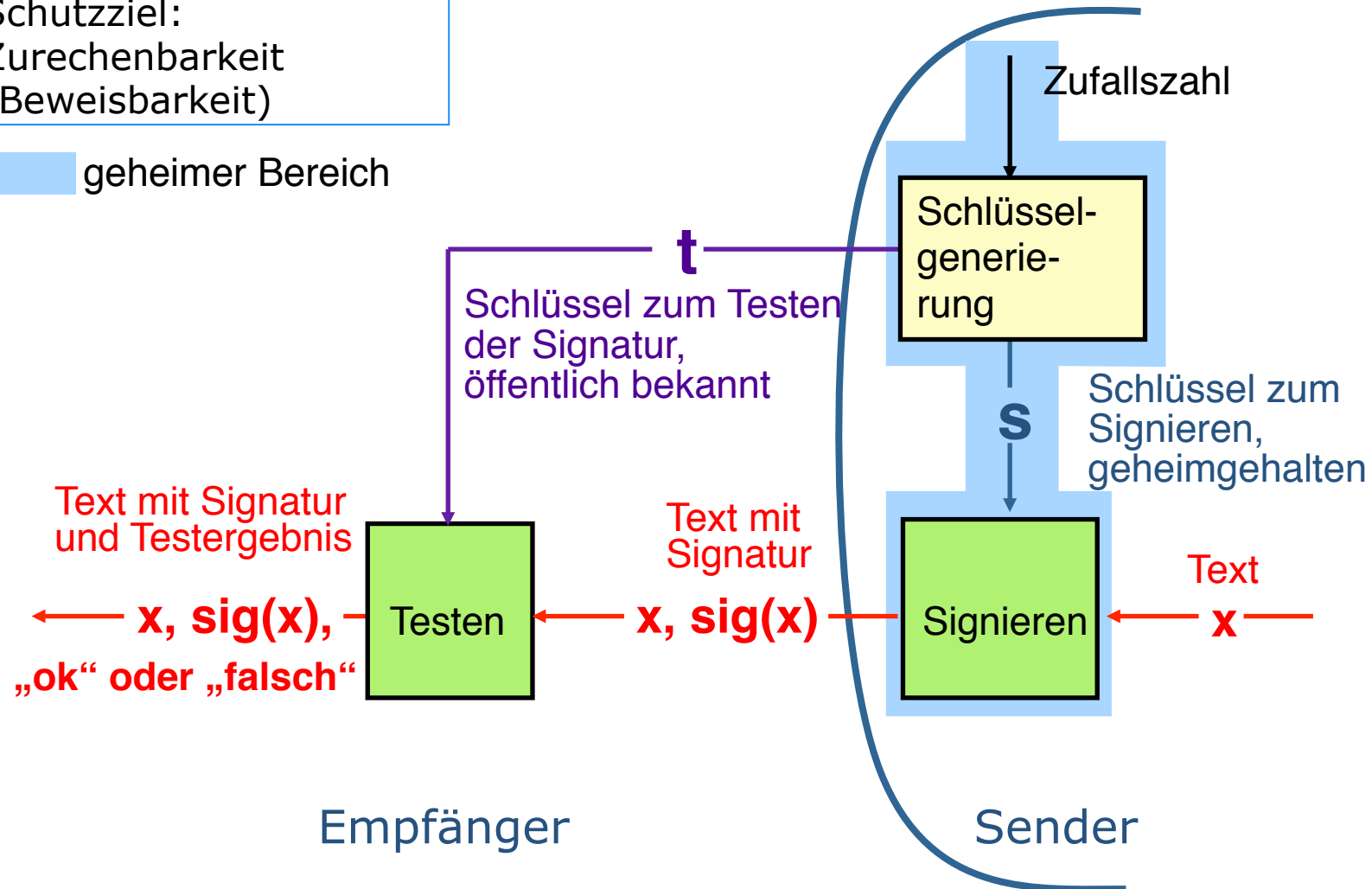
- Aktiver Angriff auf gegenseitige Authentikation auf der Basis symmetrischer Kryptosysteme
  - Angreifer **M** maskiert sich als **A**, kennt **K** *nicht*



# Digitales Signatursystem

Schutzziel:  
Zurechenbarkeit  
(Beweisbarkeit)

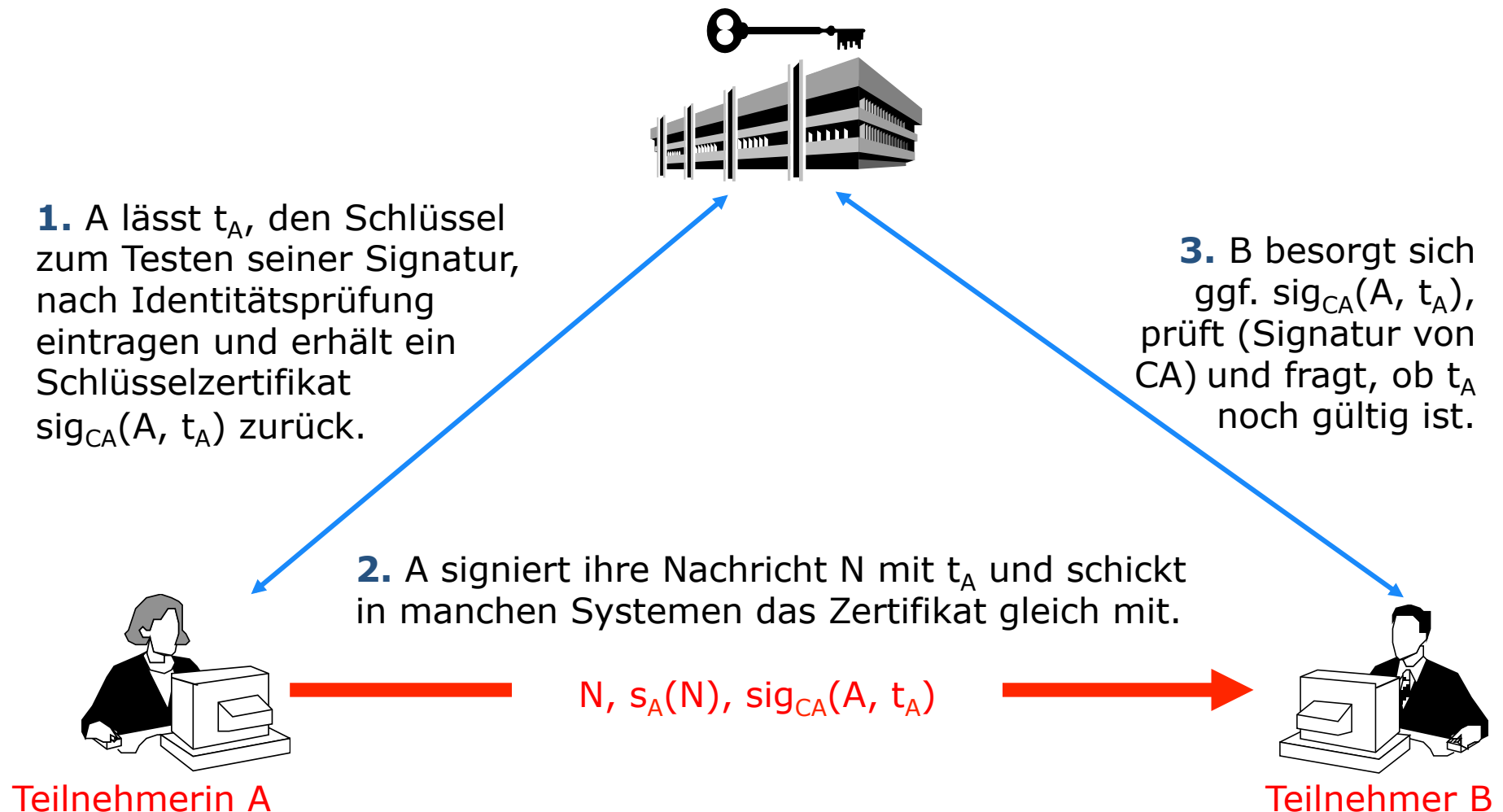
geheimer Bereich



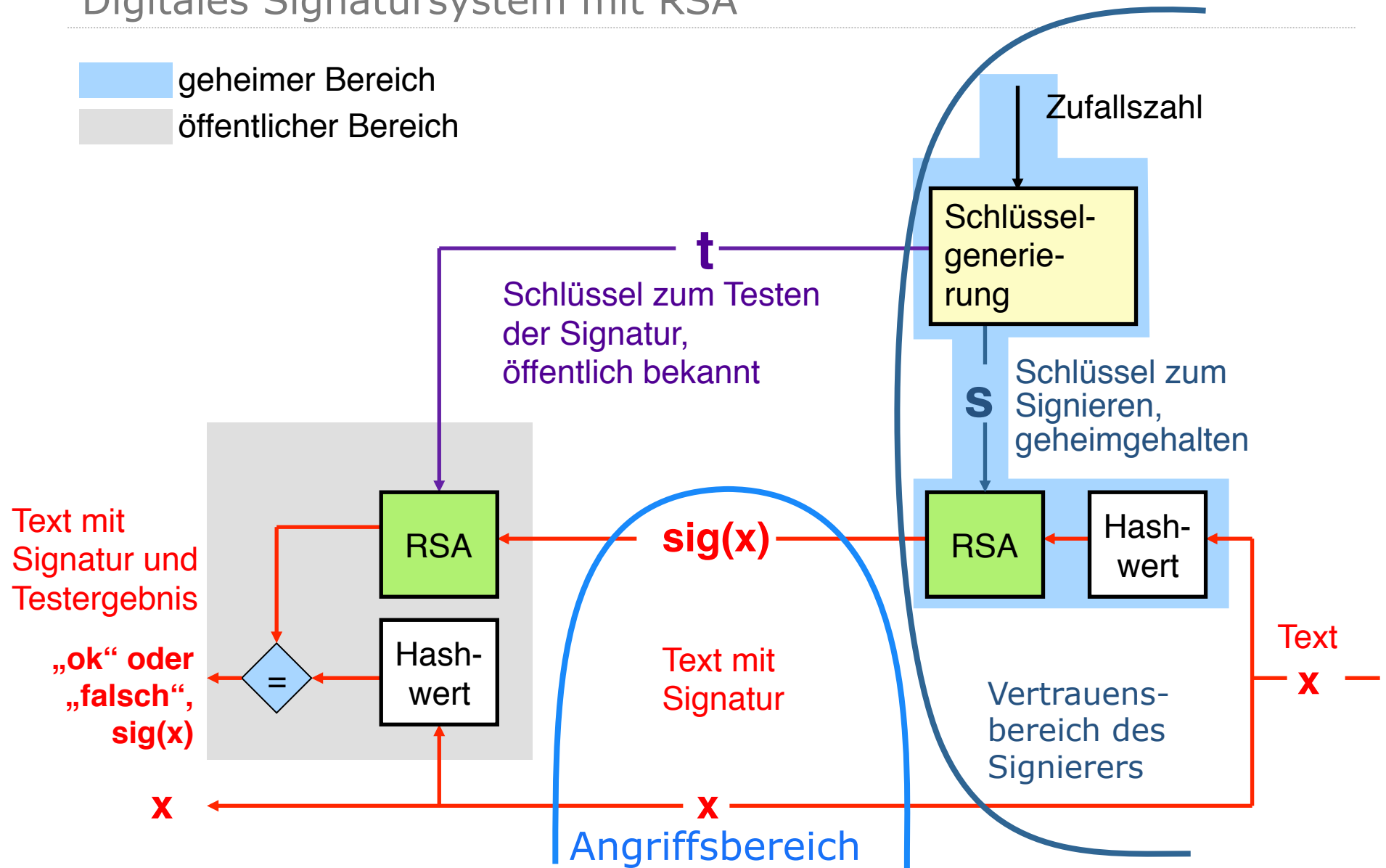
Glasvitrine mit Schloss. Es gibt nur einen Schlüssel.

# Zertifizierung des öffentlichen Testschlüssels

## Zertifizierungsstelle (Certification Authority) CA



# Digitales Signatursystem mit RSA



## Schlüssellängen

---

- **Beispielrechnung:**
  - 56 Bit (DES) sind heute unsicher.
  - 56 Bit Schlüssellänge  $\rightarrow 2^{56}$  mögliche Schlüssel (ca.  $7 \cdot 10^{16}$ )
  - Ausprobieren eines Schlüssels dauere 1 Nanosekunde ( $10^{-9}$  s)
  - Ausprobieren aller Schlüssel dauert dann:  
 $2^{56} \cdot 10^{-9} \text{ s} = 72057594 \text{ s} = 2,28 \text{ Jahre}$
- **Symmetrische Systeme:**
  - Vergrößerung des Schlüssels um 1 Bit bedeutet Verdoppelung des Schlüsselraumes
  - Schlüssellängen: 128–256-Bit auf »absehbare Zeit« sicher
  - jeder Schlüssel aus Sicht des Angreifers gleichwahrscheinlich
- **Asymmetrische Systeme:**
  - meist Vergrößerung des Zahlenbereichs nötig, da nur bestimmte Zahlen (z.B. Primzahlen) Schlüssel sein können
  - Schlüssellängen: 1024-4096 Bit, elliptische Kurven: ca. 160 Bit

## Vollständiges Durchsuchen (brute-force, exhaustive search)

- Angriff über Supercomputer und künftig Quantencomputer
  - betrifft nur komplexitätstheoretisch sichere Systeme
- Schutz gegen Supercomputer
  - Schlüssel ausreichend lang wählen
- Schutz gegen Quantencomputer
  - symmetrisch: Schlüssellänge verdoppeln auf mind. 256 Bit
  - asymmetrisch: [post-quantum cryptography]

	Key lengths	Complexity		
		Super Computer	Quantum Computer	
Symm.	128 Bit	$2^{127}$	$2^{64}$	Grover, 1996
	256 Bit	$2^{255}$	$2^{128}$	
Asymm.	1024 Bit	$\approx 2^{90}$	$\approx 2^{25}$	Shor, 1994
	2048 Bit	$\approx 2^{117}$	$\approx 2^{28}$	

nach: Bernstein, Buchmann, Dahmen: Post Quantum Cryptography. Springer, 2009



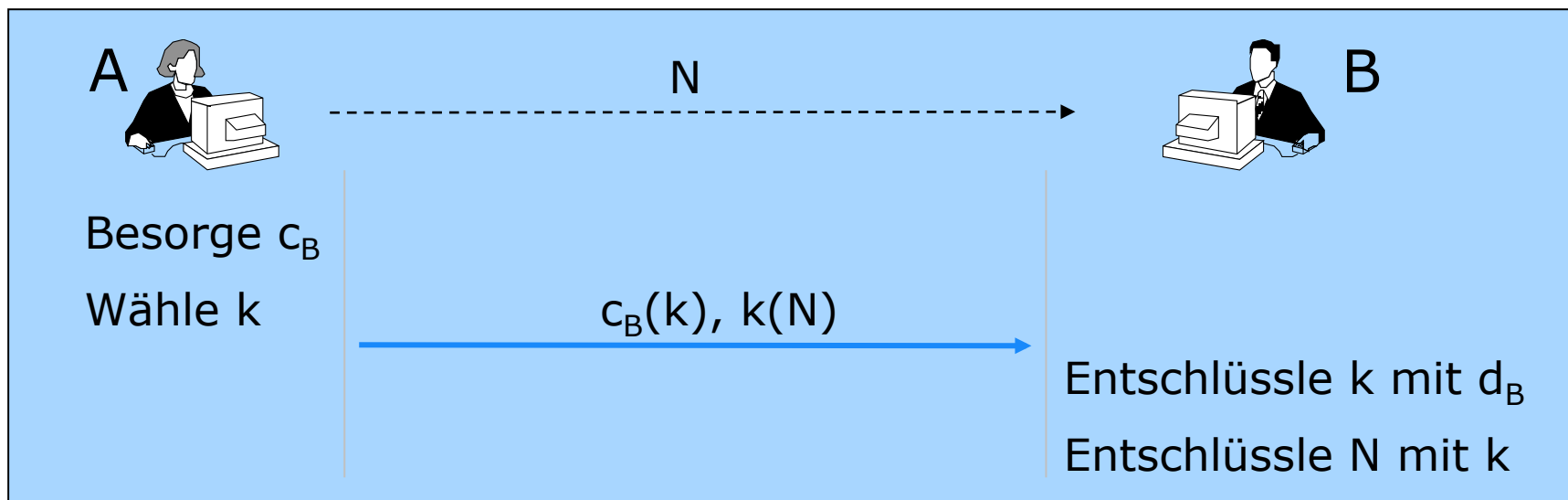
## Vergleich: symmetrische-asymmetrische Systeme

---

- Wieviele Schlüssel müssen bei  $n$  Teilnehmern ausgetauscht werden?
    - symmetrische Systeme:
    - asymmetrische Systeme:
  - Typische Schlüssellängen: (bei vergleichbarem Sicherheitsniveau)
    - symmetrische Systeme: 128–256 Bit
    - asymmetrische Systeme: 1024–4096 Bit  
Elliptische Kurven: ca. 160 Bit
  - Performance:
    - symmetrische Systeme ver- bzw. entschlüsseln etwa um den Faktor 100–10.000 schneller
- Asymmetrische Systeme: Geringere Effizienz und größere Schlüssellängen werden aufgewogen durch den stark vereinfachten Schlüsselaustausch

# Hybride Kryptosysteme

- **Kombiniere**
  - einfachen Schlüsselaustausch der asymmetrischen Systeme
  - hohe Verschlüsselungsleistung der symmetrischen Systeme
- **Verfahren**
  - Asymmetrisches Kryptosystem wird zum Austausch eines symmetrischen Sitzungsschlüssels  $k$  (session key) **verwendet**.
  - Eigentliche Nachricht  $N$  wird mit  $k$  verschlüsselt.
- Nur sinnvoll, wenn  $N$  deutlich länger als wenige Bit ist.



## Pretty Good Privacy (PGP) und Gnu Privacy Guard (GnuPG)

Deutlicher jedoch nähert sich das Präludium g-moll der Toccatta mit einem zwischen rahmende Pfeiler

gestell

in dess

eine De

element

entdeck

-----BEGIN PGP MESSAGE-----

Version: GnuPG v1.4.8 (Darwin)

Comment: Generated by Gpg Tools - <http://www.tomsci.com/gpgtools>

hQIOA2ThYngS

wDDhe4Dk9kwq

Q7baKGRNBQhV

b4ASOc+2ov6U

/pRli9HAWXjb

I/9Fh26iPoLJ

hd9HKNS1YYWN

aM9lOfL/9geu

DQjn6INv4+qM

FDw9h8a2gCsO

kLikFpvstFtC

OdLAZAF/RDOO

JcoDyK9l9jBw

WjuTZfGOOGtv

Vaml6/s2jluf

l7km72jIz83w

f6Y3FnF9DJUK

yZ6R+PS0q6c=

=x491

-----END PGP MESSAGE-----

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Deutlicher jedoch nähert sich das Präludium g-moll der Toccatta mit einem zwischen rahmende Pfeiler gestellten, ausgedehnten improvisatorischen Mittelteil, in dessen figurativer Sequenzierung Bach mit einer über eine Dezime chromatisch absteigenden Skala die elementare Farbigkeit der enharmonischen Umdeutungen entdeckte.

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.4.8 (Darwin)

Comment: Generated by Gpg Tools - <http://www.tomsci.com/gpgtools>

iEYEARECAAYFAkjh9yQACgkQ4UAgYUnvHYSahQCfaWrrH1l9s4tXeFToa6aQPryw

TX4AoL7l7WQHHPzXVG6SX9fSOAskCzn

=Ebit

-----END PGP SIGNATURE-----

<http://www.pgpi.net>  
<http://www.gnupg.org>

## Key Recovery und Key Escrow


---

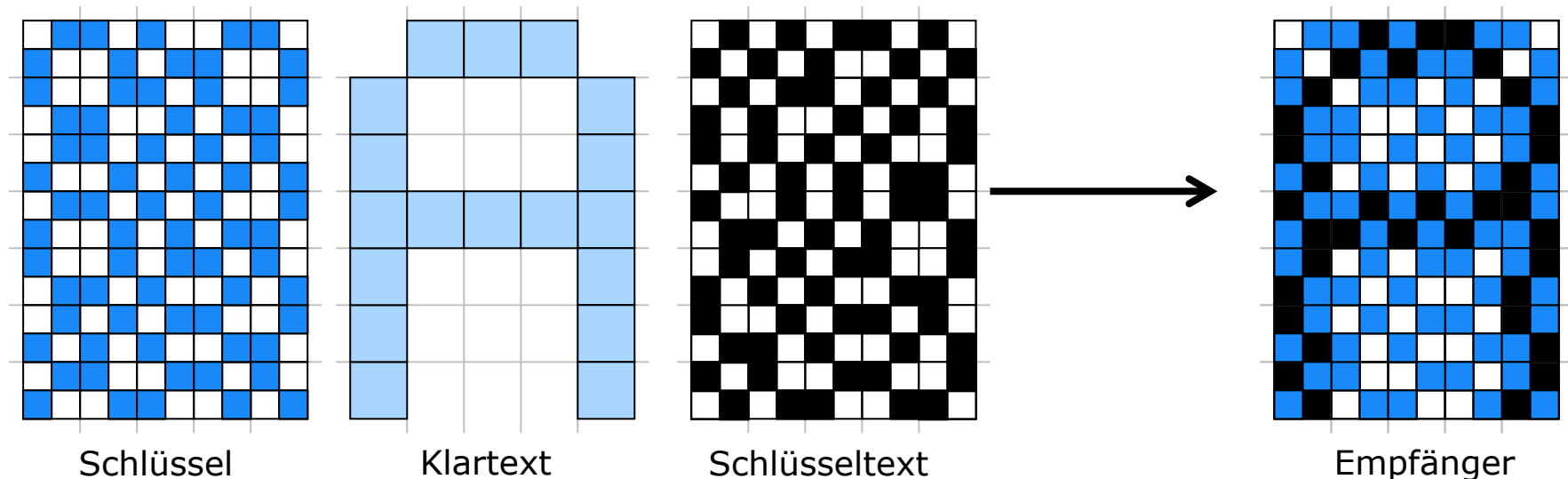
- **Key Recovery**
  - Hinterlegung des Entschlüsselungsschlüssels zum Zweck der Entschlüsselbarkeit bei Schlüsselverlust.
  - Schwellwertschema: Schlüssel wird in  $n+k$  Teile zerlegt. Zur Rekonstruktion werden wenigstens  $n$  Teile benötigt.
- **Key Escrow**
  - Hinterlegung des Entschlüsselungsschlüssels zum Zweck der Strafverfolgung.
  - so dass alle Nachrichten ab einem bestimmten Zeitpunkt entschlüsselt werden können
  - so dass Nachrichten auch rückwirkend entschlüsselt werden können
- **Beachte**
  - Signaturschlüssel müssen nie hinterlegt werden, da eine Signatur stets testbar bleibt.
  - Bei Verlust des Signierschlüssels: neuen erzeugen.

# Key Recovery

	Schutz der Kommunikation	Langfristige Speicherung
Verschlüsselung	<b>Key Recovery für Funktion unnötig, aber zusätzliches Sicherheitsrisiko</b>	<b>Key Recovery sinnvoll</b>
Authentikation		
symmetrisch (MACs) asymmetrisch (dig. Signatur)		

## Visuelle Kryptographie

- Symmetrisches Verfahren
  - Symmetrischer Schlüssel: Sender und Empfänger erzeugen sich Zufallsmuster aus zwei »Basismustern«: 
- Visuelle Botschaft:
  - Sender verwendet negiertes Muster für schwarze Bildpunkte
  - Für »weiße« Bildpunkte: keine Veränderung

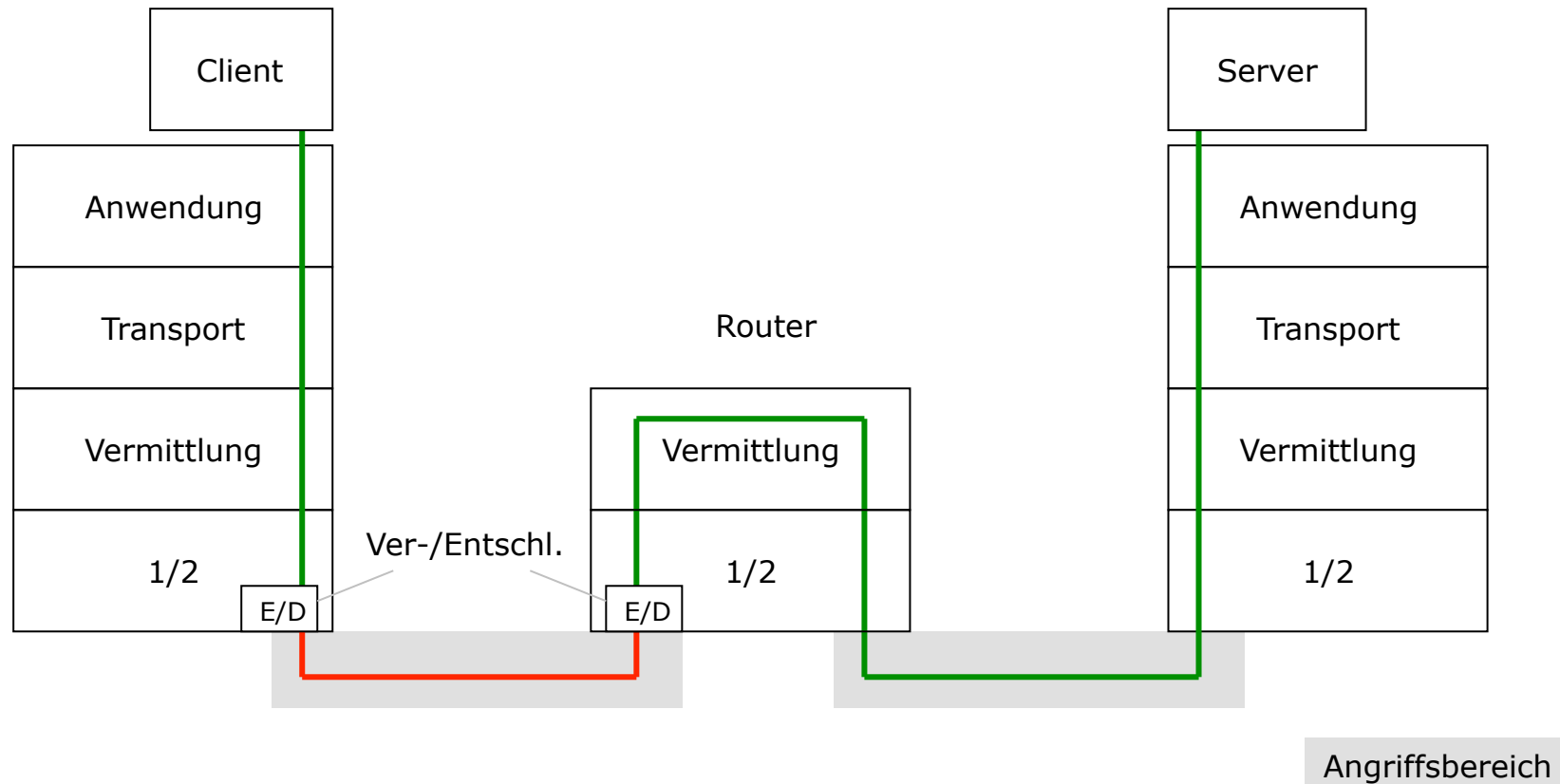


## Sicherheitsfunktionen nach Schichten geordnet

Kommunikations- schicht im OSI- Referenzmodell	Sicherheitsfunktion
Anwendungsschicht	Pretty Good Privacy (PGP), S/MIME (Secure Multipurpose Internet Mail Extensions), Secure Shell (SSH)
Transportschicht	Secure Sockets Layer/Transport Layer Security (SSL/TLS)
Vermittlungsschicht	Authentication Header (AH) zur Integritätssicherung von Datagrammen, Encapsulated Security Payload (ESP) zur Verschlüsselung von Datagrammen
Schichten 1/2	Challenge Handshake Protocol (CHAP, Passwort), Encrypt Control Protocol (ECP), WiFi Protected Access (WPA) 2

## Verschlüsselung in Schicht 1/2

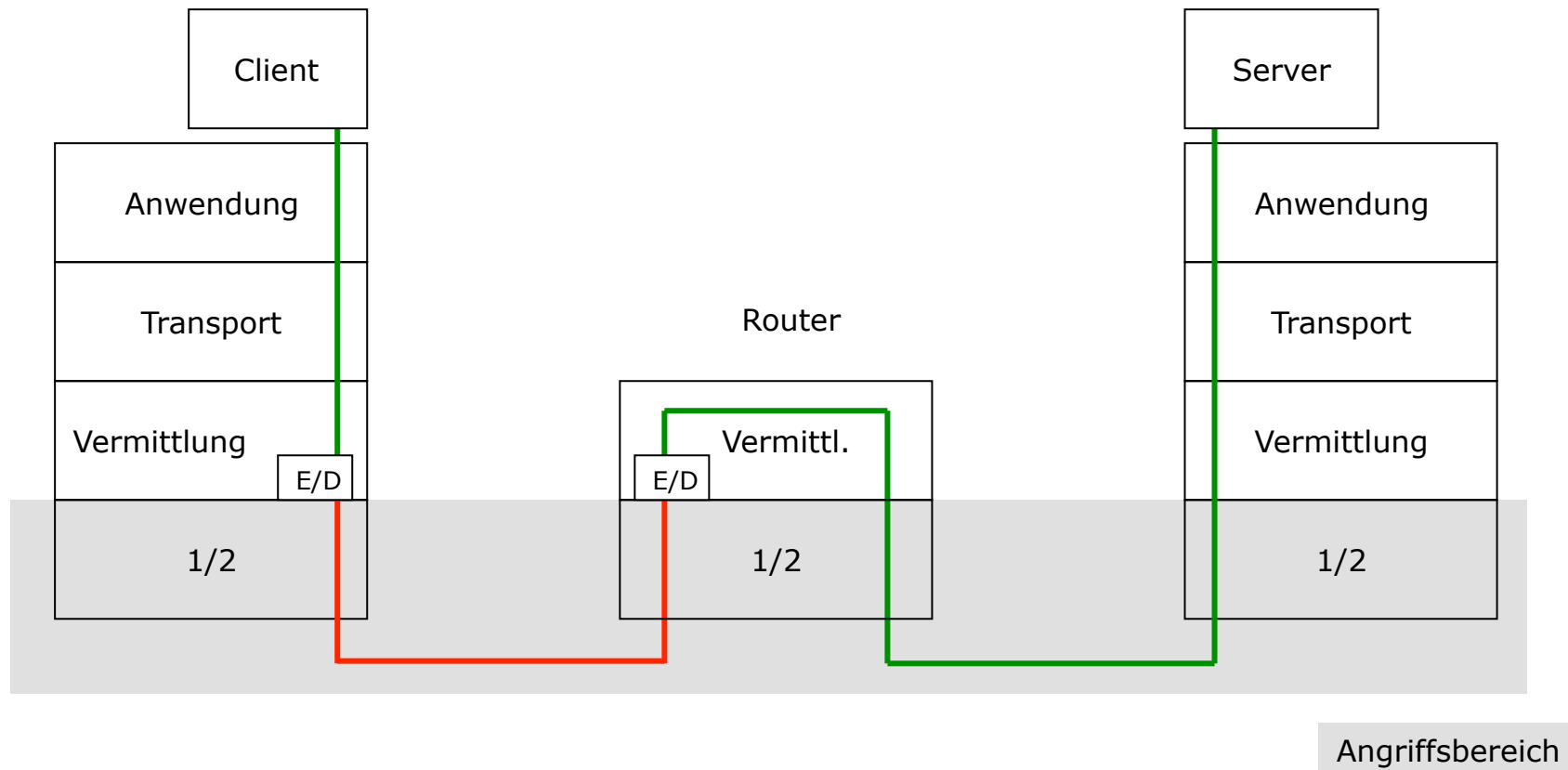
- Verschlüsselung nur bis zum nächsten Router (Verbindungsverschlüsselung)
  - Nicht alle Teilstrecken müssen verschlüsselt sein
  - Wenig Kontrolle durch den Endnutzer





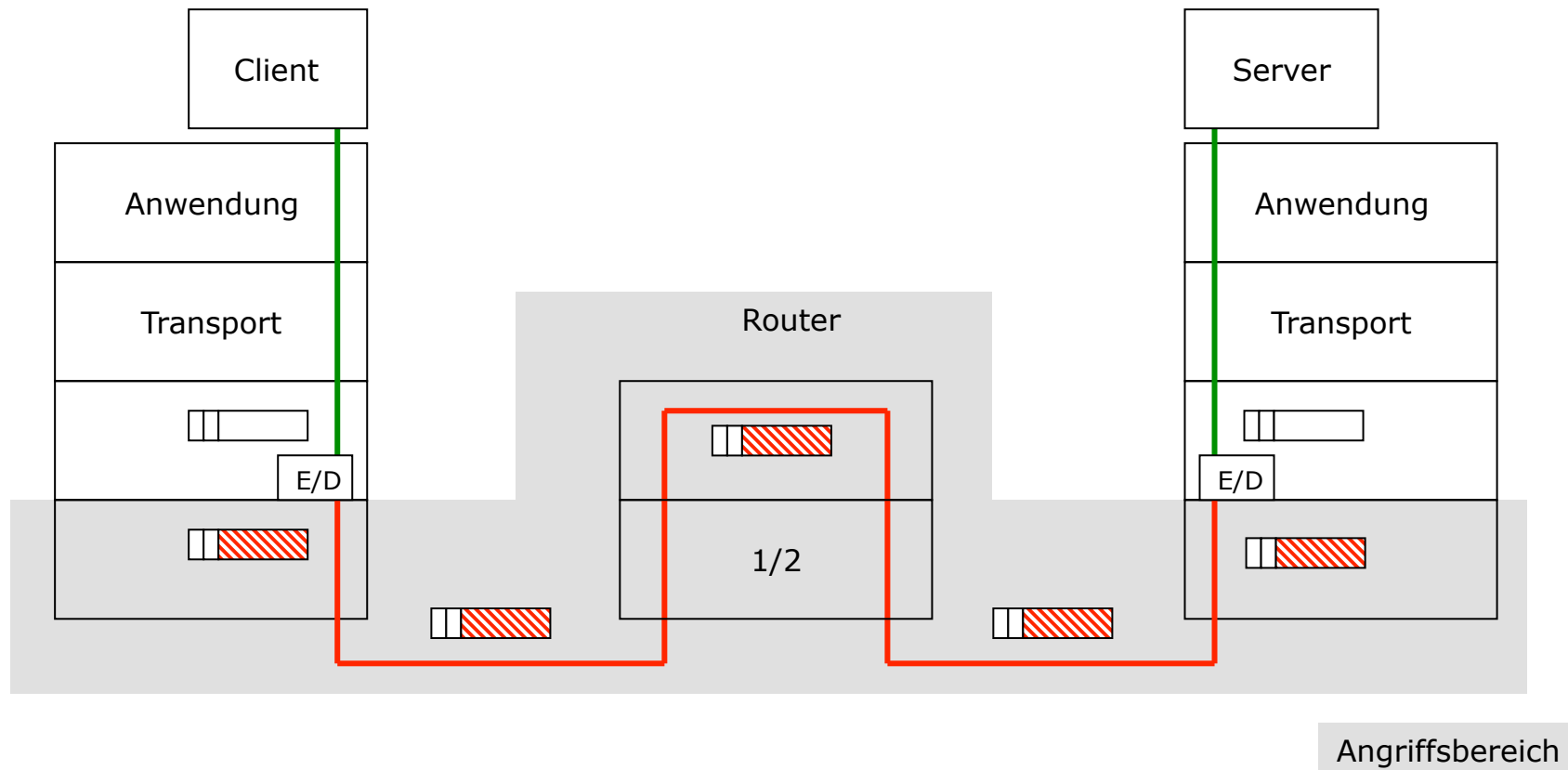
## Verschlüsselung in Vermittlungsschicht: IPSec

- Transportmodus
  - Verbindungs- und Ende-zu-Ende-Verschlüsselung möglich



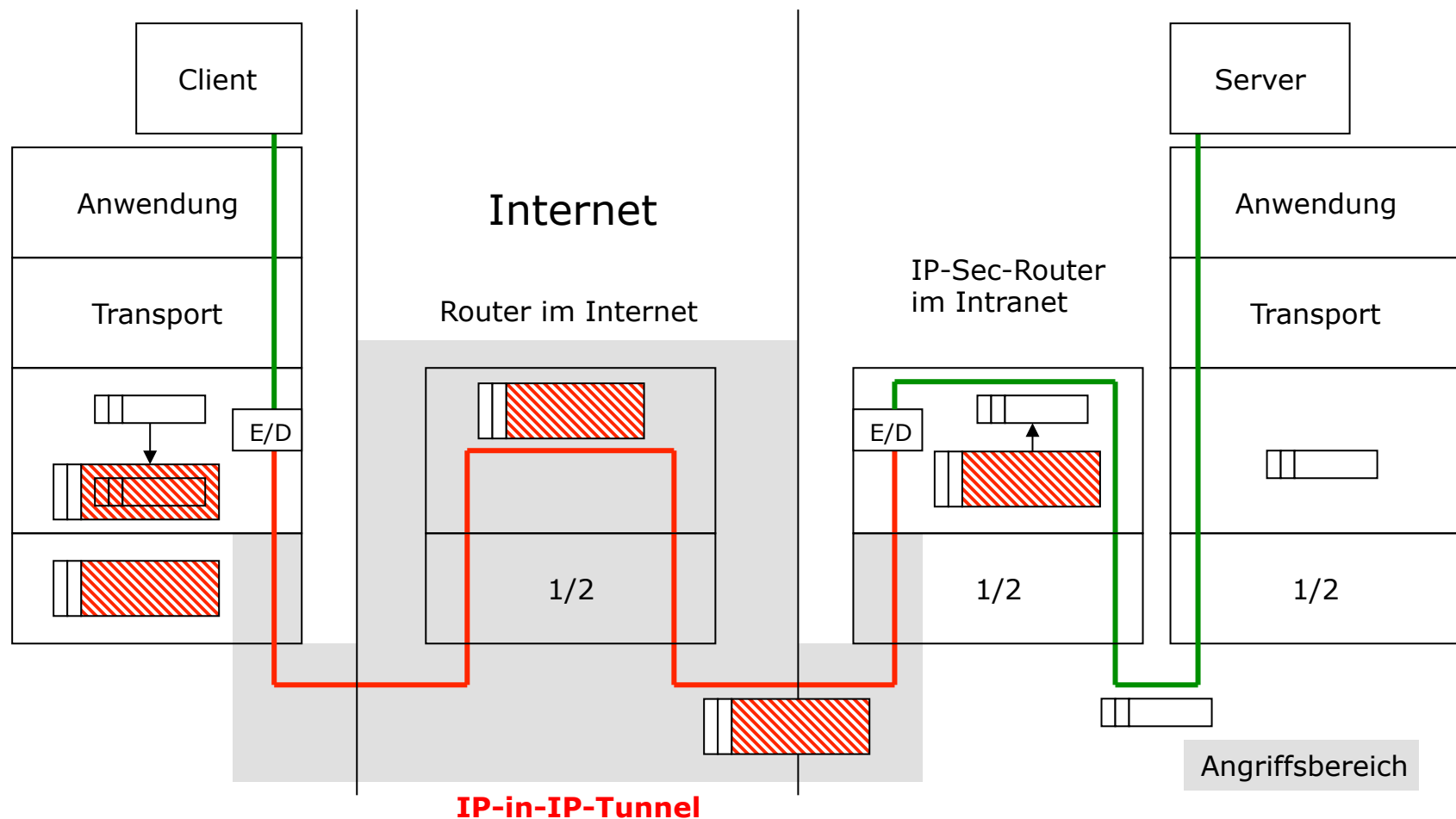
## Verschlüsselung in Vermittlungsschicht: IPSec

- Transportmodus
  - Verbindungs- und Ende-zu-Ende-Verschlüsselung möglich



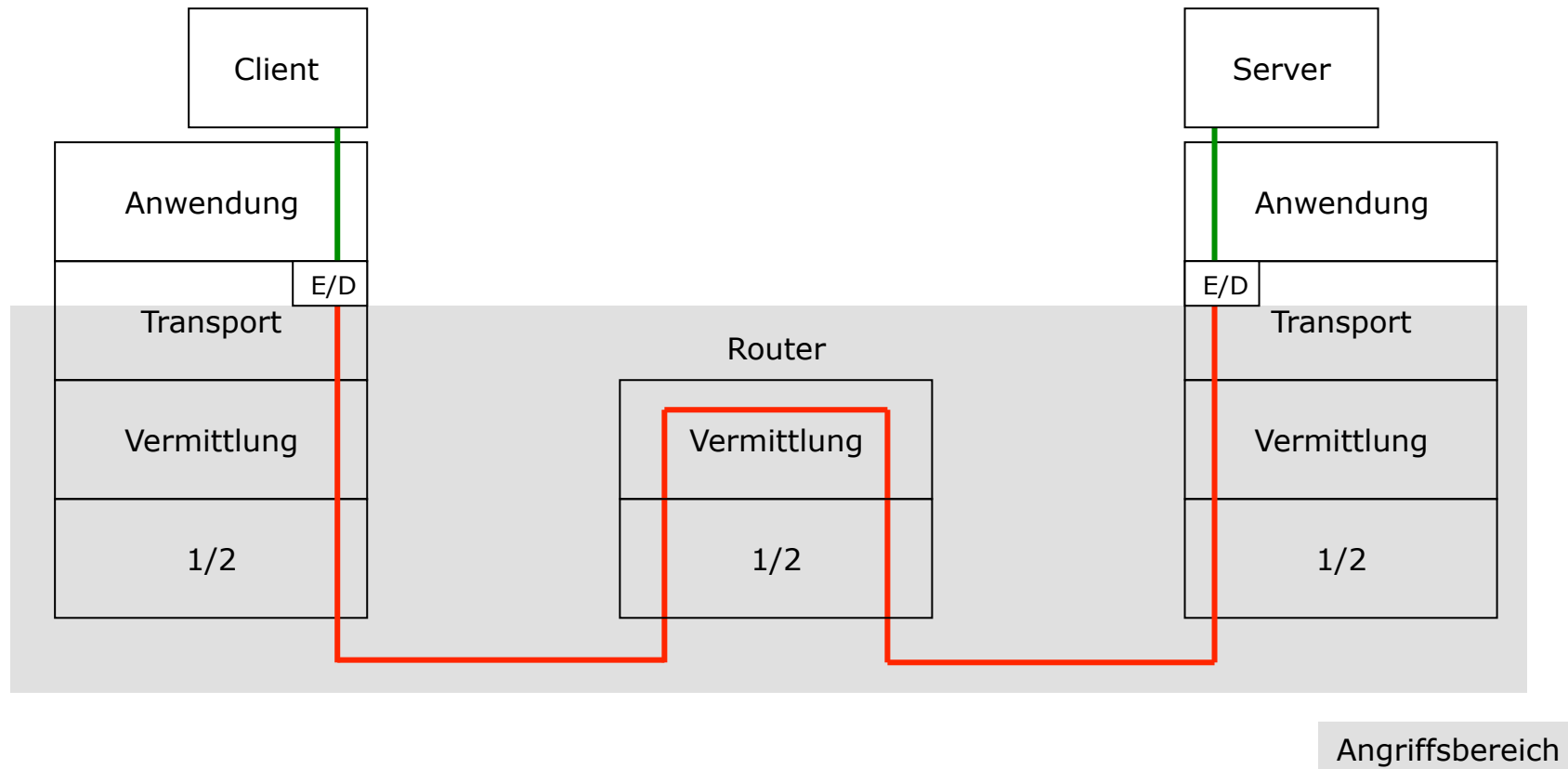
## Verschlüsselung in Vermittlungsschicht: IPSec

- Tunnelmodus
  - Momentane Hauptanwendung: Virtuelles Privates Netz



## Verschlüsselung in Transportschicht: SSL/TLS

- **Anwendung:**
  - Verschlüsselung von TCP-Verbindungen
  - von Netscape entwickelt
  - in jeden modernen Browser integriert

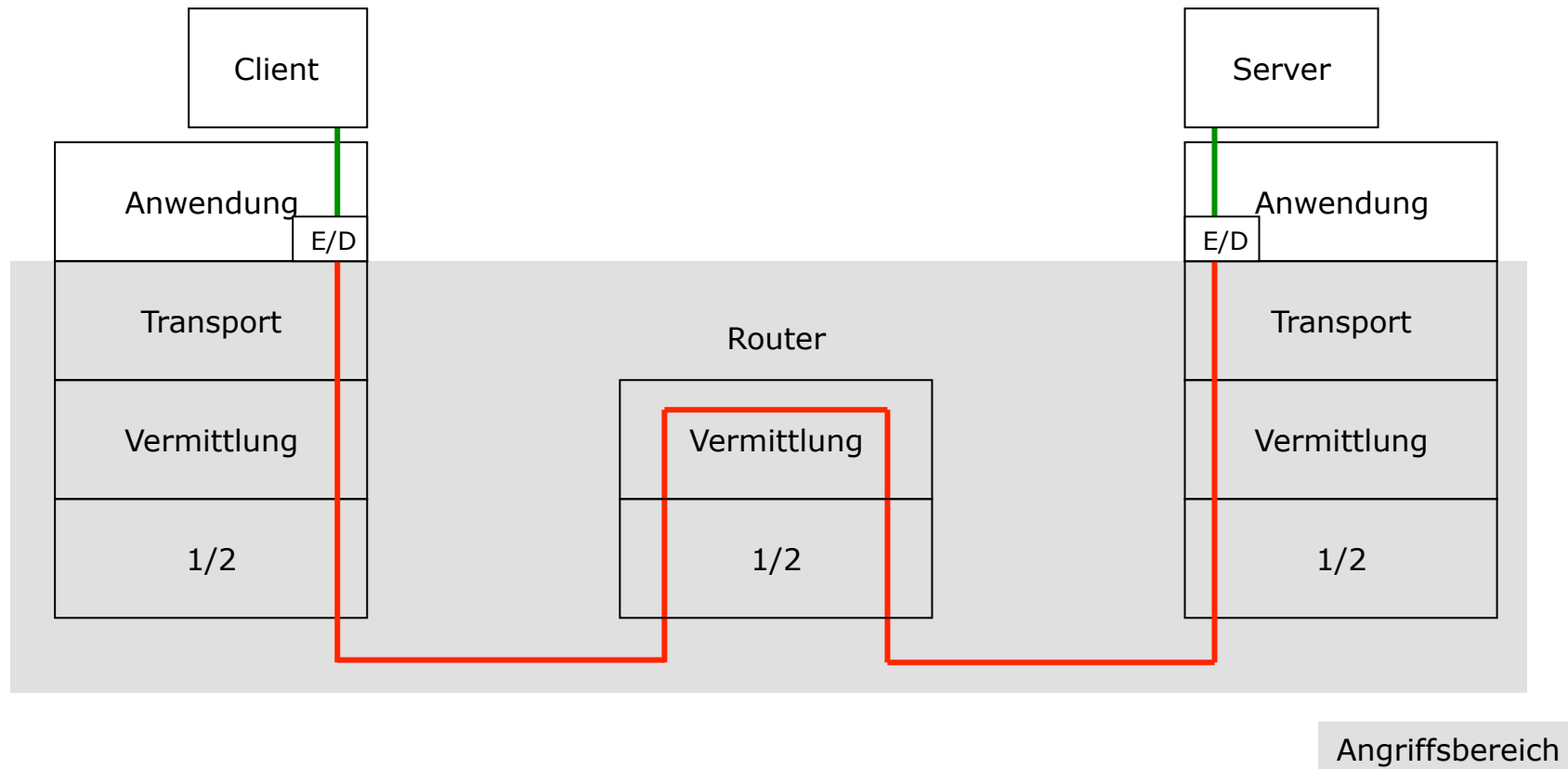


## Vergleich SSL – IPSec

	<b>SSL</b>	<b>IPSec</b>
Komplexität	hoch	gering
Anwendungsnahe	hoch	gering
Für VPNs geeignet?	nein	ja
Für paketorientierte Dienste geeignet?	nein	ja
Für verbindungsorientierte Dienste geeignet?	ja	ja

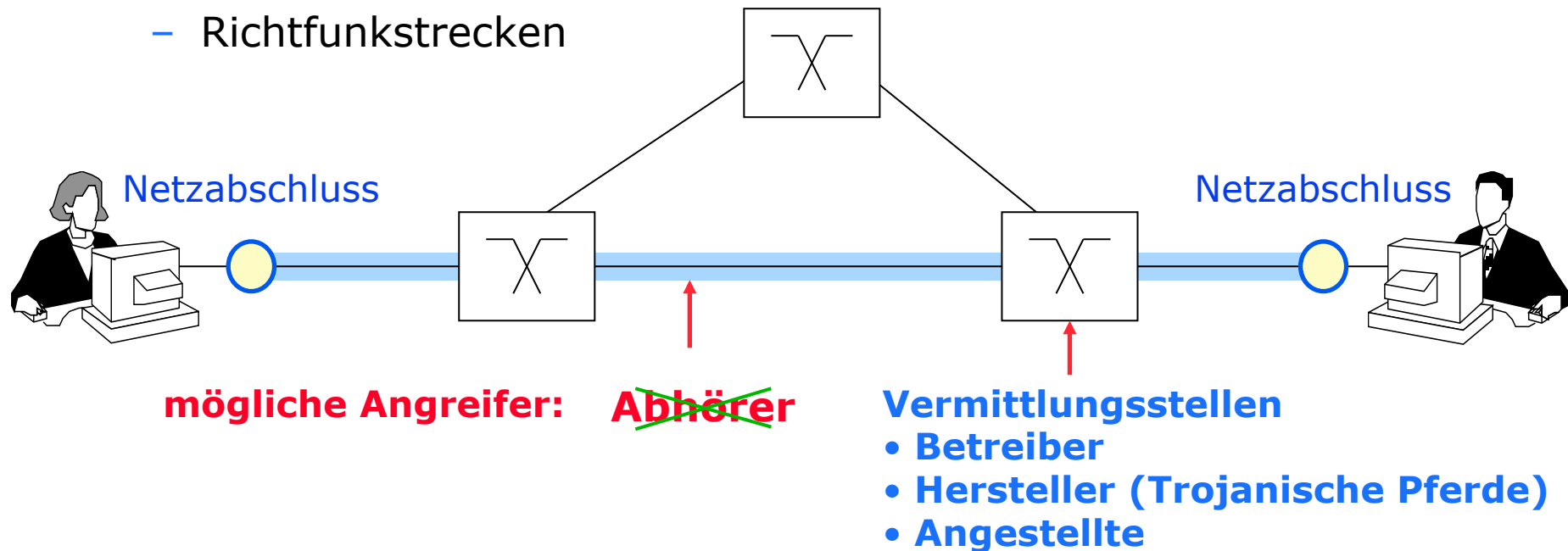
## Verschlüsselung in Anwendungsschicht

- Ende-zu-Ende-Verschlüsselung zwischen Client und Server



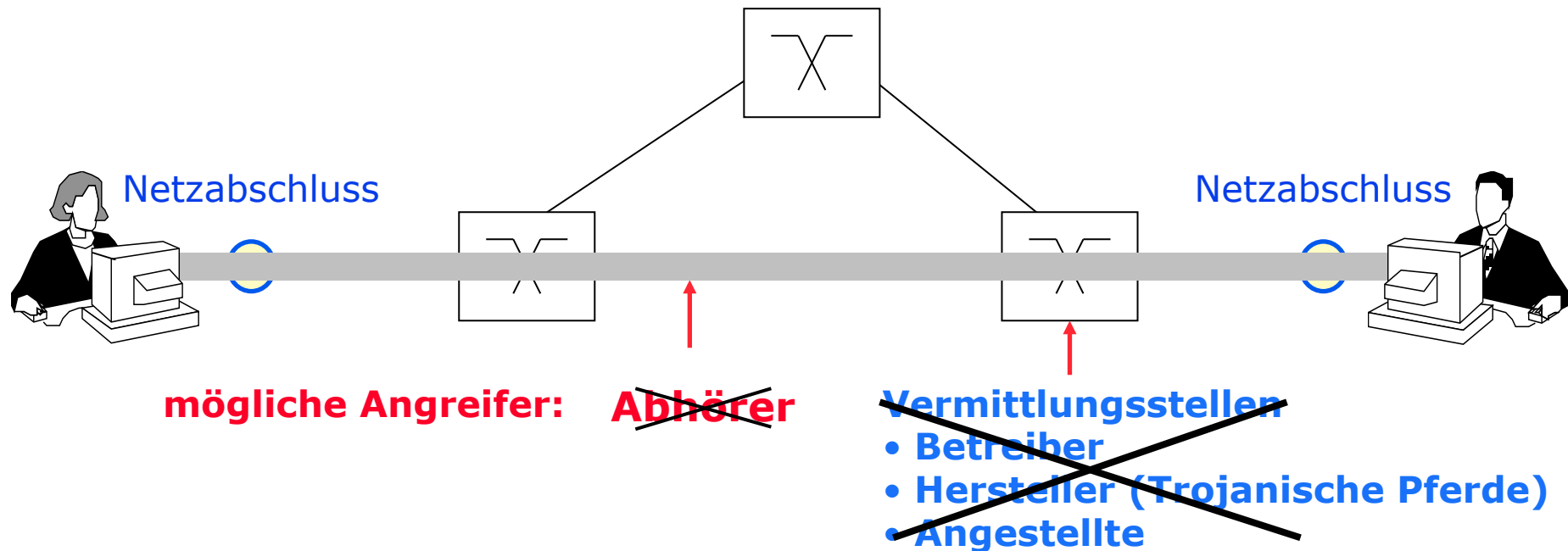
## Verbindungsverschlüsselung

- Verbindungsverschlüsselung: (meist symmetrische Verschlüsselung)
  - zwischen Netzabschluss und Vermittlungsstelle
  - zwischen Vermittlungsstelle und Vermittlungsstelle
- In Vermittlungsstelle liegt Klartext vor
- Anwendungsgebiete:
  - Virtuelle Private Netze (VPN)
  - Leitungsverschlüsselung in Telekommunikationsnetzen
  - Richtfunkstrecken



## Ende-zu-Ende-Verschlüsselung

- Ende-zu-Ende-Verschlüsselung der Inhalte
  - von Endgerät zu Endgerät
- Anwendungsgebiete:
  - E-Mail-Verschlüsselung
  - Pretty Good Privacy (PGP)
  - Secure Sockets Layer (SSL)
- Adressierungsinformation kann nicht verschlüsselt werden





## Verbindungs- und Ende-zu-Ende-Verschlüsselung

- Kombination von Verbindungs- und Ende-zu-Ende-Verschlüsselung
  - Ende-zu-Ende-Verschlüsselung allein schützt *nicht* die Adressierungsdaten vor **Außenstehenden**
  - zusätzliche Verbindungsverschlüsselung sinnvoll
- Restproblem Verkehrsdaten:
  - **Netzbetreiber** kann weiterhin feststellen, wer mit wem, wann, wie lange, wo, wieviel Information ausgetauscht hat

