



Kryptographie im Internet

Vortrag am Salza-Gymnasium

Tobias Giese HS-Harz

10.06.2005



◆ Agenda

Theorie

- **Das Internet** – Historie, Struktur, Schwächen
- **Die Kryptographie** – Begriffsdefinition, Historie, Einführung
- **Varianten** der Kryptographie
 - **Symmetrische** Verschlüsselung
 - **Asymmetrische** Verschlüsselung
- **Public-Key-Infrastrukturen**
 - **Digitale Signaturen**
 - **Hash-Funktionen**
 - **Zertifikate** und Zertifizierungsstellen
- **Sicherheitsprotokolle** im Internet
 - **SSL** (hybride Verschlüsselung)

Praxis

Paketanalyse

Paketanalyse

Paketanalyse



◆ Meine Person

- **Abitur 1999** am Salza-Gymnasium
- 10-monatige Armeezeit
- Oktober **2000** Studium der **Kommunikationsinformatik** an der **Hochschule Harz** in **Wernigerode** (www.hs-harz.de)
- 5-monatiges Praktikum bei **IBS GmbH** Hannover
- Vertiefungsrichtung: „**Distributed Computing**“
- 8-monatiges **Diplompraktikum** bei **Intershop** Jena
- Abschluss als Dipl.-Inf.(FH) im April 2005
- derzeit im **Masterstudiengang** Informatik/Mobile Systems



◆ Hochschule Harz

- 1991 gegründet
- derzeit ca. 3000 Studenten in 18 Studiengängen
- Fachbereich Automatisierung / Informatik
- Fachbereich Wirtschaftswissenschaften
- Fachbereich Verwaltungswissenschaften



Besonderheiten:

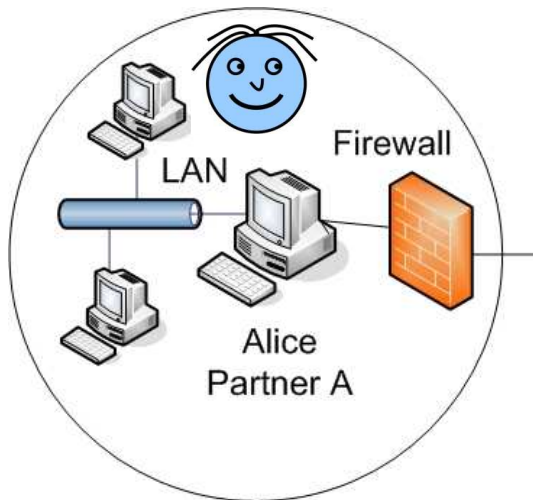
- kleine Vorlesungsgruppen
- kompakter Campus
- schicke Landschaft



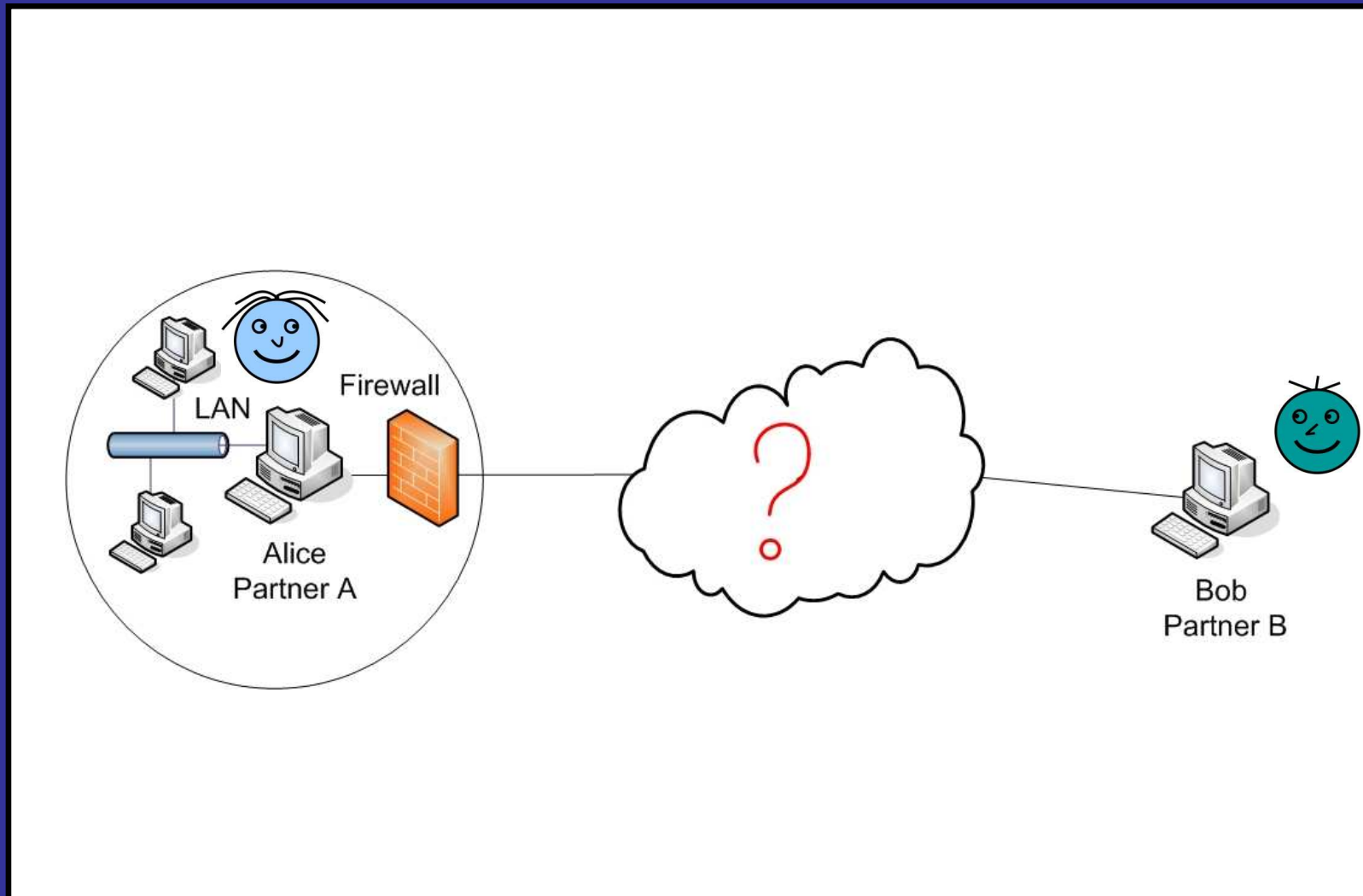
◆ Entwicklung des Internets und Schwachstellen

- historisch gewachsen → **dezentraler** Ansatz
- **Funktionalität** stand im Vordergrund
- Das Internetprotokoll **TCP/IP** hat folgende **Schwachstellen**:
 - TCP/IP verwendet **keine** Verschlüsselung
 - **Absenderadresse** kann problemlos gefälscht werden (IP-Spoofing)
- **Routerinformationspakete** können gefälscht werden
- Manipulation der **Umwandlung** Domain-Namen in IP-Adresse (DNS-Spoofing)
 - Sinneswandel Mitte der 90er Jahre: **Sicherheit**
 - E-Commerce
 - Online-Banking
 - Email- und Datentransfer

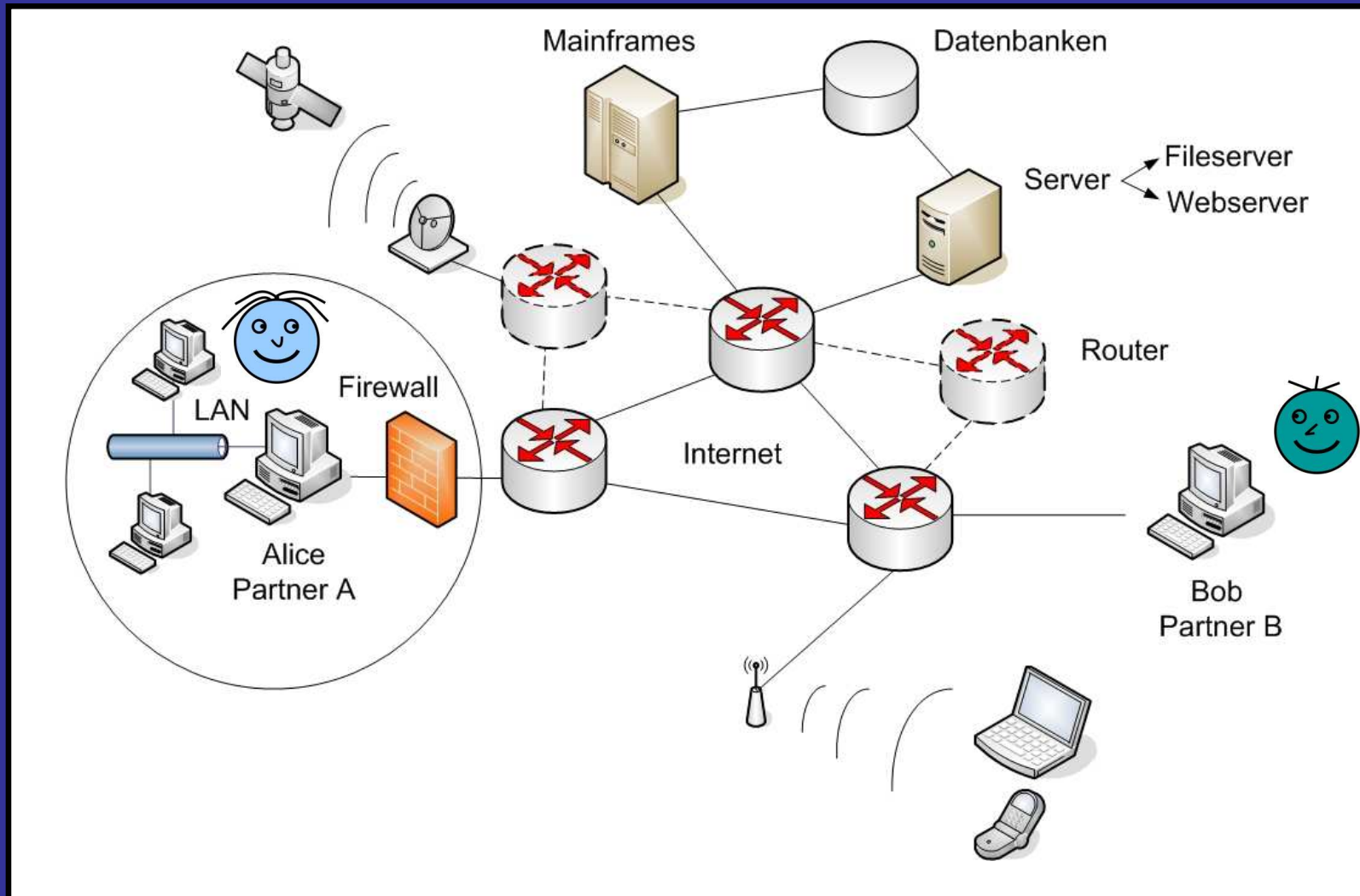
◆ Internet - Alice Partner A



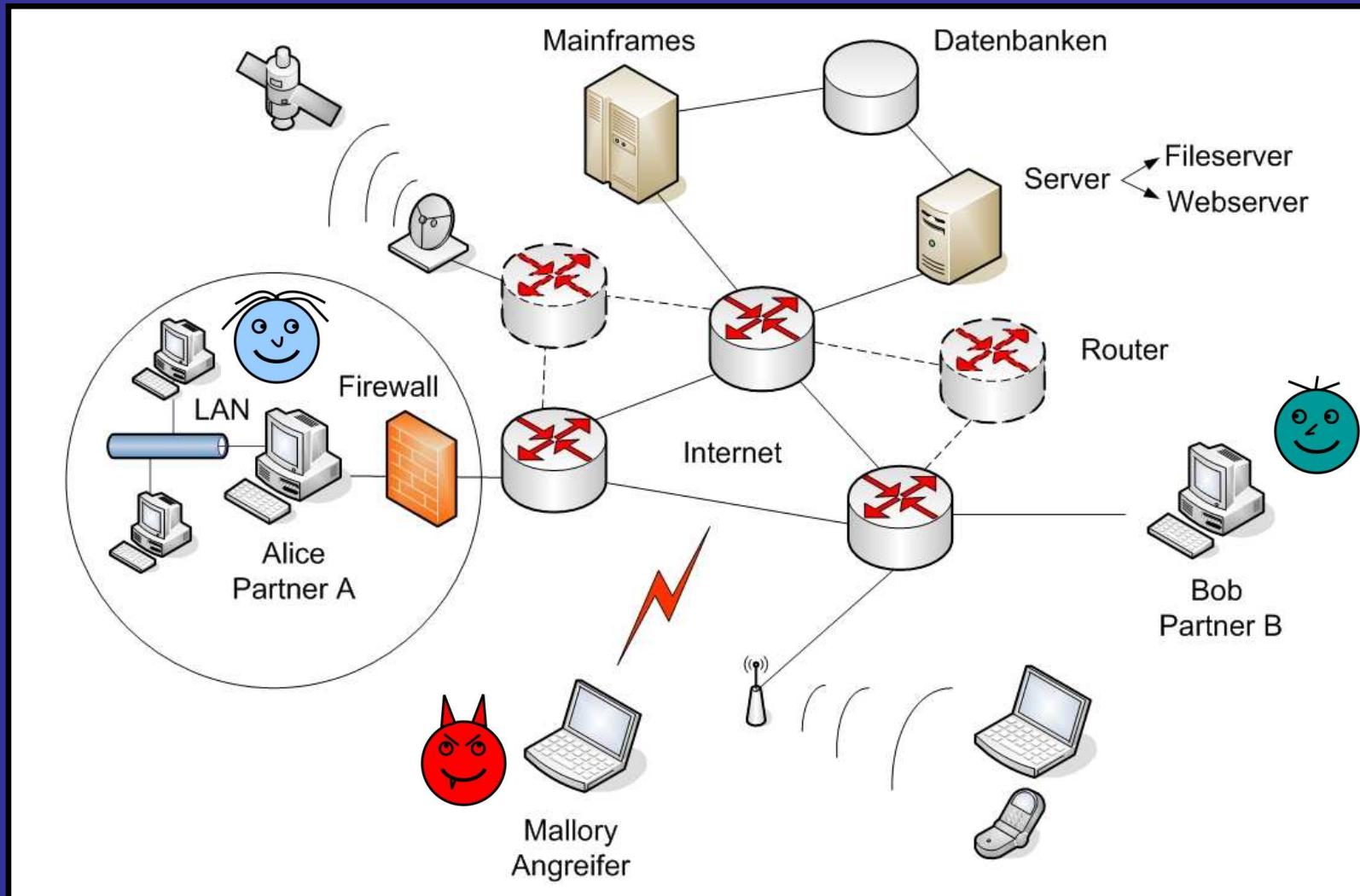
◆ Internet - Bob Partner B



◆ Internet – Router, Server und Datenleitungen

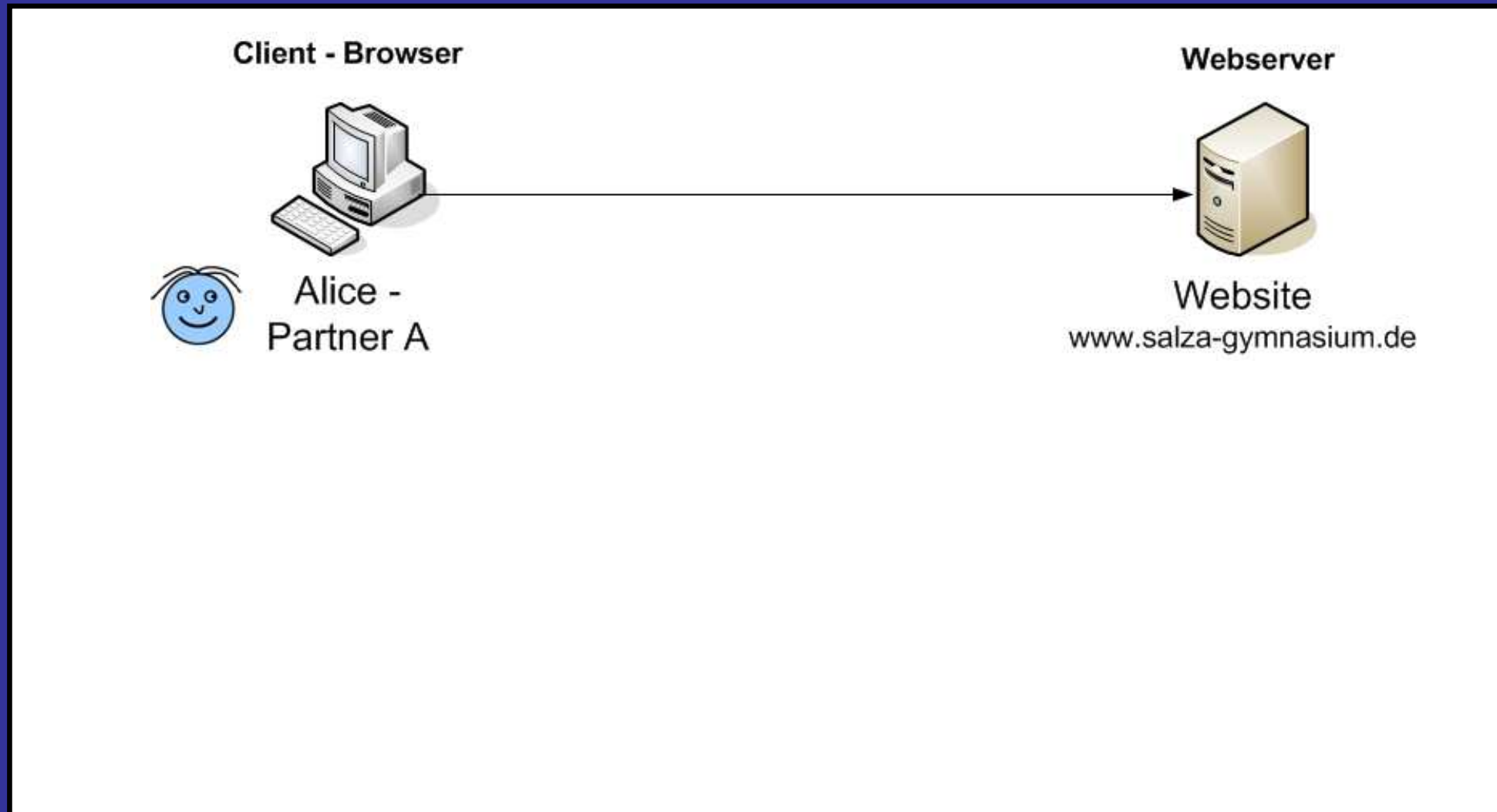


◆ Internet – eine Übersicht (mit Angreifer)



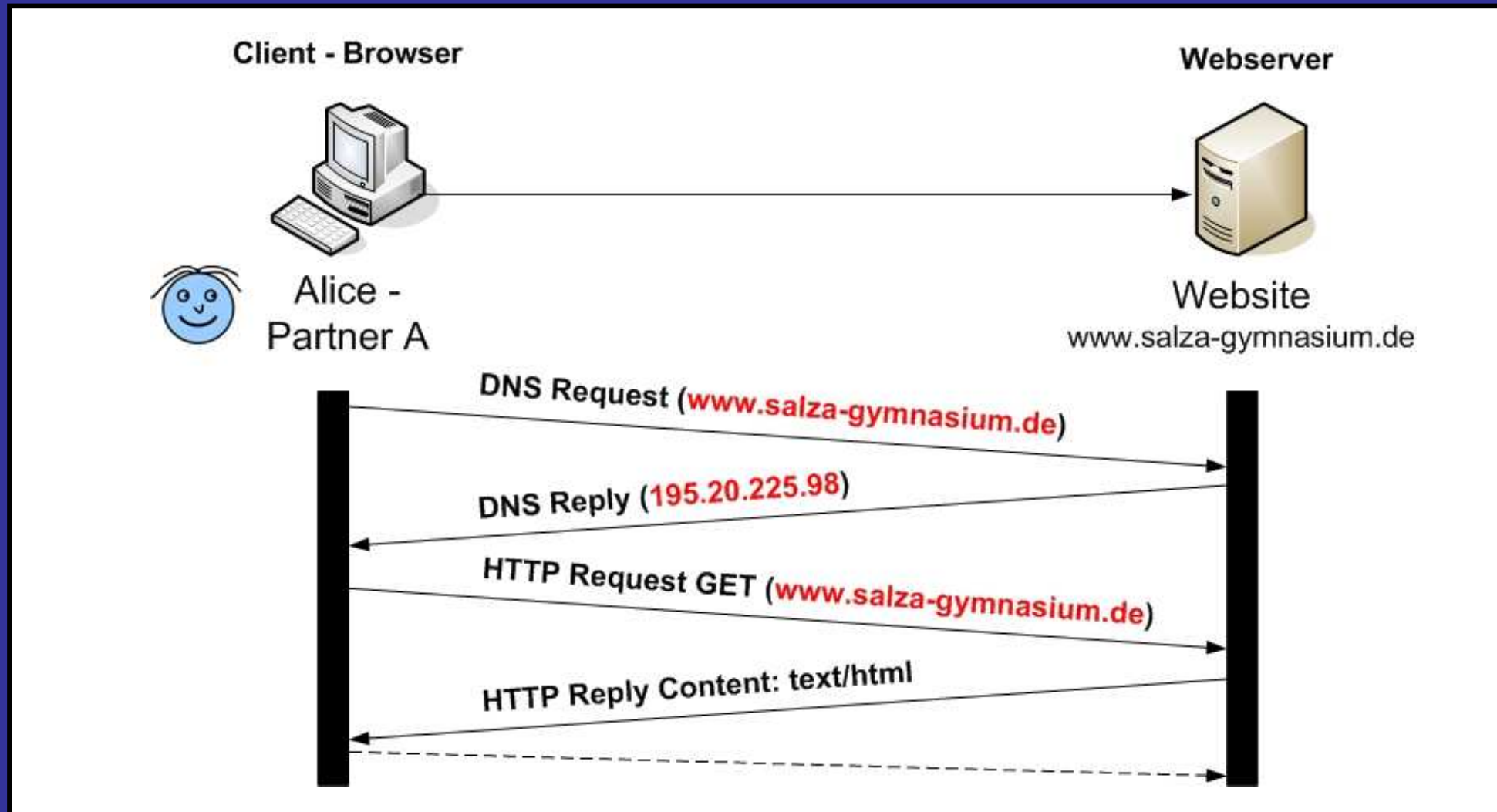
Netzwerksniffer im Einsatz 1

◆ Aufrufen einer Website – Pakete auf der Reise

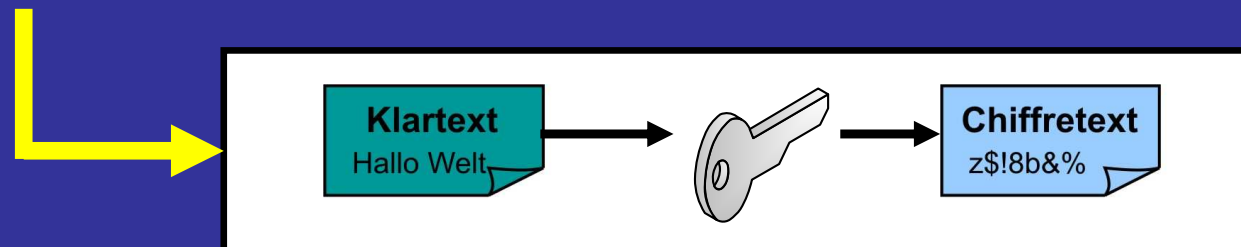
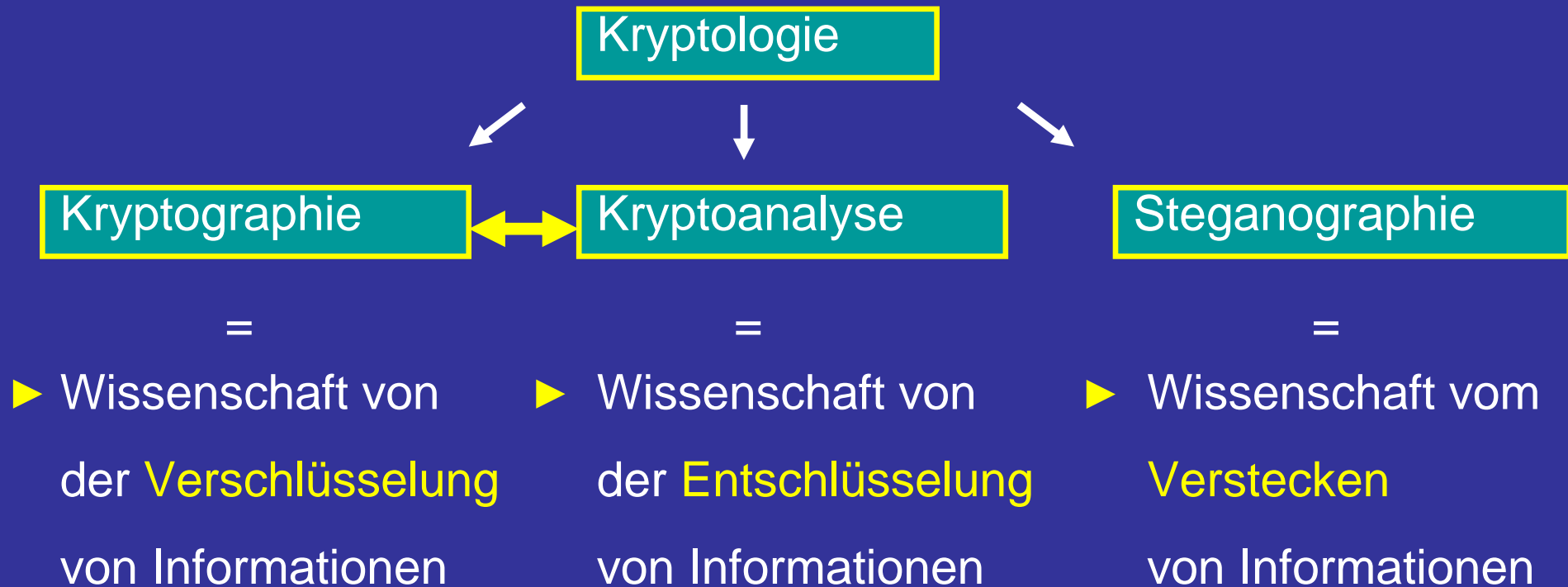


Netzwerksniffer im Einsatz 1

◆ Aufrufen einer Website – Pakete auf der Reise



◆ Was ist Kryptographie?

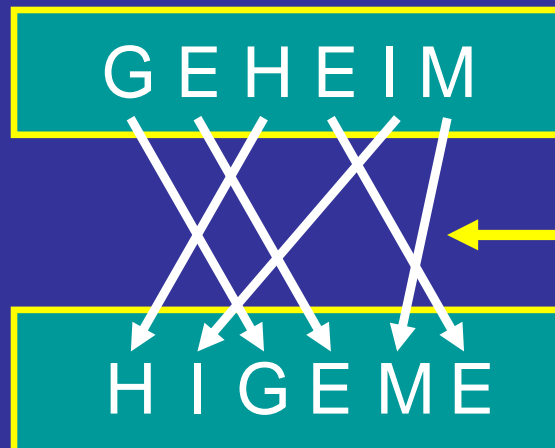


◆ Grundlagen der Kryptographie

Permutation

Text:

GEHEIM



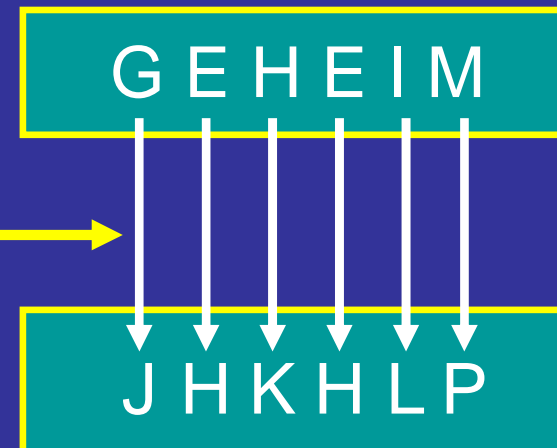
Geheimtext:

HIGEME

Buchstaben bleiben **was** sie sind, aber **nicht wo** sie sind!

Substitution

GEHEIM



Buchstaben bleiben **wo** sie sind, aber **nicht was** sie sind!

Abbildung von Text ↔ Geheimtext
= Schlüssel

◆ Monoalphabetische Verschlüsselung

Original:

ABCDEFGHI

Schlüssel:

FZUASKLTM

▶ beliebiges Alphabet

Original:

ABCDEFGHI

Schlüssel:

DEFGHIJKL

▶ Verschiebechiffren
z.B.: **Cäsar-Verschlüsselung**

Original:

ABCDEFGHI

Schlüssel:

ZYXWVUTSR

▶ Atbash

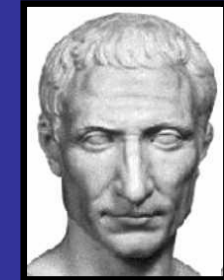
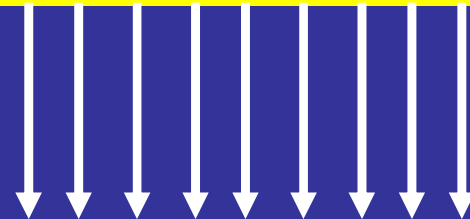
↑
hebräische Geheimschrift,
beruht auf **Umdrehung** des
Alphabets

Kryptoanalyse: **Häufigkeitsanalyse**

◆ Beispiel für eine Verschiebechiffre – Cäsarchiffre

Text:

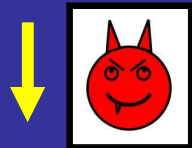
GEHEIMNIS



Geheimtext:

JHKHLPQLV

Kryptoanalyse: - vollständige Schlüsselsuche a.k.a. Brute-Force-Attacke
- Häufigkeitsanalyse



Verschiebung $n=3$

ABCDEFGHIJKLMNOPQRSTUVWXYZ

ABCDEFGHIJKLMNOPQRSTUVWXYZ



Vigenère-Verschlüsselung

◆ Polyalphabetische Verschlüsselung

Text:

GEHEIMNIS

Schlüssel:

AKEYAKEYA

Chiffretext:

GOLCIWRG

S

monoalphabetisch

polyalphabetisch

Buchstabe auf
Buchstabe im
gleichen Alphabet

Buchstabe auf
Buchstabe in einem
anderen Alphabet

S
c
h
l
u
s
s
e
r

Text

A	B	C	D	E	F	G	H	...
B	C	D	E	F	G	H	I	... C
D	E	F	G	H	I	J	...	DE
F	G	H	I	J	K	...	F	FG
H	I	J	K	L	...	F	G	H
K	L	M	...	G	H	I	J	K
M	N

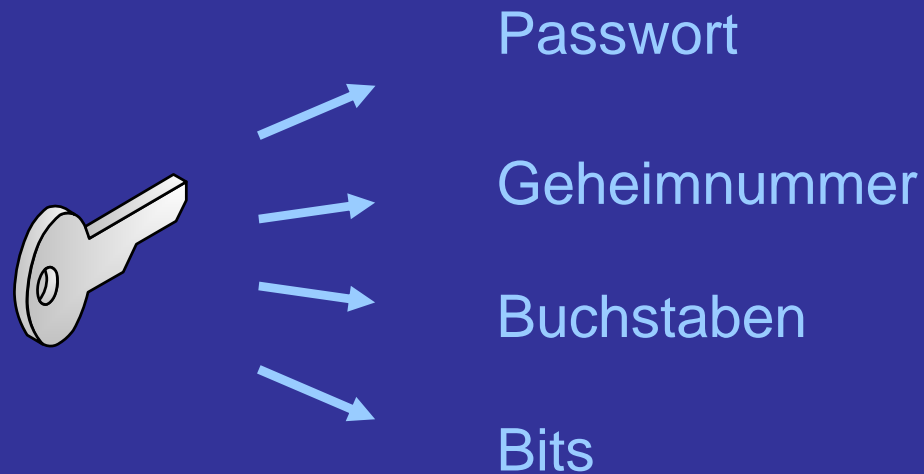
Vigenère-Verschlüsselung galt lange als sicher
Kryptoanalyse: Häufigkeitsanalyse

absolute \leftrightarrow relative Sich.

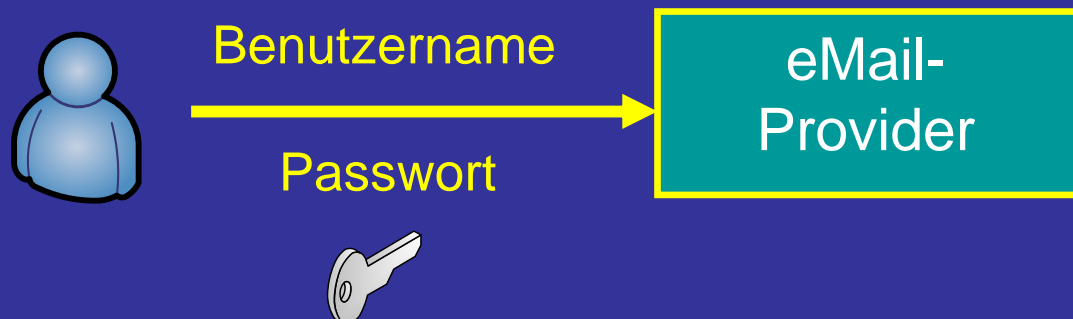
◆ Absolut sichere Verschlüsselung - One-Time-Pad

- Wenn **Schlüssellänge = Klartextlänge** \rightarrow Vernam-Verschlüsselung oder **One-Time-Pad**
- Besonderheiten: Schlüssel ist eine **zufällige** Zahlenfolge
- Der Schlüssel wird genau **einmal** genutzt und dann **verworfen**
 \rightarrow **absolut** sicher
- Problem: **sehr aufwendig** \rightarrow **keine** Nutzung im Internet

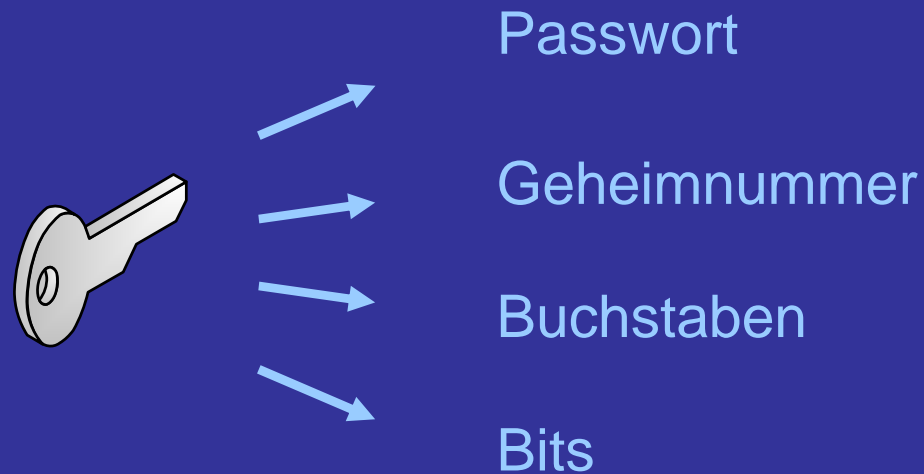
◆ Was ist eigentlich ein elektronischer Schlüssel ?



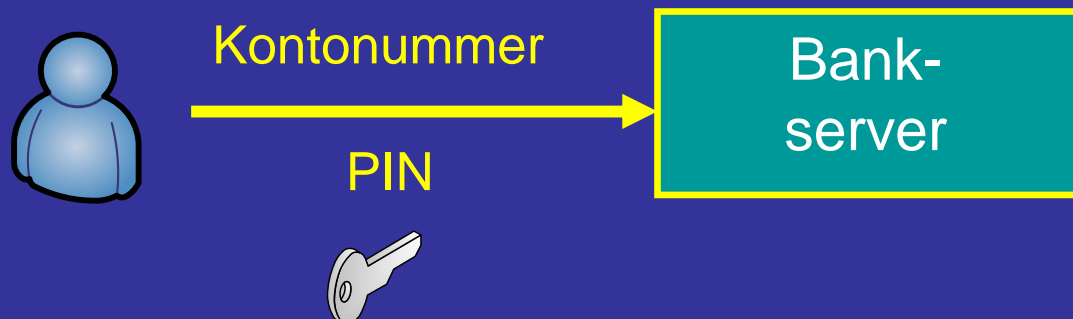
Beispiel: Abrufen einer eMail



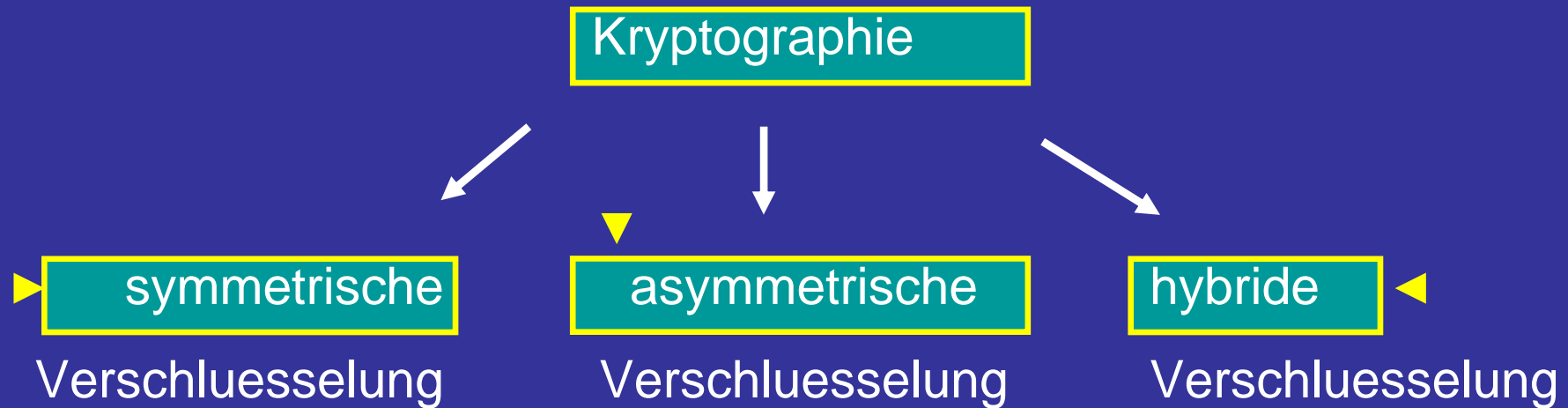
◆ Was ist eigentlich ein elektronischer Schlüssel ?



Beispiel: Online-Banking

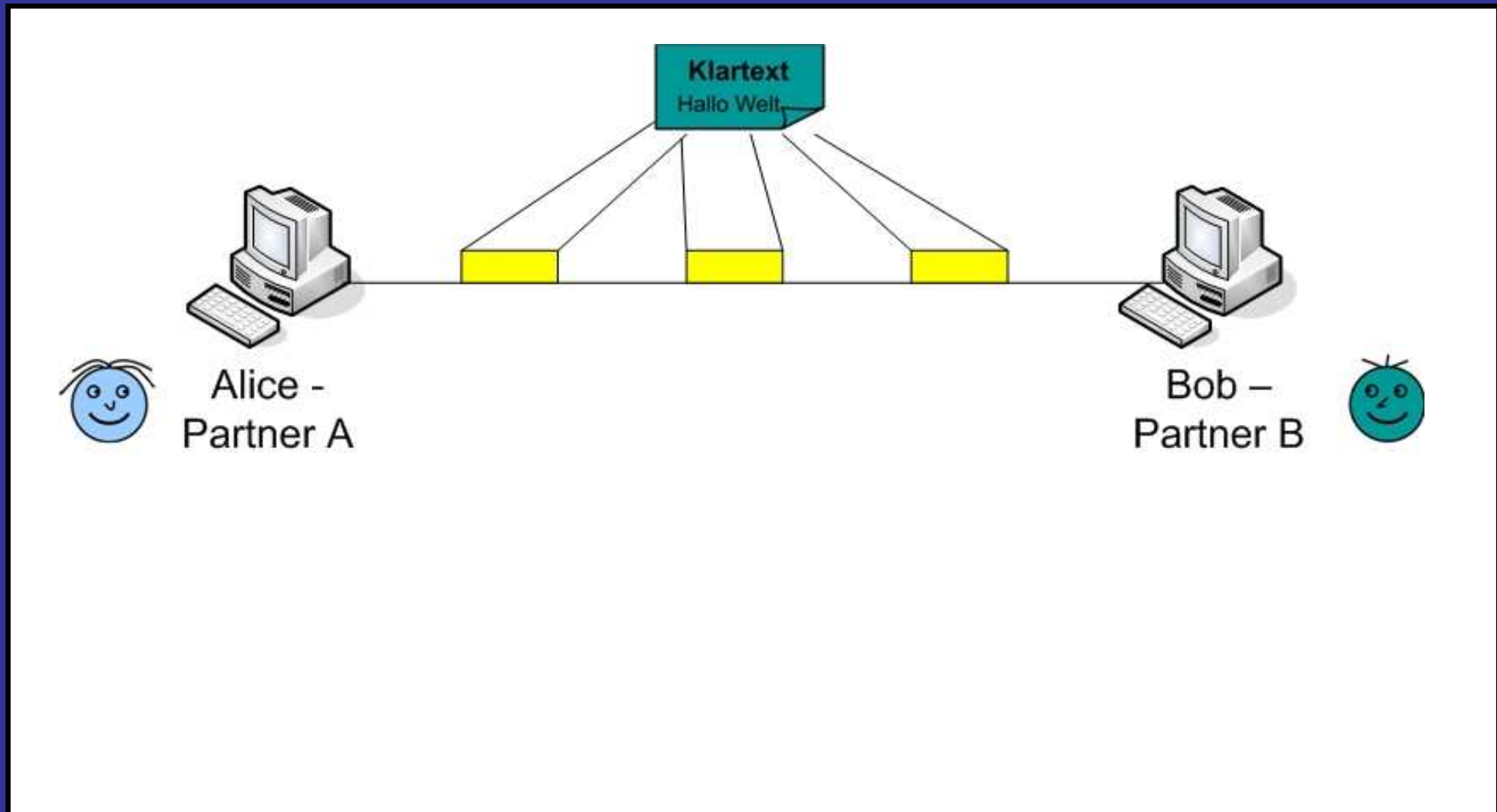


◆ Varianten der Kryptographie



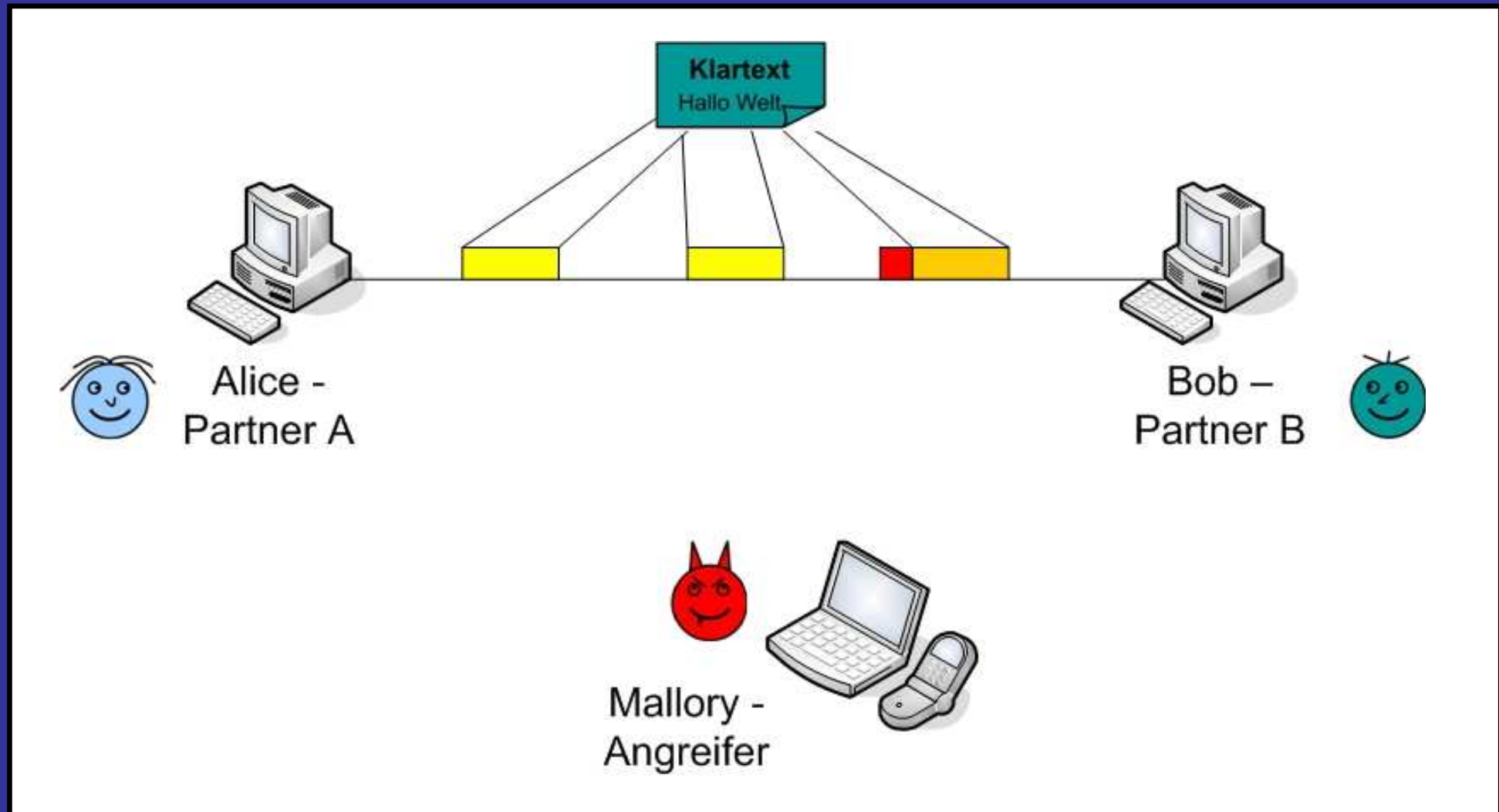
Der Normal-Fall

◆ Unverschlüsselte Datenübertragung



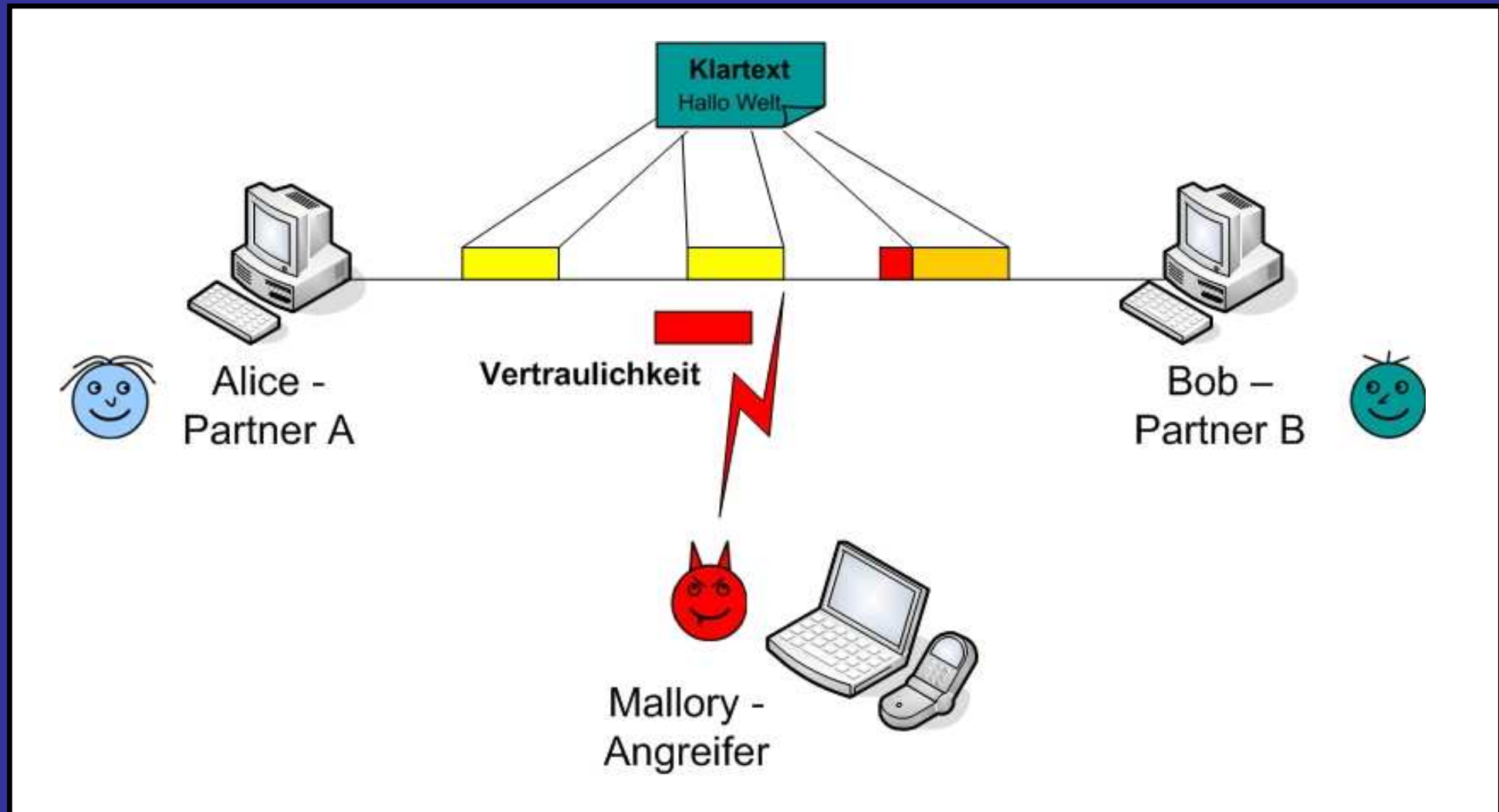
Das Böse lauert ueberall!

◆ Unverschlüsselte Datenübertragung – der Angreifer



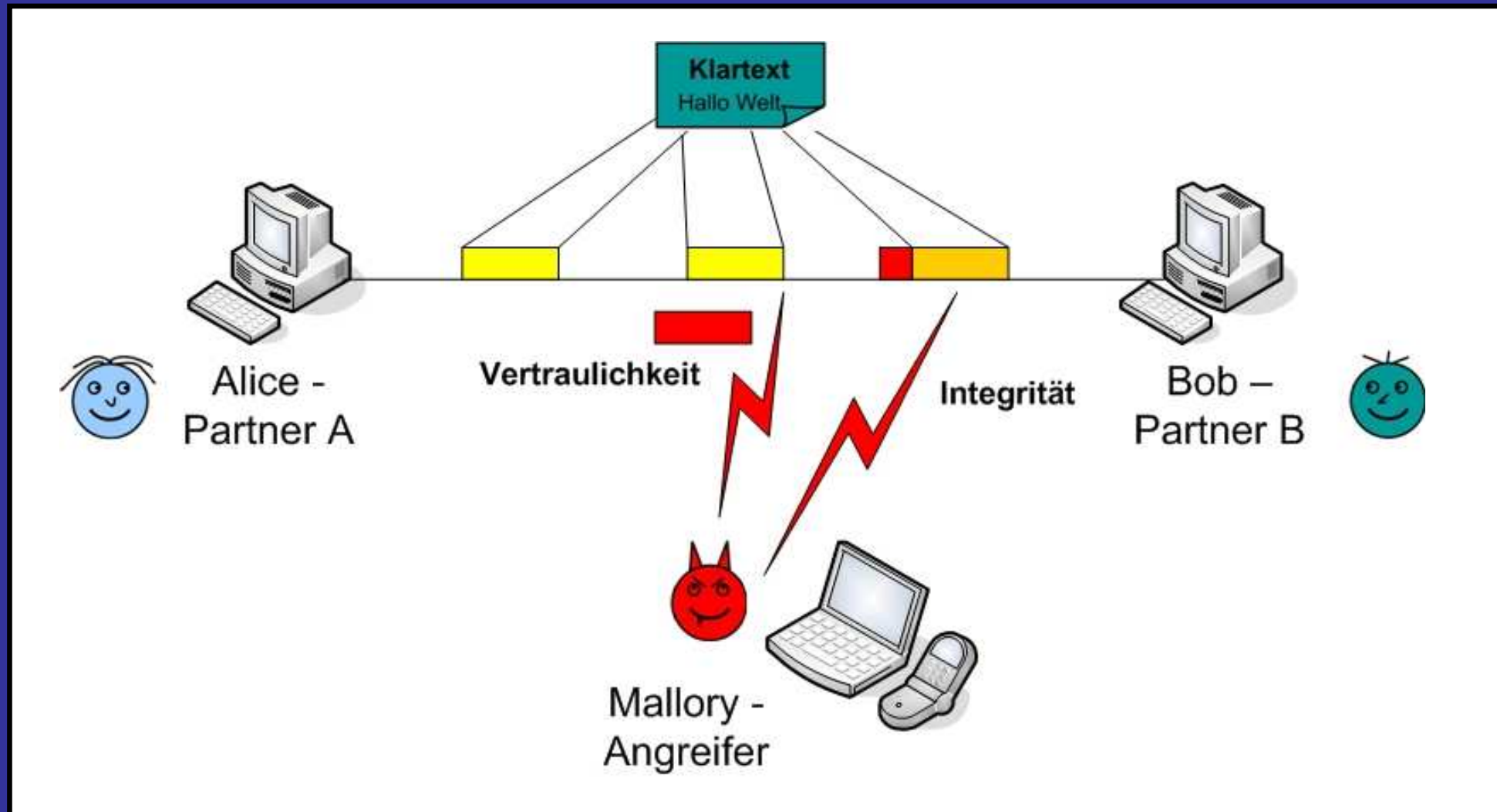
Bedrohungen der Sicherheit

◆ Unverschlüsselte Datenübertragung – Vertraulichkeit



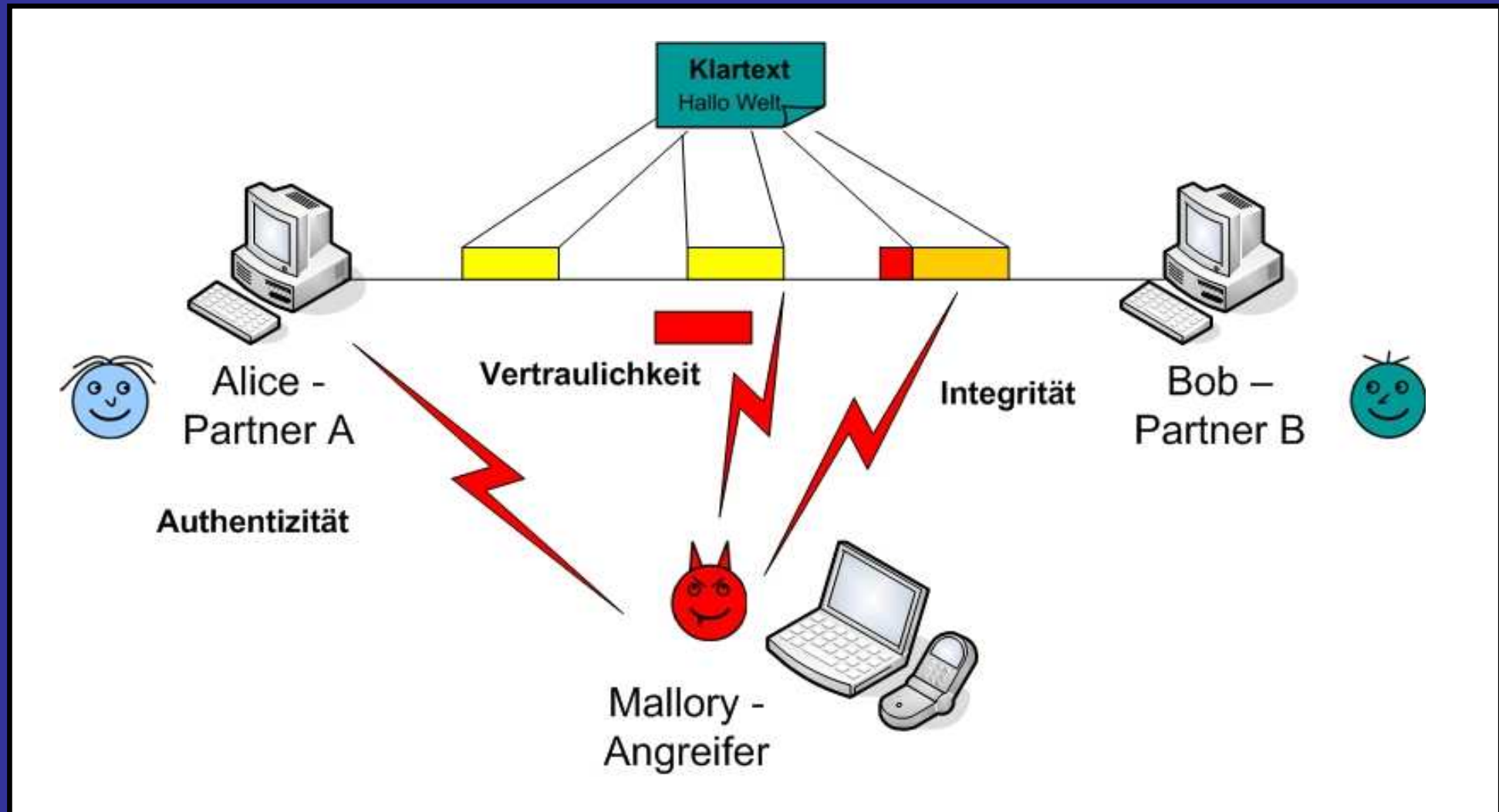
Bedrohungen der Sicherheit

◆ Unverschlüsselte Datenübertragung – Integrität



Bedrohungen der Sicherheit

◆ Unverschlüsselte Datenübertragung – Authentizität



Verlust von Sicherheitszielen

◆ Zusammenfassung – Bedrohungen durch Angreifer

Bedrohungen

Gegenmassnahmen

Vertraulichkeit

Verschlüsselung

unauthorisierte Weitergabe von Informationen



Integrität

Hash-Funktionen

unauthorisierte Veränderungen von Informationen

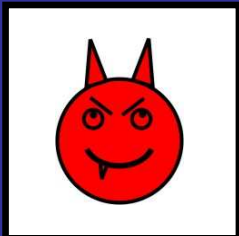
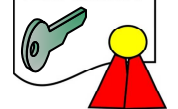


Authentizität

Digitale Signatur

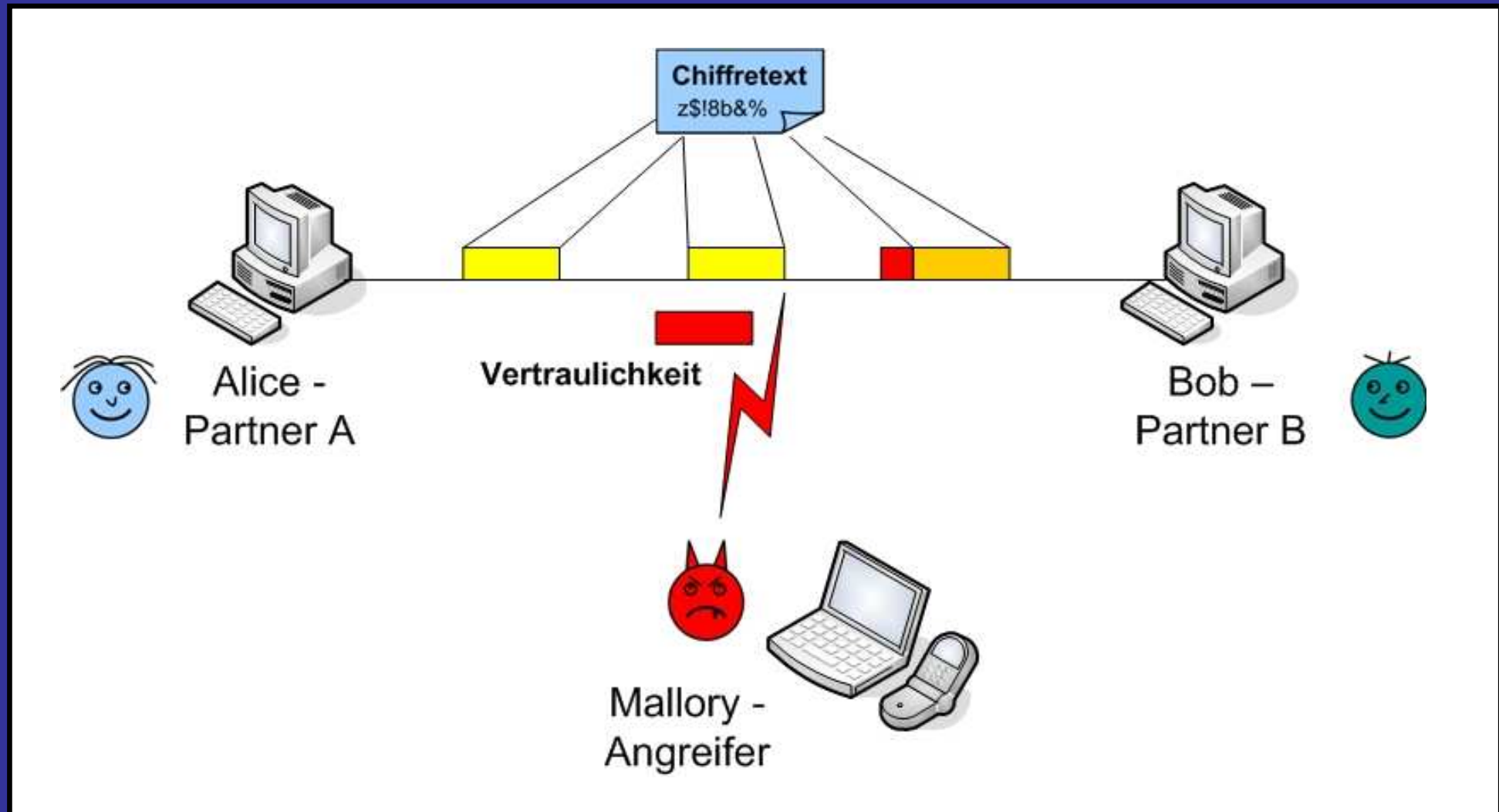
Identitätsfälschungen

Zertifikat



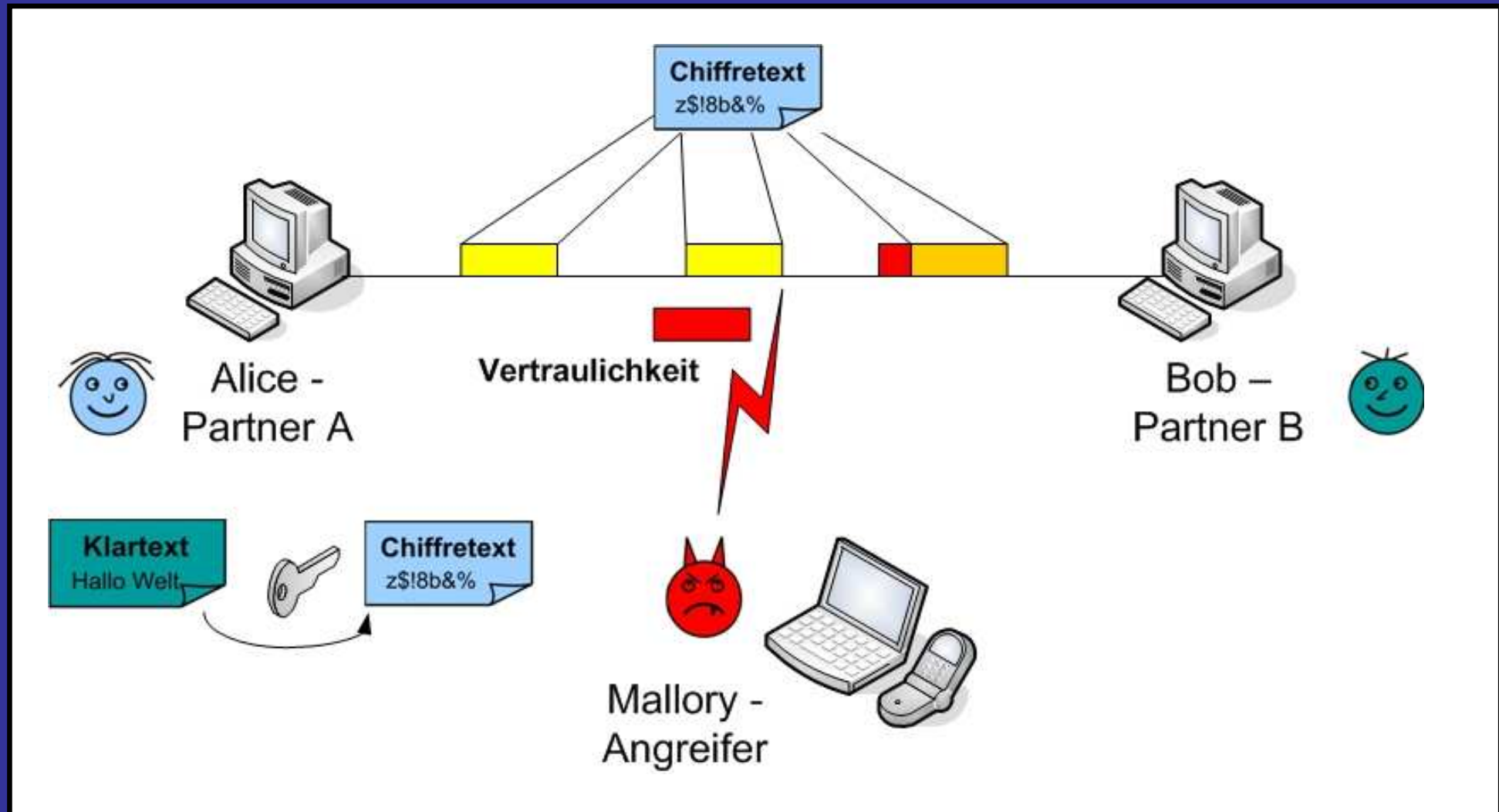
Gegenangriff!

◆ Verschlüsselte Datenübertragung – der Angriff



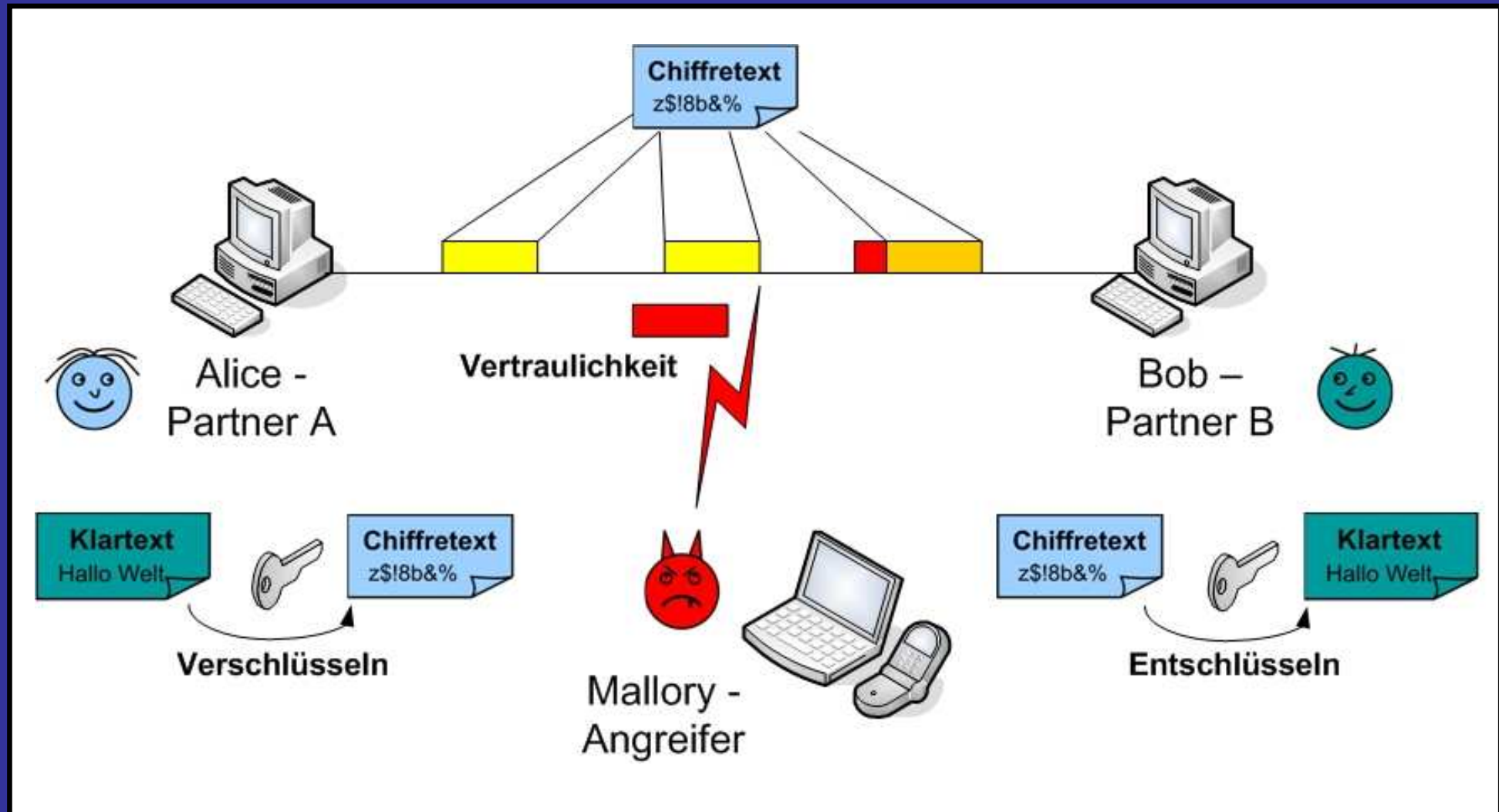
Klartext -> Chiffretext

◆ Verschlüsselte Datenübertragung – Verschlüsselung

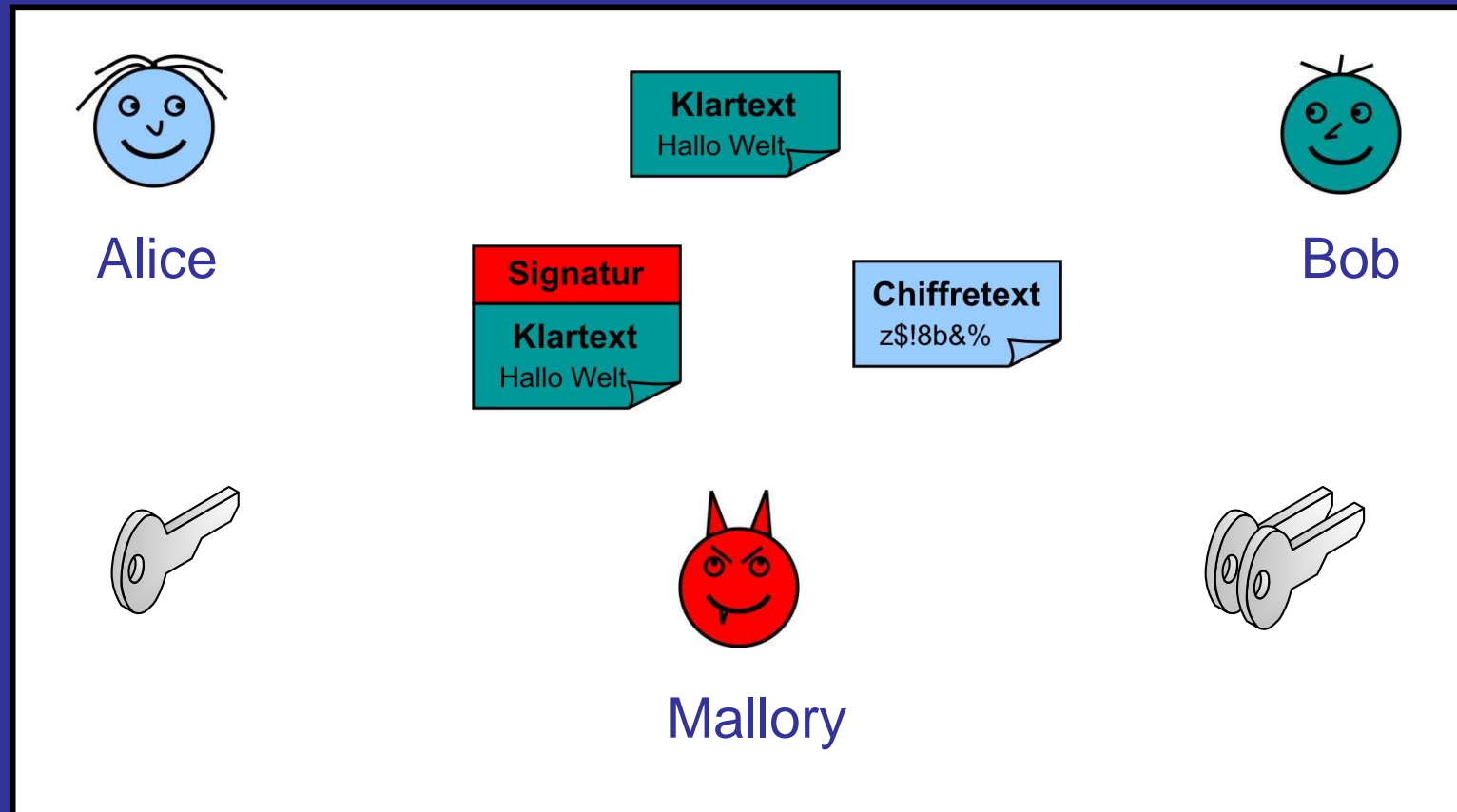


Chiffretext -> Klartext

◆ Verschlüsselte Datenübertragung – Entschlüsselung

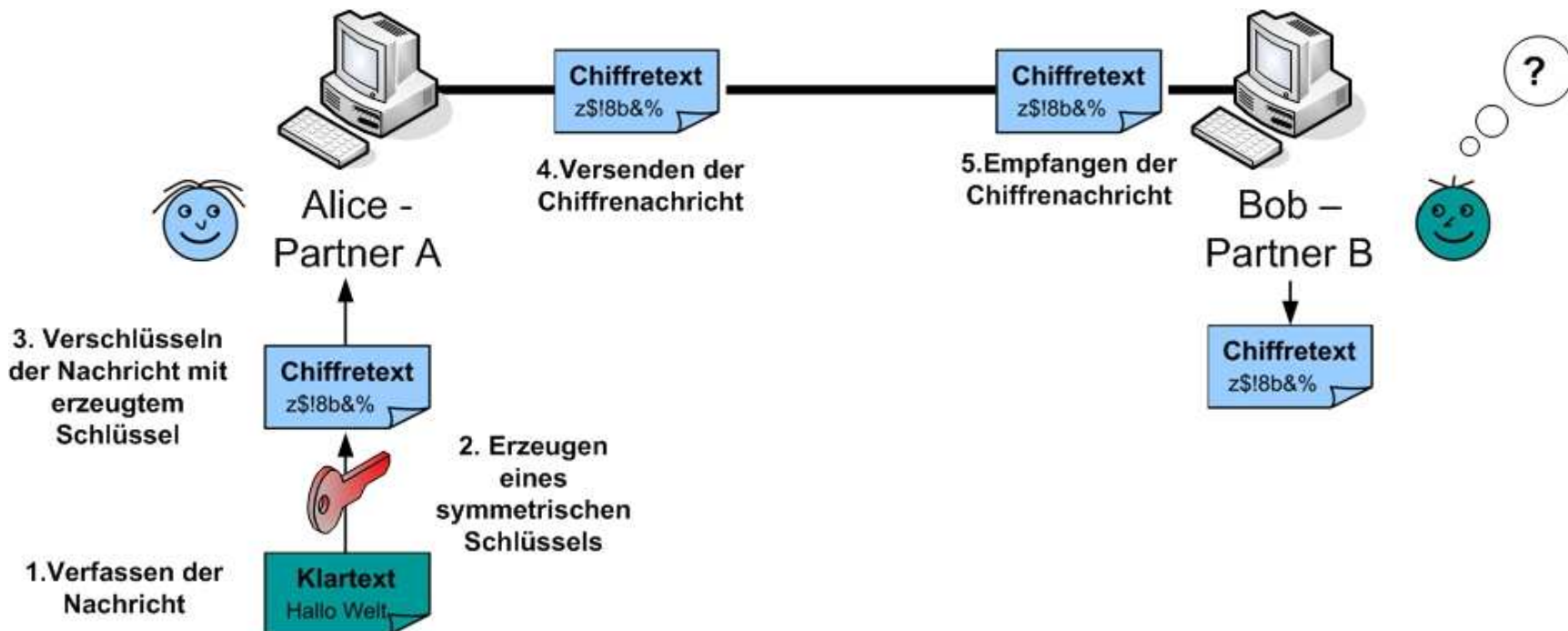


◆ Teilnehmer in den folgenden Si-Infrastrukturen



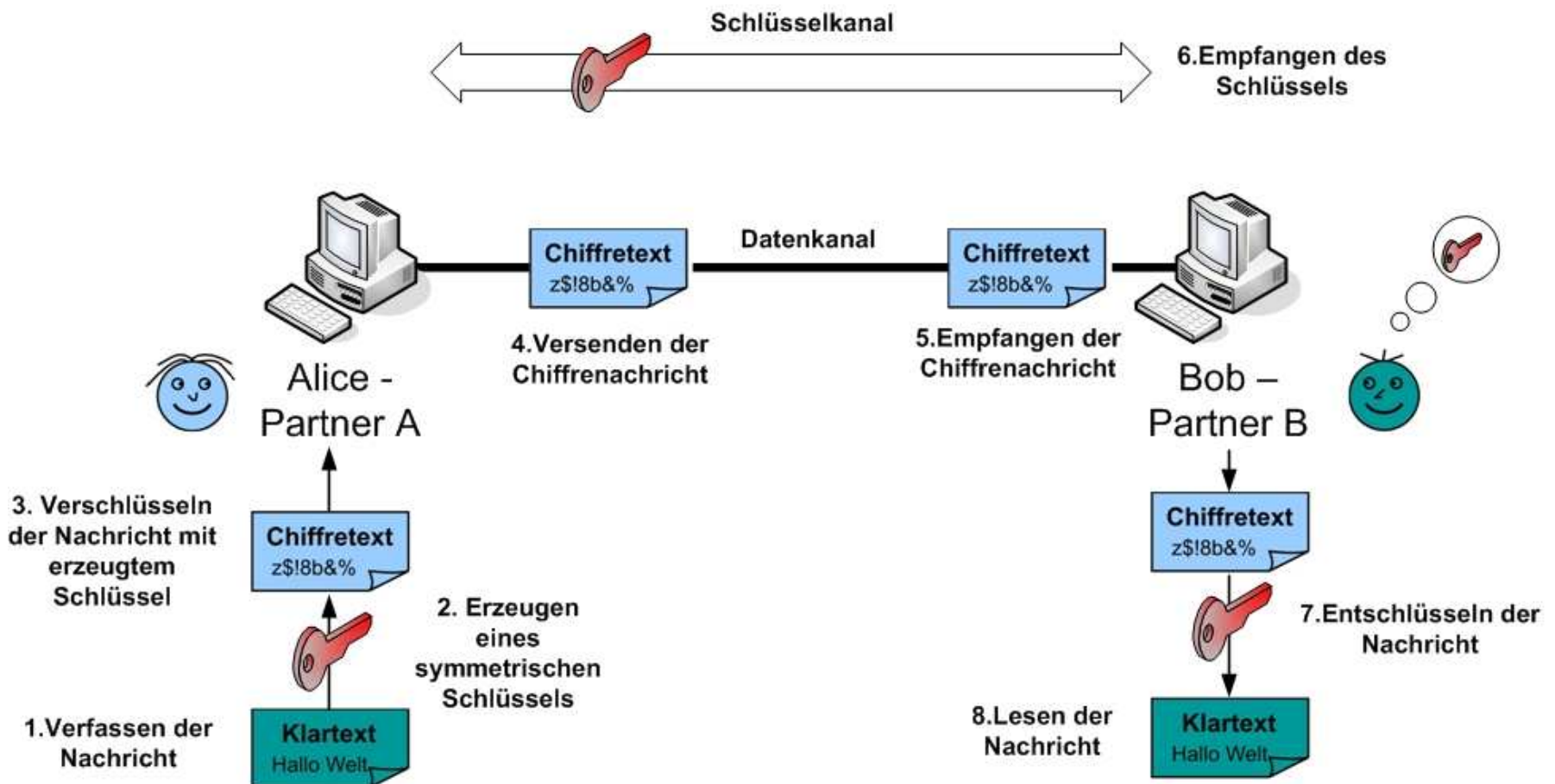
Secret-Key-Infrastructure

◆ Symmetrische Verschlüsselung



Secret-Key-Infrastructure

◆ Symmetrische Verschlüsselung

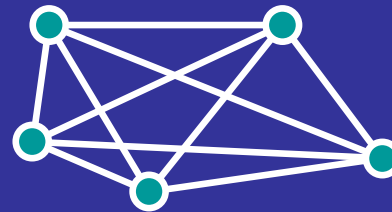


Secret-Key-Infrastructure

◆ Symmetrische Verschlüsselung – Zusammenfassung

- Probleme:

- Schlüsselaustausch aufwendig → Schlüsselaustauschproblem
- je Kommunikationspartner wird ein vertrauenswürdiger Schlüsselaustauschkanal benötigt → Aufwand steigt mit Anzahl der Partner



5 Kommunikationspartner

- aufgrund der Gleichheit des Schlüssels keine partnerindividuelle Signatur möglich

→ Schutz der Vertraulichkeit ist möglich



→ Schutz der Authentizität ist nicht möglich



Secret-Key-Infrastructure

◆ Symmetrische Verschlüsselungsalgorithmen

- Tripel-DES, IDEA, AES
- **Schlüssellänge** muß hinreichend groß gegenüber einem **Brute-Force-Angriff** sein → derzeit sind **128** Bit üblich
- Vorteile:
 - sehr **schnell**
 - **einfache** Schlüsselerzeugung

Kerckhoffs Maxime (19. Jahrh.)

- Die **Sicherheit** eines Verschlüsselungsverfahrens darf **nur** von der **Geheimhaltung** der **Schlüssel** abhängen, **nicht** von der **Geheimhaltung** des **Verschlüsselungsalgorithmus**.

◆ Kleiner Exkurs - Bedeutung der Schlüssellänge

- ▶ Schlüssellänge: 128 Bit = $2^{128} = 10^{38}$ Möglichkeiten = Schlüsselraum

1000 Chips mit 1 Milliarde Schlüssel pro Sekunde = 10^{19} Jahre

10.000.000.000.000.000.000 Jahre = 10 Trillionen Jahre!

- ▶ Schlüssellänge: 256 Bit = $2^{256} = 10^{77}$ Möglichkeiten

Kryptoanalytische Szenarien



→ weniger Grenzen der Rechner

→ Grenzen der Thermodynamik

Energie einer Supernova reicht um einen 219-Bit Schlüssel zu brechen.

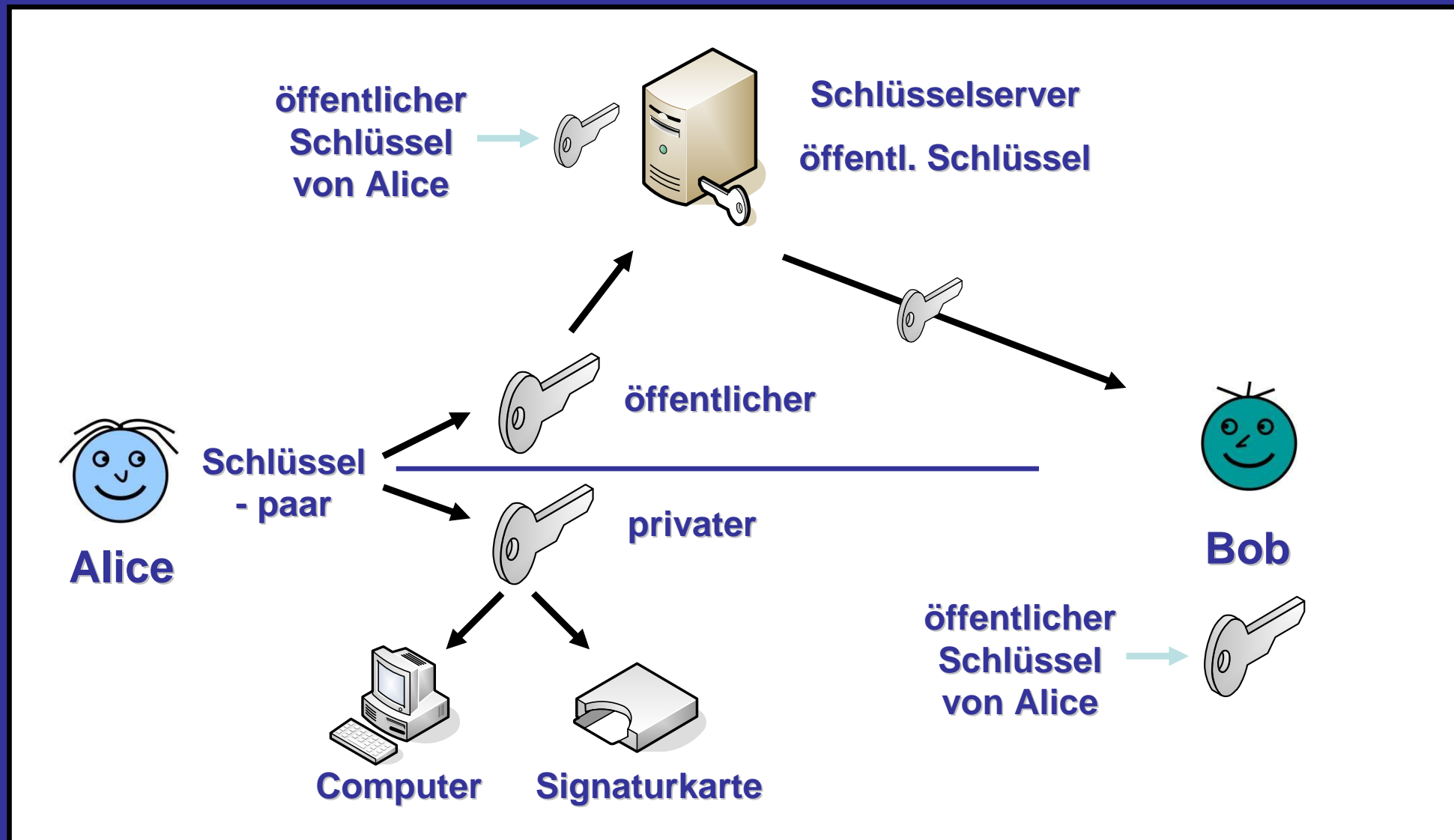
symmetris. V-Algorithmus

◆ Advanced Encryption Standard (AES)

- AES auch **Rijndael-Algorithmus** genannt
- **symmetrisches** Kryptosystem
- **Blockchiffre**
- überdurchschnittliche **Performanz** in Hardware & Software
- **keine** Methode der Kryptoanalyse soll diesen brechen können
- Wettbewerb im **Mai 2000** zu Ende
- Arbeitsweise:
 - Unterteilung in **einzelne** Blöcke die unterschiedlich **transformiert** werden in **mehreren** Runden
 - XOR
 - Substitution
 - Permutation

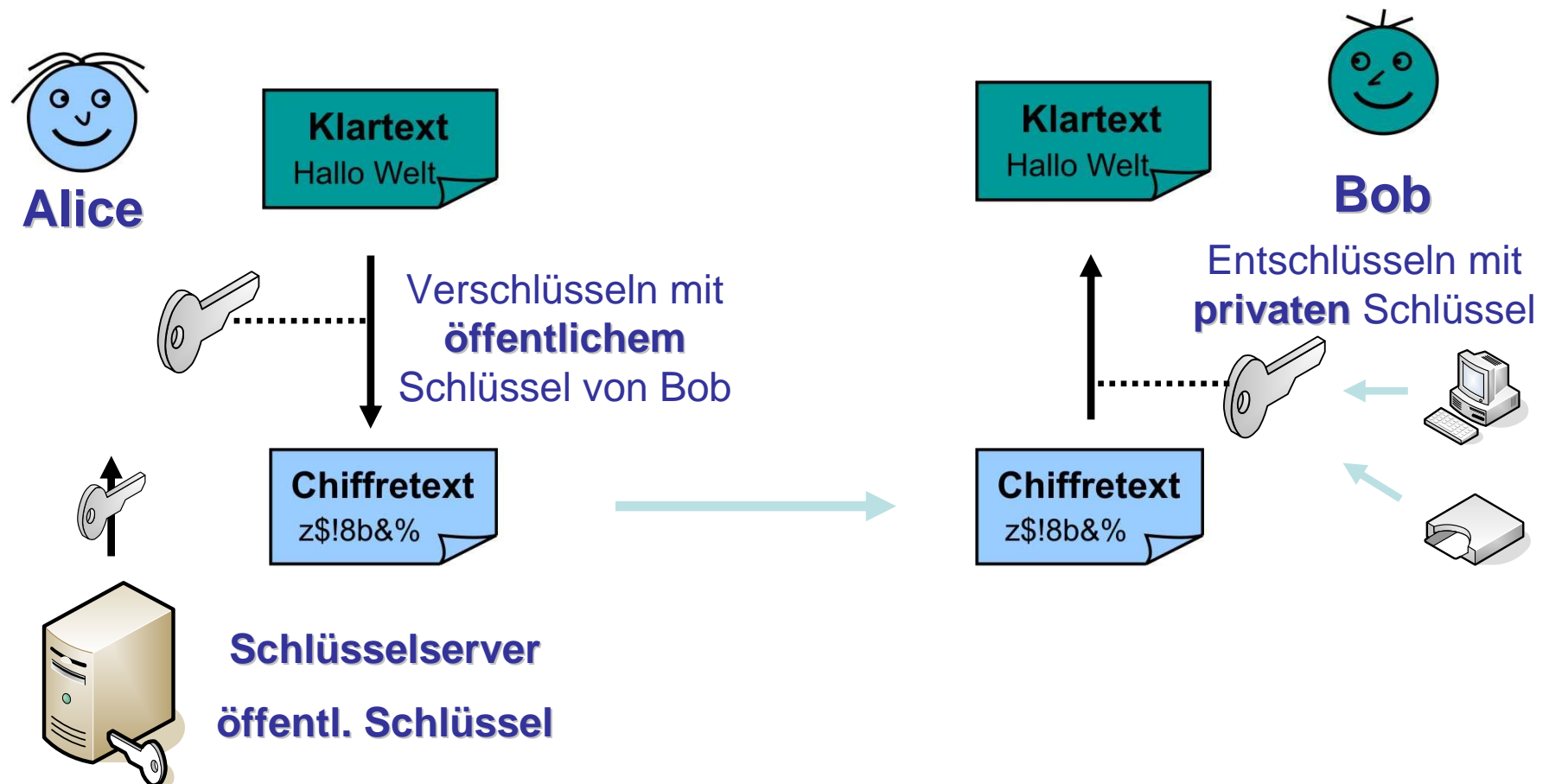
Public-Key-Infrastructure

◆ Lösung des Schlüsselaustauschproblems



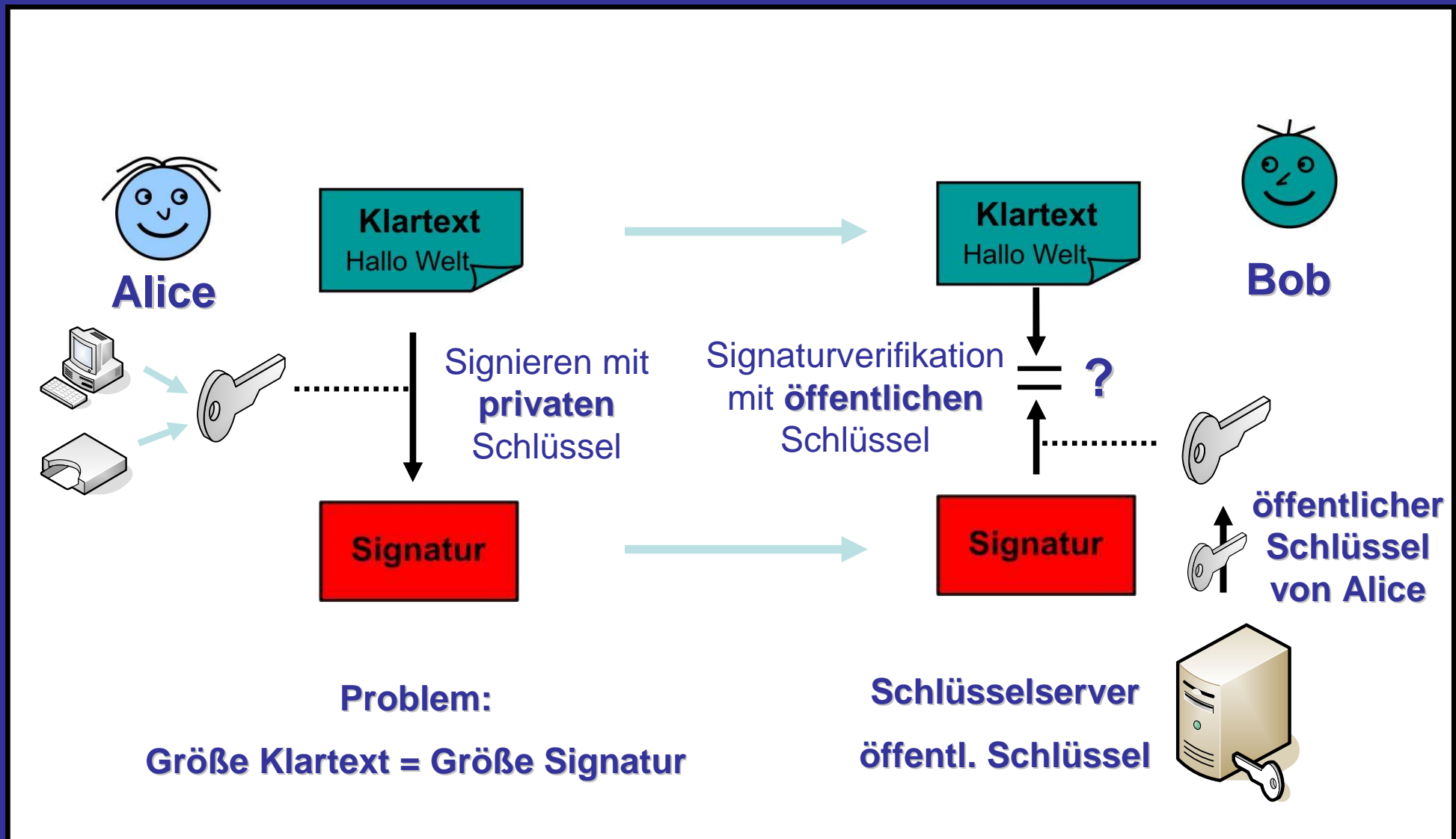
Public-Key-Infrastructure

◆ Verschlüsselung – Schutz der Vertraulichkeit



Public-Key-Infrastructure

◆ Digitale Signatur – Schutz der Authentizität



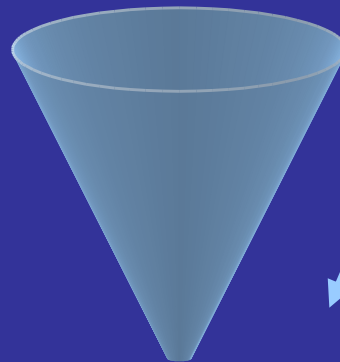
Kryptographische Prüfsumme

◆ Hash-Funktionen (Message Digest)

Eingabe = Zeichenkette
(beliebige Länge)

Zeichenkette

1 0 0 1 0 1 1



1 1 0

Einweg-Hashfunktion

Ausgabe = Hashwert
(feste Länge)

Zeichenkette

Hashfunktion

- Einwegfunktion
- kollisionsfrei
- änderungssensibel
- z.B.: **SHA-1**, MD5
160 bit 128 bit

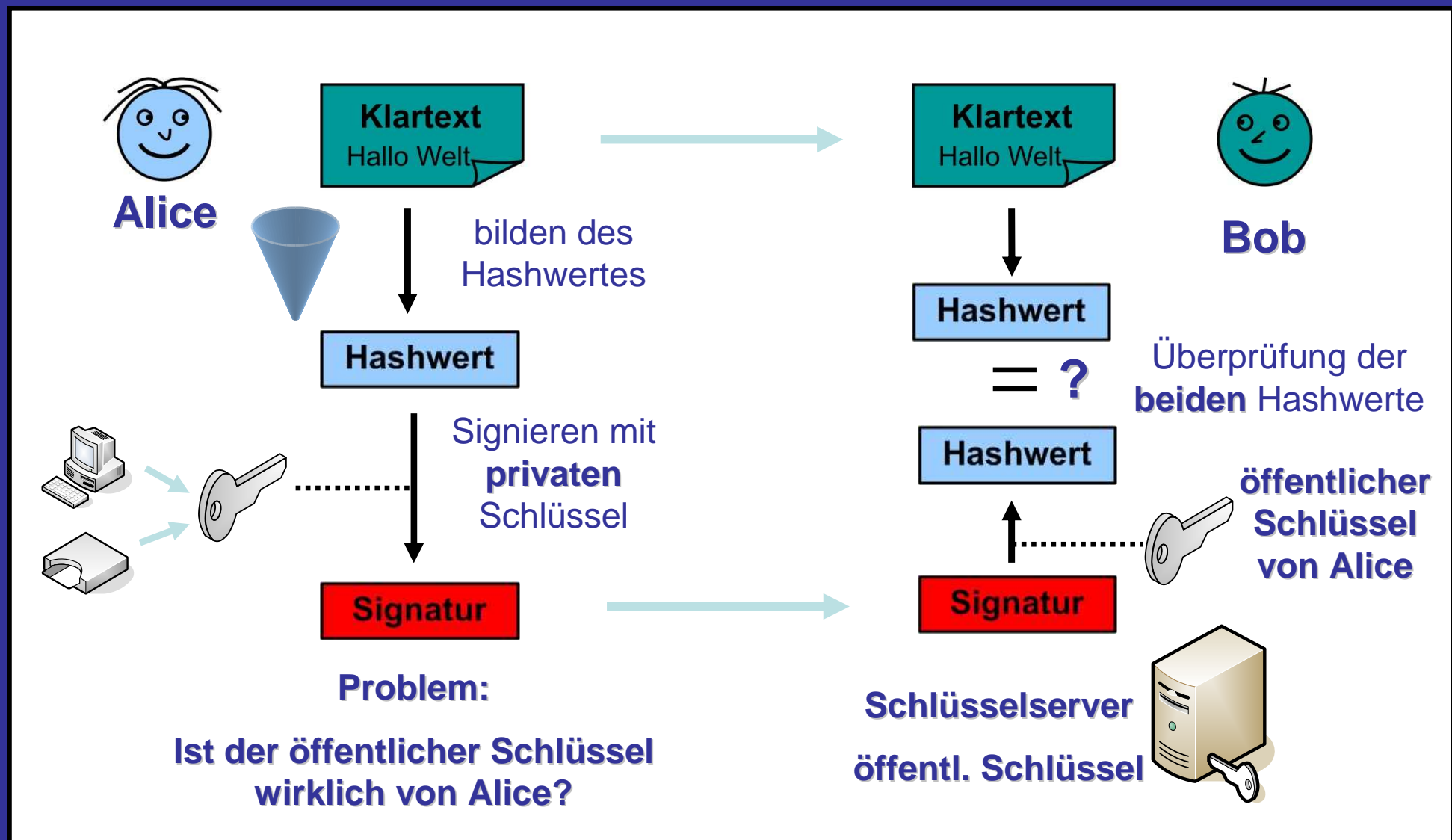
Hashwert

- repräsentativer Teil der Nachricht
- konstante Länge

Hauptfunktion: Schutz der Integrität

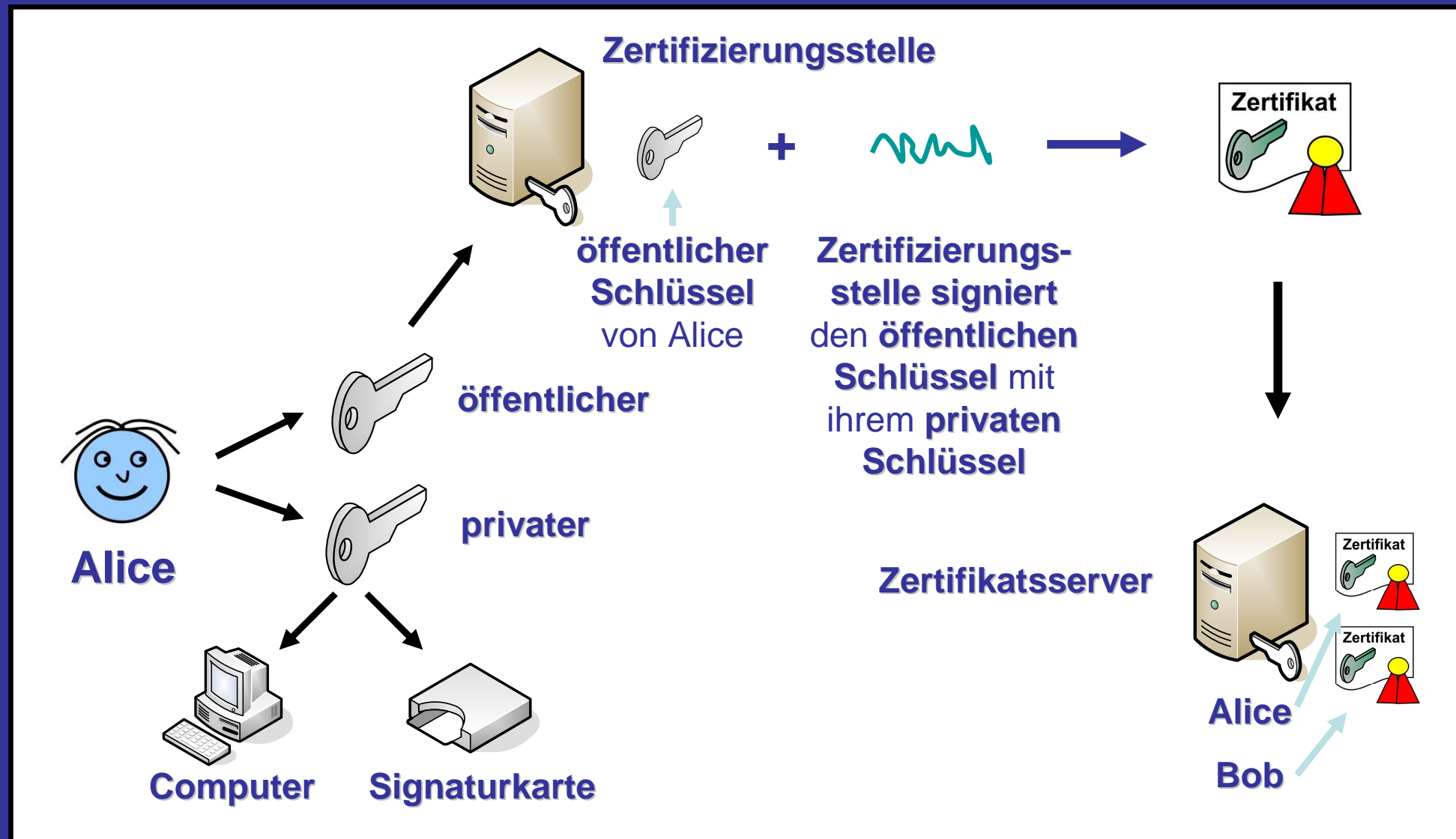
Public-Key-Infrastructure

◆ Digitale Signatur – Schutz der Integrität



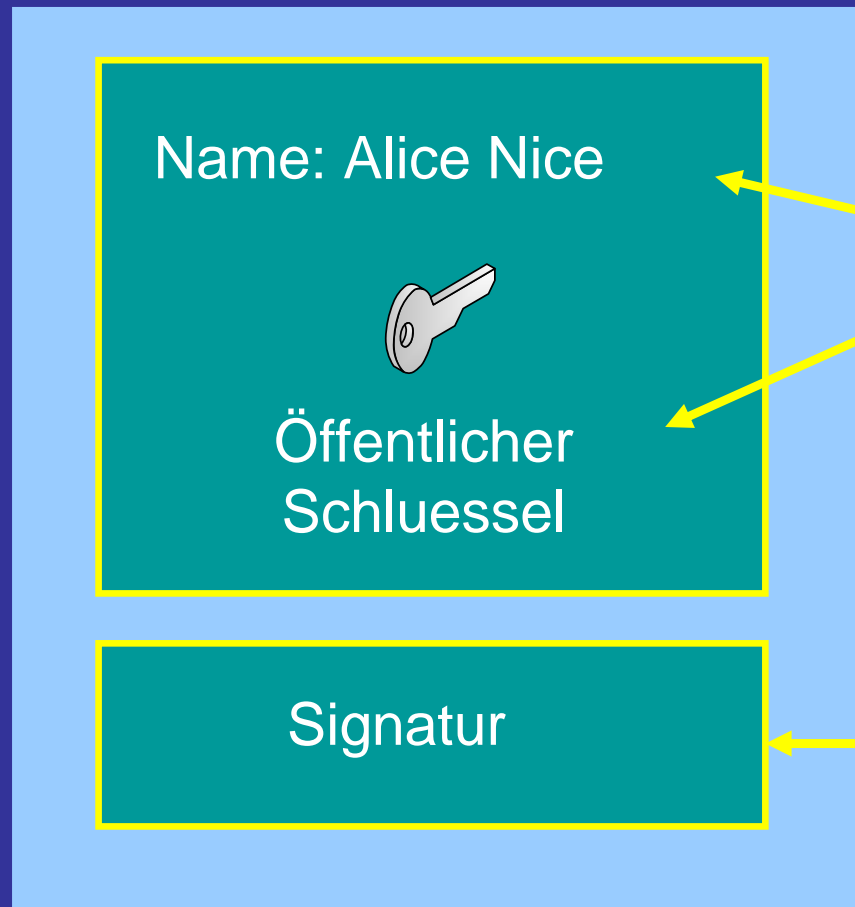
Public-Key-Infrastructure

- ◆ **Zertifikate = Zuordnung öffentl. Schlüssel → Person**



Oeffentliche Schluessel

◆ Zertifikate



Zertifikat

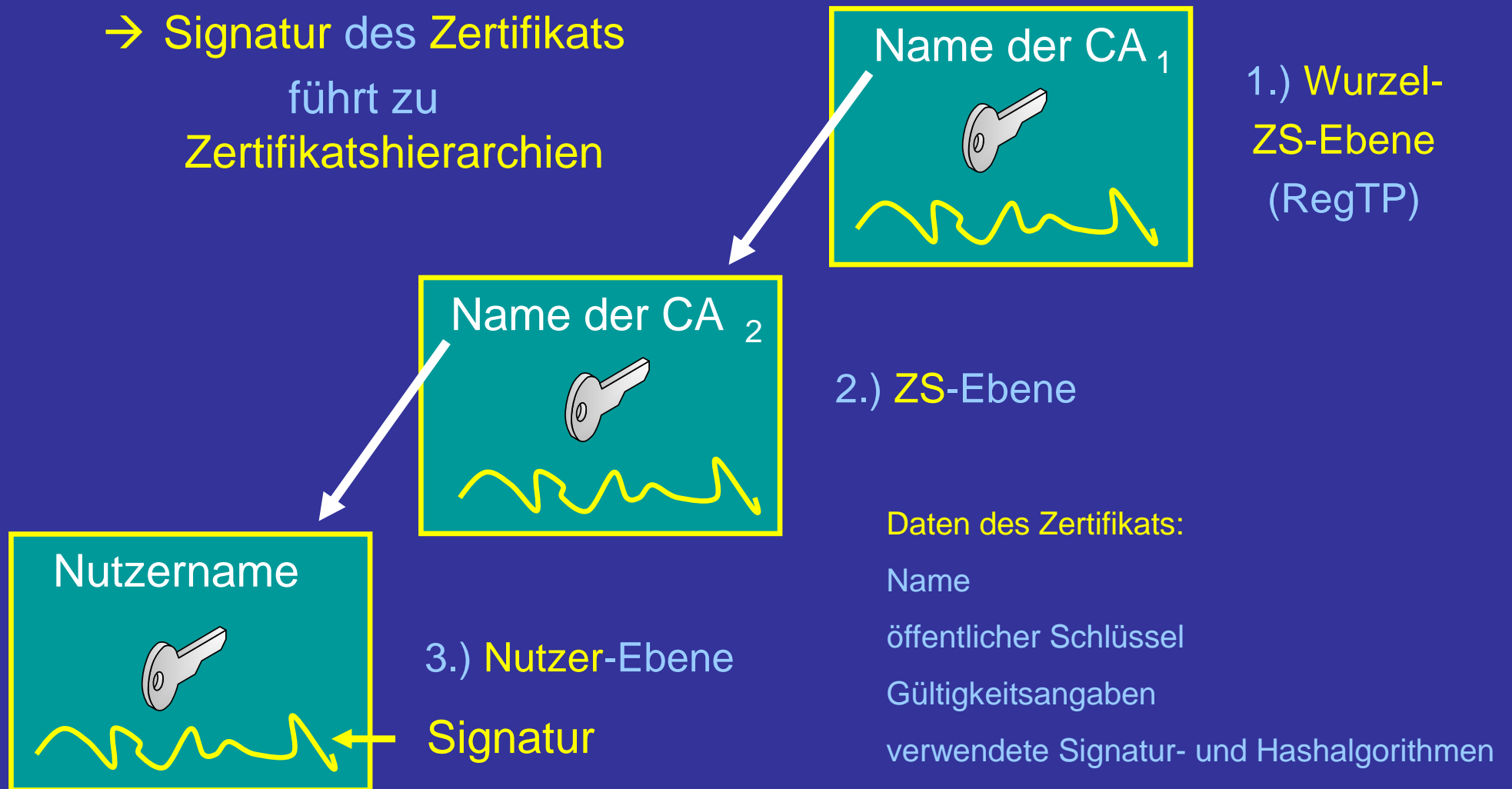
- Zuordnung eines öffentlichen Schlüssels zu einer Person
- Hinterlegung im Zertifikatsverzeichnis der Zertifizierungsstelle → zentraler Ansatz

Beglaubigung Dritter =
Zertifizierungsstelle
(Trustcenter)

Zertifikat

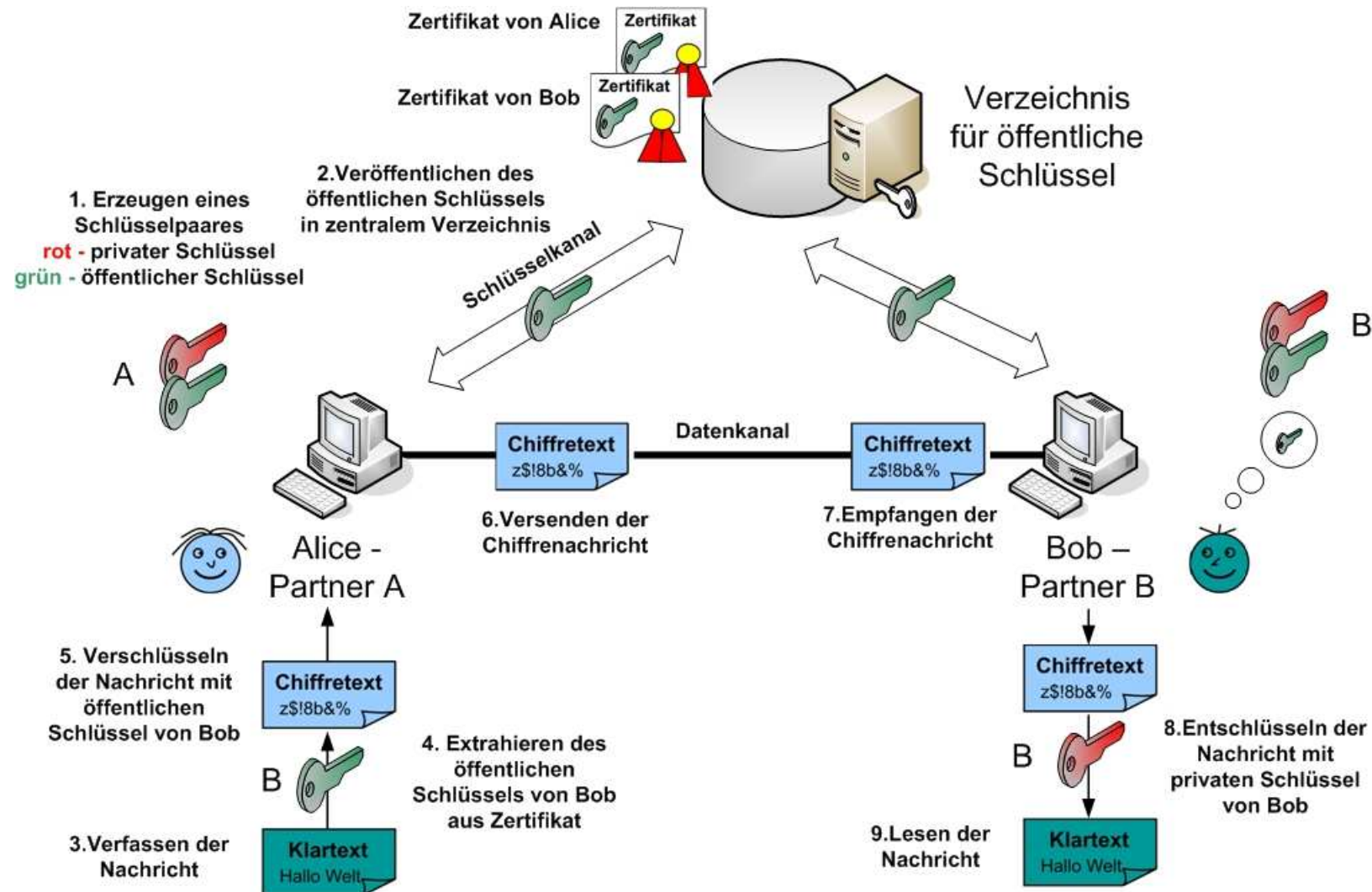
◆ Zertifikatshierarchien

→ Signatur des Zertifikats
führt zu
Zertifikatshierarchien



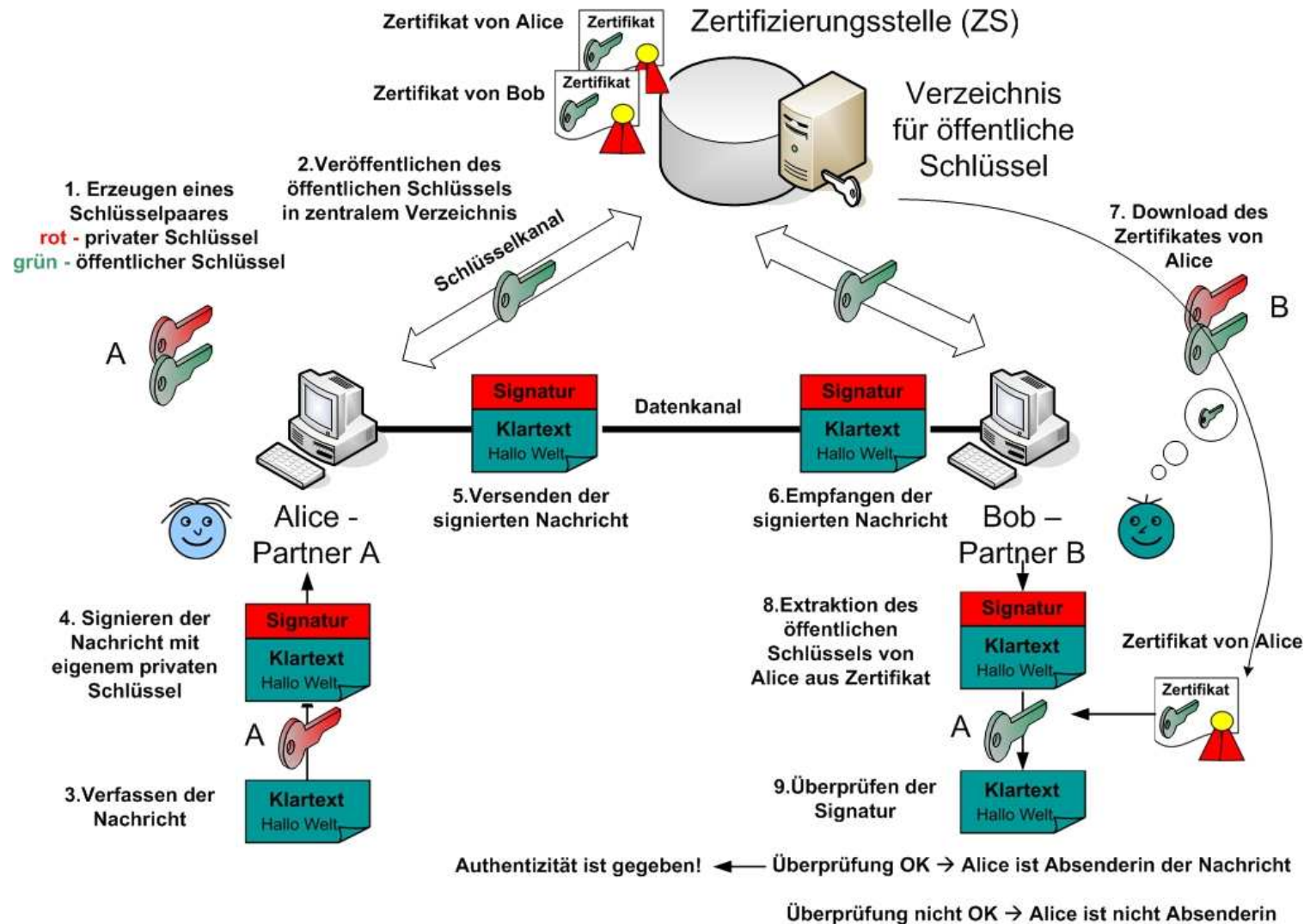
Public-Key-Infrastructure

Asymmetrische Verschlüsselung – Vertraulichkeit





Public-Key-Infrastructure

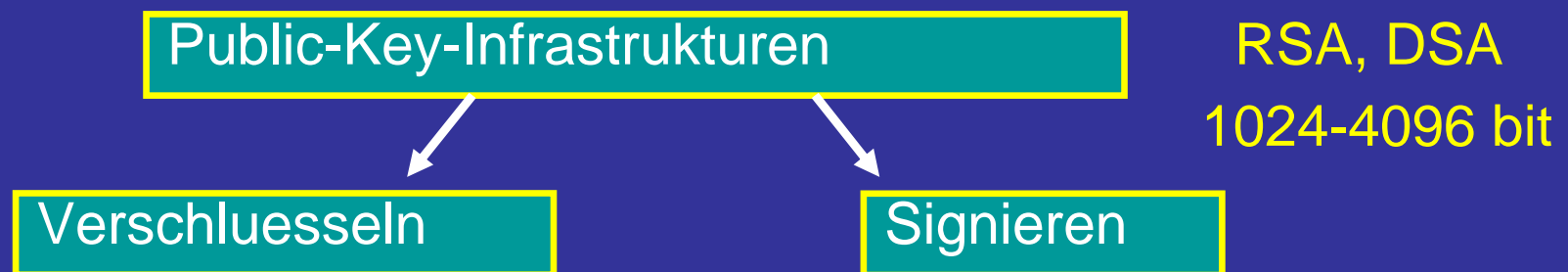
Asymmetrische Verschlüsselung – Authentizität



Public-Key-Infrastructure

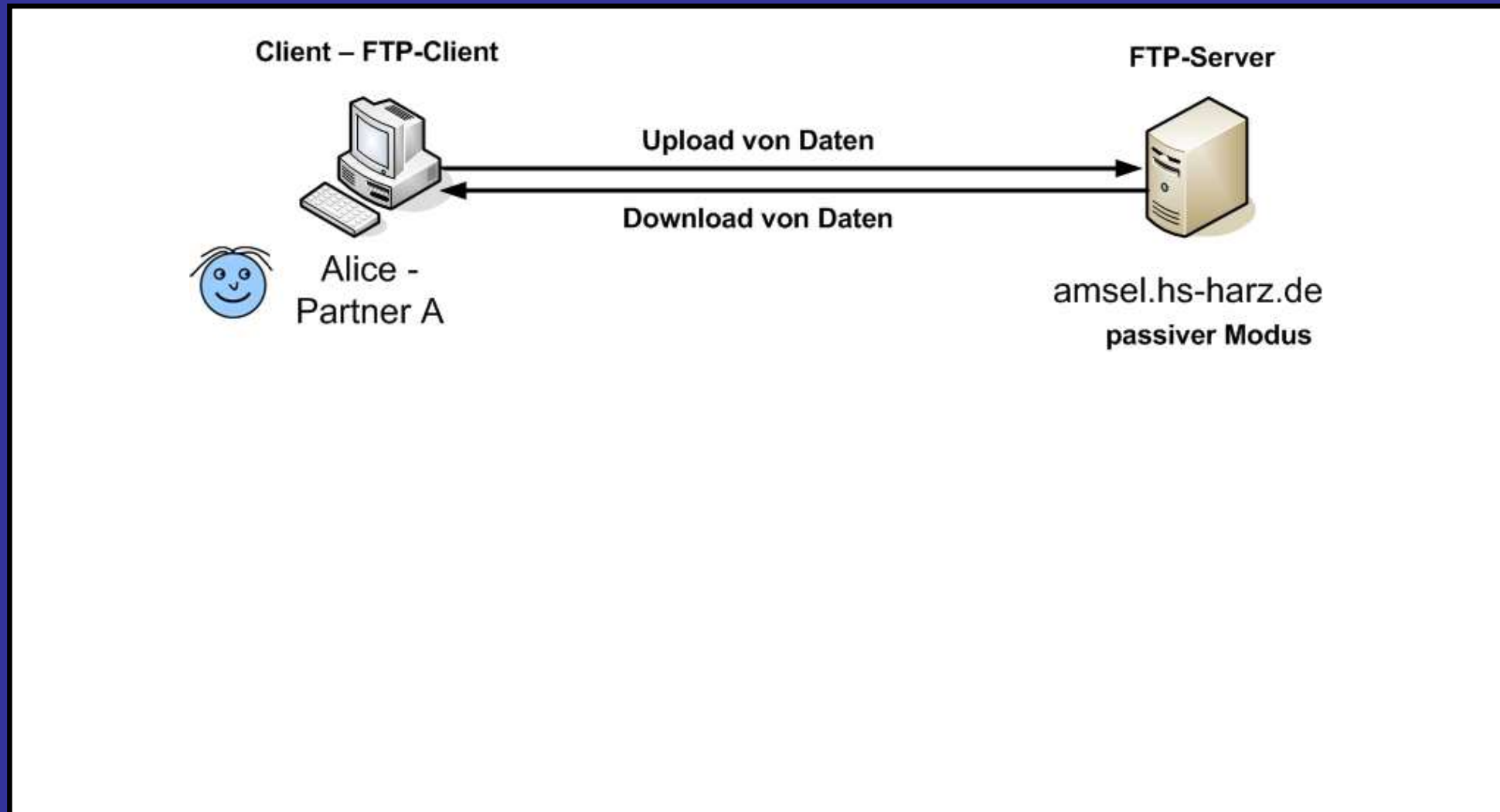
◆ Asymmetrische Verschlüsselung – Zusammenfassung

- Probleme:
 - **Schlüsselerzeugung** aufwendig (doch nur einmalig!) 
 - Anwendung **komplizierter** → schreckt Benutzer von Verwendung ab
- Vorteile:
 - **kein** sicherer **Schlüsselaustauschkanal** wird benötigt (Schlüsselmanagement)
 - durch **Verschlüsselung** mit **öffentl. Schlüssel** meines Gegenübers → **Vertraulichkeit** der Nachricht ist gewährleistet
 - durch Verschlüsselung (besser **Signieren**) mit meinem eigenem **privaten Schlüssel** → **Authentizität** und **Integrität** ist gegeben 



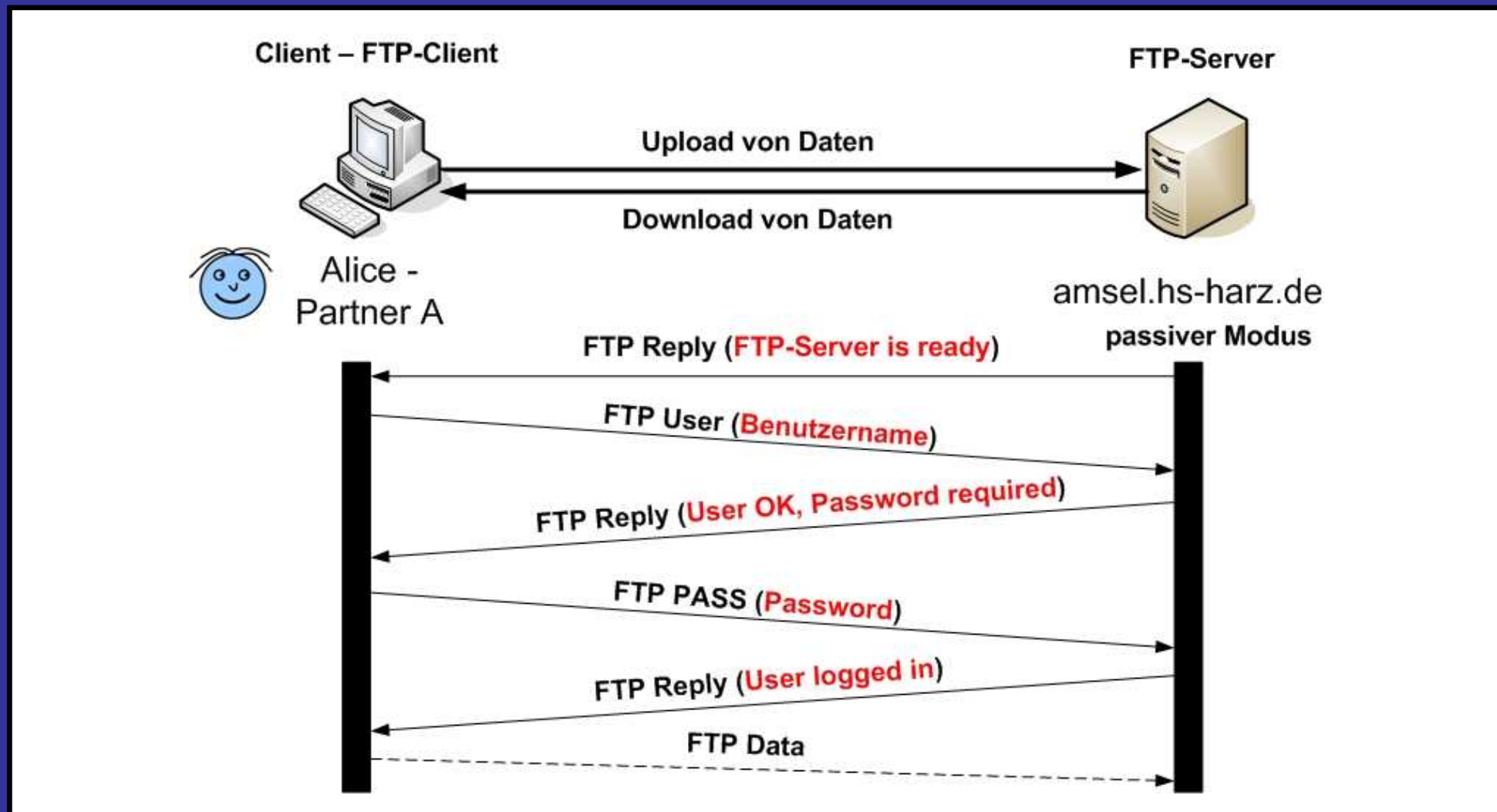
Netzwerksniffer im Einsatz 2

◆ Datenaustausch im Internet – FTP



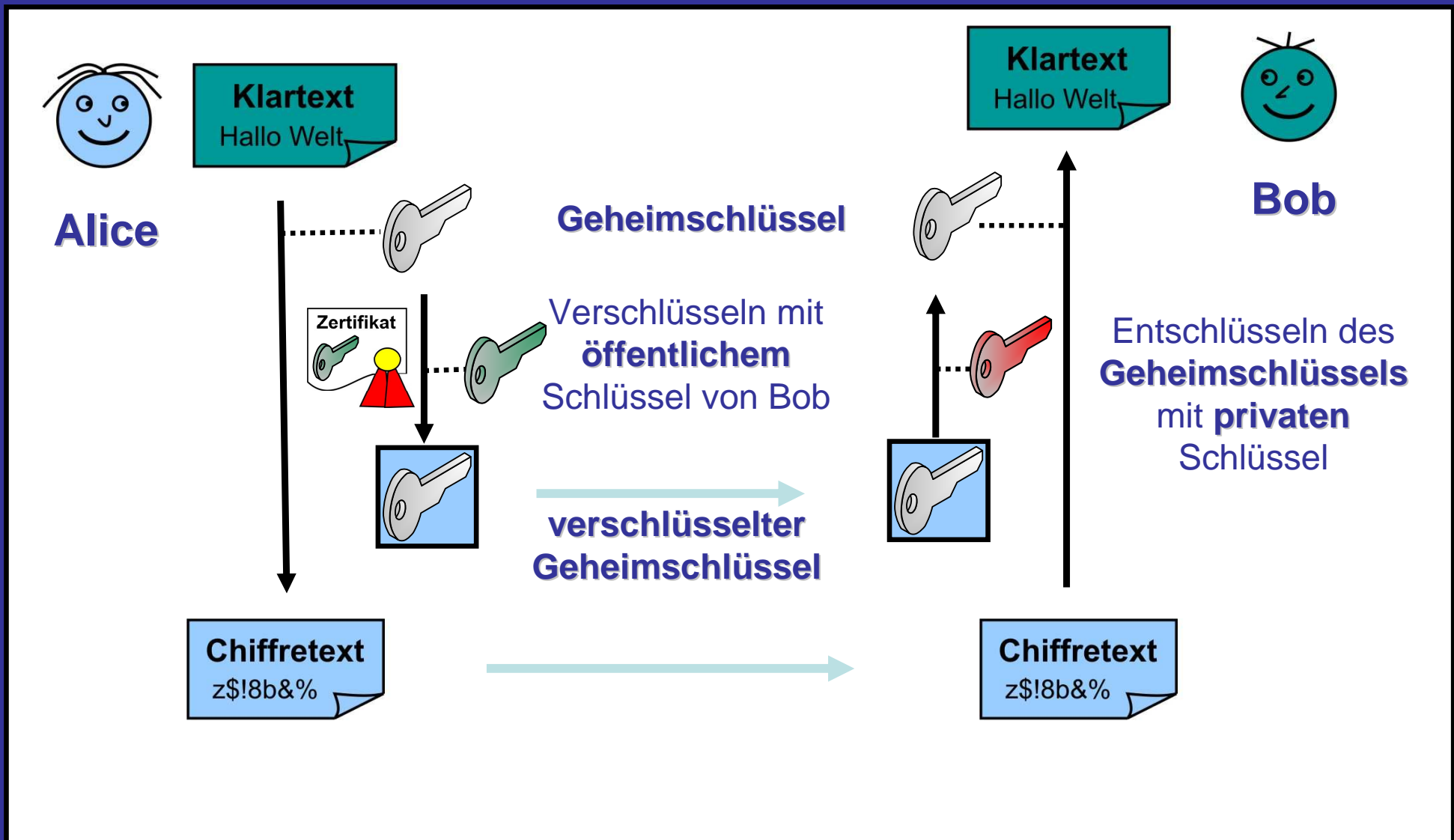
Netzwerksniffer im Einsatz 2

◆ Datenaustausch im Internet – FTP Ablauf



Public-Key + Secret-Key

◆ hybride Verschlüsselung



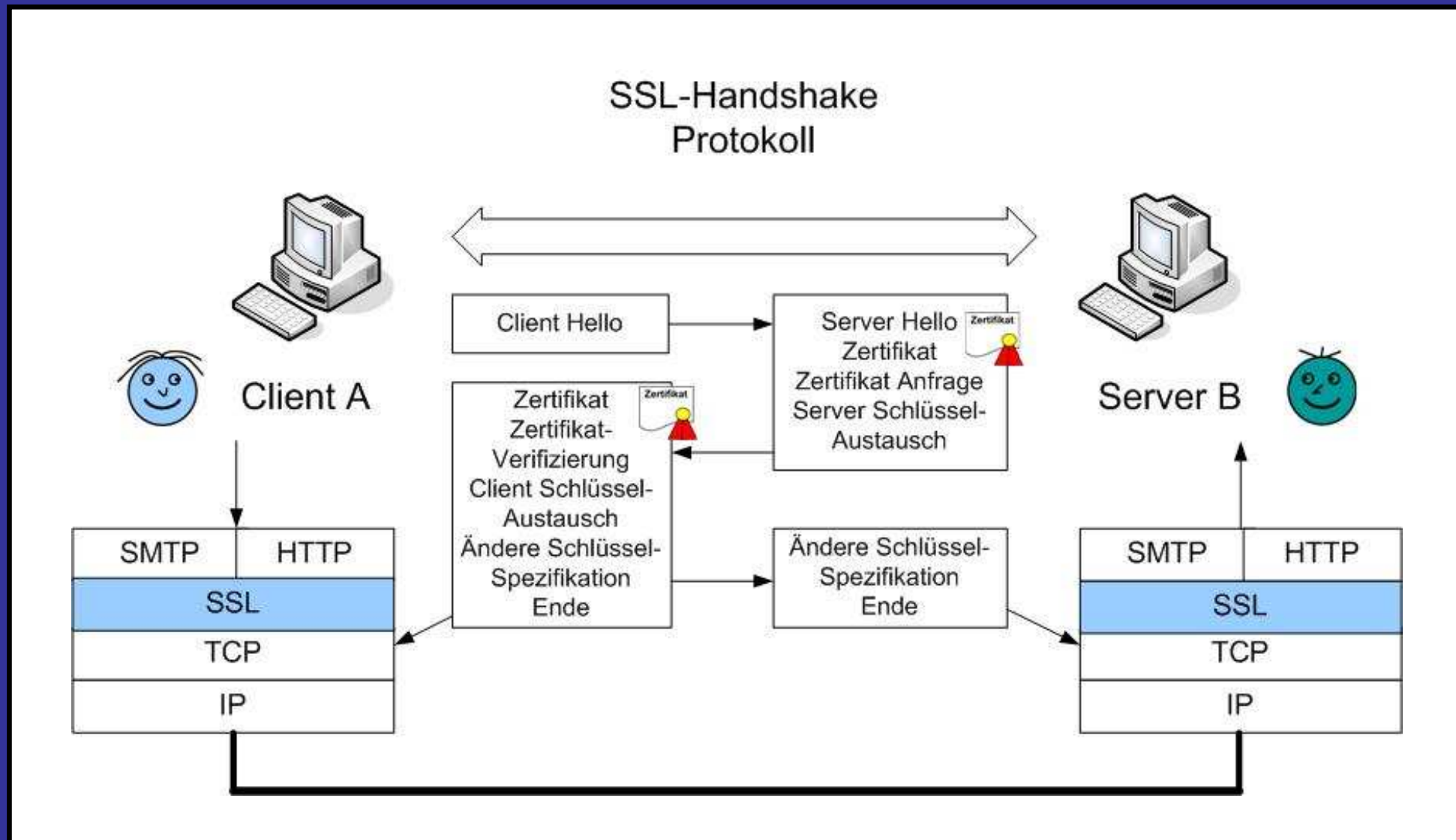
https:// statt http://

◆ Secure Socket Layer (SSL) – Hybridverschlüsselung

- Internet Protokoll für die sitzungsbasierte **Verschlüsselung** und **Authentifizierung**
- stellt **sicheren** Kanal zwischen Client und Server her
- arbeitet auf der **Transportschicht** → unabhängig vom Anwendungsprotokoll (HTTP, FTP, TELNET)
- Versionen: SSLv2, **SSLv3** und **TLS1.0**
- **SSL-Handshake Protokoll** zum Aushandeln der Sicherheitsparameter der aktuellen Sitzung
- Einsatzgebiete:
 - **Online Banking**
 - **Webshops**
 - **Formulare mit privaten Daten**

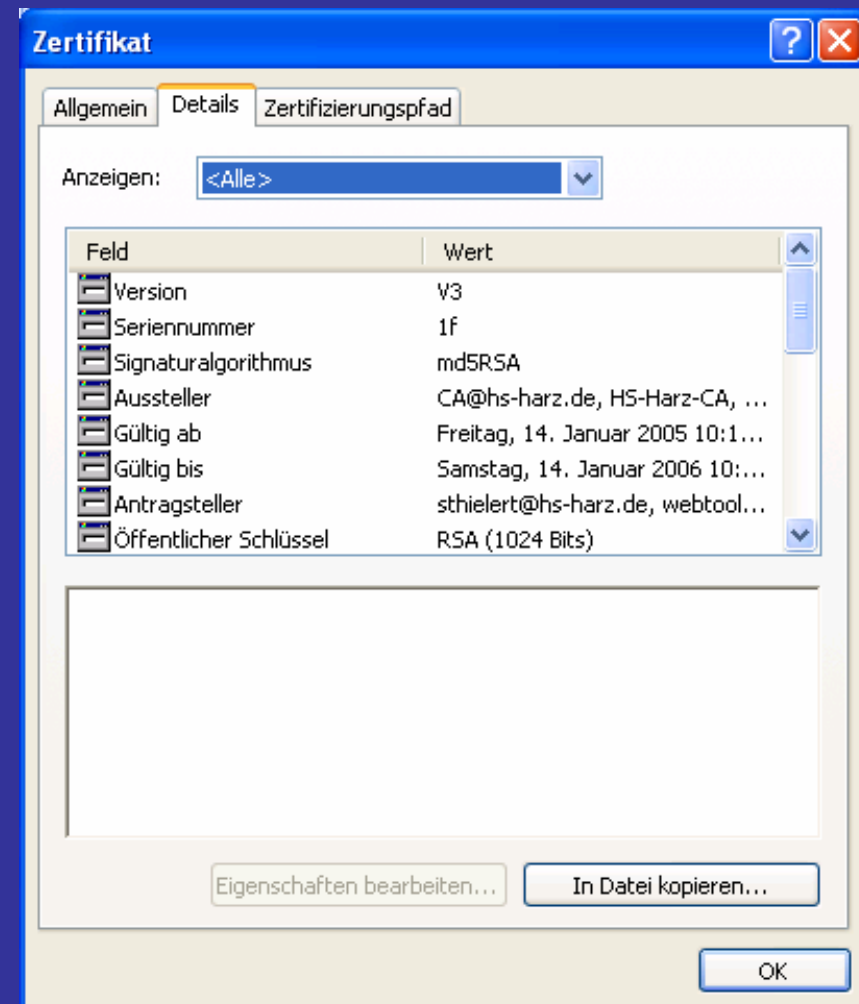
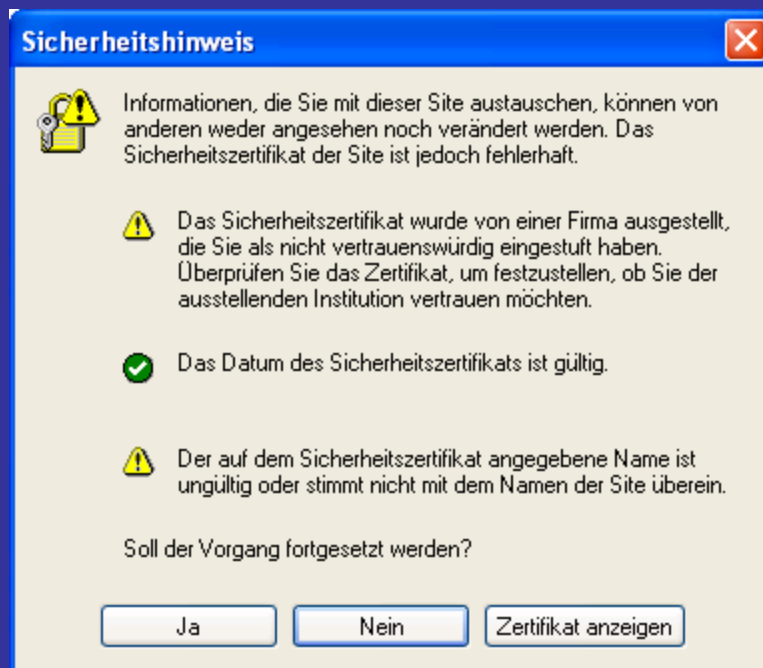
SSL

◆ SSL-Handshake Protokoll



SSL

◆ Zertifikate um Schlüssel auszutauschen



◆ Gültige Zertifizierungsstellen

The screenshot shows the 'Zertifikate' (Certificates) window in Windows. The 'Beabsichtigter Zweck' (Intended Purpose) is set to '<Alle>'. The 'Vertrauenswürdige Stammzertifizierungsstellen' (Trusted Root Certification Authorities) tab is selected, showing a list of certificates. The list includes the following entries:

Ausgestellt für	Ausgestellt von	Gültig bis	A
ABA.ECOM Root CA	ABA.ECOM Root CA	09.07.2009	D
Autoridad Certificadora de la Asociacio...	Autoridad Certificador...	28.06.2009	A
Autoridad Certificadora del Colegio Nac...	Autoridad Certificador...	29.06.2009	A
Baltimore EZ by DST	Baltimore EZ by DST	03.07.2009	D
Belgacom E-Trust Primary CA	Belgacom E-Trust Prim...	21.01.2010	B
C&W HKT SecureNet CA Class A	C&W HKT SecureNet ...	16.10.2009	C
C&W HKT SecureNet CA Class B	C&W HKT SecureNet ...	16.10.2009	C
C&W HKT SecureNet CA Root	C&W HKT SecureNet ...	16.10.2010	C

At the bottom of the window, there are buttons for 'Importieren...', 'Exportieren...', 'Entfernen', and 'Erweitert...'. Below these is a section for 'Beabsichtigte Zwecke des Zertifikats' with an 'Anzeigen' button. At the very bottom is a 'Schließen' button.

Fragen?



Antworten!

Vielen Dank für ihre Aufmerksamkeit!

Tobias Giese

10.06.2005

Kryptographie im Internet

Kontakt:

tobias.giese@gmx.de

Unterlagen:

<http://www.tobias-giese.de/salza-vortrag.ppt>

