



Kryptographie: Einführung

Systematik

Symmetrische / Asymmetrische Systeme

Verschlüsselung / Authentikation

Schlüsselverteilung

Schlüssellängen

Pretty Good Privacy

Kriterien zur Einteilung von Kryptosystemen

- Anwendungsfall
 - Konzelation
 - Authentikation
 - 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

Erreichbare Sicherheit

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

- 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 } - { **plaintext**
ciphertext } **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

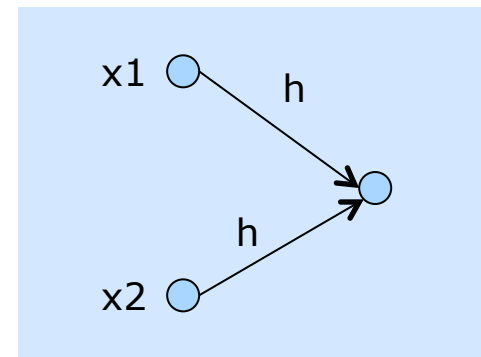
- Was wird durch den Angriff erreicht?

(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 eine vom Angreifer bestimmte Nachricht (z.B. einen abgefangenen Schlüsseltext)
 - existenzielles Brechen: für irgendeine Nachricht
- Aufwand/Kosten:
 - Einmalige Kosten, jeder Schlüssel effizient knackbar
 - Jeder Angriff verursacht Kosten beim Angreifer

Hashfunktionen

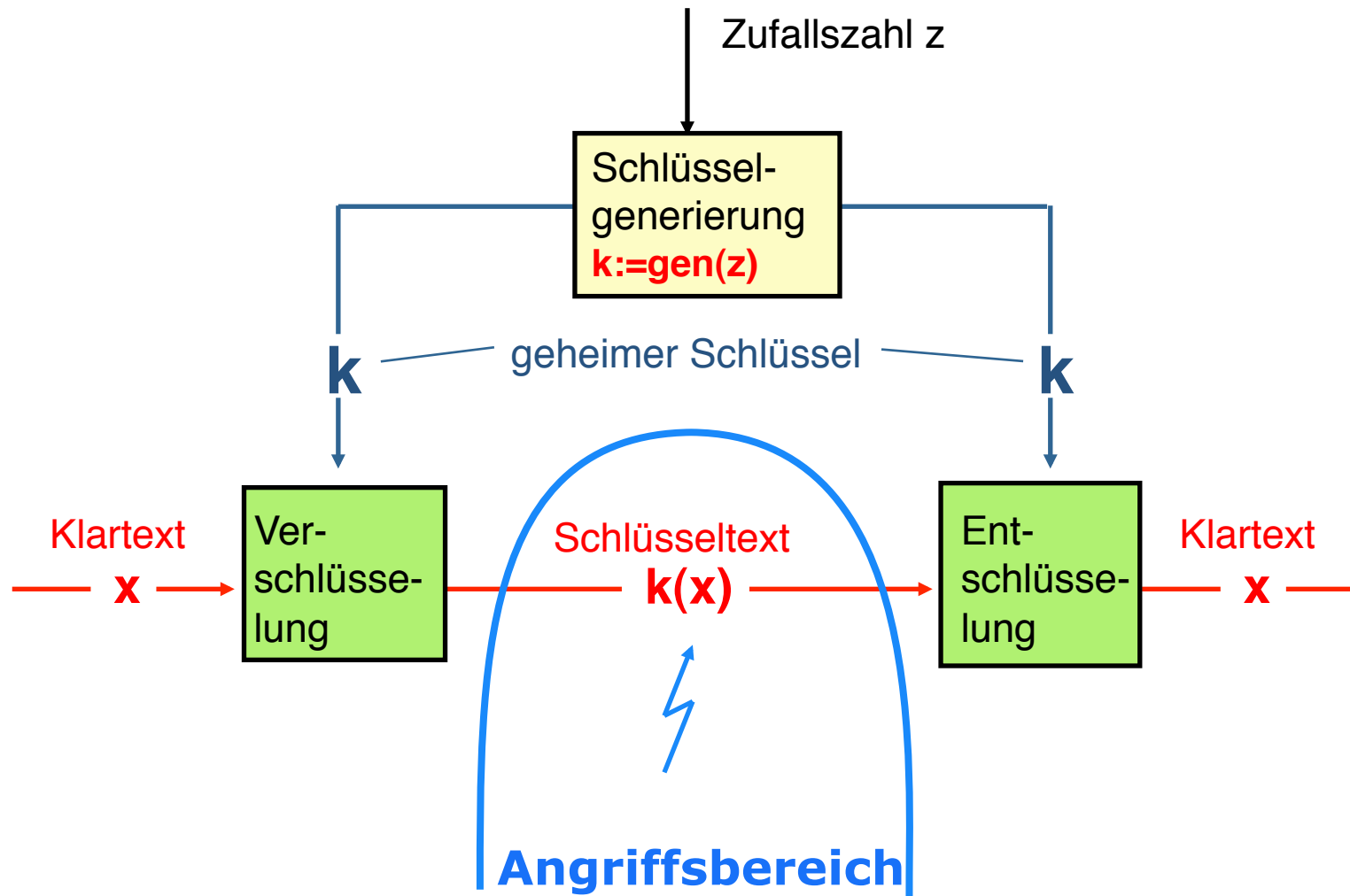
- Abbildung $h: X \rightarrow Y$
 - Einwegfunktion (auch: Falltürfunktion)
 - Umkehrfunktion nicht effizient berechenbar
- Hashfunktionen sind verkürzend:
 - Beliebige lange Inputs werden auf Output bestimmter Länge abgebildet (z.B. MD5: 128 Bit)
 - Kollision:
 - $h(x_1) = h(x_2)$ mit $x_1 \neq x_2$
- Kryptographische Hashfunktionen sind kollisionsresistent:
 - nicht mit vertretbarem Aufwand möglich, eine Kollision gezielt herbeizuführen, z.B. Finden eines x_2 zu einem gegebenen $h(x_1)$



Anwendungsfall x Schlüsselbeziehung

	Konzelation (Verschlüsselung)	Authentikation
symmetrische	DES, Triple-DES, AES, IDEA, One-time-pad	Symmetrische Authentikationscodes, GSM- Authentikation, SecurID
asymmetrische	RSA, ElGamal, McEliece	RSA, DSS, DSA, ElGamal, GMR

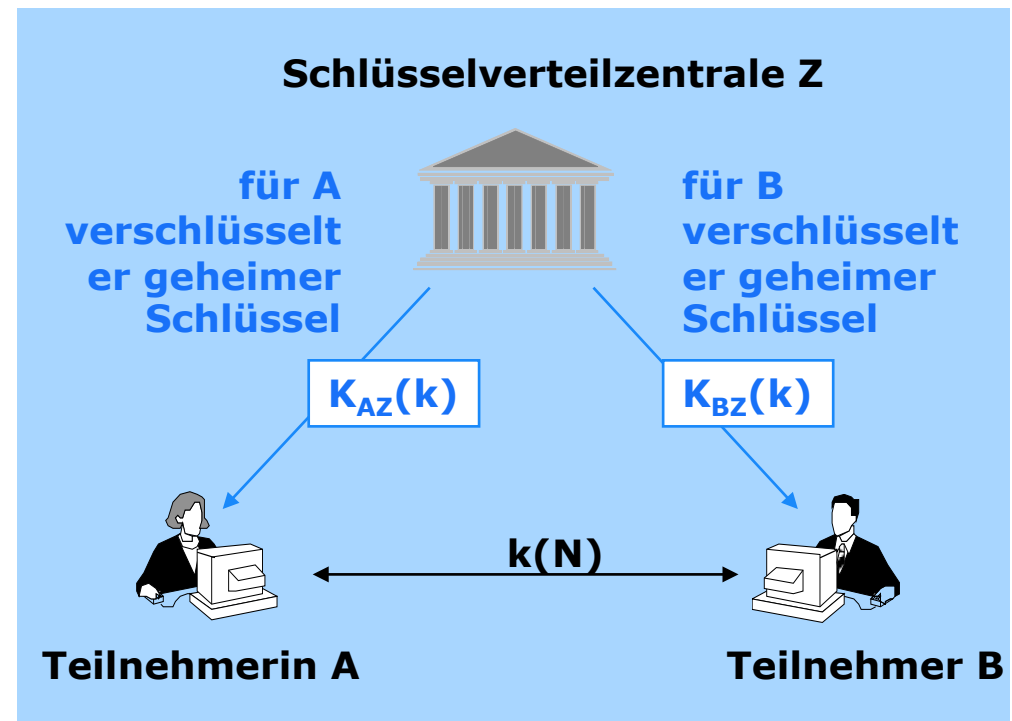
Symmetrische Verschlüsselung



Undurchsichtiger Kasten mit Schloss. Es gibt zwei gleiche Schlüssel.

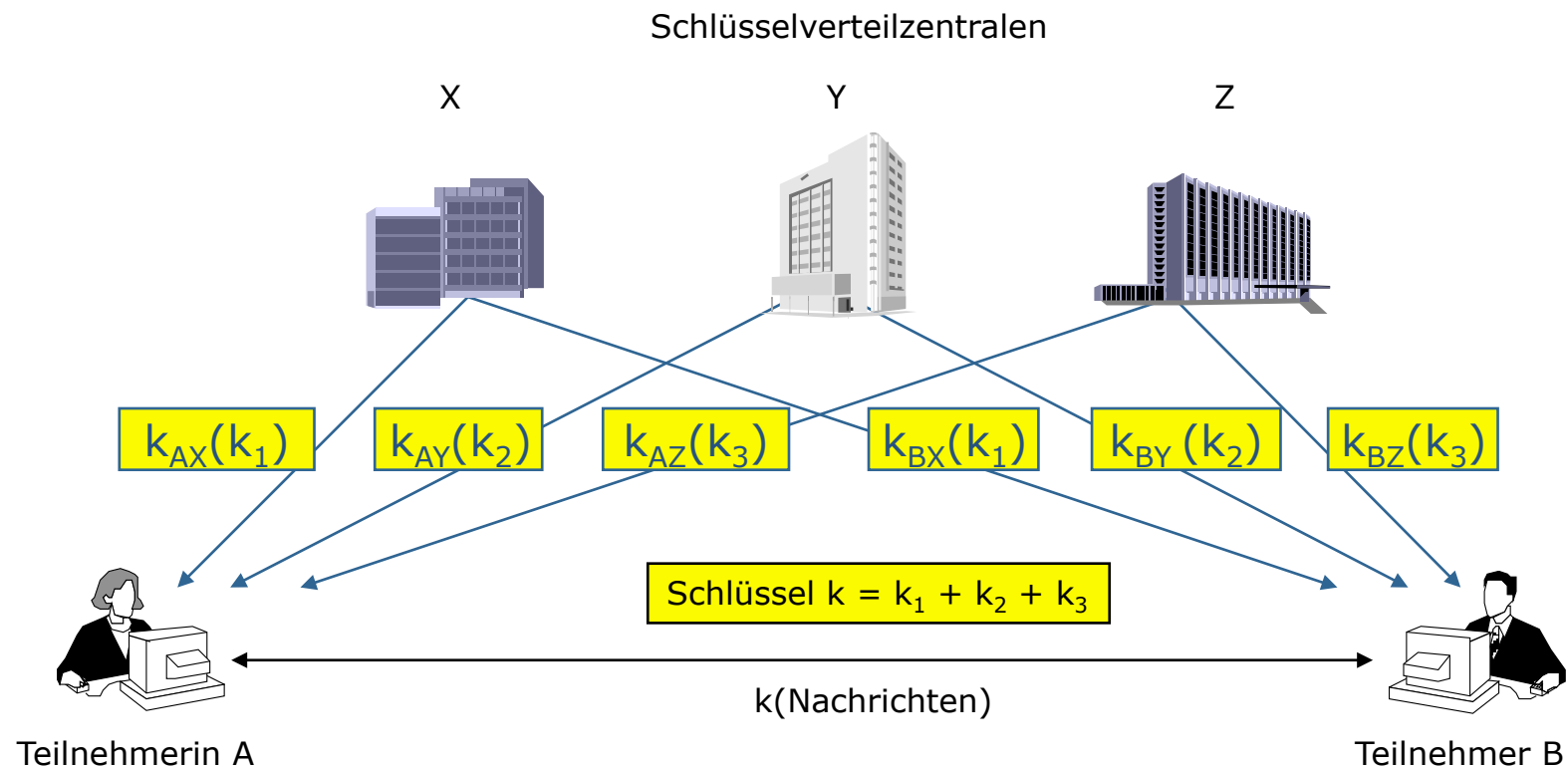
Schlüsselverteilung für symmetrische Systeme

- 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 :
 $k(N)$

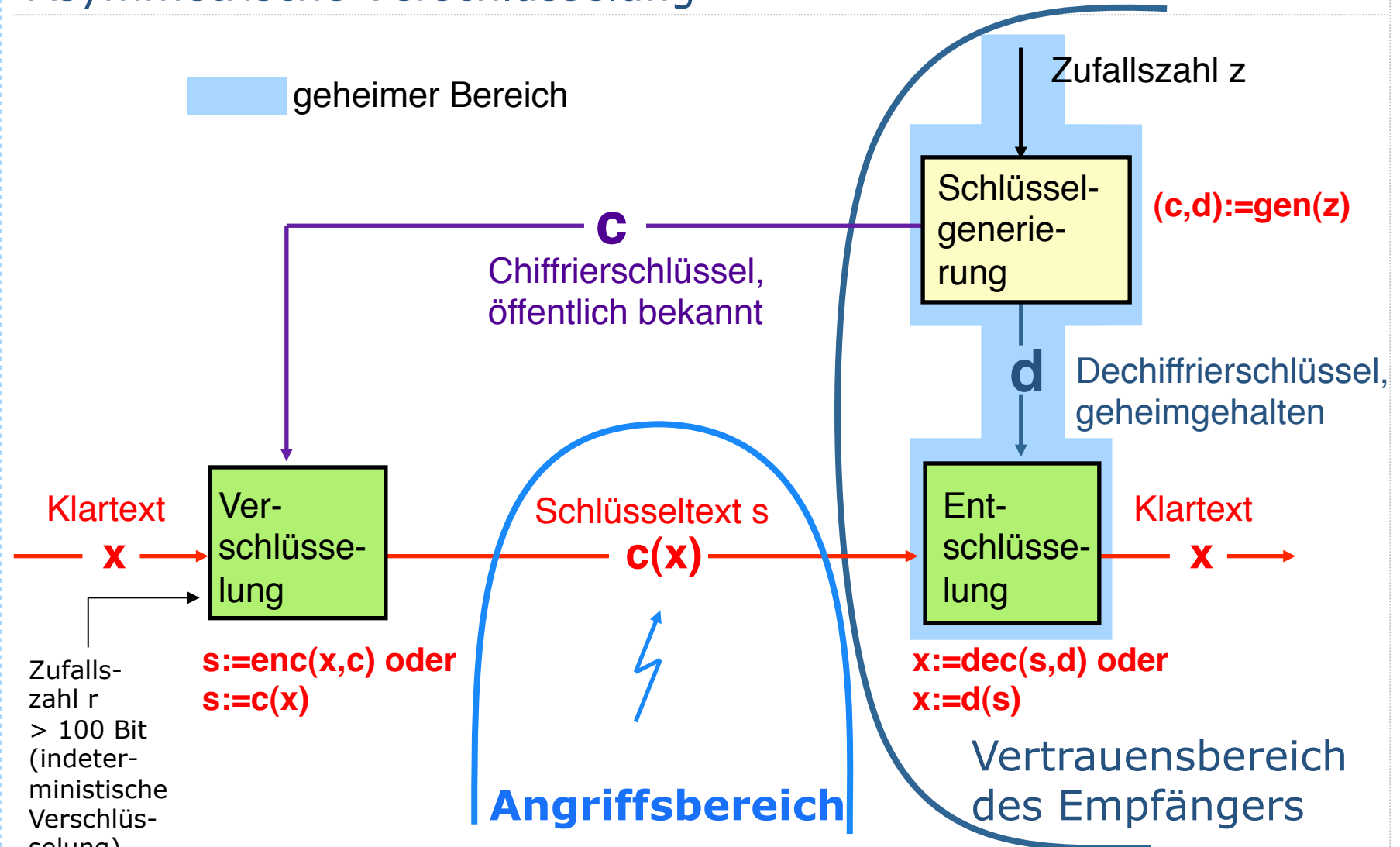


Dezentralisierte Variante

- 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

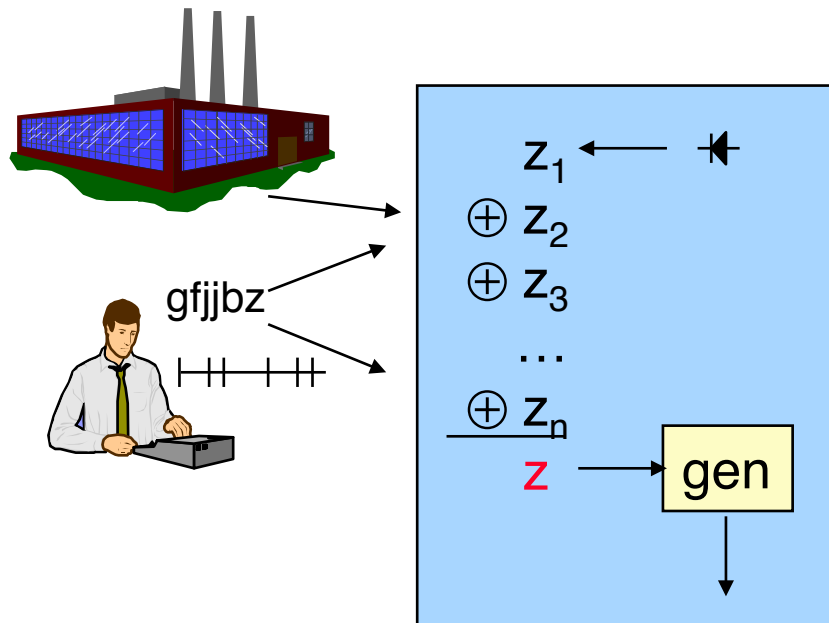


Asymmetrische Verschlüsselung



Kasten mit Schnappschloss. Es gibt nur einen Schlüssel.

Schlüsselgenerierung



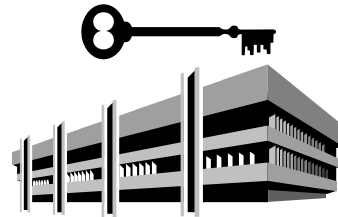
Erzeugung einer Zufallszahl z für die Schlüsselgenerierung:

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.

Schlüsselverteilung bei asymm. Kryptosystem

Öffentliches Schlüsselregister R



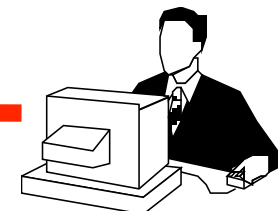
1.
A lässt seinen öffentlichen
Chiffrierschlüssel c_A
eintragen.



Teilnehmerin A

2.
B bittet das Schlüssel-
register R um den
öffentlichen Chiffrier-
schlüssel von A.

3.
B erhält von R c_A , den öffent-
lichen Chiffrierschlüssel
von A, beglaubigt
durch die Signatur
von R.



Teilnehmer B

c_A (Nachricht an A)

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+dYNnyisQEBOXcH/RGe2i30LRvRk4asX++JSTylku
8LM0lYorgW+lbmsVNxeQSdmbSAUfd3d9bI/+fGwQcz
6W8lIw2zyQkfDaF7xPI7oVZUY1I7cqEfTvic003bgL
sUZytg1nEfxqifxgukKj01066wVmqlnXcbi2XUebka
L0ViFDNkla2aw590ZW59gf5I0eUBevSmydIaliH9Pm
-----END PGP PUBLIC KEY BLOCK-----
```

c_{Alice}



Angreifer:

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

c_{Mask}

Bert besitzt jetzt nicht authentischen Schlüssel von Alice

```
Alice <alice@abc.de>
-----BEGIN PGP PUBLIC KEY BLOCK-----
OTUAoLncfli6Yit0Kqgp/N9h37uopJHbiQCVAw
xBBPLRdmalP22ij0dARxbJL07u7XOrnyV3b4m0
l4ydps/ruj9yaY62BwQNMEoGjAnZGA5t3MMGDF
7ZLp1dmFYYVYPL4xRf0J+MF5ifb8RXaDA1+1P8
CwMBAgAKCRDhQCBhSe8dhOYYAJsEEURK2o+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_{Mask}
- verschlüsseln von N mit c_{Alice}

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

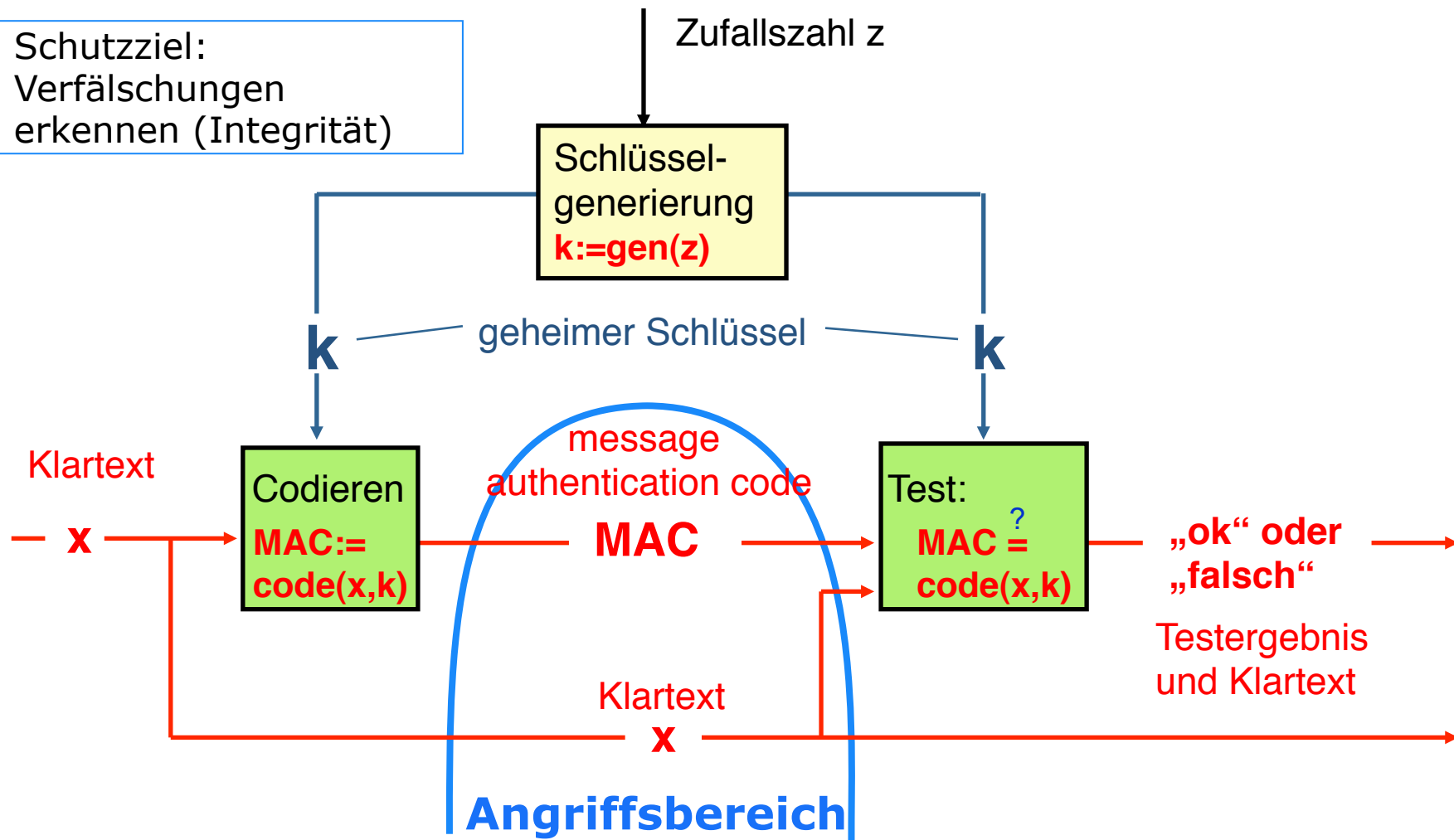
Alice erhält Nachricht N verschlüsselt mit ihrem öff. Schlüssel



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

Symmetrische Authentikation

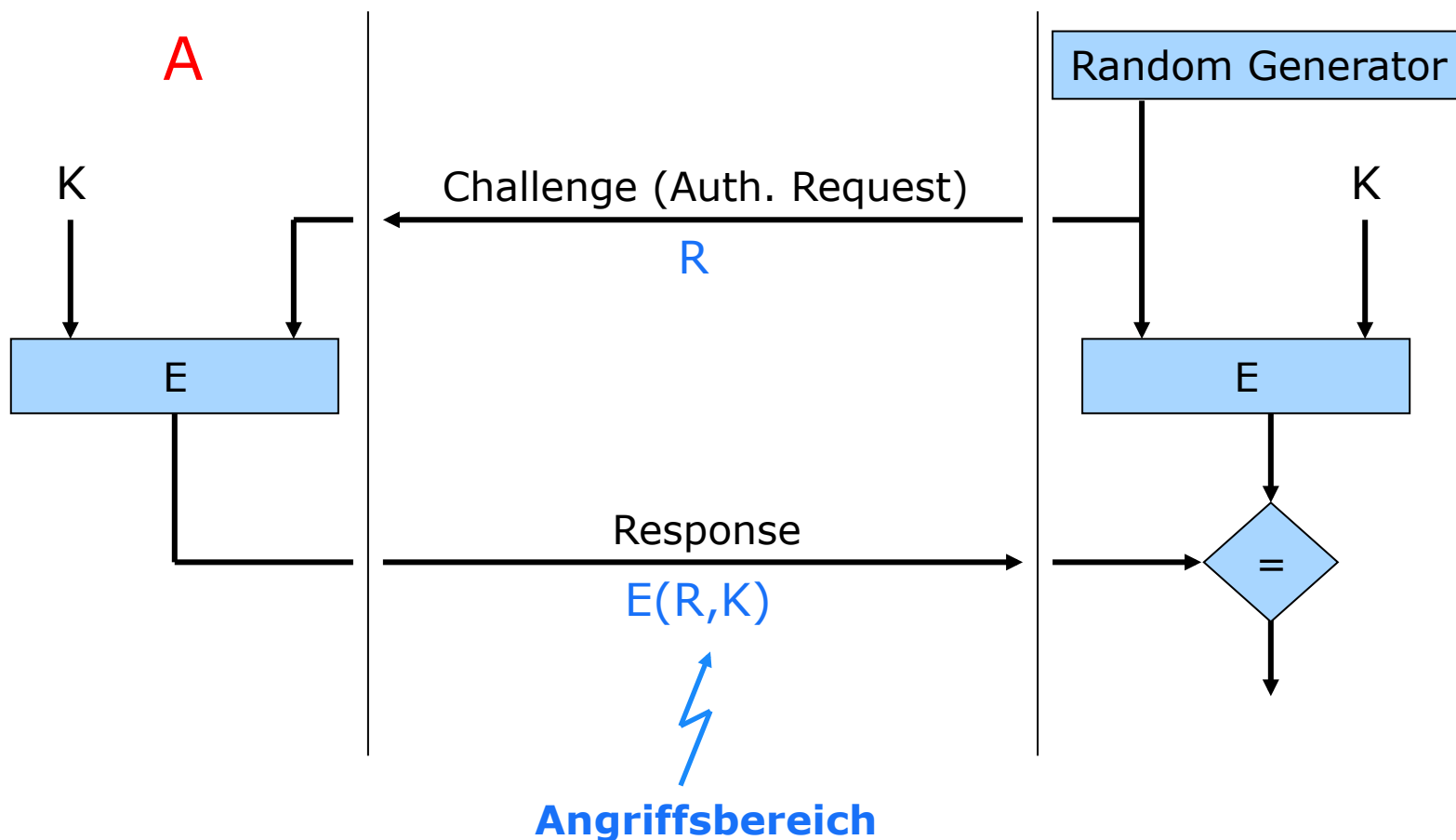
Schutzziel:
Verfälschungen
erkennen (Integrität)



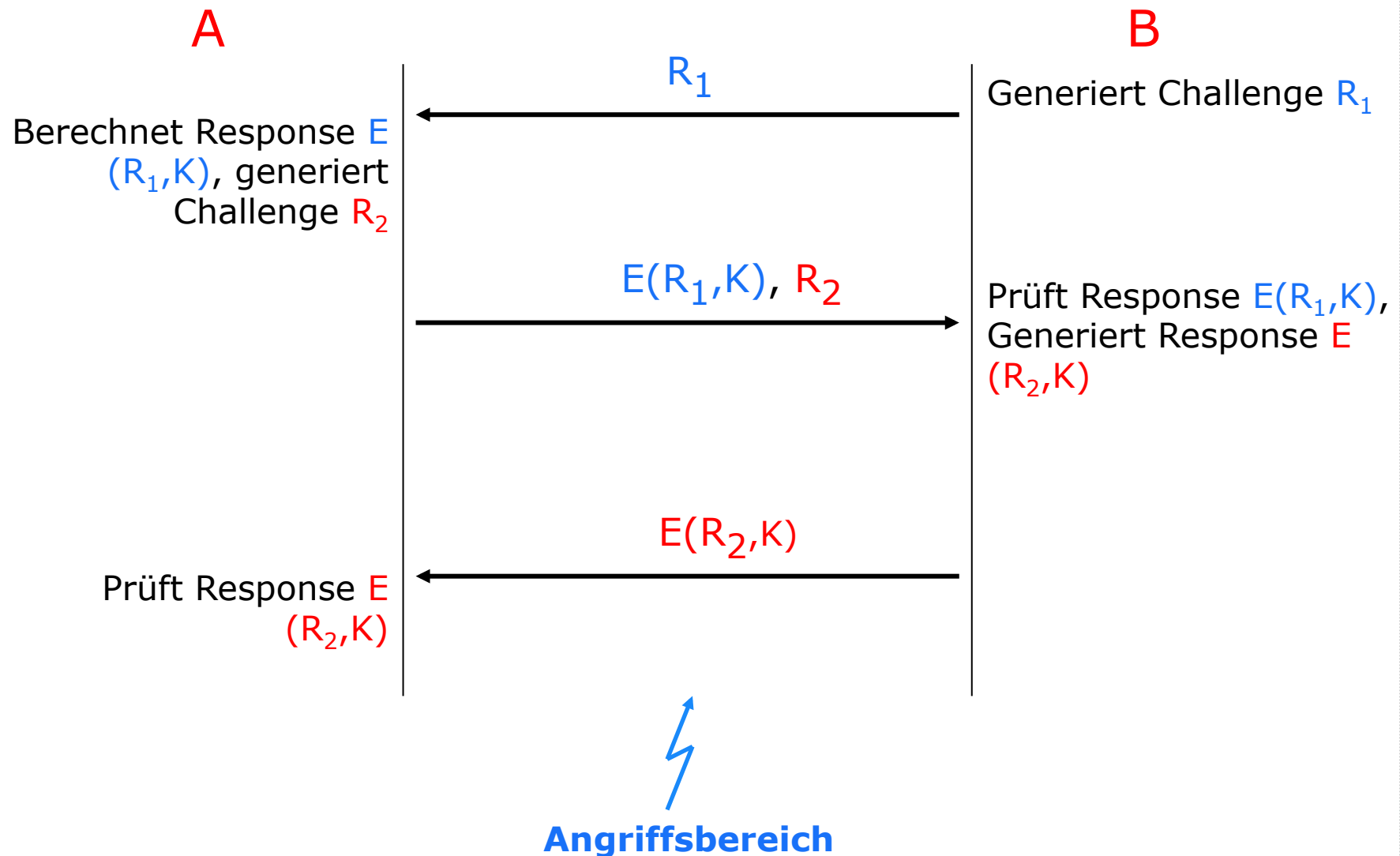
Glasvitrine mit Schloss. Es gibt zwei gleiche Schlüssel.

Challenge-Response-Authentikation

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

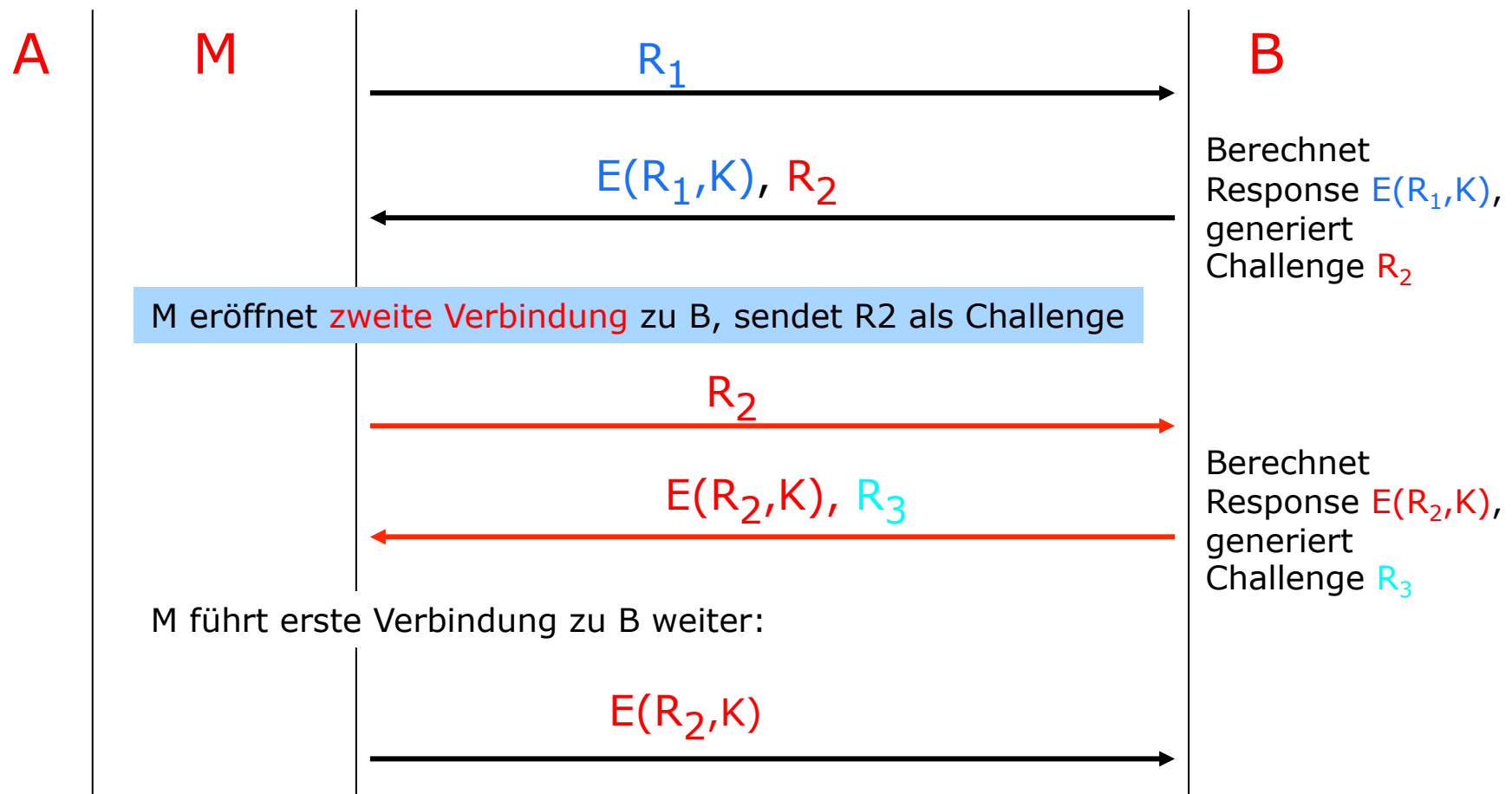


Gegenseitige Authentikation



Gegenseitige Authentikation

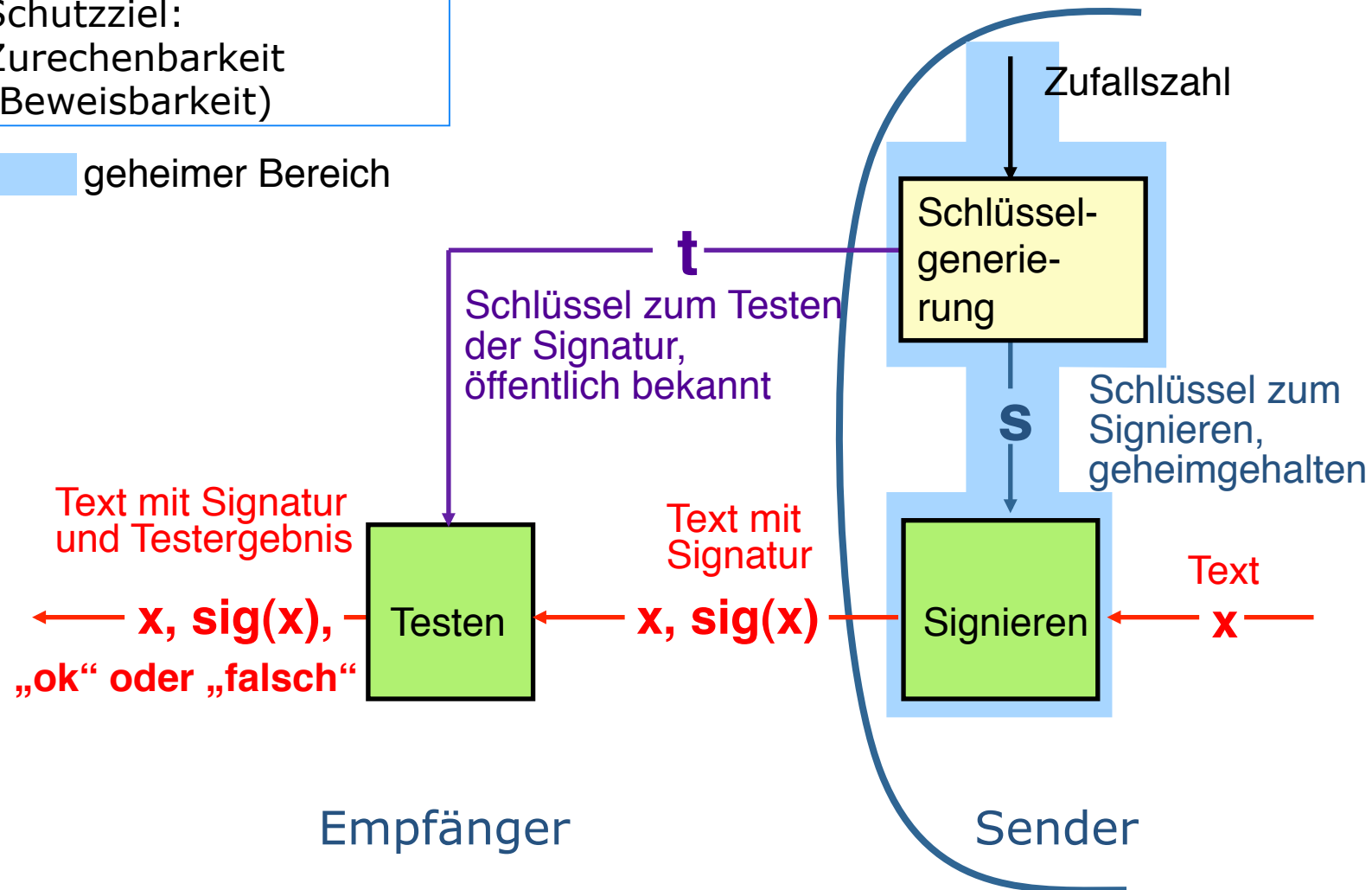
- Angriff auf gegenseitige Authentikation auf der Basis symmetrischer Kryptosysteme
 - Angreifer **M** maskiert sich als **A**, kennt **K** *nicht*



Digitales Signatursystem

Schutzziel:
Zurechenbarkeit
(Beweisbarkeit)

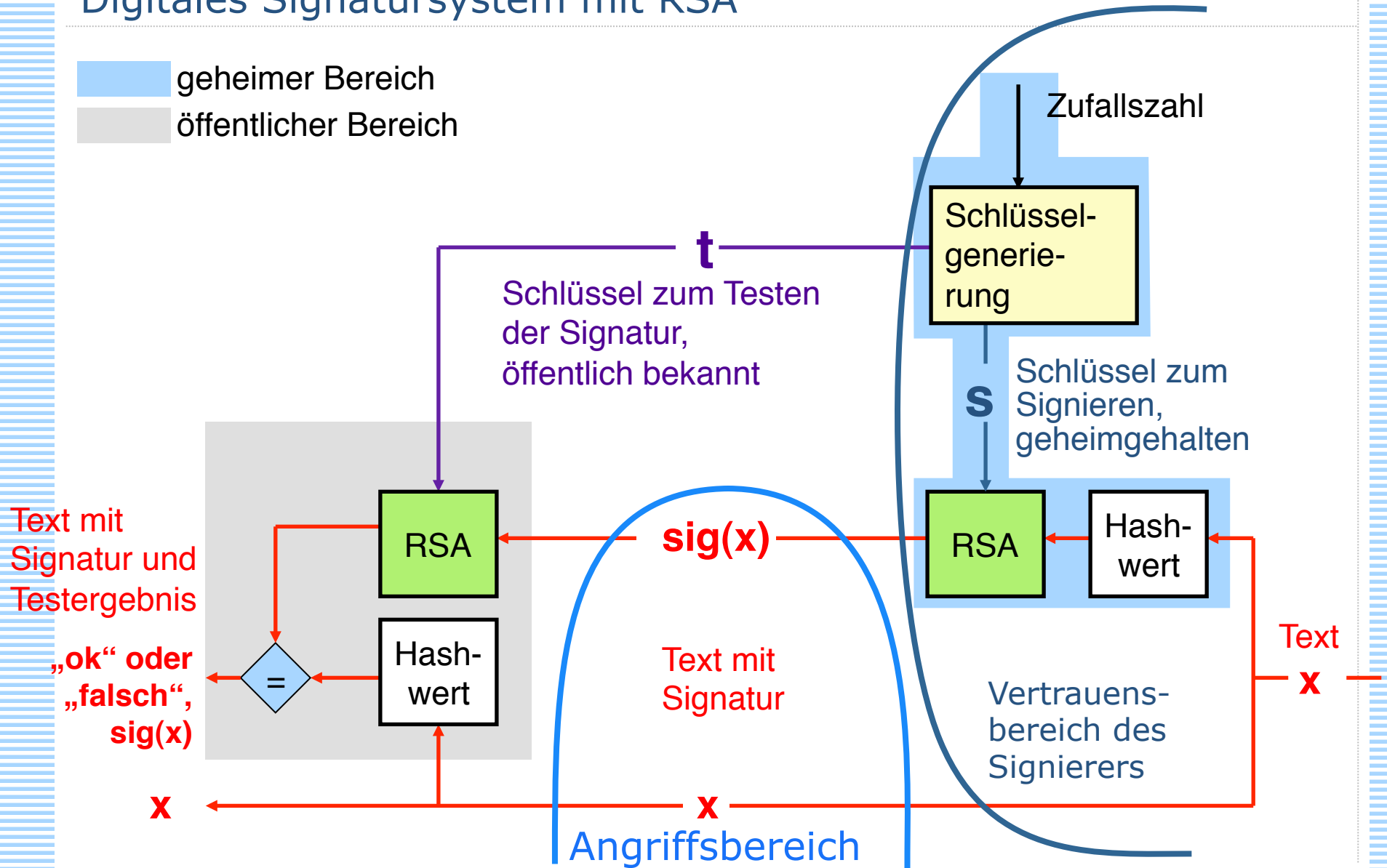
geheimer Bereich



Glasvitrine mit Schloss. Es gibt nur einen Schlüssel.

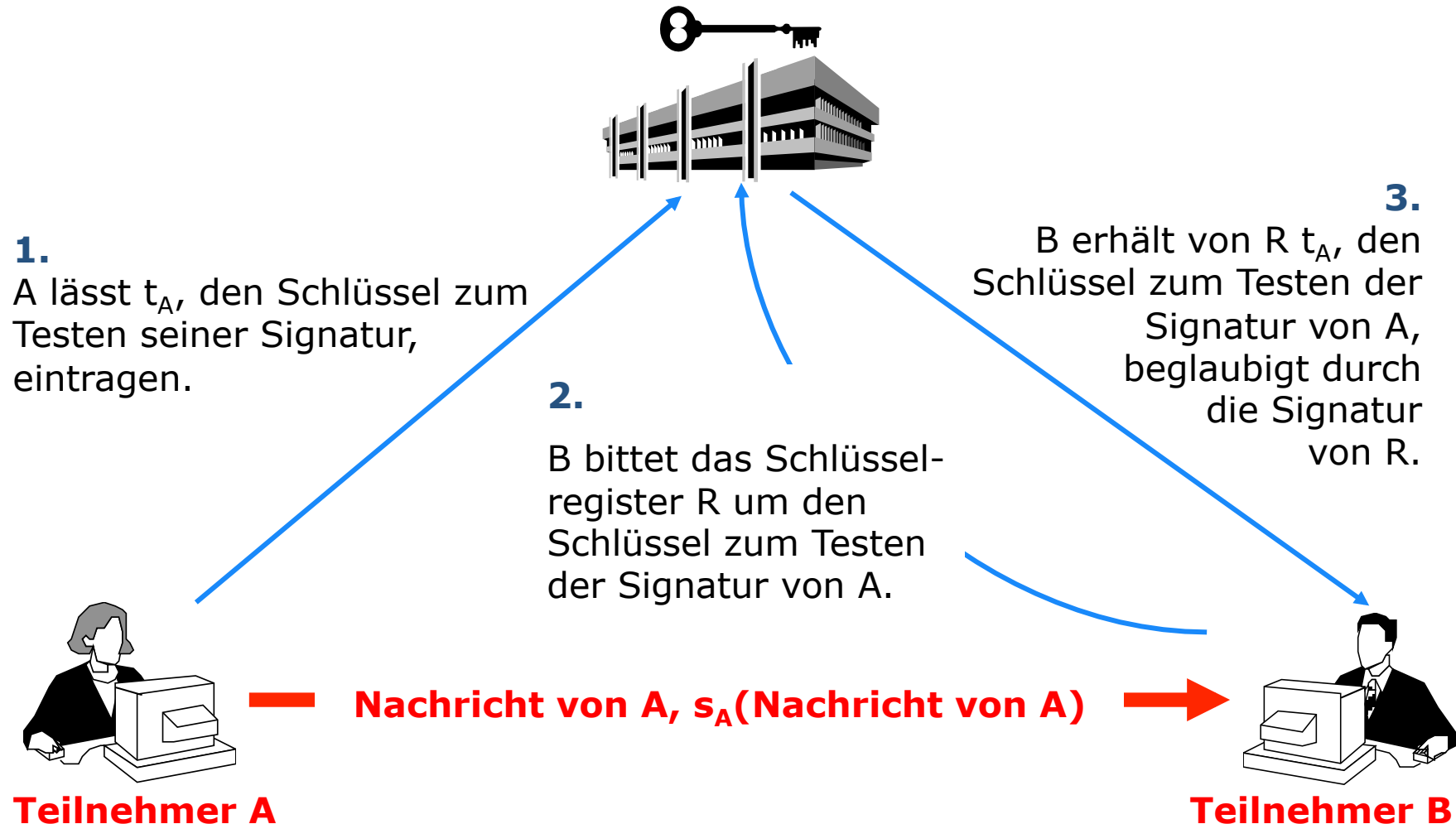
Digitales Signatursystem mit RSA

- geheimer Bereich
- öffentlicher Bereich



Schlüsselverteilung bei Signatursystem

Öffentliches Schlüsselregister R



Schlüssellängen

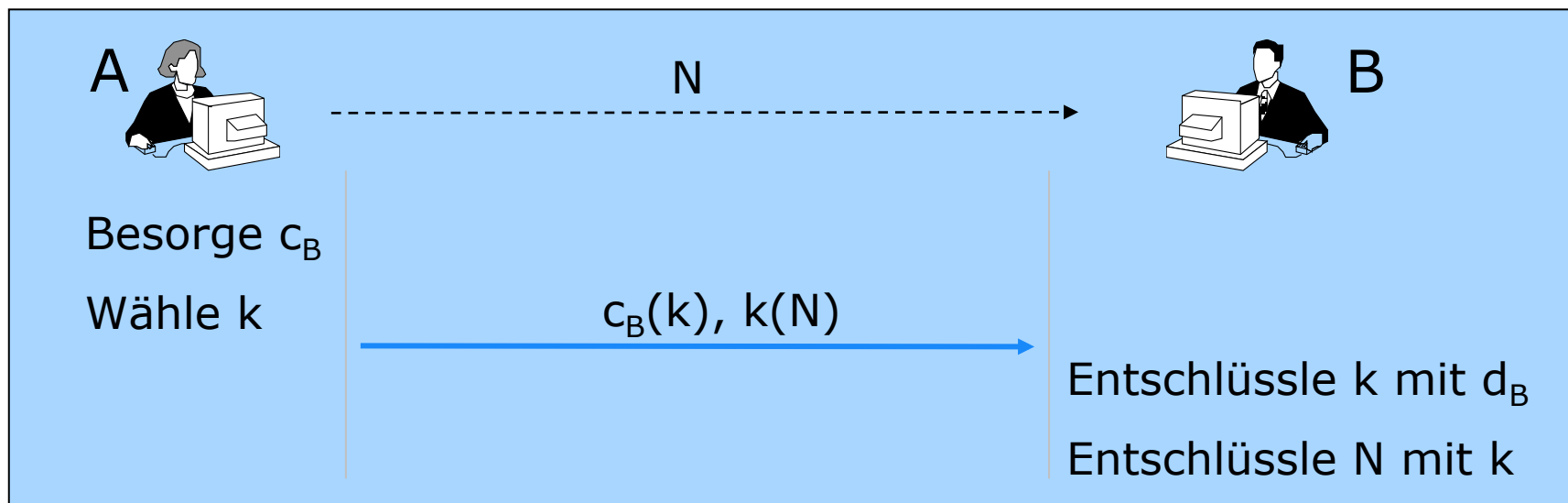
- 56 Bit (DES) sind heute unsicher
- Beispielrechnung:
 - 56 Bit Schlüssellänge → 2^{56} mögliche Schlüssel (ca. $7 \cdot 10^{16}$)
 - Ausprobieren eines Schlüssels dauere 1 Nanosekunde (10^{-9} s)
 - Ausprobieren aller Schlüssel dauert dann:
 $2^{56} \cdot 10^{-9}$ s = 72057594 s = 2,28 Jahre
- Symmetrische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

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
- Geringere Effizienz und größere Schlüssellängen werden jedoch 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/RDO0
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-----
```

```
MIKYUAp65X6E19IapJdAnrvJBzWv9XwImPypJICF5KTXL8vOLCtu
-----END PGP MESSAGE-----
```

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


Key Recovery und Key Escrow

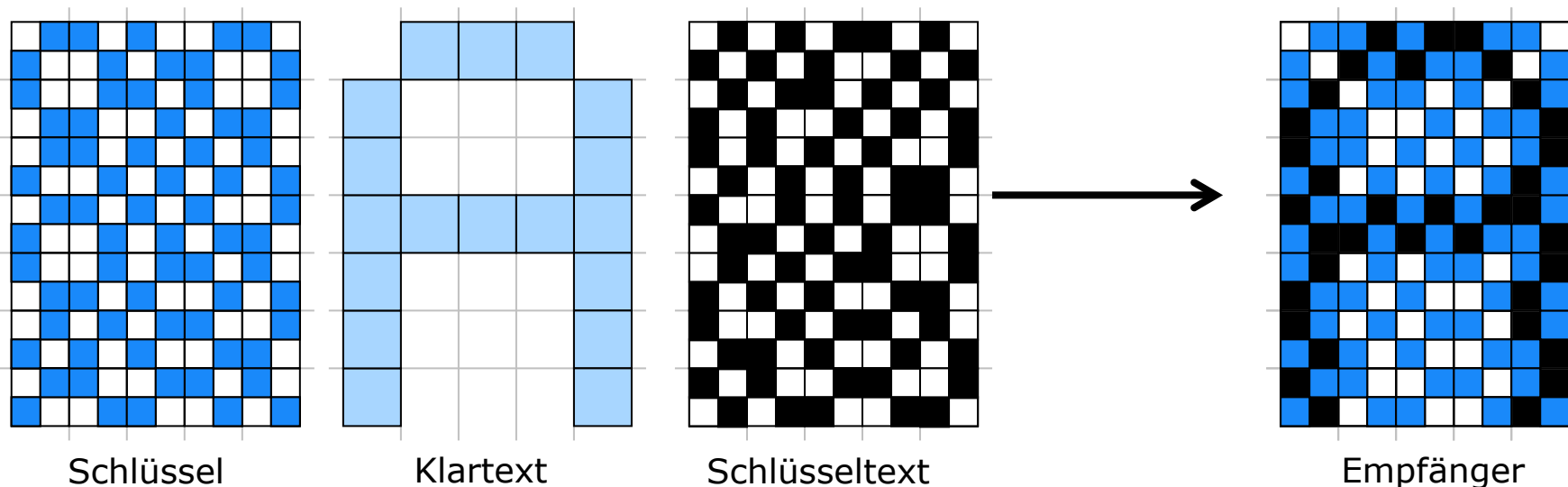
- Key Recovery
 - Hinterlegung des Entschlüsselungsschlüssels zum Zweck der Entschlüsselbarkeit bei Schlüsselverlust.
 - Schwellwertschema: Schlüssel wird in $n+k$ Teile zerlegt. Zur Rekonstruktion werden wenigstens n Teile benötigt.
- Key Escrow
 - Hinterlegung des Entschlüsselungsschlüssels zum Zweck 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.

Wann ist Key Recovery sinnvoll?

	Schutz der Kommunikation	Langfristige Speicherung
Verschlüsselung	Key Recovery für Funktion unnötig, aber	Key Recovery sinnvoll
Authentifikation	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
- Schöne Demos:
 - <http://www.tcs.uni-luebeck.de/de/forschung/software/vc/>
 - <http://www-sec.uni-regensburg.de/vc/>

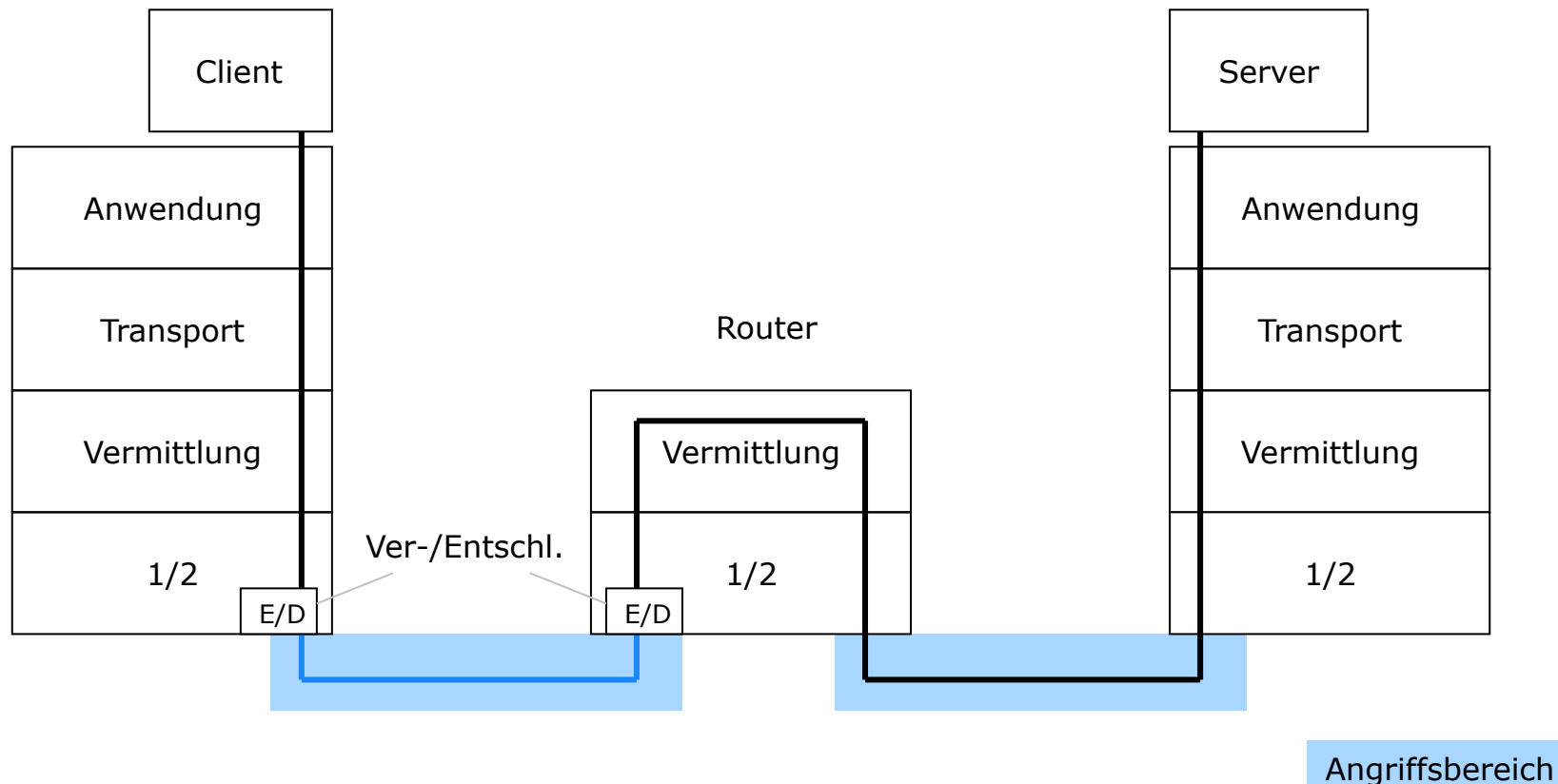


Sicherheitsfunktionen nach Schichten geordnet

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), Wireless Equivalent Privacy (WEP)

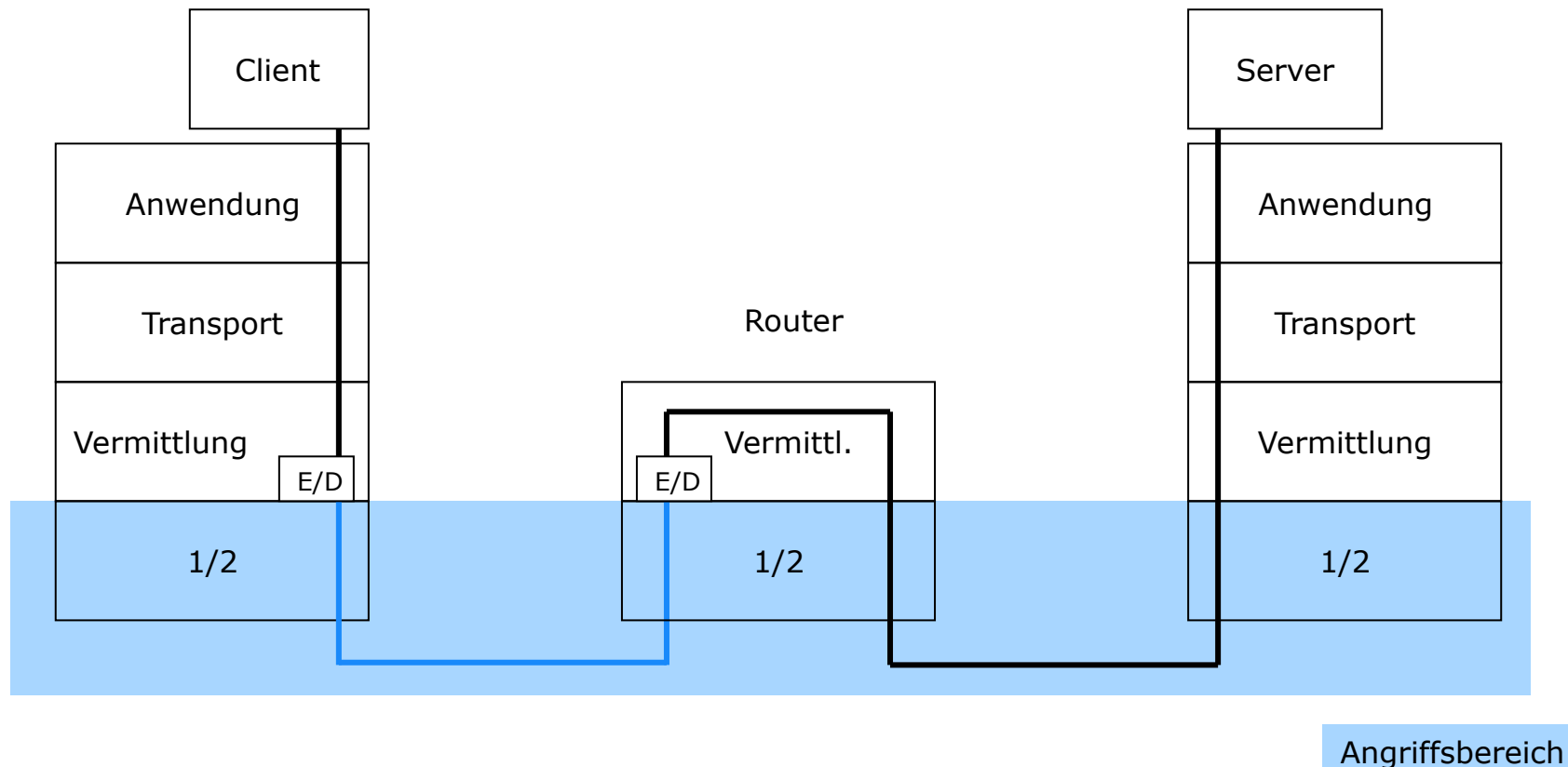
Verschlüsselung in Schicht 1/2

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



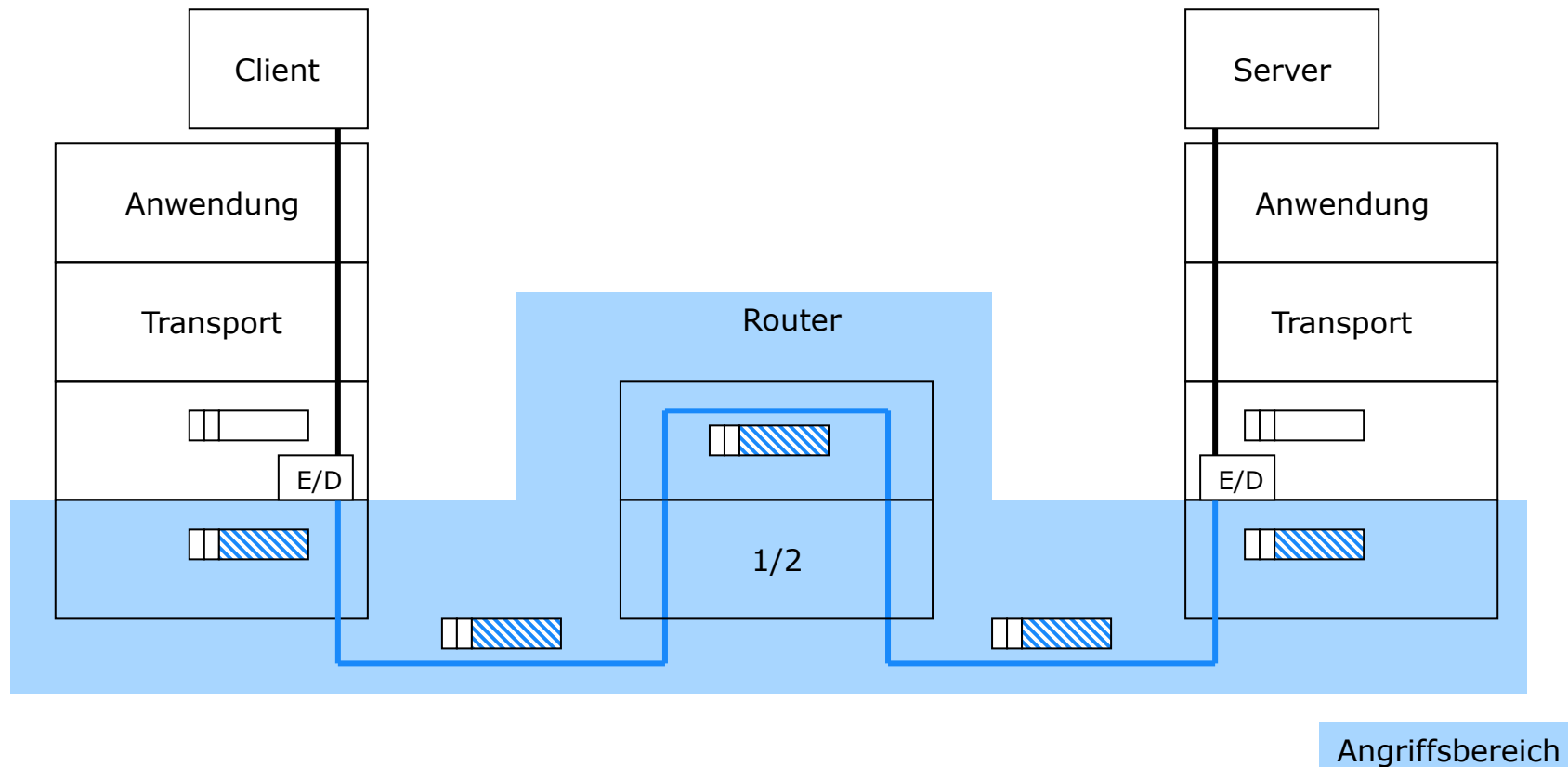
Verschlüsselung in Vermittlungsschicht: IPSec

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



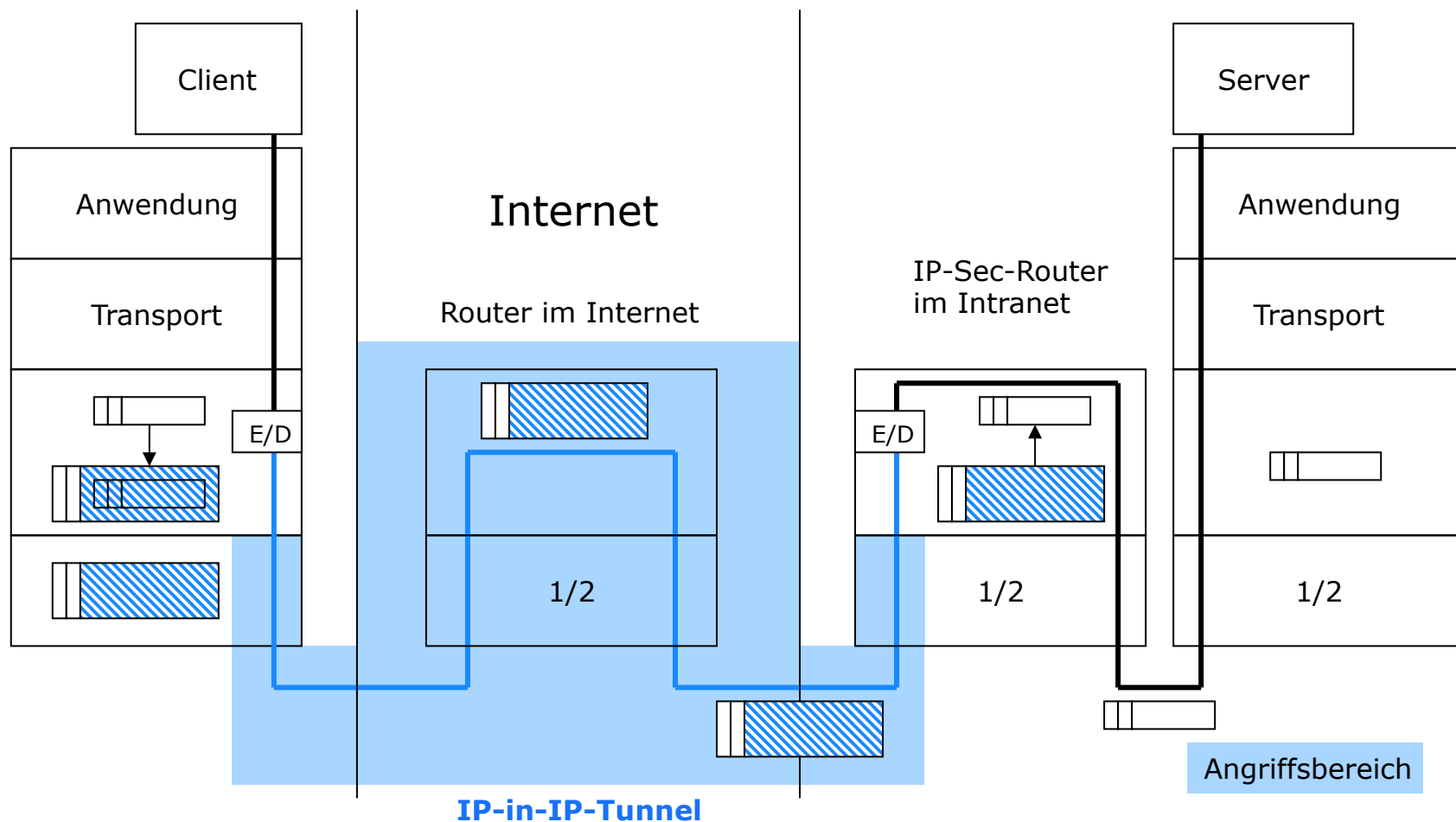
Verschlüsselung in Vermittlungsschicht: IPSec

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



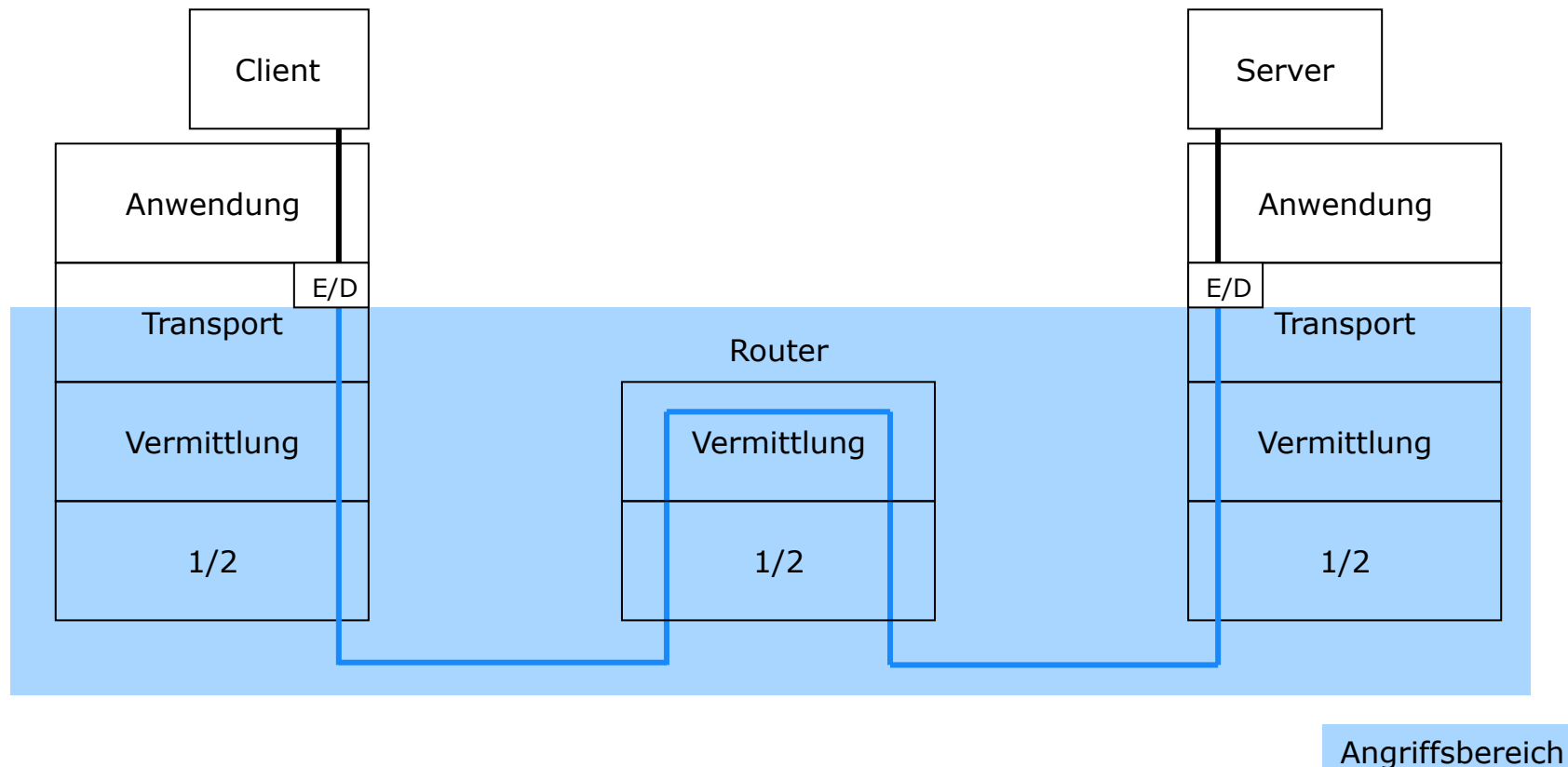
Verschlüsselung in Vermittlungsschicht: IPSec

- Momentane Hauptanwendung: Virtuelles Privates Netz
 - «Tunnelmodus»



Verschlüsselung in Transportschicht: SSL/TLS

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

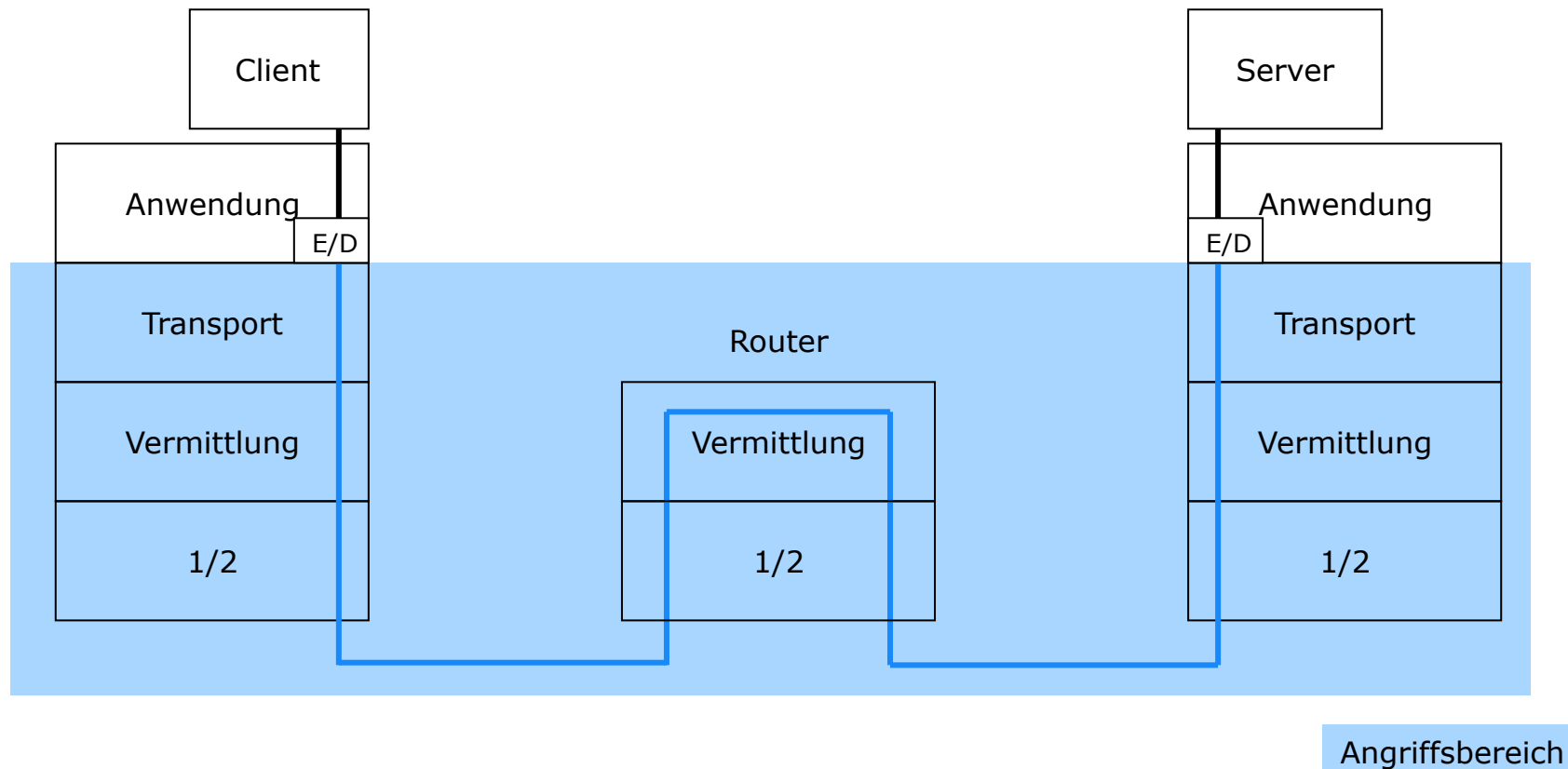


Vergleich SSL – IPSec

	SSL	IPSec
Komplexität	hoch	gering
Anwendungsnahe	hoch	gering
Für VPNs geeignet?	nein	ja
Für paketorientierte Dienste geeignet?	nein	ja
Für verbindungsorientierte Dienste geeignet?	ja	ja

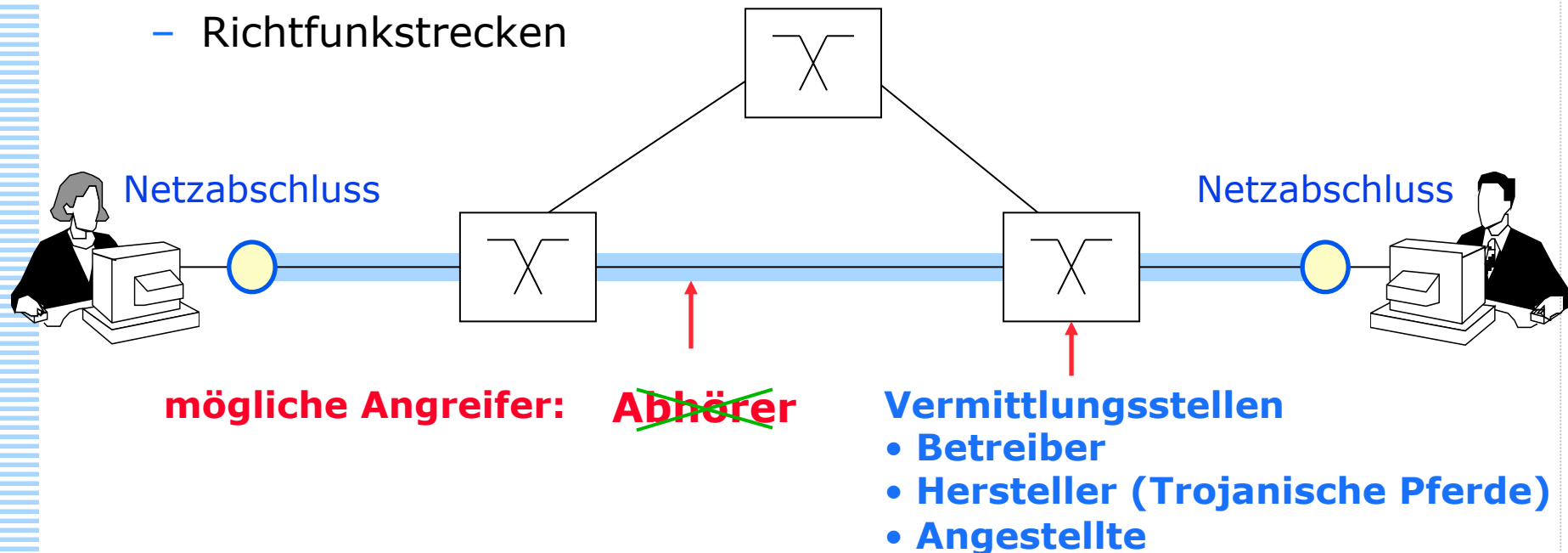
Verschlüsselung in Anwendungsschicht

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



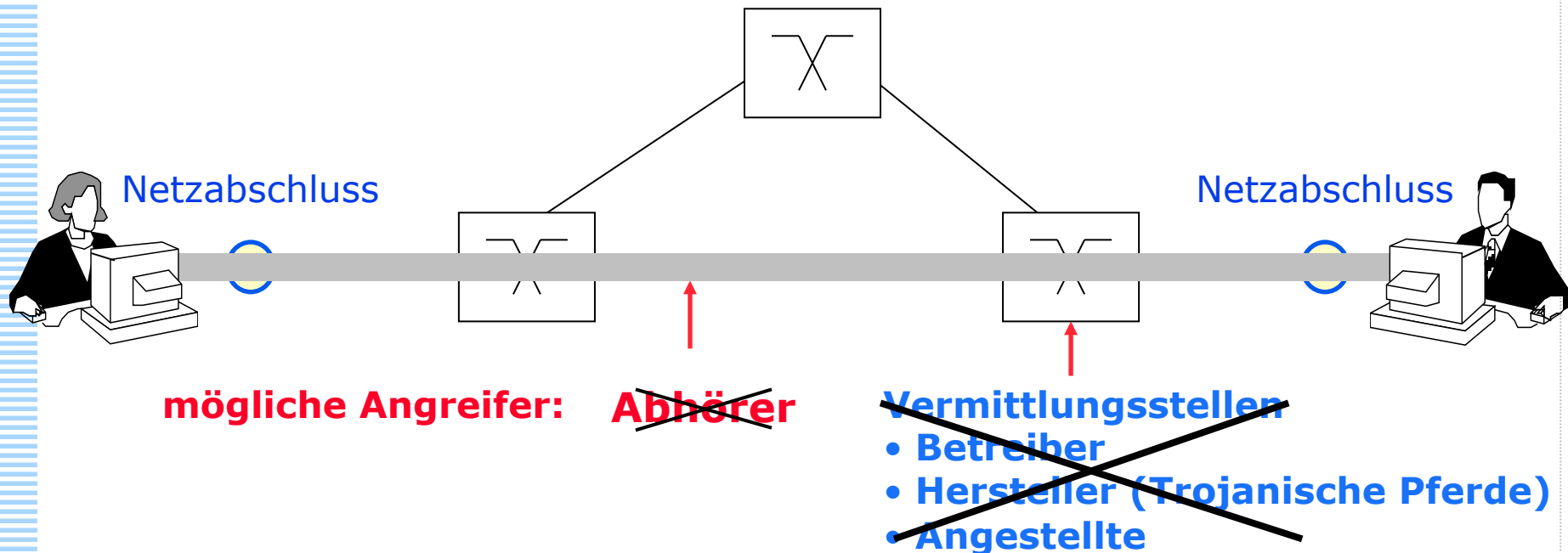
Verbindungsverschlüsselung

- 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

