WERNER WINKELMANN

KRYPTOLOGIE 2

Basierend auf

- https://www.inf-schule.de/
- http://ip-klaeden.selfhost.eu/netz/iuk99/kap8/kap8.htm
- https://www.wikipedia.org/
- https://oinf.ch/kurs/informationsgesellschaft/verschluesselung/
- Diverse Videos

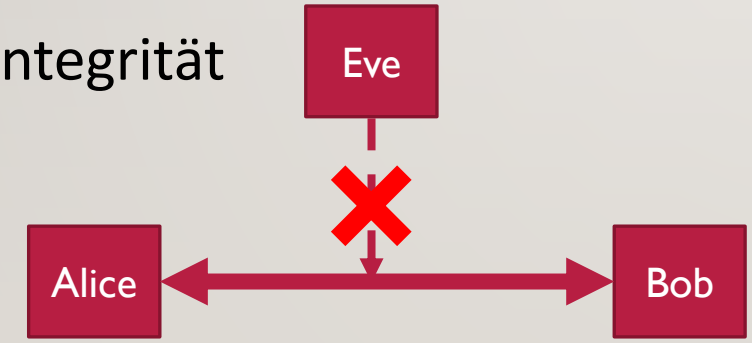
REPETITION

- Kryptologie
  - Kryptographie
  - Kryptoanalyse
  - Steganographie

Welche Ziele verfolgt die Kryptographie?

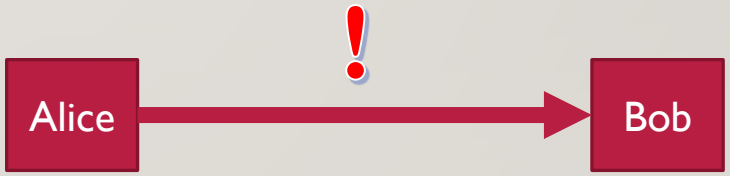
1. Vertraulichkeit

2. Integrität



3. Authentizität

4. Verbindlichkeit

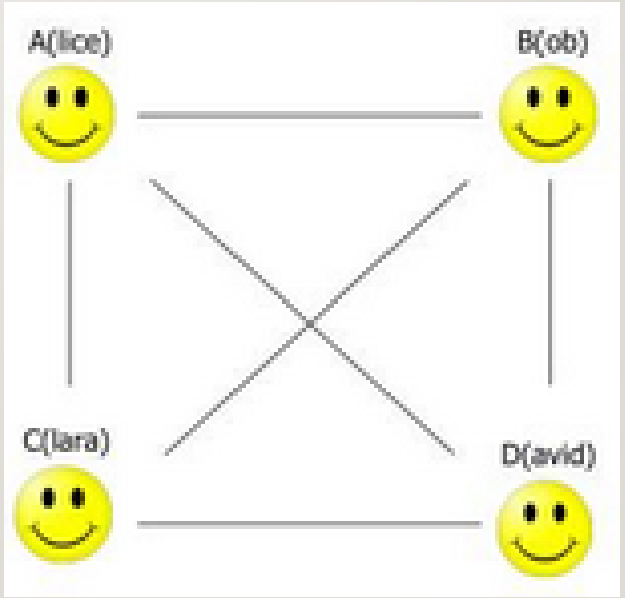


SYMMETRISCHE VERSCHLÜSSELUNG

1. Transposition: Skytale
2. Substitution
   - Monoalphabetisch: Cäsar
   - Polyalphabetisch: Vigenère, One-Time-Pad

PROBLEME VON SYMMETRISCHEN VERSCHLÜSSELUNGEN

- Schlüsselaustausch
- Schlüsselverwaltung

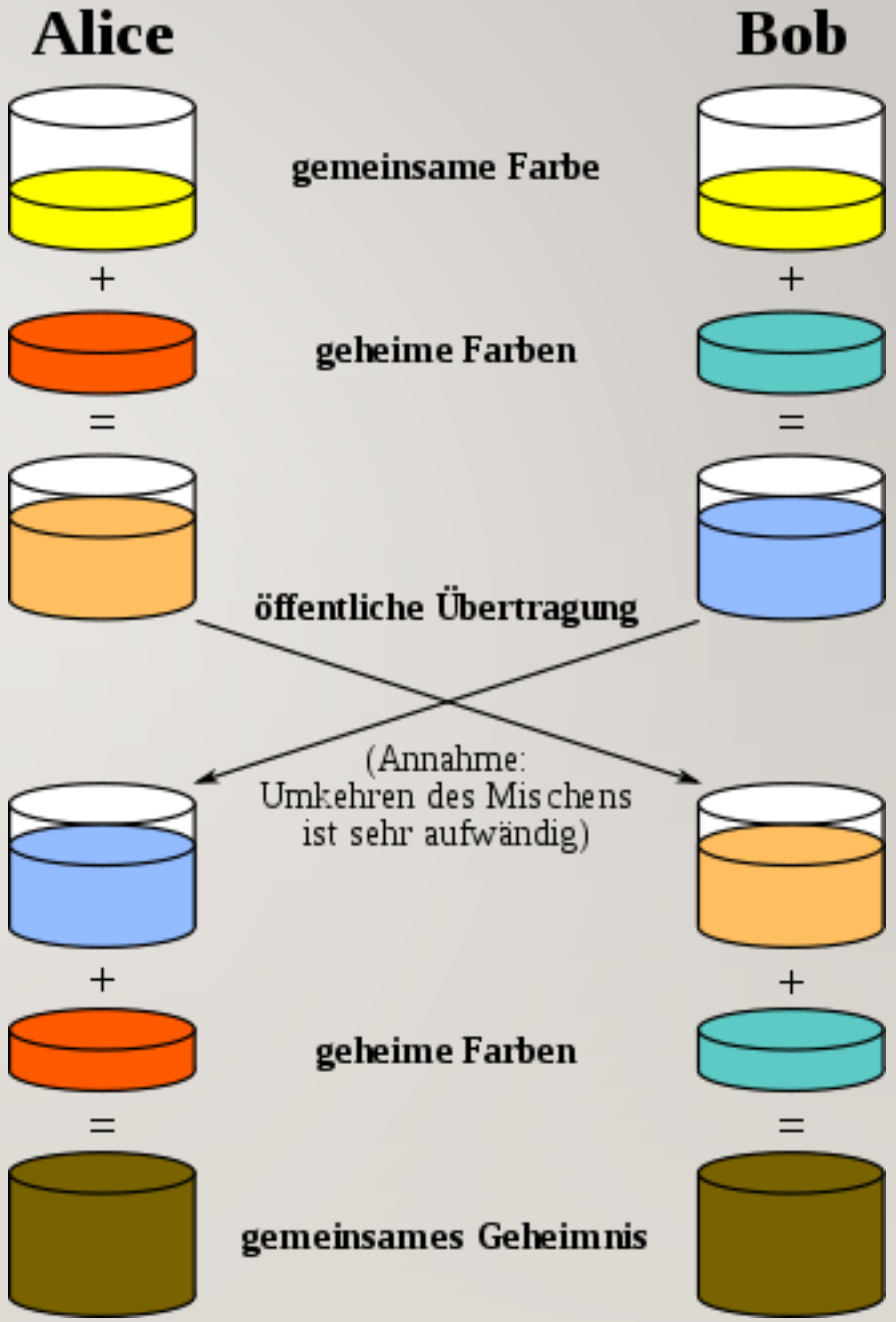


EINSTIEG

- Diffie-Hellman-Merkle
- Kerckhoff

DIFFIE-HELLMAN-MERKLE

- Schlüsselaustausch über einen nicht sicherem Kanal



D-H-M mit Zahlen

Gemeinsame Zahlen (Öffentlicher Schlüssel)	
p (Primzahl):	13
g (< p):	2
Alice x (zufällig)	5
Bob y (zufällig):	8
Berechnete öffentliche Werte:	
Alice	$a = g^x \bmod p = 2^5 \bmod 13 = 6$
Bob	$b = g^y \bmod p = 2^8 \bmod 13 = 9$
Berechnete Schlüsselwerte:	
Alice	schlüssel = $b^x \bmod p = 9^5 \bmod 13 =$ **3**
Bob	schlüssel = $a^y \bmod p = 6^8 \bmod 13 =$ **3**

Was ist ein sicheres Kryptosystem?

„In einem guten Kryptosystem muss nur der Schlüssel geheim bleiben.“

Kerckhoff (1883):

"Ein Kryptosystem ist sicher, wenn man trotz Veröffentlichung der Funktionsweise des Kryptosystems ohne die Kenntnis des verwendeten Schlüssels aus empfangenen Geheimtexten die ursprünglichen Klartexte nicht ableiten kann.“

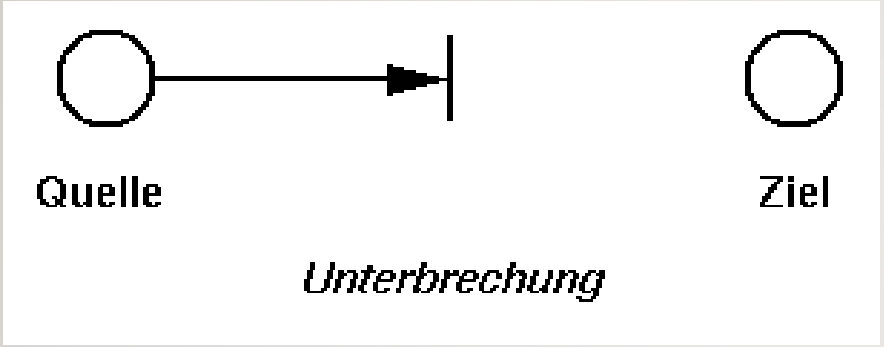
⇒ **Je weniger Geheimnisse ein Kryptosystem braucht, desto robuster ist es!**

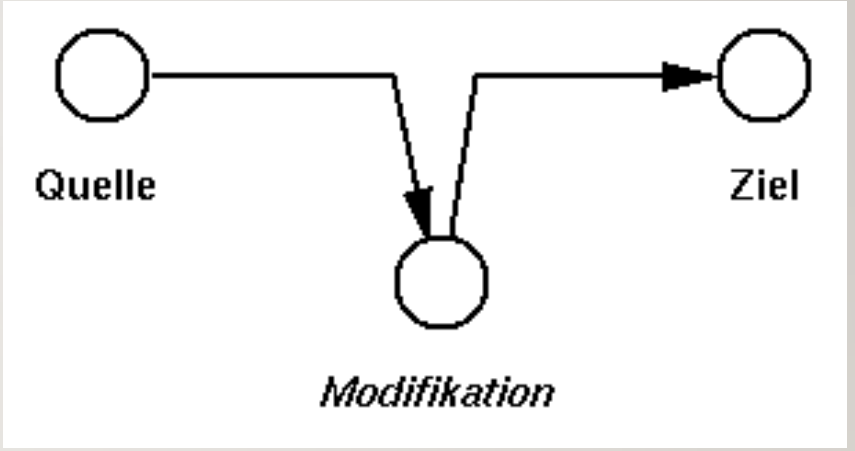
Lernkontrolle

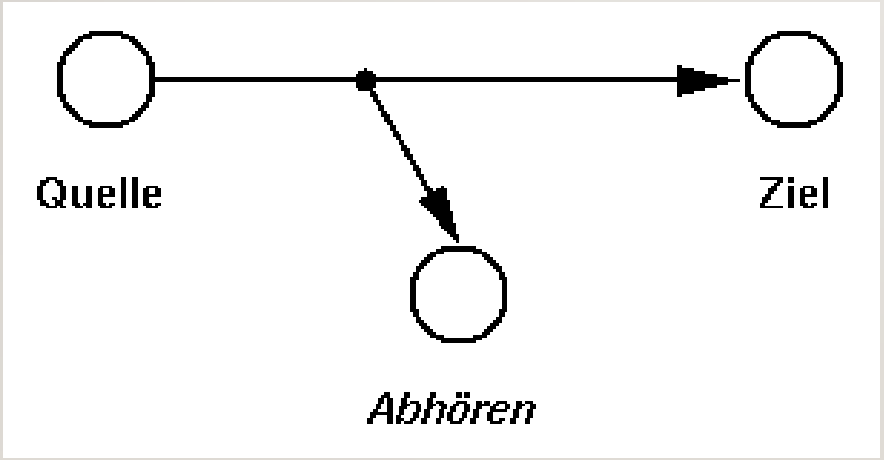
- https://learningapps.org/display?v=pdg5wrpz320

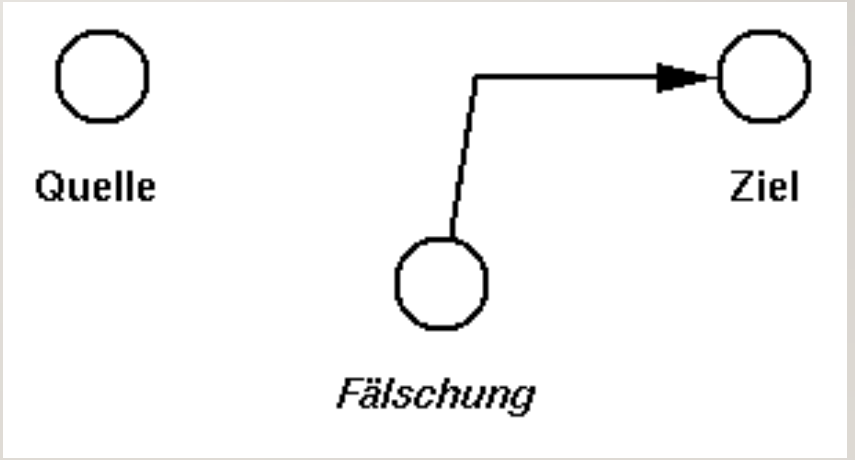
KRYPTOANALYSE

Krypto-Attacken









Kryptoanalytische Attacken

- Nur-Geheimtexte Attacke
- Known-plaintext Attacke
- Chosen-plaintext Attacke

Kryptoanalytische Strategien

- Vollständige Suche
- Wörterbuch Suche
- Statistische Methode
- Strukturanalyse bzw. reduzierte Suche

HYBRIDE SYSTEME & MESSAGE AUTHENTICATION CODES (MAC)

STÄRKEN UND SCHWÄCHEN DER CHIFFRIERSYSTEME

SYMMETRISCHE

- Schlüsselaustausch-Problem
- Schüsselinflation
- Effizienter

ASYMMETRISCHE

- Kein Schlüsselaustausch
- Keine Schüsselinflation
- Aufwendiger

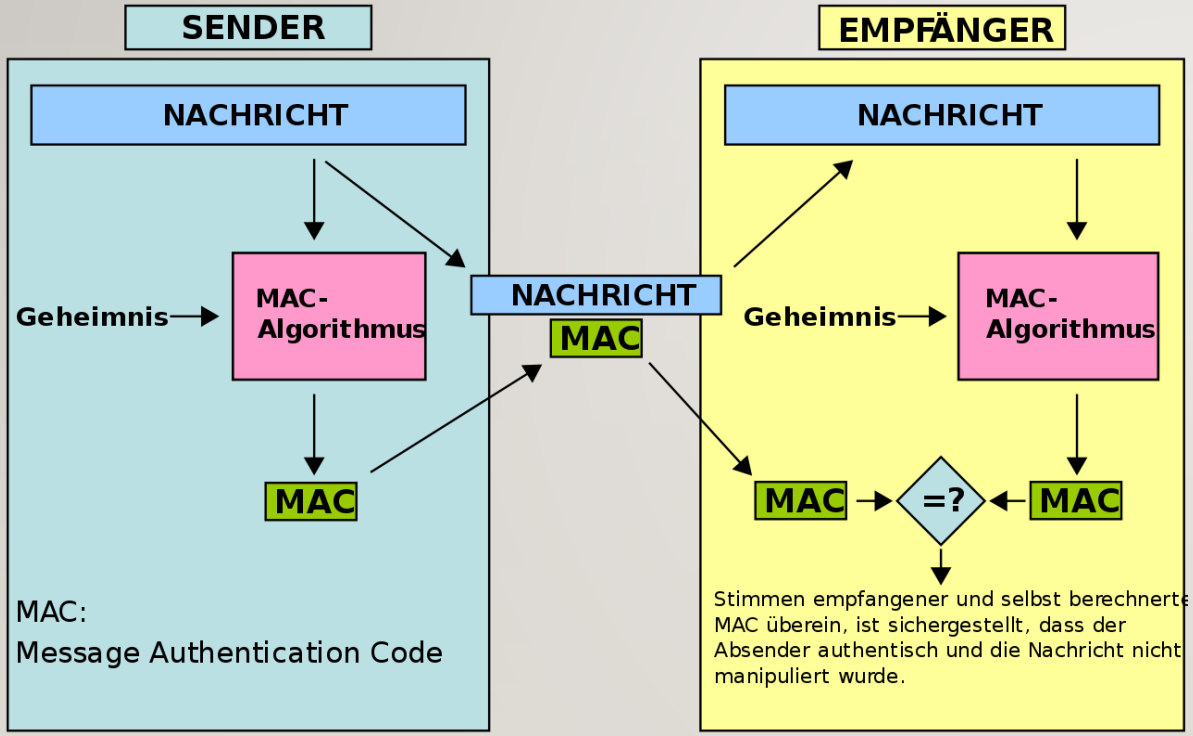
➢ **Hybride System**

Schlüssel der 3 Kryptographie-Verfahren

1. Einweg-Hashfunktionen **ohne** Schlüssel.
2. Symmetrische Verfahren **ein geheimer** Schlüssel
3. Asymmetrischen Verfahren **ein öffentlicher** und **ein privater** Schlüssel

MESSAGE AUTHENTICATION CODE (MAC)

schlüsselabhängige Einweg-Hashfunktion:



- verschlüsselte Prüfsummen
- Authentizität & Integrität

Welche Ziele verfolgt die Kryptographie?

Vertraulichkeit

Zugriffsschutz: Nur dazu berechtigte Personen sollen in der Lage sein, die Daten oder die Nachricht zu lesen oder Informationen über ihren Inhalt zu erlangen.

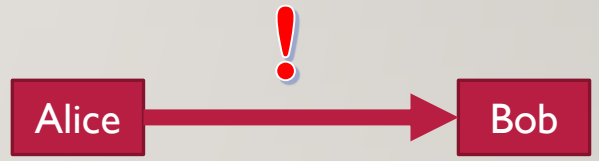
Authentizität

Fälschungsschutz: Der Urheber der Daten oder der Absender der Nachricht soll eindeutig identifizierbar sein, und seine Urheberschaft sollte nachprüfbar sein.

Integrität

Änderungsschutz: Die Daten müssen nachweislich vollständig und unverändert sein.

Verbindlichkeit



Nicht-abstreitbarkeit: Der Urheber der Daten oder Absender einer Nachricht soll nicht in der Lage sein, seine Urheberschaft zu bestreiten, d. h., sie sollte sich gegenüber Dritten nachweisen lassen.

DIGITALE SIGNATUREN

Welche Ziele verfolgt die Kryptographie?

Vertraulichkeit

Zugriffsschutz: Nur dazu berechtigte Personen sollen in der Lage sein, die Daten oder die Nachricht zu lesen oder Informationen über ihren Inhalt zu erlangen.

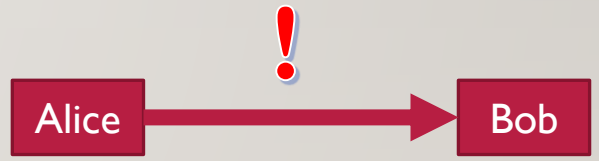
Authentizität

Fälschungsschutz: Der Urheber der Daten oder der Absender der Nachricht soll eindeutig identifizierbar sein, und seine Urheberschaft sollte nachprüfbar sein.

Integrität

Änderungsschutz: Die Daten müssen nachweislich vollständig und unverändert sein.

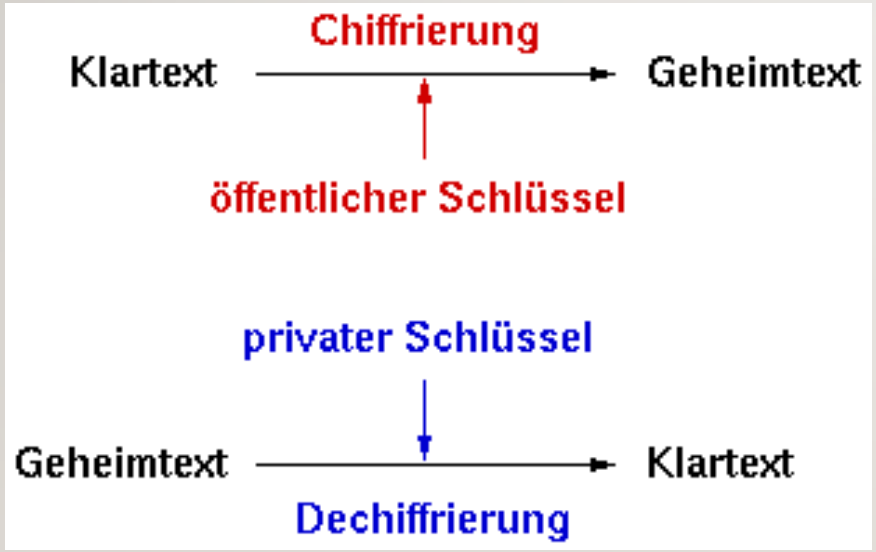
Verbindlichkeit



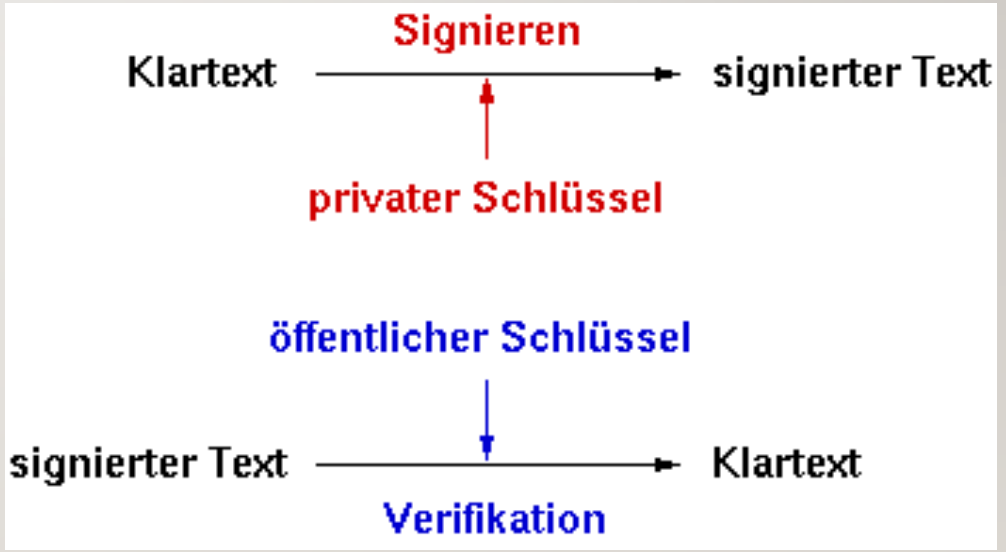
Nicht-abstreitbarkeit: Der Urheber der Daten oder Absender einer Nachricht soll nicht in der Lage sein, seine Urheberschaft zu bestreiten, d. h., sie sollte sich gegenüber Dritten nachweisen lassen.

PUBLIC-KEY KRYPTOGRAPHIE

ASYMMETRISCHE VERSCHLÜSSELUNG



DIGITALE SIGNATUR



Man-in-the-middle-Angriff

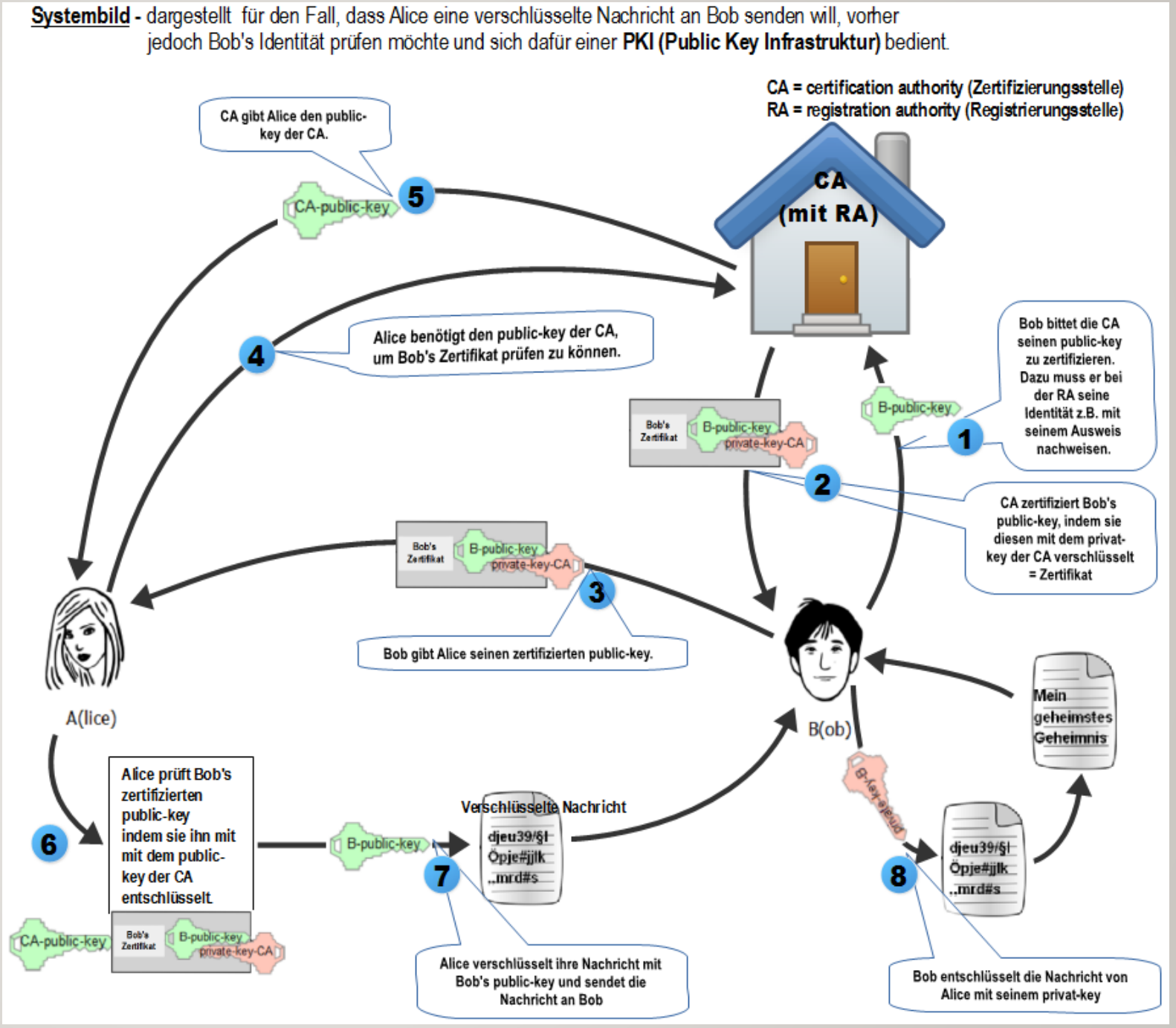
Analoge Zertifikate

DIGITALE SIGNATUREN & ZERTIFIKATE

Public-key infrastructure

Web of trust

Public-key infrastructure



Probleme mit Zertifikaten bzw. public-key-infrastructure

- Es kostet Zeit und Geld, ein Zertifikat von einer (weitgehend) anerkannten Zertifizierungsstelle zu bekommen.
- Die Überprüfung der Vertrauenswürdigkeit des Antragsstellers durch die Zertifizierungsstelle ist (notwendigerweise) lückenhaft.
- Auch Zertifizierungsstellen wurden schon gehackt.
- Auch korrekt zertifizierte Webseiten können gehackt sein.
- Zertifikate haben eine begrenzte Gültigkeitsdauer – evtl. vergisst ein vertrauenswürdiger Anbieter das Zertifikat zu erneuern.
- Browser unterscheiden sich darin, welche Root-Zertifikate sie akzeptieren und wie schnell sie auf bekannt gewordene Zertifikat-Hacks reagieren.
- Die wenigsten Benutzer wissen genug von Zertifikaten, um mit einer allfälligen Browserwarnung angemessen umgehen zu können.

Web of trust

```
uid Sebastian Nerz <snerz@bvpk.org>
sig  sig3  449D222E 2008-11-28 __________ __________ [selfsig]
sig  sig3  022CE281 2009-08-30 __________ __________ Matthias Binninger <mail@matthias-binninger.de>
sig  sig3  62A25E4E 2009-08-30 __________ __________ Benedikt Delker <BenediktDelker@web.de>
sig  sig3  FE1DD1DF 2009-08-30 __________ __________ Alexander Scheurer <mail@aspepex.net>
sig  sig   D58CB000 2009-08-30 __________ __________ david <david.maendlen@web.de>
sig  sig3  2C8C1429 2009-09-02 __________ __________ Axel Wagner <mail@merovius.de>
sig  sig   5FF25B4D 2010-04-19 __________ __________ branleb <branleb@gmail.com>
sig  sig2  14FE16C1 2010-06-01 __________ __________ Andreas Bittner <abittner@nobit.info>
sig  sig2  33742D65 2010-06-01 __________ __________ Andreas Bittner <abittner@nobit.info>
sig  sig2  0191D5ED 2010-12-27 __________ __________ Oliver Schrader <oliver.schrader@ymail.com>
```

Pretty Good Privacy (PGP)

Praxis

- https://
- GnuPG

ABSCHLUSS

Welche Ziele verfolgt die Kryptographie?

Vertraulichkeit

Zugriffsschutz: Nur dazu berechtigte Personen sollen in der Lage sein, die Daten oder die Nachricht zu lesen oder Informationen über ihren Inhalt zu erlangen.

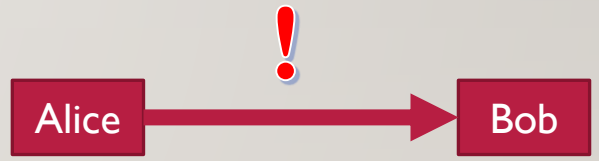
Authentizität

Fälschungsschutz: Der Urheber der Daten oder der Absender der Nachricht soll eindeutig identifizierbar sein, und seine Urheberschaft sollte nachprüfbar sein.

Integrität

Änderungsschutz: Die Daten müssen nachweislich vollständig und unverändert sein.

Verbindlichkeit



Nicht-abstreitbarkeit: Der Urheber der Daten oder Absender einer Nachricht soll nicht in der Lage sein, seine Urheberschaft zu bestreiten, d. h., sie sollte sich gegenüber Dritten nachweisen lassen.

Kryptographische Ziele und Verfahren (vereinfacht)

	Hash	MAC	Digitale Signatur
Integrität	Ja	Ja	Ja
Authentizität	-	Ja	Ja
Verbindlichkeit	-	-	Ja
Verschlüsselung	**Keine**	**Symmetrisch**	**Asymmetrisch**