



KRYPTOGRAFIE

M114 / ARJ / 3-2025

Die Themen:

- Symmetrische Verschlüsselung
Klassische Verfahren: ROT, Vigenere, XOR
Moderne Verfahren: AES
- Asymmetrische Verschlüsselung
Schlüsseltausch: Diffie-Hellman Schlüsseltausch
Verschlüsselung: RSA
- Digitale Signatur
Verfahren: RSA
Hashfunktion: MDx, SHAx
- Public Key Infrastruktur
Hierarchisch, X509-Zertifikate
Web-of-Trust, OpenPGP
- Sicheres Internet
HTTPS, TLS, Zertifikate
- Praxis: OpenPGP
gpg4win, Kleopatra
- Praxis: Sichere E-Mails
OpenPGP versus S-MIME, Mailclient Thunderbird

Die verwendeten Tools:

- Cryptool1
Lern-SW, Kryptographie Konzepte & Analyse
<https://www.cryptool.org/de/ct1>
- Wireshark
Network-Sniffer
Datenprotokolle: Analyse + grafische Aufbereitung
<https://www.wireshark.org>
- Gpg4win
Zertifikatsmanager Kleopatra
Dateiverschlüsselung Kleopatra
<https://www.gpg4win.de>
- Mozilla Thunderbird
Mail-Client
Unterstützt OpenPGP- und S/MIME-Zertifikate
<https://www.thunderbird.net/de>

**Bitte zeitnah auf ihren Notebook installieren.
Cryptool1 werden wir in Kürze einsetzen.**

**Geheimhaltung bedeutet:
Nachrichten unter **Verschluss****

**Verschluss bedeutet:
Abgeschlossen mit **Schlüssel****

**Schlüssel bedeutet:
Muss sicher **verschickt** werden**

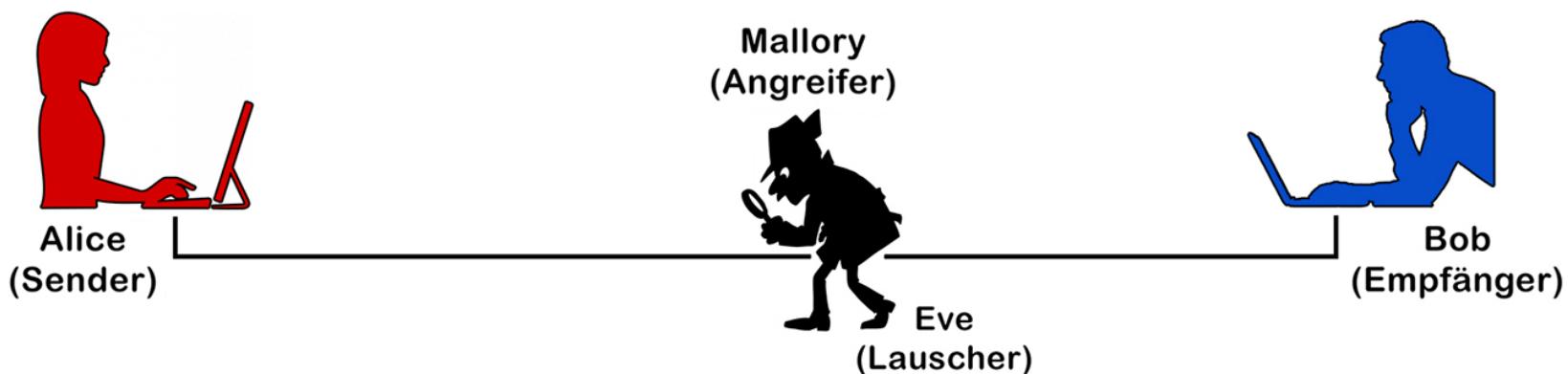


Wenn etwas geheim
oder vertraulich sein
soll, schützen wir es
vor neugierigen Blicken

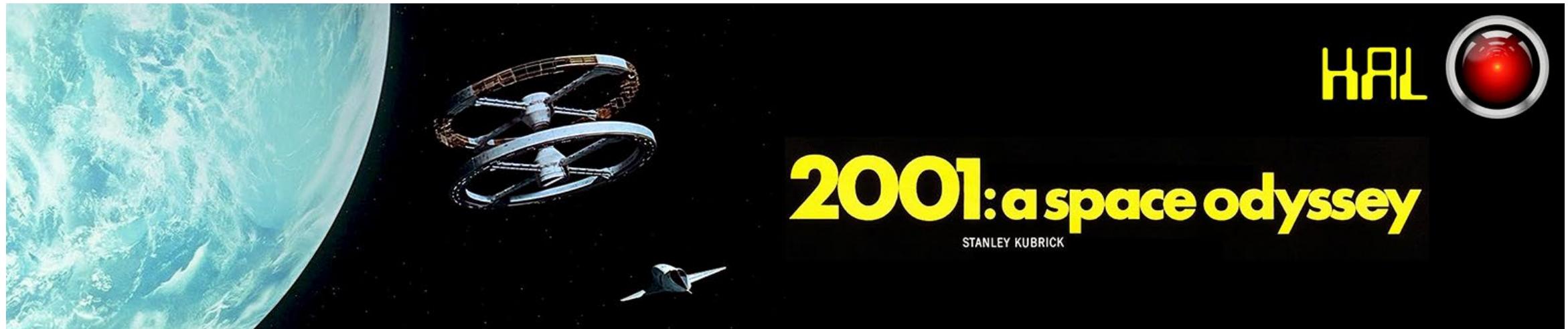
... oder man schliesst
es ein, mit einem
Schlüssel, den man
sicher aufbewahrt

Schlüssel in falschen
Händen = Geheim-
haltung dahin!
Der Schlüssel ist
gleich geheim, wie
die Botschaft selbst

Die Akteure werden in der Krypto-Literatur so benannt:



Klassische, symmetrische Verfahren:

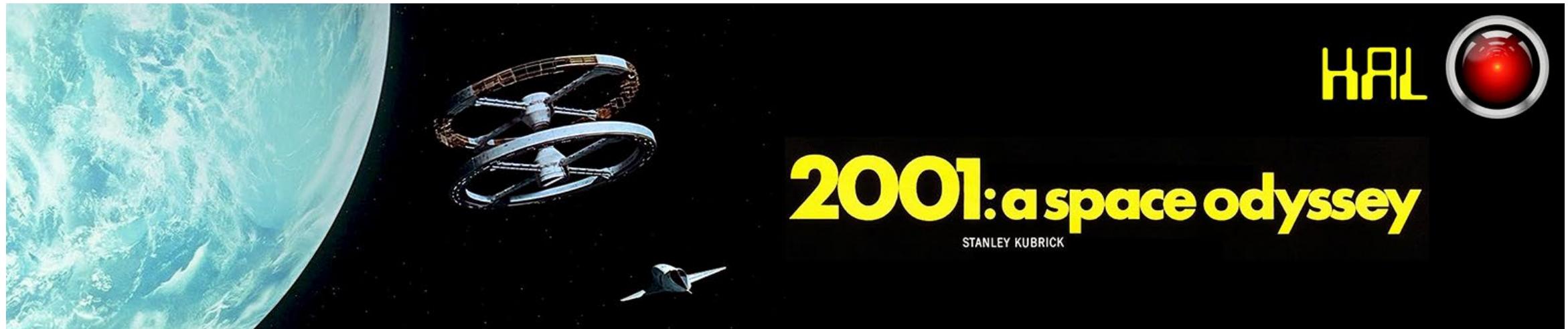


HAL 9000 ist im Film "2001:a space odyssey" der neurotische, fehleranfällige Bord-Computer im Raumschiff "Discovery".

Welchen Computermarkennamen wollte der Regisseur Stanley Kubrick wohl aufs Korn nehmen?

HAL
?

Klassische, symmetrische Verfahren:



HAL 9000 ist im Film "**2001:a space odyssey**" ein "neurotischer" Bord-Computer des Raumschiffs "Discovery".

Welchen **Computermarkennamen** wollte der Regisseur Stanley Kubrick wohl aufs Korn nehmen?

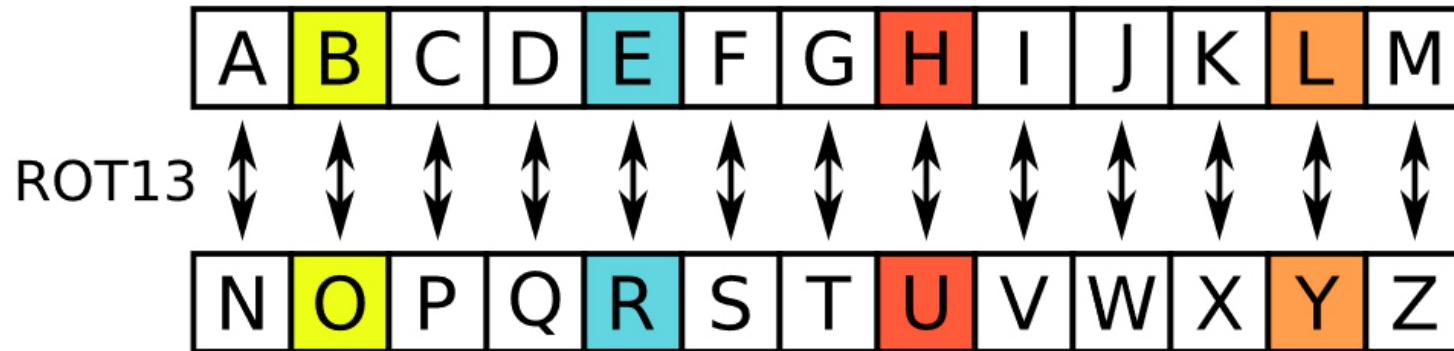
HAL



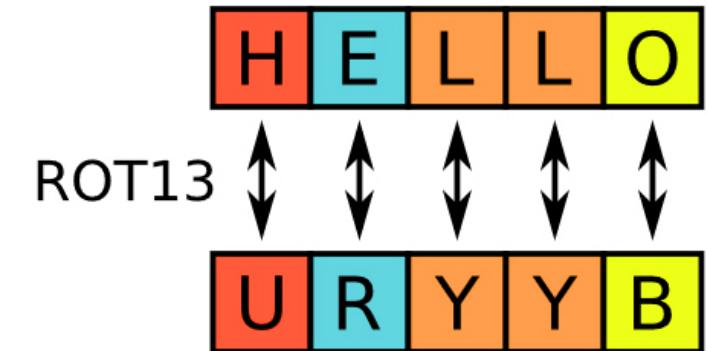
*Dies entspricht einer
Rotations-Chiffre:
Einen Buchstaben im
Alphabet vorwärts*

*Kubrick hat sich später korrigiert:
Gemeint sei:
**Heuristisch programmiert
ALgorithmischer Computer***

Klassische, symmetrische Verfahren: Rotationschiffre



Der Schlüssel lautet hier: 13



Aus HELLO wird URYYB

Klassische, symmetrische Verfahren: Rotationschiffre



Julius Cäsar kannte bereits den folgenden Verschlüsselungstrick:

"Ersetze jeden Buchstaben durch den, der eine bestimmte Anzahl Stellen später im Alphabet folgt!"

Was waren Cäsar's geheime Botschaften die hinter dieser Chiffre stecken?

**GHU DQJULII HUIROJW CXU WHHCHLW GLH ZXHUIHO VLQG
JHIDOOHQ LFK NDP VDK XQG VLHJWH WHLOH XQG KHUVFKH**

Tipp:

CrypTool1 benutzen

Rotationschiffre ist ein klassisches, symmetrisches Verfahren.

Machen Sie Kryptoanalyse mit einem ASCII-Histogramm. (Häufigkeitsanalyse der im Text enthaltenen Buchstaben)

Klassische, symmetrische Verfahren: Rotationschiffre



Julius Cäsar kannte bereits den folgenden Verschlüsselungstrick:

"Ersetze jeden Buchstaben durch den, der eine bestimmte Anzahl Stellen später im Alphabet folgt!"

Was waren Cäsar's geheime Botschaften die hinter dieser Chiffre stecken?

**GHU DQJULII HUIROJW CXU WHHCHLW GLH ZXHUIHO VLQG
JHIDOOHQ LFK NDP VDK XQG VLHJWH WHLOH XQG KHUVFKH**

**DER ANGRIFF ERFOLGT ZUR TEEZEIT
DIE WUERFEL SIND GEFALLEN
ICH KAM SAH UND SIEGTE
TEILE UND HERRSCHE**

Das ASCII-Histogramm ergibt als häufigstes Zeichen im chiffrierten Text das «H». Da in deutschen Sprache (wie auch der englischen) Schriften das «E» am Häufigsten vorkommt, wurde der Text mit dem Schlüssel 3 (ROT-3) verschlüsselt

Klassische, symmetrische Verfahren: Vigenèrechiffre



Blaise de Vigenère
1523–1596

SCHLÜSSEL: GEHEIM

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
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
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	
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	
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	
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	
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	
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	
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	
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	
K	L	M	N	O	P	Q	R	S	T	U	V	W	W	X	Y	Z	A	B	C	D	E	F	G	H	
L	M	N	O	P	Q	R	S	T	U	V	W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	
M	N	O	P	Q	R	S	T	U	V	W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	
N	O	P	Q	R	S	T	U	V	W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	M	
O	P	Q	R	S	T	U	V	W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	M	

TEXT: VULKAN

CHIFFRE: BYSOIZ

Klassische, symmetrische Verfahren: Vigenèrechiffre

1. "BEEF" mit Schlüsselwort "AFFE" ergibt welche Vigenèrechiffre? (Ohne Cryptool!)
2. Vigenèrechiffre "WRKXQT" mit Schlüsselwort "SECRET" ergibt welchen Klartext? (Ohne Cryptool!)
3. Vigenèrechiffre "knacken":
USP JHYRH ZZB GTV CJ WQK OCLGQVFQK GAYKGVFGX NS ISBVB MYBC MWCC NS JOEVB GTV KRQFV AGK XCUSP VFLVBLLBE ESSEILUBCLBXZU SENSWFGVRCES SER CZBCE ILUOLBPYISL CCSZG VZJ
4. Klartext aus Aufgabe 3 neu verschlüsseln mit Key:
Lore ipsum dolor sit amet consectetur adipiscing elit Aenean commodo ligula eget dolor Aenean massa Cum sociis natoque penatibus et magnis dis parturient montes nascetur ridicul usmus Done

Was stellen wir fest? Funktioniert der "Hack" aus Aufgabe 3 immer noch?

Klassische, symmetrische Verfahren: Vigenèrechiffre

1. "BEEF" mit Schlüsselwort "AFFE" ergibt welche Vigenèrechiffre? **BJJJ**
2. Vigenèrechiffre "WRKXQT" mit Schlüsselwort "SECRET" ergibt welchen Klartext? **ENIGMA**
3. Vigenèrechiffre "knacken":

USP JHYRH ZZB GTV CJ WQK OCLGQVFQK GAYKGVFGX NS ISBVB MYBC MWCC NS JOEVB GTV
KRQFV AGK XCUSP VFLVBLLBE ESSEILUBCLBXZU SENSWFGVRCES SER CZBCE ILUOLBPYISL
CCSZG VZJ

Das ASCII-Histogramm bringt hier nichts. Besser bedient sind wir mit einer Vigenère-Analyse. Die Analyse erfolgt in zwei Schritten.

A. Ermittlung der verwendeten Schlüssellänge (Umso länger der Schlüssel, desto schwieriger die Ermittlung der Schlüssellänge.)

B. Ermittlung des eingesetzten Schlüssels

Der Originaltext lautet somit:

DER STAAT BIN ICH

ES IST AEUSSERST SCHWIERIG ZU REDEN OHNE VIEL ZU SAGEN

ICH MACHE MIT JEDER ERNENNUNG NEUNUNDNEUNZIG UNZUFRIEDENE UND EINEN UNDANKBAREN

LOUIS XIV (Das sind übrigens Zitate vom französischen Sonnenkönig Ludwig XIV)

Ist Vigenère knackbar? Dazu zwei Beispiele:

Text: EBEEEE

Schlüssel: B

Chiffre: FCCFFF

Text: EBEEEE

Schlüssel: BC

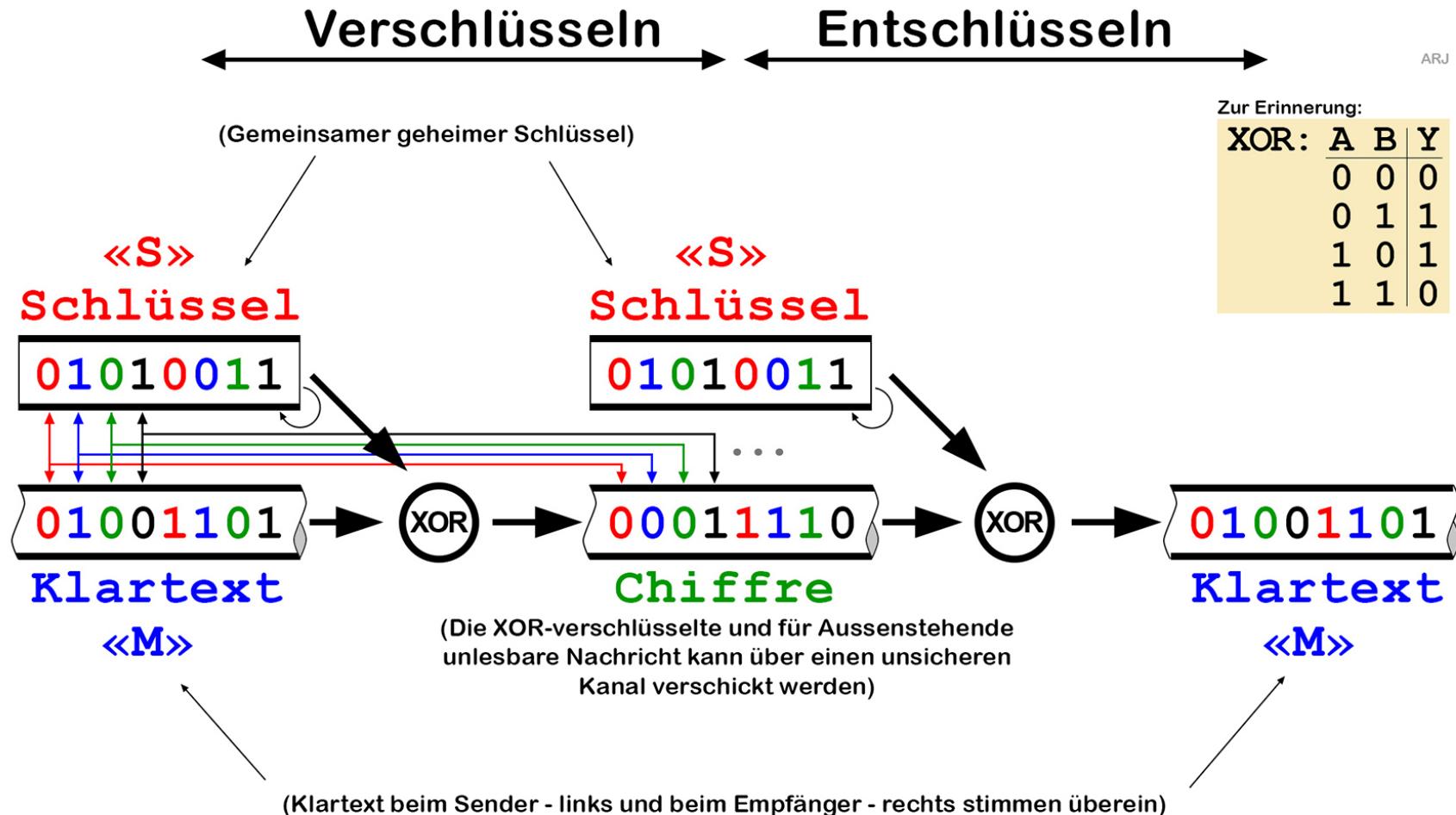
Chiffre: FDCGFG

Was stellen wir fest?

Klassische, symmetrische Verfahren: XOR-Stromchiffre

Was ist eine Strom-Chiffre: Es wird **bitweise verschlüsselt**

Was ist eine Block-Chiffre: Es wird **blockweise verschlüsselt**. Ein Block entspricht z.B. einem **Character**



Klassische, symmetrische Verfahren: XOR-Stromchiffre

XOR-Verschlüsselung von Hand (ohne Cryptool)

Die Dezimalzahl **4711** ergibt mit dem binären Schlüssel **1000'1101** welche XOR-Chiffre?

Kontrolle: Entschlüsseln sie die erhaltene Chiffre mit demselben Schlüssel.

Hinweis:

Dezimalzahl in 16-Bit Binärzahl umwandeln. Führende Nullen nicht weglassen.

Ist der Schlüssel zu kurz, diesen mehrmals wiederholen.

Datenstrom beginnt mit der Übertragung des MSB's, also von links nach rechts.

Klassische, symmetrische Verfahren: XOR-Stromchiffre

XOR-Verschlüsselung von Hand (ohne Cryptool)

Die Dezimalzahl **4711** ergibt mit dem binären Schlüssel **1000'1101** welche XOR-Chiffre?

Kontrolle: Entschlüsseln sie die erhaltene Chiffre mit demselben Schlüssel.

Hinweis:

Dezimalzahl in 16-Bit Binärzahl umwandeln. Führende Nullen nicht weglassen.

Ist der Schlüssel zu kurz, diesen mehrmals wiederholen.

Datenstrom beginnt mit der Übertragung des MSB's, also von links nach rechts.

«4711» ergibt binär «0001'0010'0110'0111»

«0001'0010'0110'0111» (Den Klartext...)

«1000'1101'1000'1101» (...mit 2x wiederholtem Key XOR verknüpft...)

«1001'1111'1110'1010» (...ergibt diese Chiffre)

Moderne, symmetrische Verfahren: AES

AES bedeutet Advanced Encryption Standard

Algorithmus:	Rijndael
Entwickler:	Joan Daemen und Vincent Rijmen (ca. Jahr 2000)
Blocklänge:	128 Bit
Schlüssellänge:	128, 192 oder 256 Bit
Lizenzkosten:	Keine
Bemerkungen:	AES ist Nachfolger von DES. AES-192 und AES-256 sind in den USA für staatliche Dokumente mit höchstem Geheimhaltungsgrad zugelassen
Aufbau:	Blockchiffre als Substitutions-Permutations-Netzwerk

AES wird in der Crypttol-Onlineversion genauer erklärt: <https://www.cryptool.org/de/cto/aes-animation>



Fragen?

Symmetrische Verschlüsselungsverfahren:

(ROT, Vigener, XOR, AES und weitere)

- **Warum «symmetrisch»?**
- **Was zeichnen diese aus?**

Symmetrisch: Schlüsseltausch ?



Verschlüsselt und
Entschlüsselt wird
mit demselben
Schlüssel



Das Problem ist
nur der sichere
Schlüsseltausch...



... damit der Adressat,
und nur dieser,
auf seine Mitteilung
zugreifen kann

Symmetrisch: Schlüsselanzahl ?

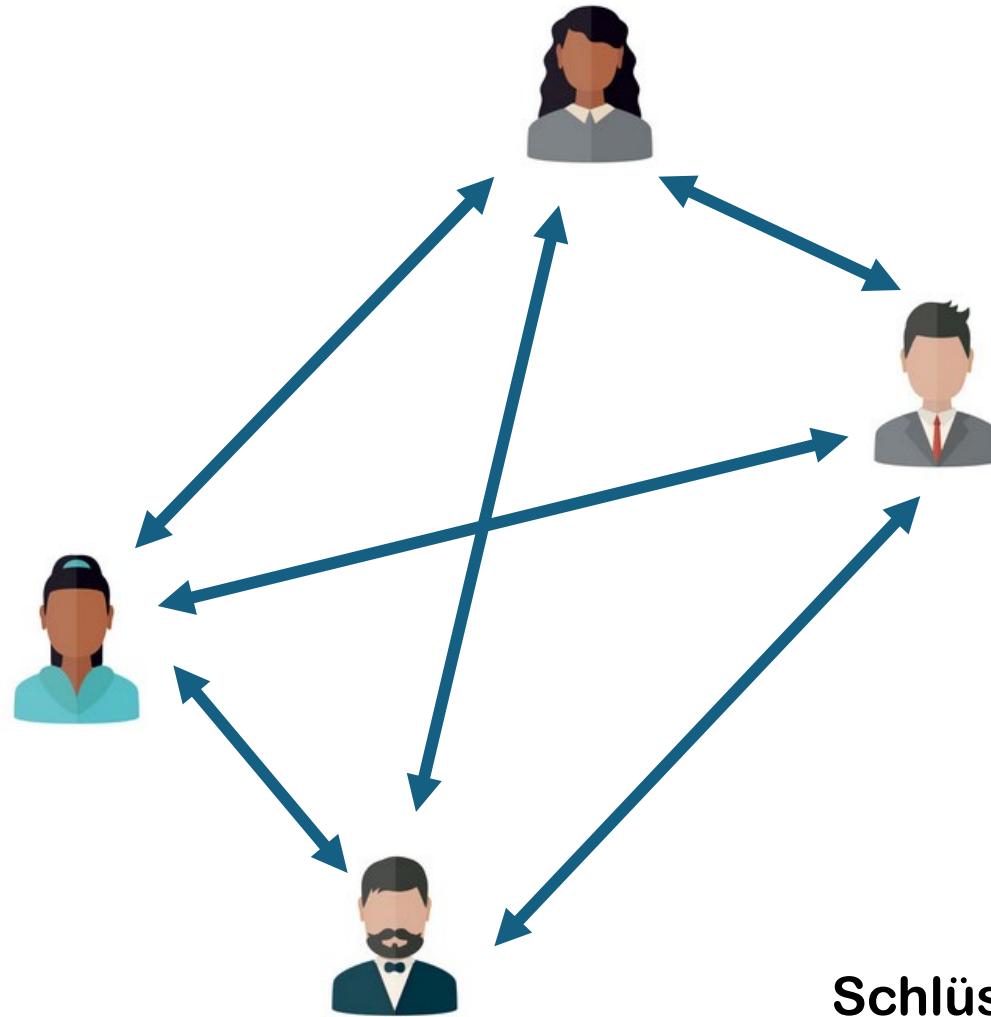
Teilnehmer: 4



Schlüssel:

Symmetrisch: Schlüsselanzahl ?

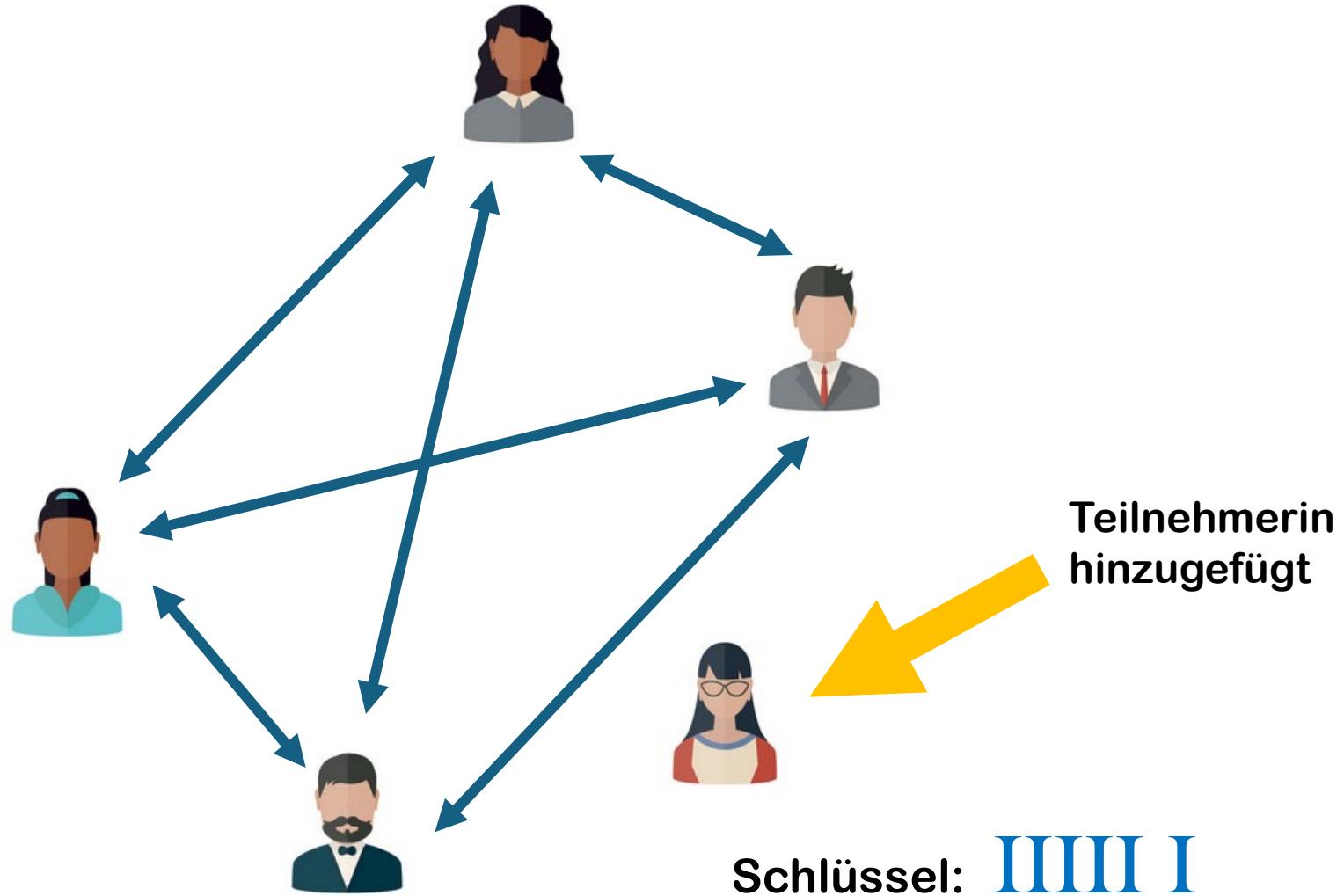
Teilnehmer: 4



Schlüssel: **IIII I**

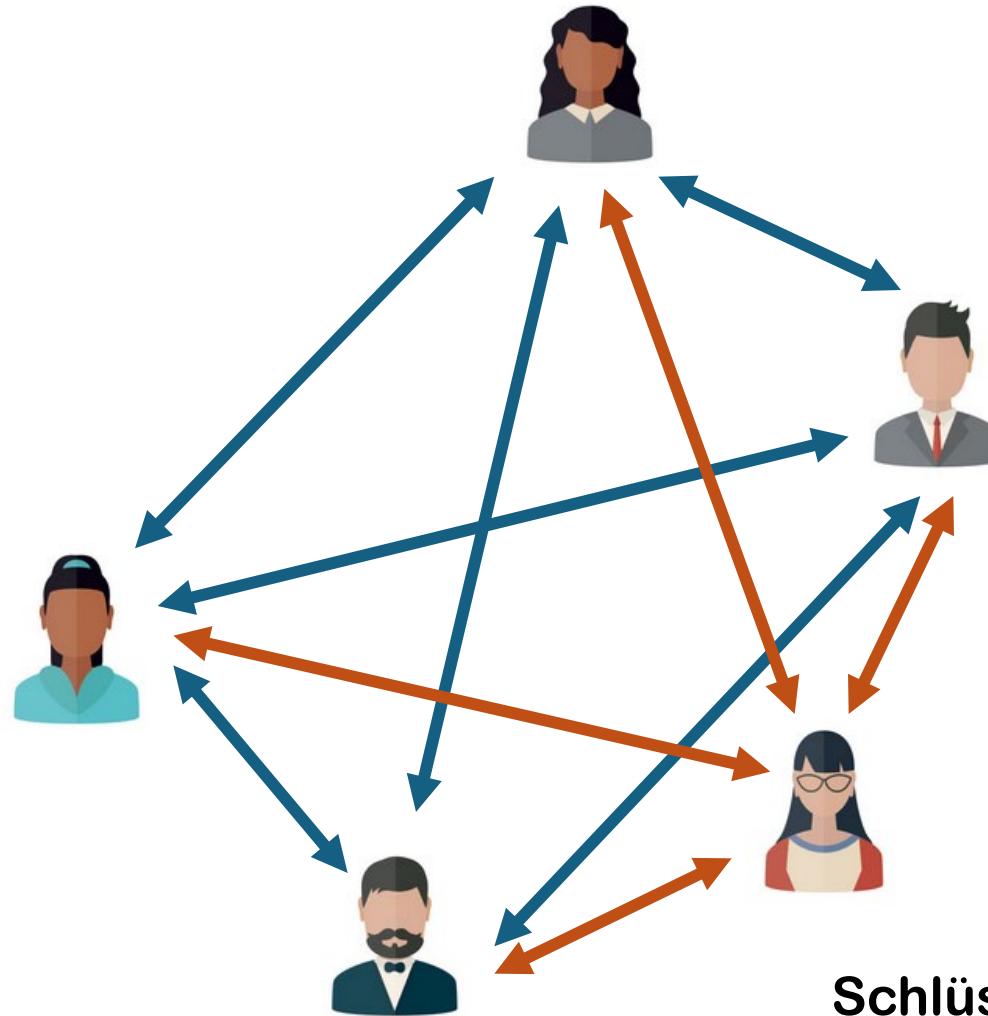
Symmetrisch: Schlüsselanzahl ?

Teilnehmer: 5



Symmetrisch: Schlüsselanzahl ?

Teilnehmer: 5

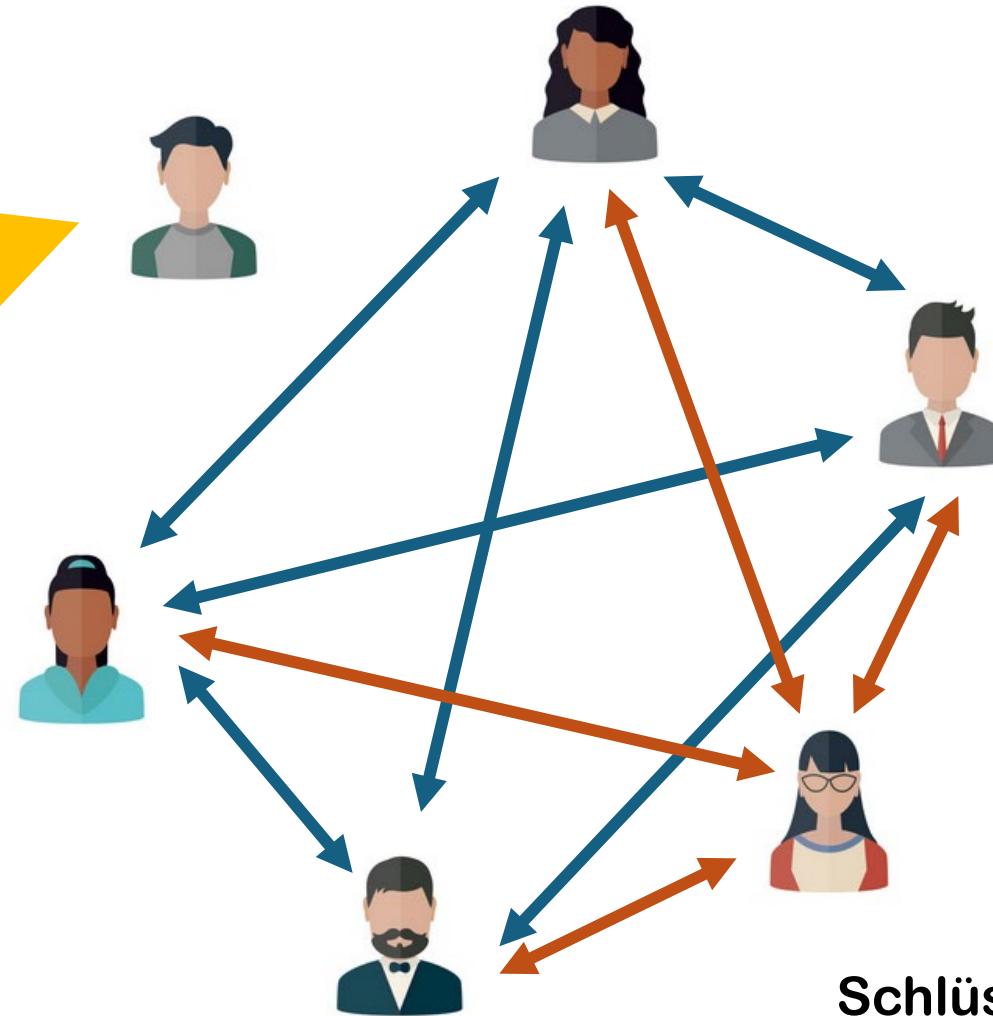


Schlüssel: **I** **II** **III** **I** **II** **III**

Symmetrisch: Schlüsselanzahl ?

Teilnehmer: 6

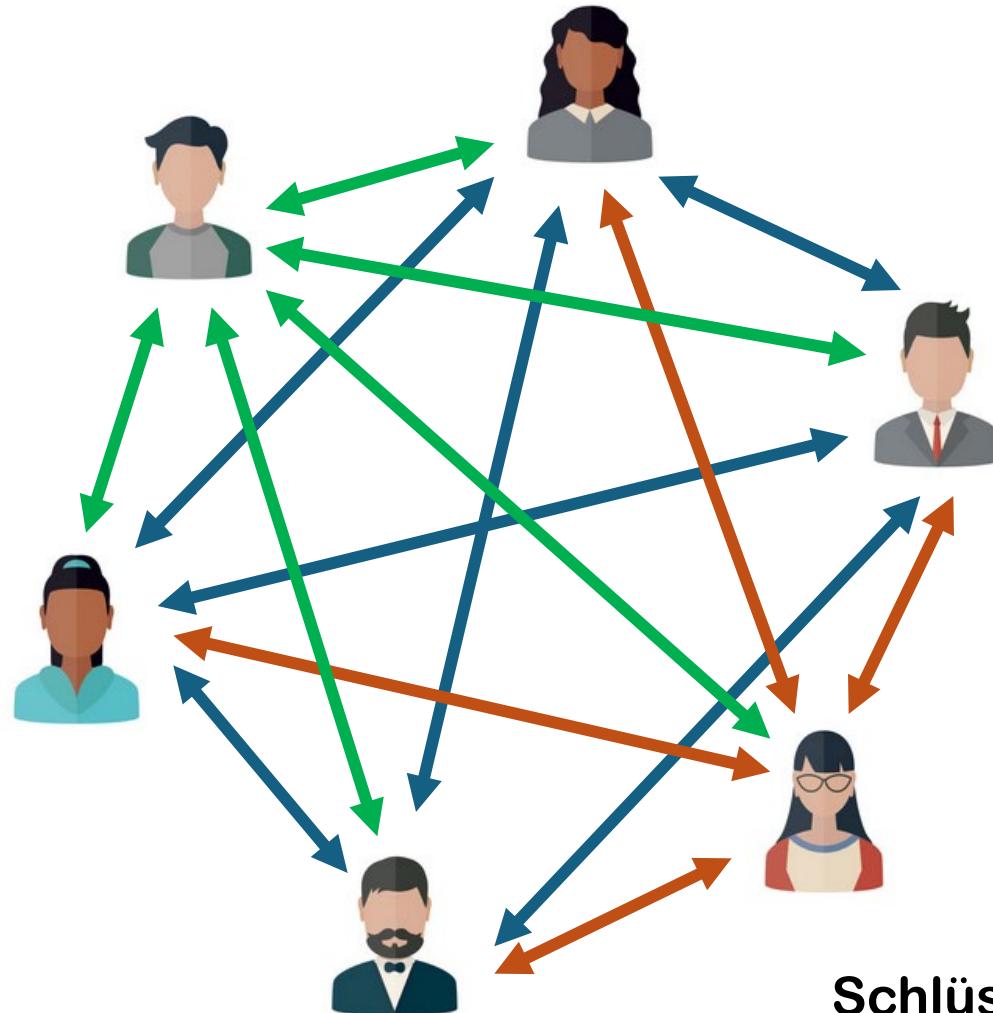
Teilnehmer
hinzugefügt



Schlüssel: **I**III **I**III

Symmetrisch: Schlüsselanzahl ?

Teilnehmer: 6



Symmetrisch: Schlüsselanzahl ?



Beispiel:
Teilnehmer: 12
Schlüssel: 66

Berechnung:

$$S=T*(T-1)/2$$
$$S=12*11/2=66$$

$S=T^2/2 - T/2$
**Quadratische
Funktion**

Symmetrisch: Schlüsselanzahl ?

Aufgabe:

Wie viele Schlüssel sind erforderlich, damit sich
1000 Personen gegenseitig symmetrisch verschlüsselte
Botschaften zukommen lassen können?

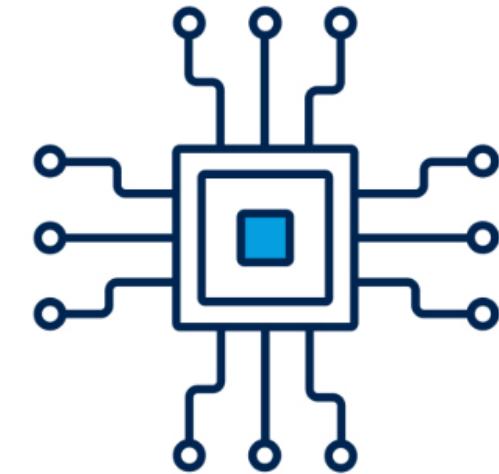
Symmetrische Verschlüsselung:



(-) Schlüsseltausch



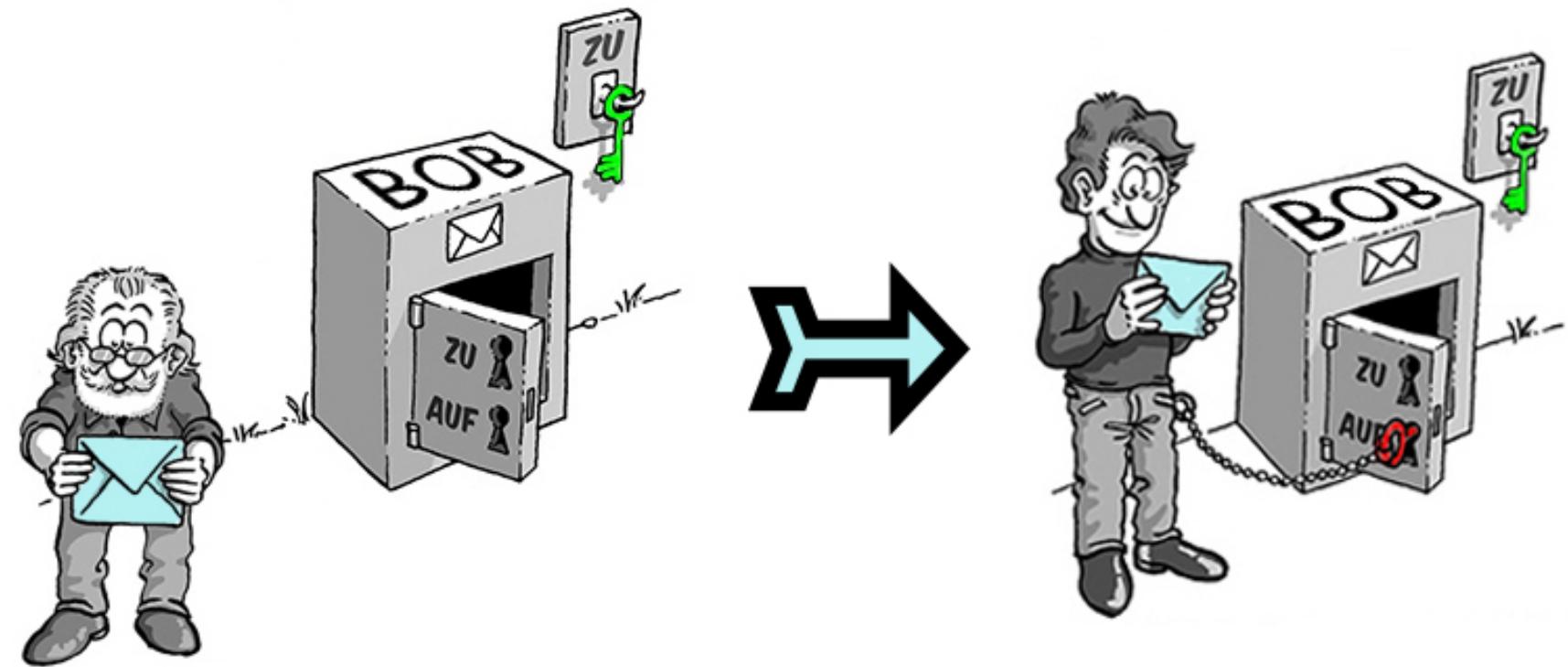
(-) Schlüsselanzahl



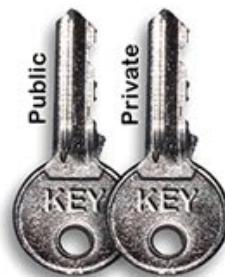
(+) Digitale Verarbeitung

Die Lösung des Problems:

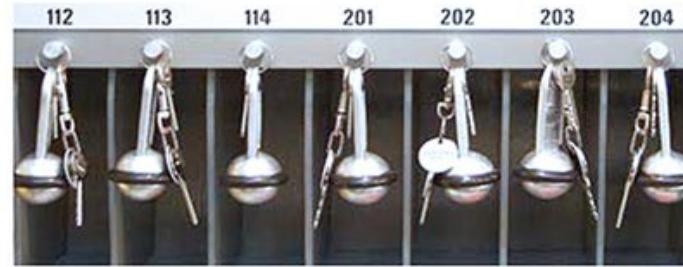
Asymmetrische Verschlüsselung



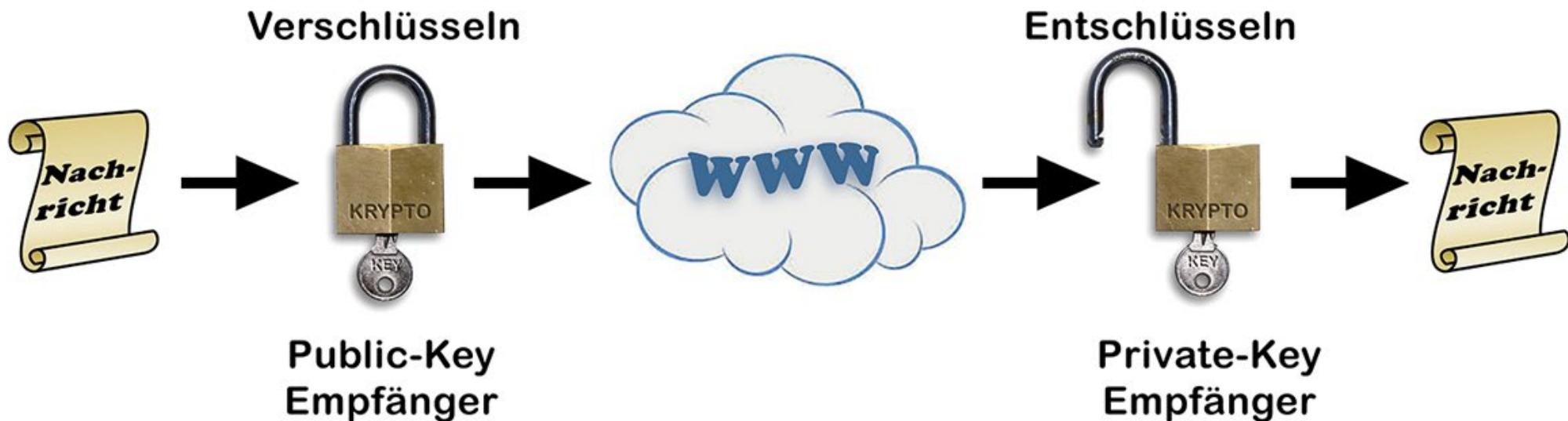
Asymmetrische Verschlüsselung



Schlüsselpaar
erzeugen



Public-Key veröffentlichen
Private-Key geheim halten



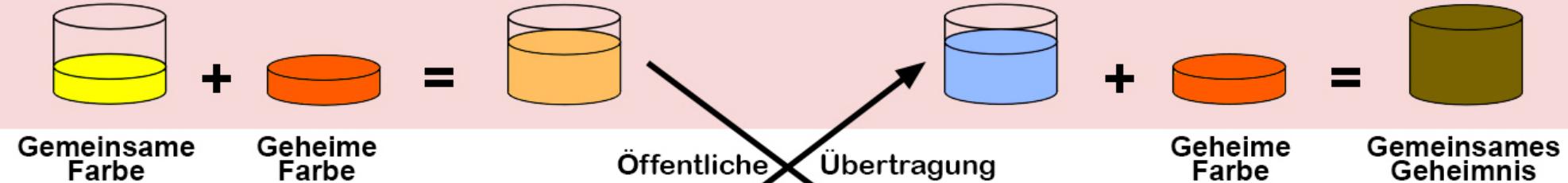
Asymmetrische Verschlüsselung

Q: Kann aus dem öffentlichen Schlüssel der private Schlüssel hergeleitet oder berechnet werden?

**A: Ist praktisch unmöglich!
Es folgt eine Erklärung anhand einer Farb-Analogie...**

Asymmetrische Verschlüsselung: Diffie-Hellman Schlüsseltausch

ALICE:



Bob:



Öffentlicher Schlüssel von Alice:

Privater Schlüssel von Alice:

↓
Farbmischung kann nicht
rückgängig gemacht werden.

Öffentlicher Schlüssel von Bob:

Privater Schlüssel von Bob:

1. Verwenden sie im Cryptool1 unter "Einzelverfahren→Protokolle" die "Diffie-Hellman-Demo" um den Diffie-Hellman- Schlüsseltausch zu studieren. Experimentieren sie mit verschiedenen Parametern wie

- **Bitlänge**
- **Primzahlen**
(Wählen sie auch bewusst kleine Primzahlen im ein oder zweistelligen Bereich)
- **Geheimnis**

Fragen:

- **Wie werden die Teilschlüssel berechnet? (Math. Funktion)**
- **Was bewirkt die Wahl von kleinen Primzahlen wie z.B. 7,11 oder 13?**
- **Als Resultat erhalten sie einen "geheimen Schlüssel". Was haben sie damit erreicht?**

2. Verwenden sie im Cryptool1 bei "Ver-/Entschlüsseln→Asymmetrisch" die "RSA-Demo" um das RSA-Verfahren zu studieren.

Experimentieren sie mit verschiedenen Parametern wie

- Primzahl p**
(Wählen sie auch bewusst kleine Primzahlen im ein oder zweistelligen Bereich)
- Primzahl q**
(Wählen sie auch bewusst kleine Primzahlen im ein oder zweistelligen Bereich)
- Öffentlicher Schlüssel e**
- Eingabe von Nachrichten verschiedener Längen**

Fragen:

- Was bewirkt die Eingabe von kleinen Werten für p, q und e?**
- Welche mathematische Funktion verwendet RSA?**
- Was ist der wesentliche Unterschied zu Diffie-Hellman?**

3. Erstellen sie im Cryptool1 bei "Digitale Signaturen/PKI→PKI" unter "Schlüssel erzeugen/importieren" ein eigenes Schlüsselpaar.

Erstellen sie danach auf ihrem Desktop eine kleine Textdatei.

Verwenden nun sie im Cryptool1 bei "Ver-/Entschlüsseln→Hybrid" die "RSA-AES-Verschlüsselung" und verschlüsseln sie ihre Textdatei.

Verwenden nun sie im Cryptool1 bei "Ver-/Entschlüsseln→Hybrid" die "RSA-AES-Entschlüsselung" und entschlüsseln sie ihre Textdatei.

Fragen:

- **Was bezweckt der Session-Key?**
- **Was ist der wesentliche Unterschied zu RSA oder Diffie-Hellman?**



Fragen?

Bedürfnis «A»

- Informationssicherheit
- Widerstandsfähigkeit gegen Manipulation und unbefugtes Lesen

DATEN VERSCHLÜSSELN

Bedürfnis «B»

- Authentisierung - Sicherstellung der Identität eines Kommunikationspartners
- Vertraulichkeit - Zugänglichkeit der Nachricht nur für bestimmten Empfängerkreis
- Integrität - Schutz vor Verfälschung von Nachrichten bei der Übermittlung
- Autorisierung - Prüfung der Zugriffsberechtigung auf Ressourcen
- Verfügbarkeit - Schutz vor Datenverlust, Sicherstellung des laufenden Betriebs
- Verbindlichkeit - Sicherer Nachweis der Absendung bzw. des Empfangs

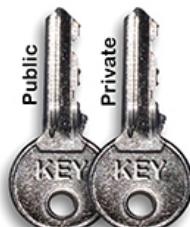
DATEN SIGNIEREN

Bedürfnis «C»

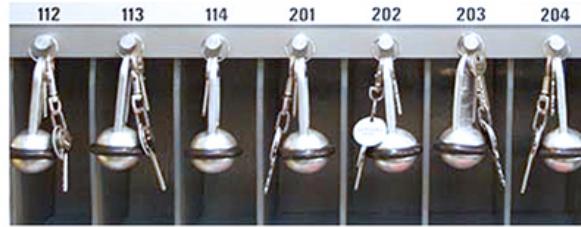
- Kombination von Bedürfnis «A» UND Bedürfnis «B»

DATEN VERSCHLÜSSELN UND SIGNIEREN

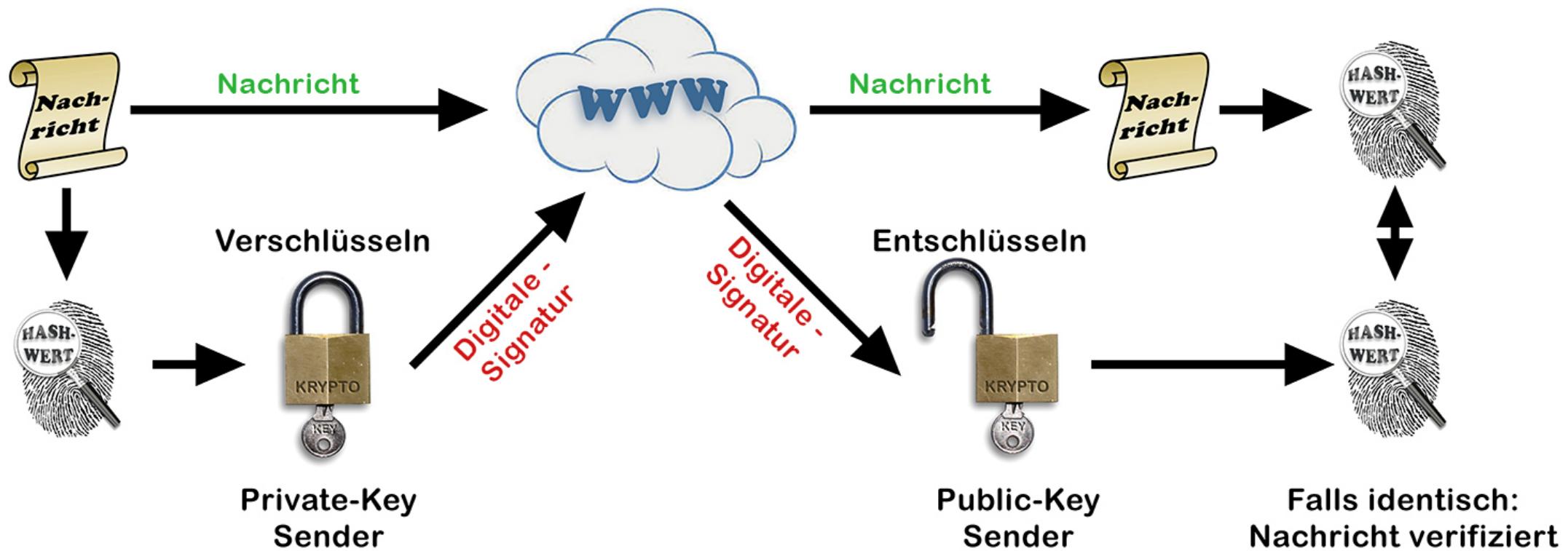
Asymmetrisches Verfahren: Digitale Signatur



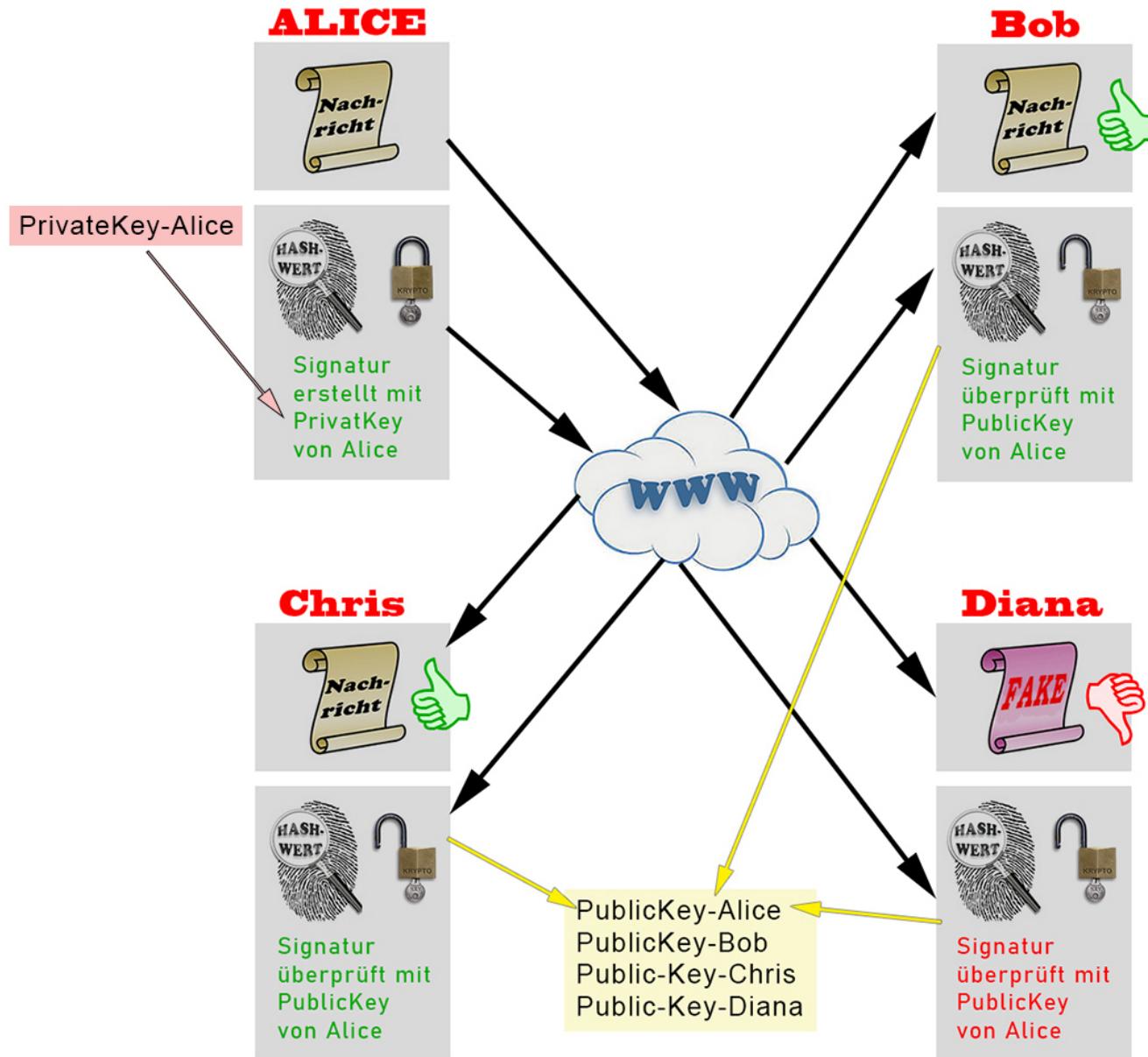
Schlüsselpaar
erzeugen



Public-Key veröffentlichen
Private-Key geheim halten



Asymmetrisches Verfahren: Digitale Signatur



Alices Originalnachricht wurde von jemand anderem, aus welchen Gründen auch immer, abgeändert. Der von Alice stammende und entschlüsselte Hashwert stimmt nicht mit dem Hashwert des FAKE-Dokuments überein und dieses ist somit als Fälschung enttarnt.

1. Verwenden sie im Cryptool1 unter "**Einzelverfahren→Hashverfahren**" die "**Hash-Demo**" um den Hash-Algorithmus zu studieren. Experimentieren sie mit verschiedenen Parametern wie

- **Hashfunktion**
- **Inhalt des aktuellen Dokuments:** Tauschen sie beim Originaltext z.B. einen Buchstaben aus oder fügen sie ein Leerzeichen ein.

Beobachten sie, wie sich der Hashwert auch bei subtilen Textmodifikationen ändert. Wie unterscheiden sich eigentlich die Hashfunktionen? Welche erfüllt die aktuellen Sicherheitsanforderungen?

2. Erstellen sie auf ihrem Desktop eine kurze Textdatei.

**Verwenden sie im Cryptool1 unter "Digitale Signaturen/PKI"
das Tool "Dokument signieren" um ihre Textdatei zu signieren.**

**Verwenden sie im Cryptool1 unter "Digitale Signaturen/PKI"
das Tool "Signatur überprüfen" um die Signatur ihrer Textdatei zu
überprüfen.**

Ändern sie in ihrer Textdatei z.B. den ersten Buchstaben.

**Überprüfen sie im Cryptool1 unter "Digitale Signaturen/PKI"
mit "Signatur überprüfen" erneut die Signatur ihrer Textdatei.
Was stellen sie fest?**

3. Wie sicher ist die Hash-Funktion?

**Verwenden sie im Cryptool1 unter "Analyse → Hashverfahren"
das Tool "Angriff auf den Hashwert der digitalen Signatur".**

Text und Hashwert müssen übereinstimmen.

**Unsichere, veraltete Hashverfahren sind ein Problem:
wenn bei verschiedenen Nachrichten der Hashwert überein stimmt.
Probieren wir das doch gleich mal aus:**

1. Erstelle **original.txt** mit Text «**Verkaufe mein Notebook zu CHF 1500.-**»
2. Erstelle von **original.txt** eine Kopie mit Dateinamen **backup.txt**.
3. Erstellen **fake.txt** mit Text «**Verkaufe mein Notebook zu CHF 150.-**»
4. Erstellen zu Kontrollzwecken mit Einzelverfahren→Hashverfahren→MD2 je einen **MD2-Hashwert**.
Feststellung: **original.txt** und **backup.txt** haben denselben Hashwert, **fake.txt** einen anderen.
5. **backup.txt** kann nun gelöscht werden, brauchen wir nicht mehr.
6. Analyse→Hashverfahren→**Angriff auf den Hashwert der digitalen Signatur**
Harmlose Datei: **original.txt**
Gefährliche Datei: **fake.txt**
7. Den schwächsten **Hashalgorithmus MD2** mit einer signifikante Bitlänge von **16 Bit** verwenden!
Optionen für die **Nachrichtenmodifikation**: Zeichen anhängen / Nicht druckbare Zeichen
8. Man erhält zwei Varianten von den beiden Textdateien:
Von «**original.txt**»: «**Harmlose Nachricht: MD2, <92 14>**»
Von «**fake.txt**»: «**Gefährliche Nachricht: MD2, <92 14>**»
Cryptool hat von beiden Dateien Varianten mit kleinen Ergänzungen/Änderungen gefunden bzw. erstellt, die sich in den ersten 16 Bit des Hashwerts nicht unterscheiden: <92 14>
9. Den Vorgang mit längerer signifikanten Bitlänge von z.B. 24,32, etc. wiederholen.
Der Suchvorgang in Cryptool wird immer länger dauern.
*Bei einer signifikanten Bitlänge von 128 wäre der Hashwert bei der Textdatei **original.txt** und **fake.txt** komplett berechnet. Das heisst, es liegen nun zwei Dokumente vor, die denselben Hashwert besitzen.*

Wie kann ich das nun ausnutzen?

Ich habe nun zwei neue Dokumente:

- original_neu.txt
- fake_neu.txt

Zudem weiss ich, wenn ich den Hash-Algorithmus MD2-16Bit benutze, dies bei beiden Dokumenten denselbe Hashwert aufweisen.

Ich brauche nur noch das richtige Dokument original_neu.txt meinem Opfer zur Signatur vorzulegen. Diese Signatur hat bekanntlich für das fake_neu.txt auch seine Gültigkeit.

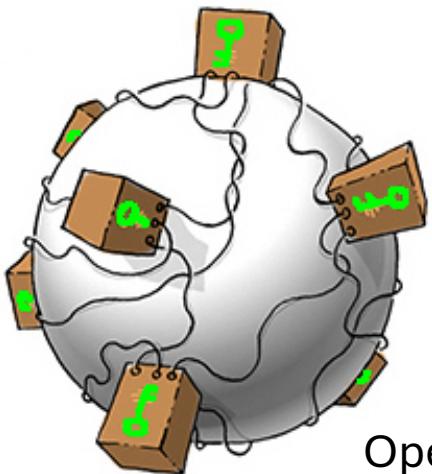
Nun nenne ich fake_neu.txt in original.txt um, ergänze es mit der soeben erstellten Signatur und verteile das Fake-Angebot unter die Leute. Diese können nun das mittels Signatur überprüfte Fake-Verkaufsangebot zum Schaden meines Opfers nutzen.



Fragen?



Web of Trust



OpenPGP

Public-Key-Infrastruktur



X.509

PKI - Public-Key-Infrastruktur-Begriffe:

- **PKI** stellt digitale Zertifikate aus
- **Zertifizierungsstelle (Certificate Authority, CA)**
- **Registrierungsstelle (Registration Authority, RA)**
- **Zertifikatsperlliste (Certificate Revocation List, CRL)**
- **Verzeichnisdienst (Directory Service)**
- **Validierungsdienst (Validation Authority, VA)**
- **Dokumentationen: CP (Certificate Policy), CPS (Certification Practice Statement), DS (Policy Disclosure Statement)**
- **Subscriber: Inhaber von Zertifikaten**
- **Participant: Nutzer von Zertifikaten**

Sicherheit im Internet

Zertifikate im Internet

Mindestanforderungen für Validierungsmethoden:

- **Domain Validated: (0-\$)** Nachweis der Kontrolle über die Domain via DNS, HTTP, E-Mail.
- **Individual Validated: (\$\$)** Zusätzlich überprüfte Identität des Antragstellers im Zertifikat.
- **Organization Validated: (\$\$\$)** Zusätzlich amtlich bestätigter Firmennamen.
- **Extended Validation: (\$\$\$\$)** Strengste Prüfkriterien bezüglich Identität, Geschäftssadresse, Domainbesitz. Antragssteller unterschreibt rechtlich bindende Dokumente als zeichnungsberechtigter Firmenvertreter. Überprüfte Zertifizierungsstelle erforderlich.

Klassifizierung der E-Mail-Zertifikate von Anbietern sicherer E-Mail-Kommunikation:

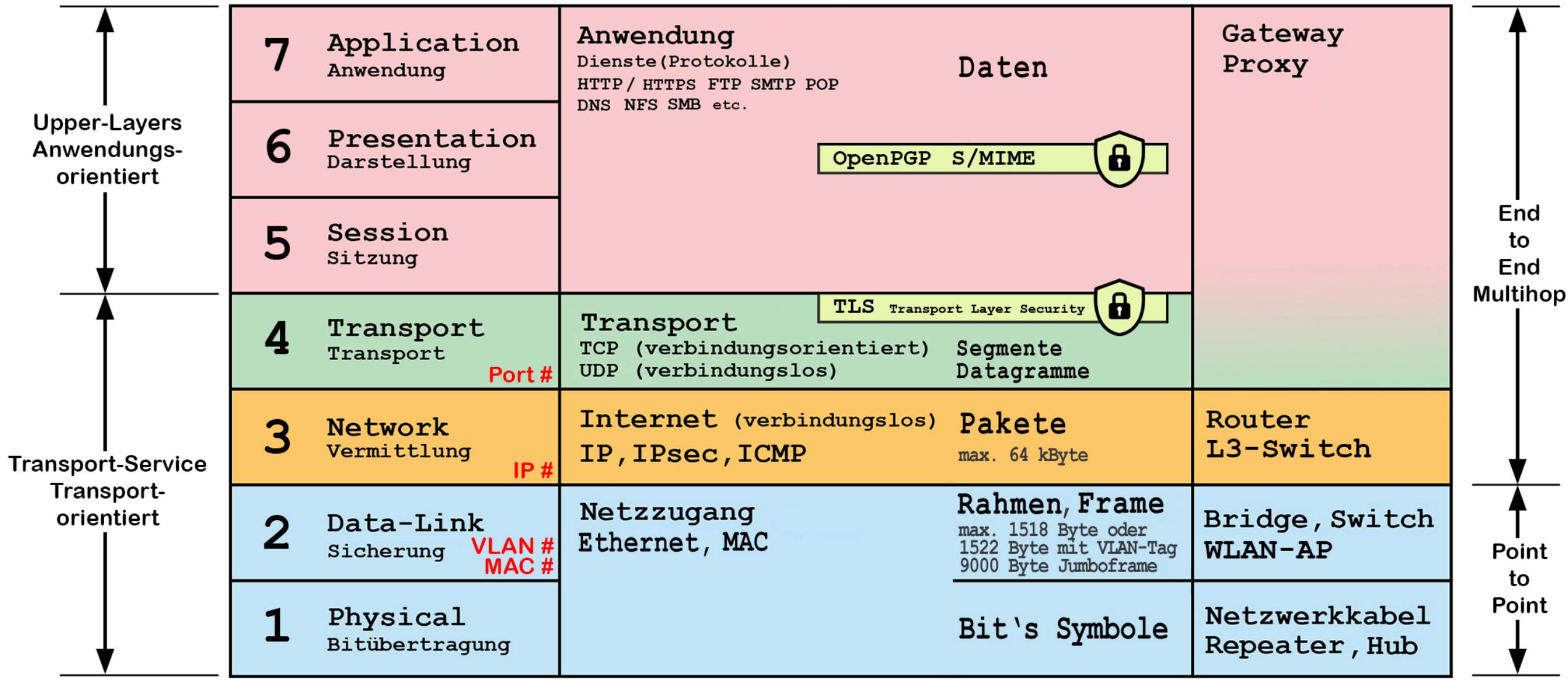
1. Echtheit der E-Mail-Adresse wird durch Zertifizierungsstelle bestätigt.
2. Zusätzlich wird der dazugehörende Name ggf. Organisation/Firma in das Zertifikat mit aufgenommen.
3. Verifizierung der Angaben mithilfe Drittdatenbanken, Ausweiskopien, Handelsregisterauszügen etc.
4. Antragsteller muss sich zusätzlich persönlich ausweisen.

Auswahl:

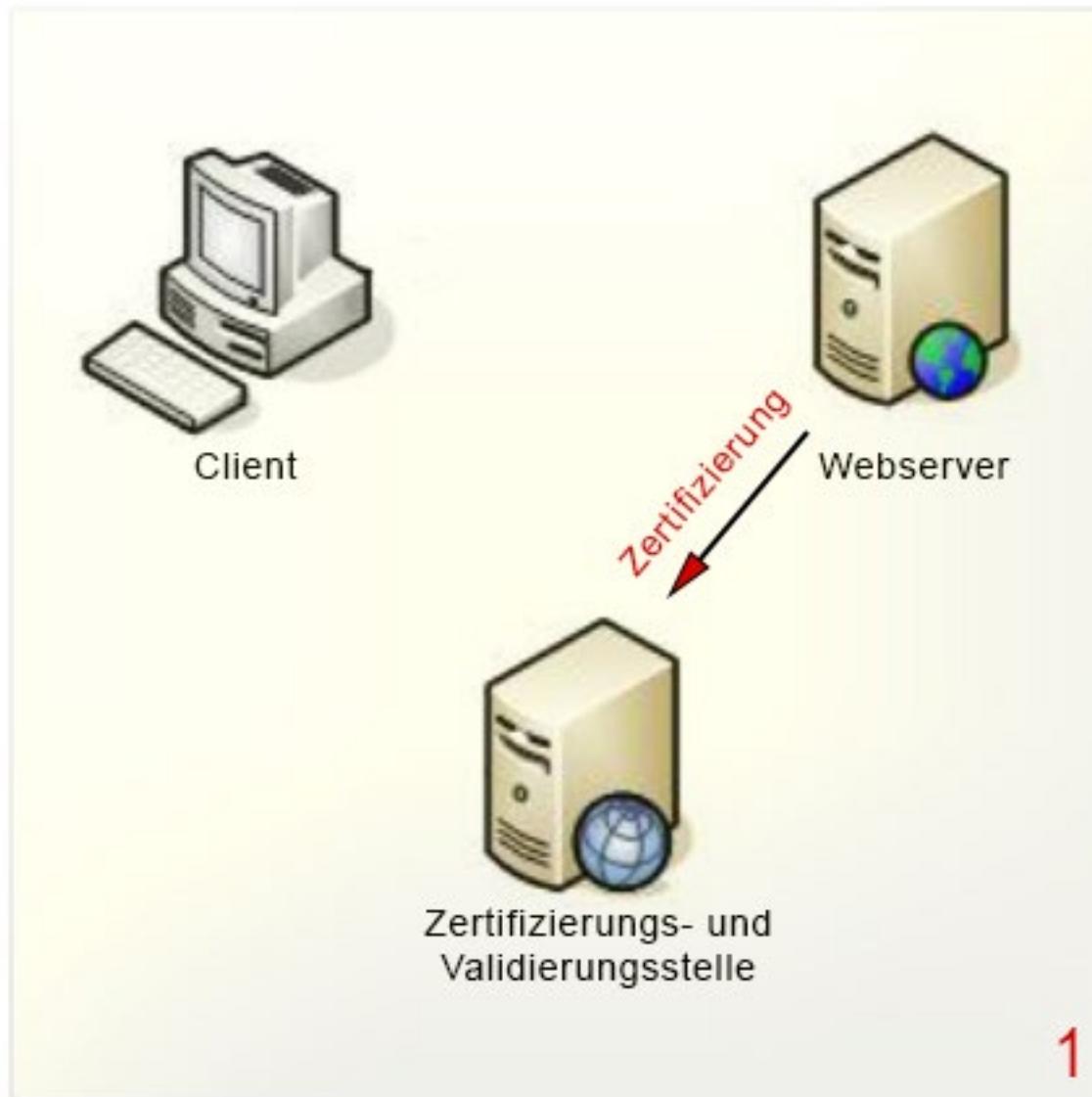
- **Letsencrypt**: Kostenlos, Domain validiertes Zertifikat <https://letsencrypt.org/de/>
- **CaCert**: Nichtkommerziell, kostenfreie X.509-Zertifikate <http://www.cacert.org/>
- **Verisign**: Kommerziell, USA <https://www.verisign.com/>
- **Globalsign**: Kommerziell, Japan <https://www.globalsign.com/en>
- **DigiCert/Quovadisglobal**: Kommerziell, Schweiz <https://www.quovadisglobal.com/ch/>
- **Swisssign**: Kommerziell, Schweiz <https://www.swisssign.com/>

OSI-Layer TCP/IP-Stack

Kopplung

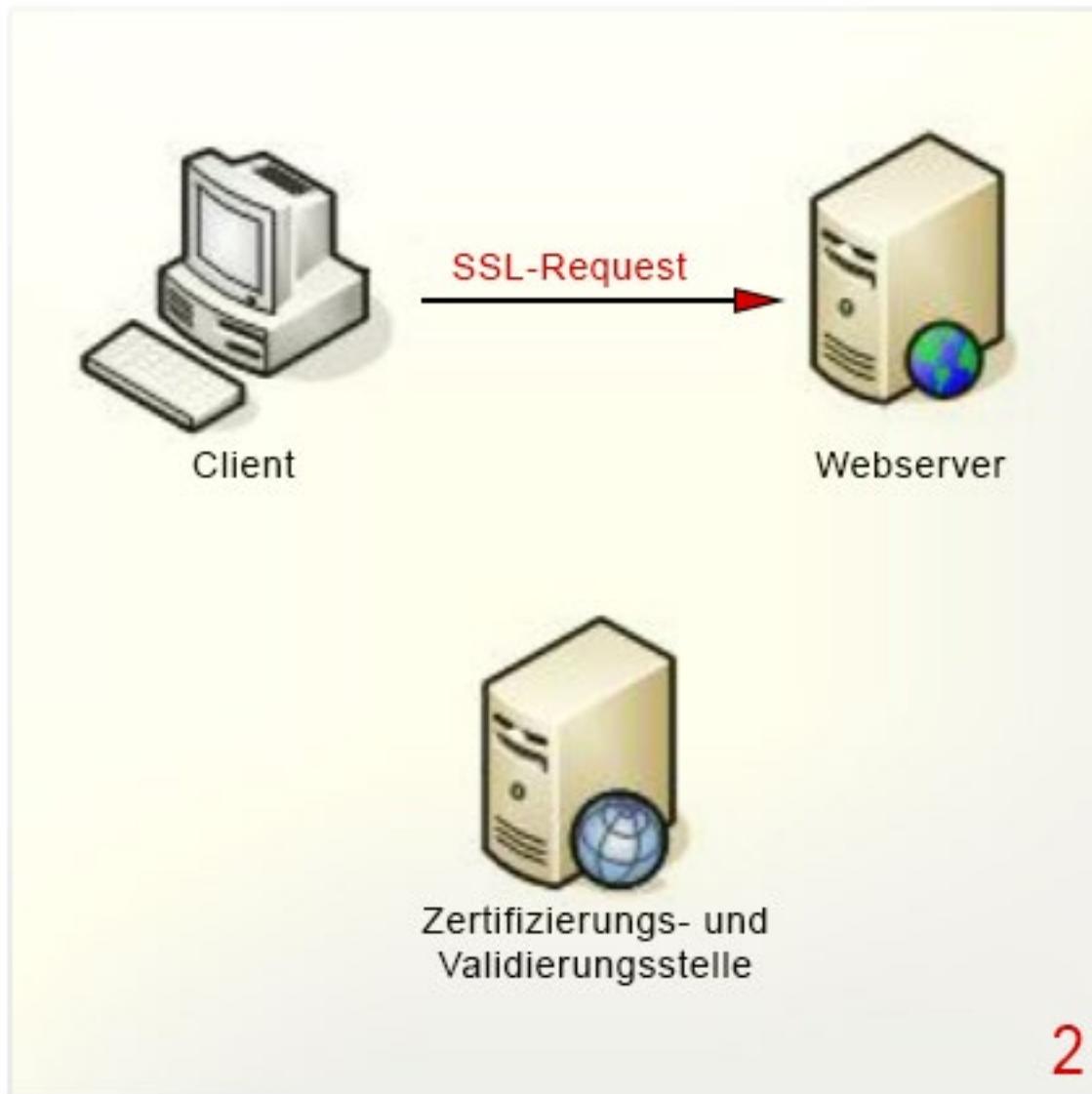


SSL-Handshake mit Schlüsselaustausch



Webserver lässt sich von einer Zertifizierungsstelle ein Zertifikat ausstellen

SSL-Handshake mit Schlüsselaustausch



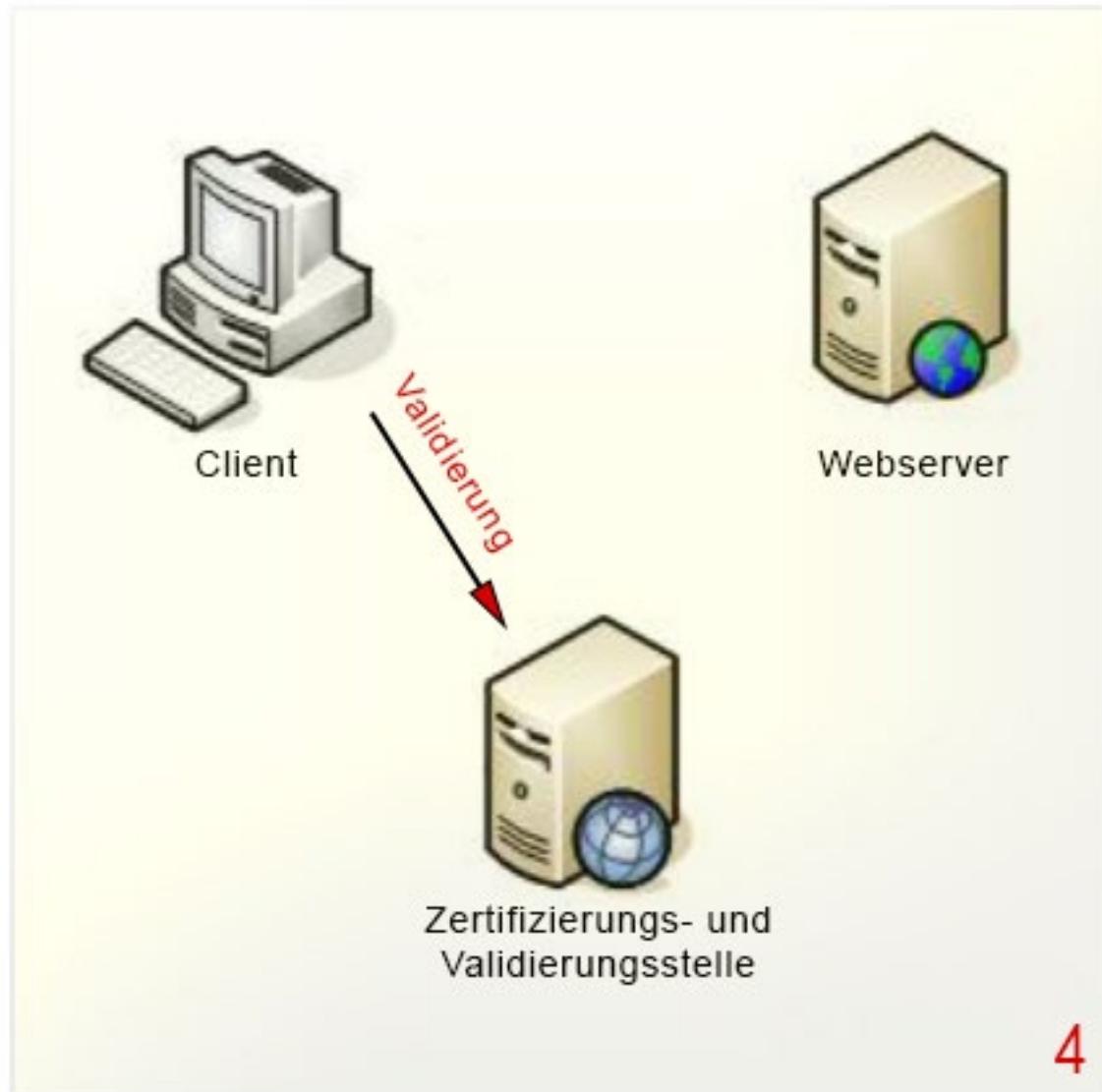
Webbrowser möchte eine HTTPS-Webseite aufrufen und verlangt das Zertifikat des Webservers.

SSL-Handshake mit Schlüsselaustausch



Webbrowser erhält vom Webserver das Zertifikat.

SSL-Handshake mit Schlüsselaustausch



Webbrowser lässt sich das erhaltene Zertifikat bei der Zertifizierungsstelle auf seine Gültigkeit überprüfen.

Untersuchen wir nun ein paar Webseiten:

- <http://www.example.com>
- <https://www.zkb.ch>
- <https://www.tbz.ch>

Was sagt der Browser zum Zertifikat?
Was zeigt uns Wireshark?



Wireshark ist hier erhältlich:
<https://www.wireshark.org/>

Achtung: Wireshark ist ein Sniffer-Tool.
Für die Verwendung am Arbeitsplatz bitte zuerst
bei ihrem Boss um Erlaubnis bitten.

Wireshark-Displayfilter:

`ssl.handshake.extensions_server_name` Zeigt alle Client Hello HTTPS
`tcp.port eq 80 && http` Zeigt alle HTTP-Anfragen auf Port 80



Fragen?

PGP

Pretty Good Privacy

Phil Zimmermann, 1991

Hybrides Verfahren (Asym/Sym) IDEA, RSA

Web-of-Trust (keine zentrale Zertifizierungsstelle)

Nachricht signieren, verschlüsseln oder signieren und verschlüsseln

Kommerziell

OpenPGP

OpenPGP-Standard ab 1998

OpenSource

GnuPG

Implementierung vom OpenPGP-Standard

GNU-GPL

GPG4WIN

Implementierung vom OpenPGP-Standard

Persönliche OpenPGP-Schlüsselpaare (Dezentral, Web-of-Trust)

X.509-Schlüsselpaare (Zentrale Zertifizierungsinstanz)

OpenPGP-Schlüssel und X.509-Schlüssel nicht untereinander kompatibel!

Öffentlicher OpenPGP-Schlüssel FelixMusterPublic.asc:

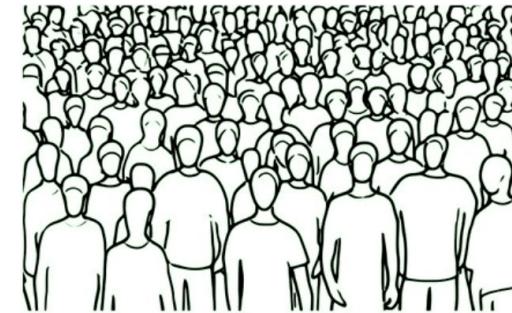
-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: GnuPG v2

mHjzBFYjc.

...

-----END PGP PUBLIC KEY BLOCK-----



Privater OpenPGP-Schlüssel FelixMusterSecret.asc :

-----BEGIN PGP PRIVATE KEY BLOCK-----

Version: : GnuPG v2

Wqdsf

...

-----END PGP PRIVATE KEY BLOCK-----



- **Verschlüsseln**
- **Signieren**
- **Verschlüsseln und Signieren**



gpg4win / Kleopatra
Zertifikatsmanagerin

Bitte die gpg4win-Aufgaben im Skript jetzt bearbeiten...

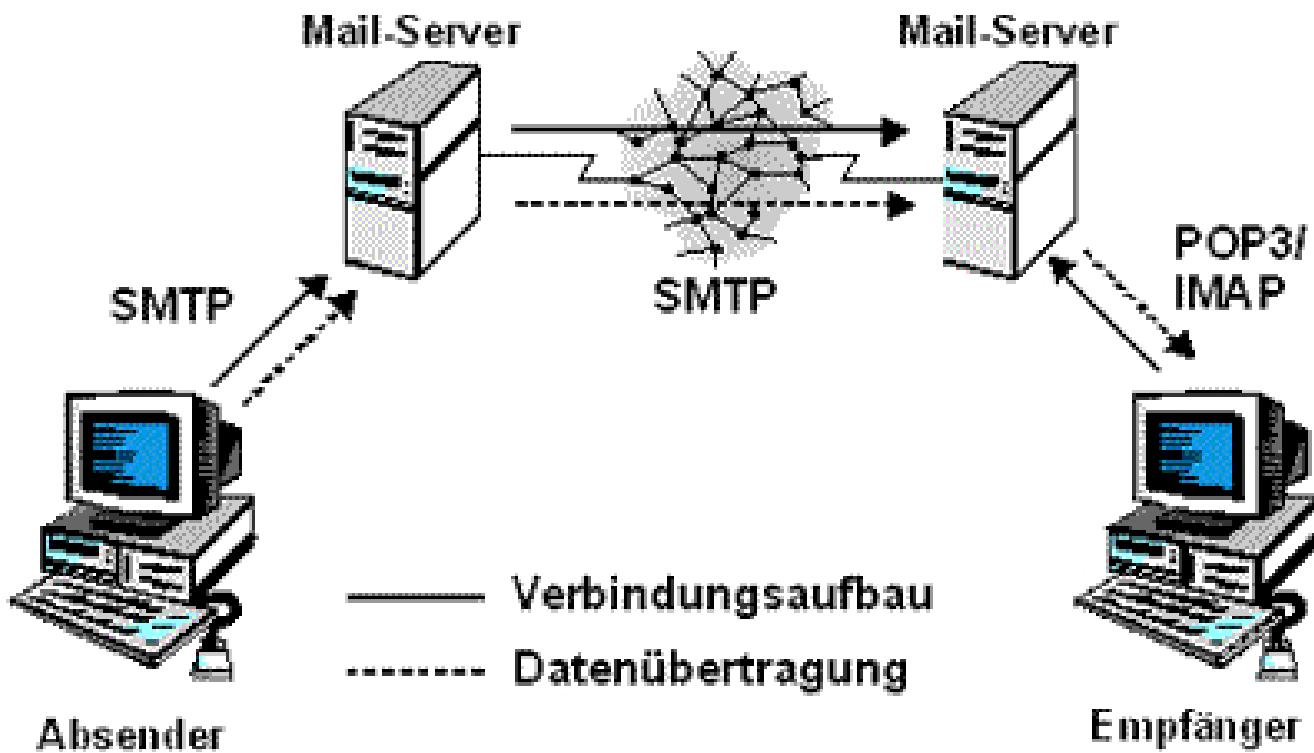


Fragen?



mit





Zugangsdaten:

- Username/Passwort
- SMTP-Ausgangsserver
- SMTP-Port-Nr.
- POP3-Eingangsserver
- POP3-Port-Nr.

Oder:

- IMAP-Eingangsserver
- IMAP-Port-Nr.

Hinweis zur Thunderbird-Aufgabe:

Erst wenn der unverschlüsselte eMail-Verkehr einwandfrei funktioniert,
soll mit dem verschlüsselten eMail-Austausch begonnen werden!

Angaben für den TBZ-Email-Account vorname.name@edu.tbz.ch

	Posteingang POP ^{1.)}	Posteingang IMAP ^{2.)}	Postausgang SMTP ^{3.)}
Servername	outlook.office365.com	outlook.office365.com	smtp.office365.com
Portnummer	995	993	587
Verschlüsselung	TLS	TLS	STARTTLS

Stand: 2024

- 1.) Die E-Mail-Nachrichten werden nach dem Abrufen auf dem E-Mail-Server gelöscht.
- 2.) Die E-Mail-Nachrichten werden zwischen E-Mail-Client und E-Mail-Server synchronisiert.
- 3.) Die E-Mail-Nachrichten werden über dieses Protokoll versendet.

Einrichtbeispiel für Outlook

Authentifizierungsmethode: OAuth2

	Server-Adresse	Port	Verschlüsselung	Authentifizierung	Benutzername
Posteingang IMAP	outlook.office365.com	993	TLS	Passwort, Normal	E-Mail-Adresse
Postausgang SMTP	smtp.office365.com	587	STARTSSL	Passwort, Normal	E-Mail-Adresse



Fragen?