# Datensicherheit

## Vorlesung 4: 15.12.2025

### *Wintersemester 2025/2026 h_da*

***Heiko Weber, Lehrbeauftragter***

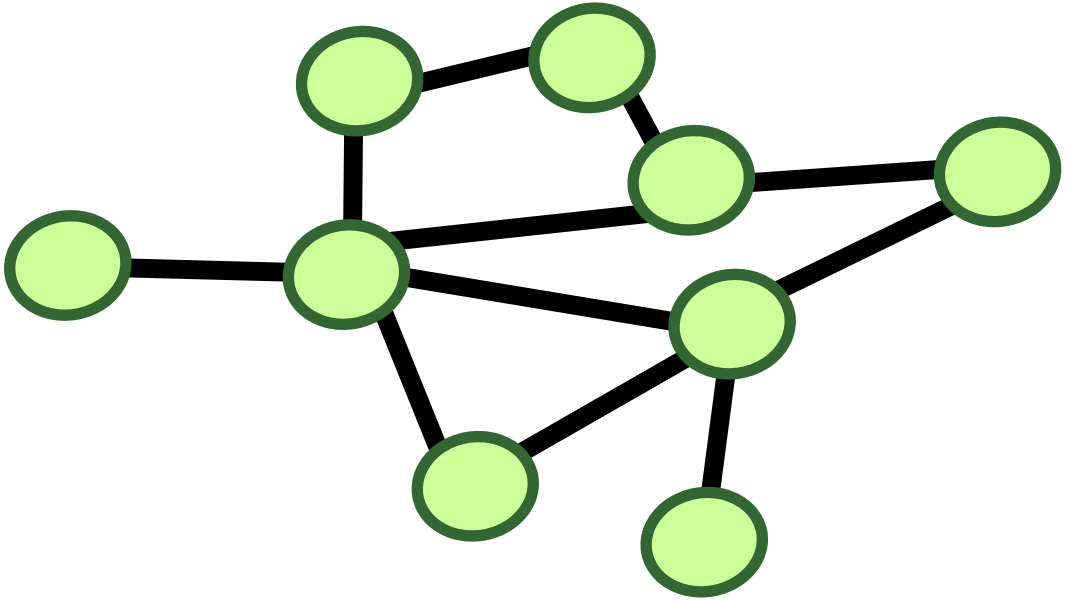
# Teil 2: Datensicherheit
# Themenübersicht der Vorlesung

1. Einführung / Grundlagen / Authentifizierung & Autorisierung
2. Kryptografie / Verschlüsselung & Signaturen / Vertrauen / Blockchain
3. Softwaresicherheit / Schadsoftware
4. **Netzwerksicherheit / TLS / PGP & S/MIME / Firewalls & Netzwerksegmentierung**
5. Hacking / Phishing / Einführung in den Datenschutz / Anonymität / Darknet
6. Datenschutzgesetze / Technische & Organisatorische Maßnahmen
7. Organisationssicherheit / Managementsysteme / Zusammenfassung

# Wiederholung aus IT- und Medientechnik

- Wie funktionieren Netzwerke?
  - Netzwerktoplogien, Knoten, Hops, ...
- Wie funktioniert das Internet?
  - teilvermaschtes Netzwerk mit Backbone und vielen Knoten
  - Kommunikationsprotokoll hauptsächlich TCP/IP

# Internet = Teilvermaschtes Netzwerk



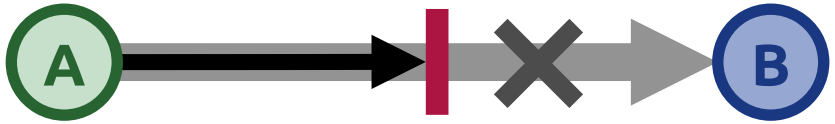
# Gängige Angriffstypen auf die Netzwerkkommunikation

- Denial of Service (DoS)
- Sniffing
- Man in the Middle (MitM)
- Spoofing
- Replay

# Denial of Service (DoS)

- Unterbrechung der Netzwerkverbindung
- Schutzziel **Verfügbarkeit** verletzt

- Knoten A kann mit Knoten B nicht mehr kommunizieren

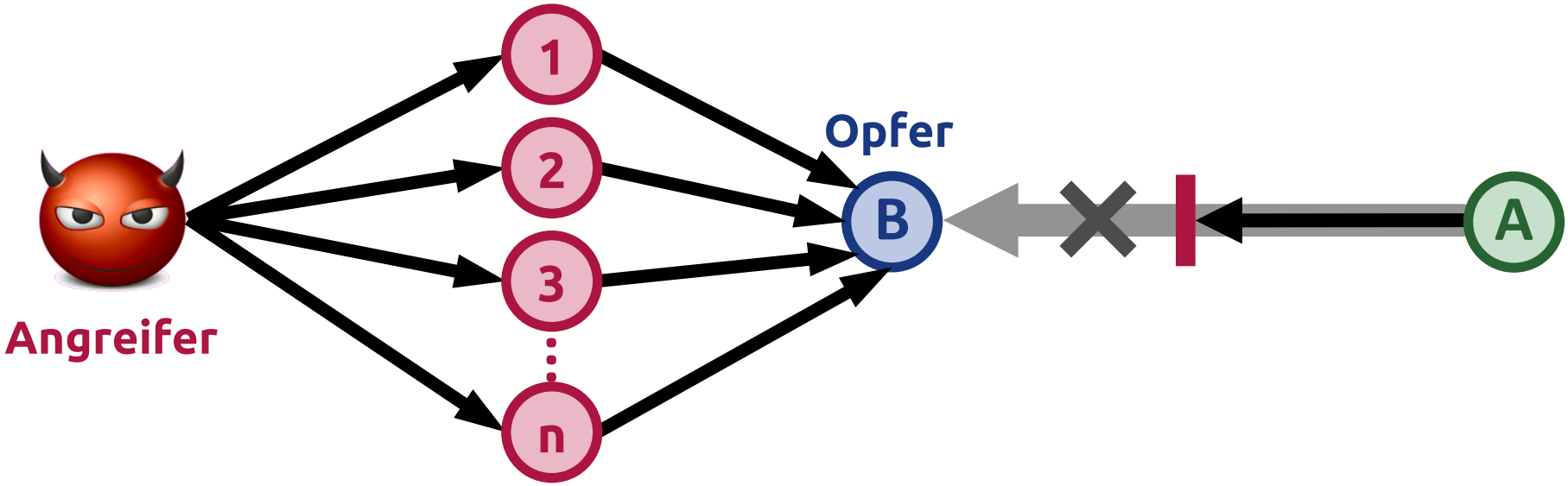


# Denial of Service (DoS)

- meistens findet keine physische Unterbrechung der Netzwerkverbindung statt, sondern eher wird durch einen Angriff eine Software- oder Hardwarekomponente dazu gebracht, dass sie nicht mehr normal Daten verarbeiten kann
- ein häufiges Angriffsmuster (Attack Pattern) ist die Überflutung einer Netzwerkkomponente mit so vielen Anfragen, dass sie nicht mehr mit den Antworten nach kommt

# Distributed Denial of Service (DDoS)

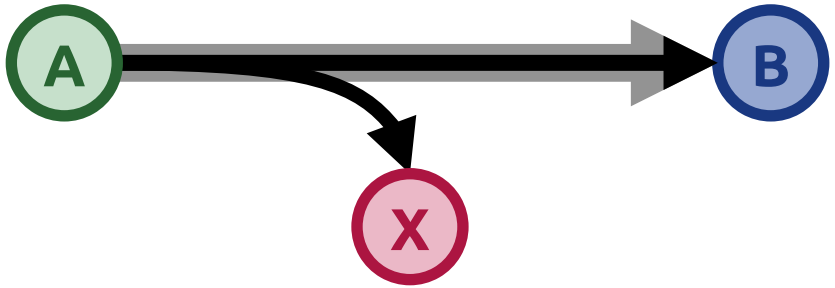
- ein Angreifer verteilt seinen Angriffs-Code auf viele verschiedene Knoten im Internet und diese schicken alle gleichzeitig Anfragen an das Opfer des Angriffs
- oft sind die Knoten, die am Angriff beteiligt sind, selber Opfer eines vorangegangen Angriffs und beteiligen sich unbewusst an dem Angriff



# Sniffing

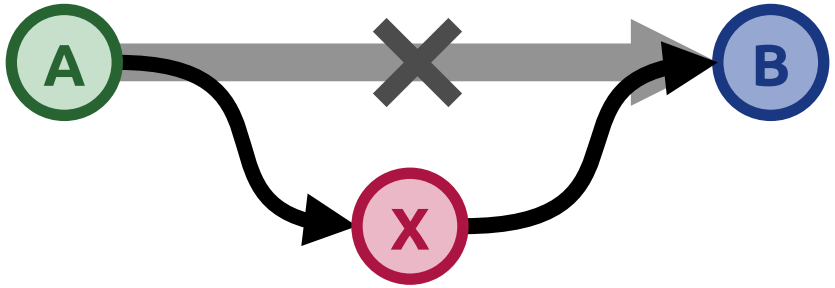
- Abhören
- Schutzziel **Vertraulichkeit** verletzt

- Daten die von Knoten A zu Knoten B gesendet werden, hört der Angreifer X mit



# Man in the Middle (MitM)

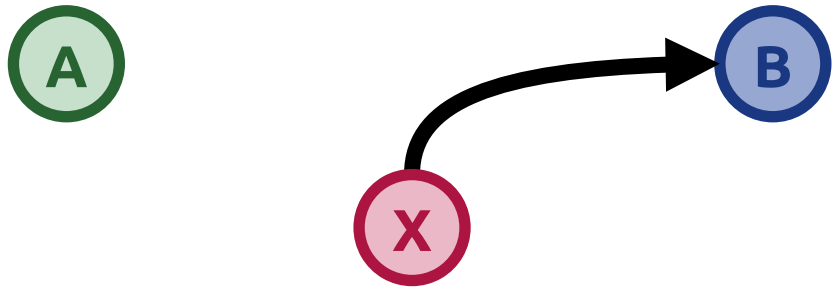
- Abfangen und Modifizieren
- Daten die von Knoten A zu Knoten B gesendet werden, fängt der Angreifer X ab, verändert sie und schickt sie an den Knoten B weiter (meistens so, dass Knoten B denkt, dass die Daten von Knoten A kommen)
- Schutzziel **Integrität** verletzt – zusätzlich Vertraulichkeit und Authentizität verletzt



# Spoofing

- Erzeugen
- Schutzziel **Authentizität** verletzt

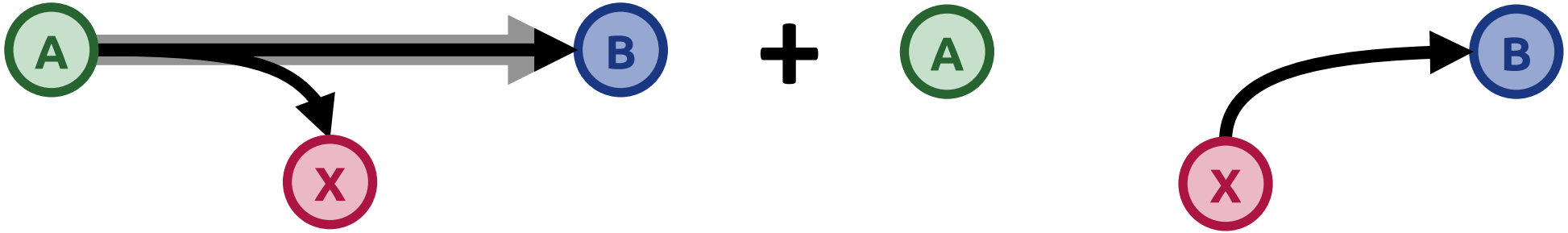
- Angreifer X schickt Daten an Knoten B und täuscht vor, dass die Daten von Knoten A kommen würden



# Replay

- Abhören und erneut senden
- Schutzziel **Authentizität** verletzt

- Daten die von Knoten A zu Knoten B gesendet werden, hört der Angreifer X mit und sendet sie zu einem späteren Zeitpunkt erneut



# Sicherheit auf verschiedenen Ebenen der Netzwerkprotokolle

- **IPsec** (Internet Protocol Security)
  - Verschlüsselung und Authentisierung auf Paket-Ebene
- **TLS** (Transport Layer Security) und **SSH** (Secure Shell)
  - Verschlüsselung und Authentisierung auf Verbindungs-Ebene
- **SFTP, FTPS, HTTPS, ...**
  - Verschlüsselung und Authentisierung auf Anwendungs-Ebene
  - basiert meiste auf TLS, SSH oder vergleichbaren Protokollen
- **PGP, S/MIME, ...**
  - Verschlüsselung und Authentisierung eingebettet in unsichere Protokolle

# Gängige Angriffstypen auf die Netzwerkkommunikation

- Denial of Service (DoS)
- Sniffing
- Man in the Middle (MitM)
- Spoofing
- Replay

**können mit TLS oder SSH verhindert werden!**

**Vertraulichkeit** sicherstellten durch **Verschlüsselung**

**Integrität** und **Authentizität** sicherstellten durch **Signaturen**

# Transport Layer Security (TLS)

- TLS ist ein Netzwerkverschlüsselungsprotokoll, welches die Basis für einen Großteil der verschlüsselten Datenkommunikation im Internet ist – z. B. für HTTPS und SSH
- Vorgänger war SSL (Secure Socket Layer), welches heute auch noch teilweise im Einsatz ist

# TLS-Funktionalität

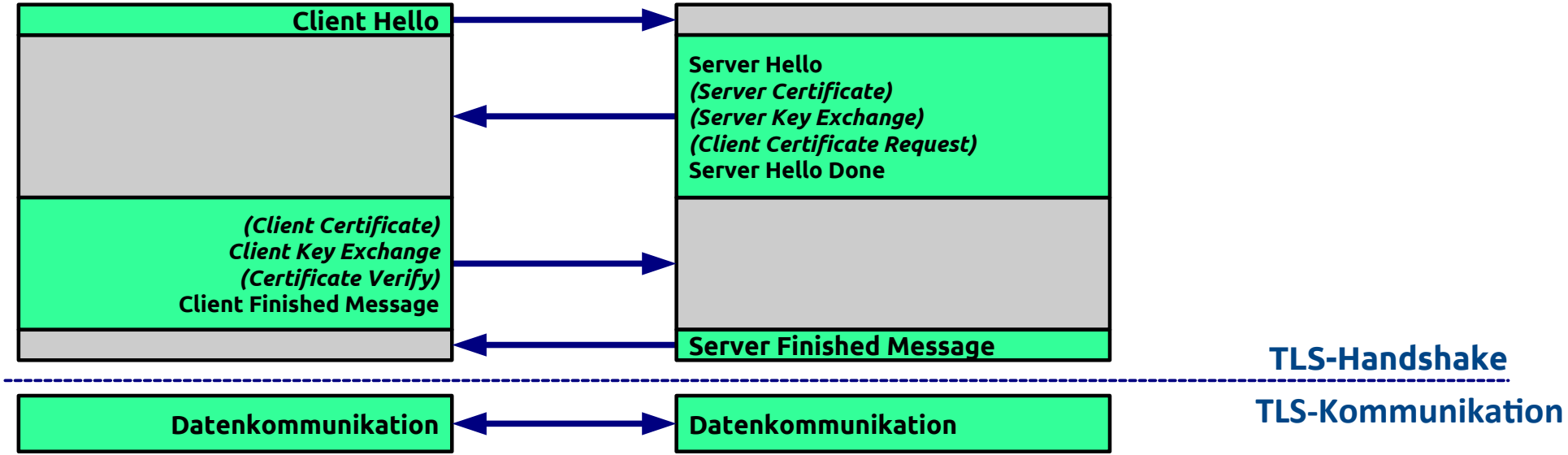
- **Authentifizierung**
  - asymmetrische Verschlüsselung > Zertifikate
  - 4 Varianten:
    - keine Authentifizierung
    - nur Server
    - nur Client
    - Server und Client
- **Verschlüsselung**
  - symmetrische Verschlüsselung

- nur wenn Authentifizierung UND Verschlüsselung eingesetzt werden, besteht ein Schutz gegen die gängigen Angriffe auf die Netzwerkkommunikation

# Transport Layer Security (TLS)

## 2 Phasen der Kommunikation

1. TLS-Handshake zum Aufbau der Kommunikation, Festlegen des Verschlüsselungsalgorithmus und Austausch des Schlüssels – optional auch Authentifizierung der Gegenseite(n)
2. TLS-Kommunikation mit symmetrischer Verschlüsselung



# TLS-Versionen und SSL

- **SSL 1.0** *(1994 – nie offiziell freigegeben)*
- **SSL 2.0** (1995) *– seit März 2011 offiziell verboten!*
- **SSL 3.0** (1996) *– seit Juni 2015 offiziell veraltet!*
  - unterstützt nur RC4 für Verschlüsselung als Non-Block-Cypher
- **TLS 1.0** (1999) *– seit Juni 2018 nicht mehr für Zahlungssysteme erlaubt*
  - wie SSL 3.0, zzgl. AES
- **TLS 1.1** (2006)
  - Schutz gegen Cypher-Block-Chaining-Attacks
- **TLS 1.2** (2008)
  - MD5-SHA1 durch SHA-2 ersetzt, GCM-Modus für AES eingeführt
- **TLS 1.3** (2018)
  - einige neue Algorithmen ergänzt und unsichere Algorithmen entfernt

**gelten aktuell als sicher**

# Gängige Angriffstypen in Webanwendungen

- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)

# Cross-Site Scripting (XSS)

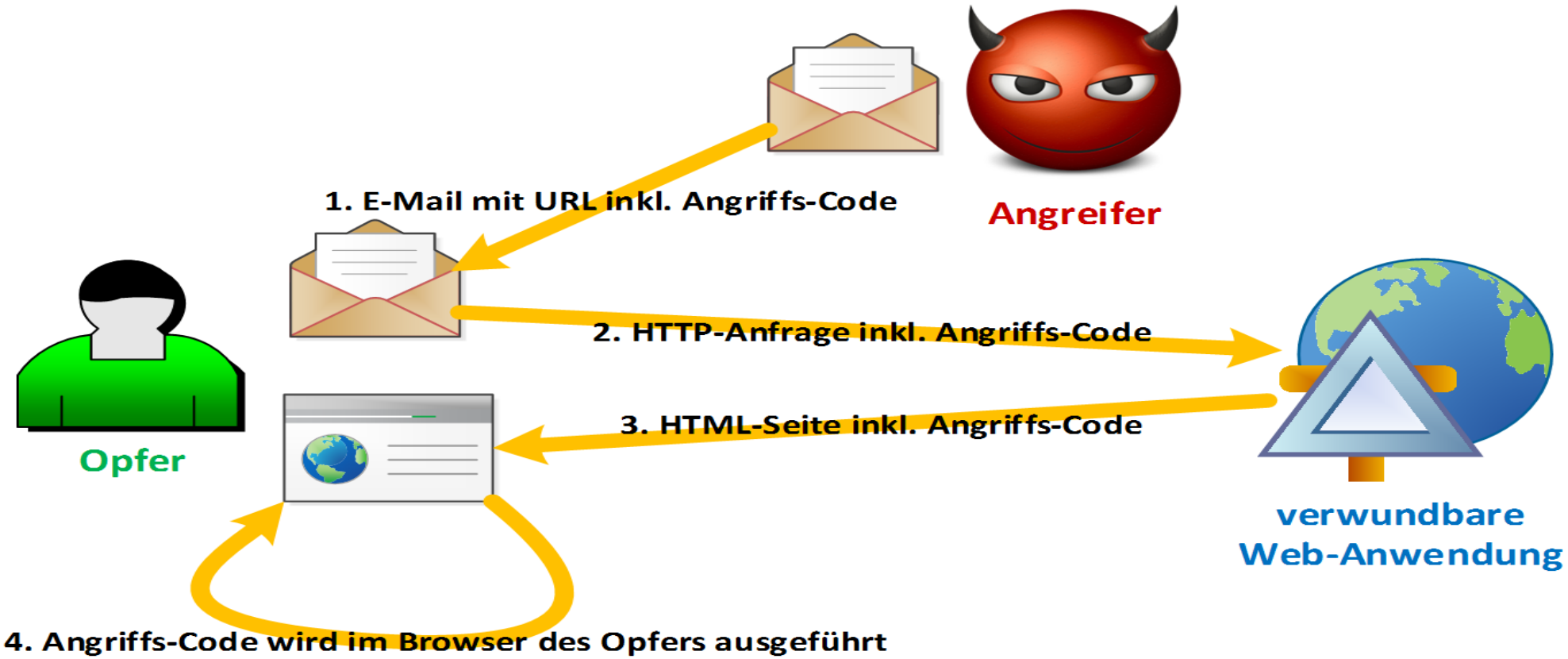
- Eine Web-Anwendung empfängt Daten und gibt diese in einer HTTP-Antwort zurück, ohne dass problematische Zeichen oder Zeichenfolgen ausgefiltert (neutralisiert) werden.
- Dies ermöglicht, dass ein Angreifer speziellen JavaScript-Code in eine Webseite injizieren kann, der dann im Browser eines Opfers ausgeführt wird.

| Mögliche Auswirkungen | Schutzziel verletzt |
|---|---|
| Schutzmechanismen umgehen | Vertraulichkeit |
| unberechtigten Code oder Programme ausführen | Integrität<br>Vertraulichkeit<br>Verfügbarkeit |
| Anwendungsdaten lesen | Vertraulichkeit |

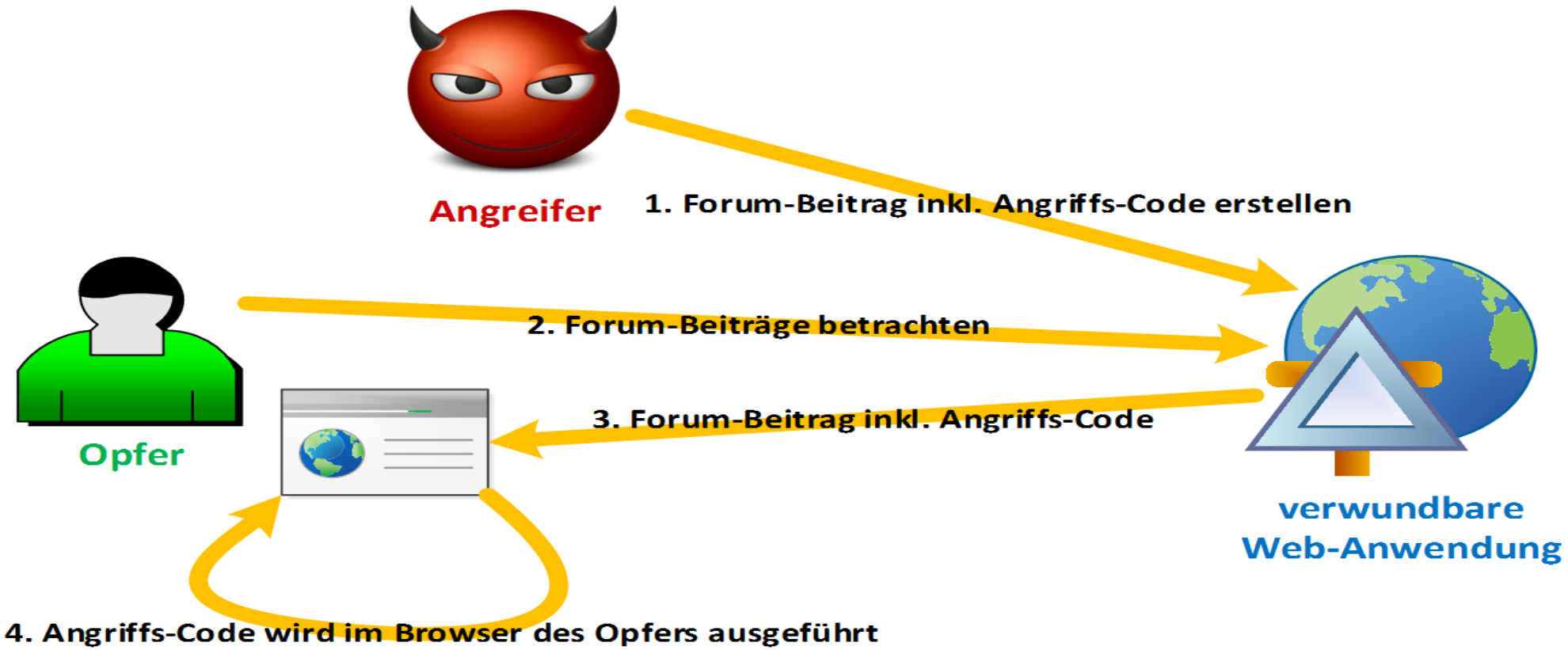
# Typen von Cross-Site Scripting (XSS)

- **Reflected XSS / Non-Persistent XSS**
  - Der verwundbare Web-Server empfängt gefährliche Daten aus der HTTP-Anfrage und schickt diese direkt zurück in der HTTP-Antwort. Die Daten werden an den Absender zurück-reflektiert und werden nicht zwangsweise auf dem Web-Server gespeichert.
- **Stored XSS / Persistent XSS**
  - Der Web-Server speichert gefährliche Daten und gibt diese bei HTTP-Anfragen in der HTTP-Antwort zurück.
- **DOM-based XSS**
  - Der Angreife-Code manipuliert den Inhalt der aufgerufenen Webseite, indem die HTML-Dokument-Struktur über die Manipulationsmöglichkeiten des DOM (Document Object Model).

# Beispiel: Reflected XSS / Non-Persistent XSS



# Beispiel: Stored XSS / Persistent XSS



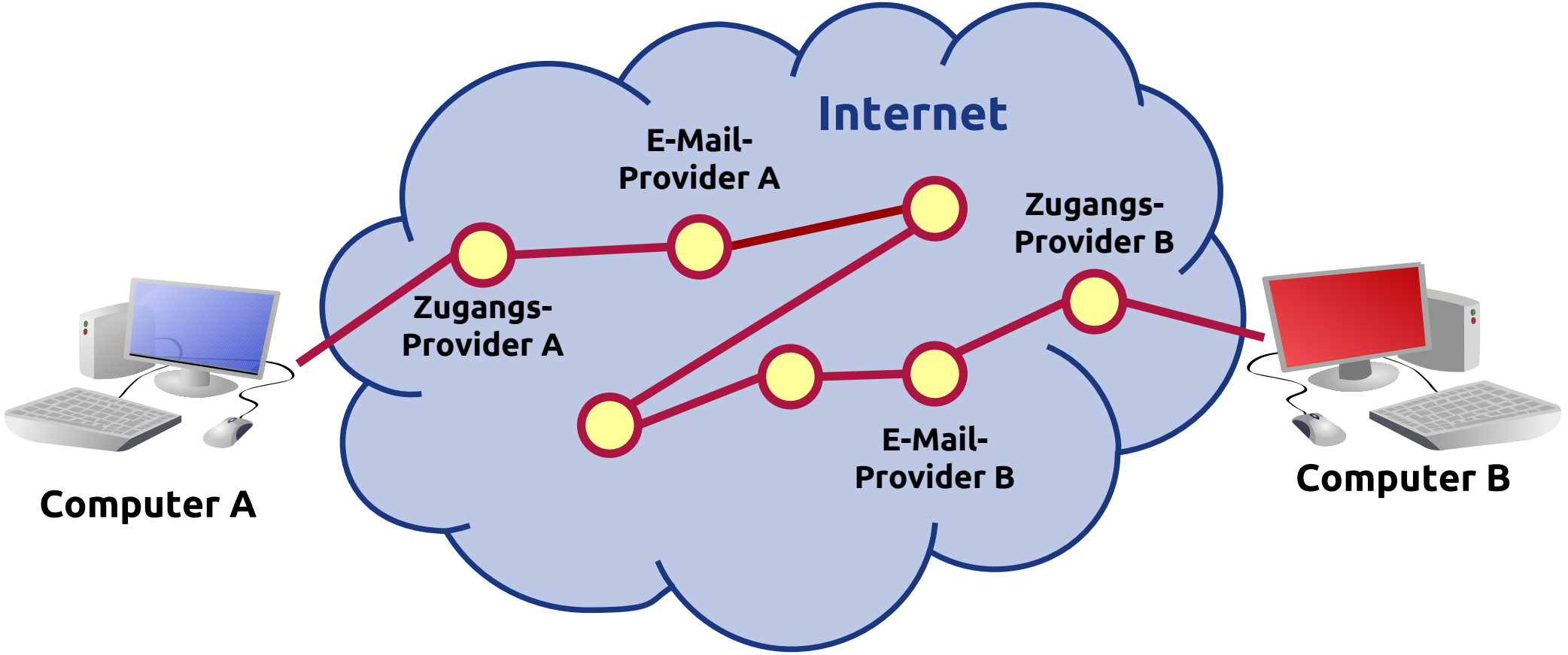
# Cross-Site Request Forgery (CSRF)

- Eine Web-Anwendung überprüft nicht ausreichend, ob eine gültige HTTP-Anfrage auch beabsichtigt von einem Absender geschickt wurde.
- Wenn eine Cross-Site Scripting Attacke ausgeführt wird und im Browser eines Opfers Anfragen generiert werden, sollte eine Web-Anwendung das erkennen und diese Anfrage nicht ausführen.

# Beispiel: XSS+CSRF-Angriffs-Szenario auf Online-Shop

# Beispiel: XSS+CSRF-Angriffs-Szenario auf Online-Shop

# Computer-Kommunikation für E-Mails



# Probleme bei der E-Mail-Kommunikation

- Standard-E-Mails sind einfach nur Text, die von jedem gelesen werden können, die/der die E-Mails in die Hand bekommt
- vom Absendeort zum Empfangsort durchläuft eine E-Mail in der Regel bis zu hundert Knotenpunkte, auf denen jeweils die E-Mails abgefangen werden können
- Sicherheitsbehörden, Nachrichtendienste, Hacker, etc. fangen ganz gezielt E-Mails ab und können diese automatisiert nach speziellen Inhalten durchsuchen
- viele Menschen gehen davon aus, dass E-Mails nicht öffentlich seien

# PGP

- **PGP = Pretty Good Privacy**
- PGP stellt keine neuen Kryptoalgorithmen vor, sondern beschreibt wie existierende Algorithmen genutzt werden können, um Daten im Internet sicher auszutauschen
- **PGP benutzt:**
  - asymmetrische Verschlüsselung
  - symmetrische Verschlüsselung
  - Hash-Funktionen
  - Kompression
- **Schlüsselpaare** (öffentlich+privat) werden genutzt

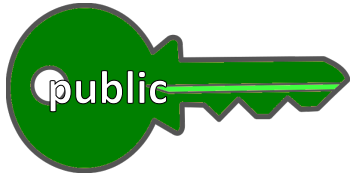
# PGP: Geschichte

- 1991 von Phil Zimmermann entwickelt
- Ziel: Privatsphäre von Bürger/innen schützen
- anfangs durfte PGP nicht außerhalb der USA genutzt werden, weil es wie Waffen unter das Exportgesetz fiel
- Phil Zimmermann wurde kriminalisiert – ihm wurde vorgeworfen, dass er die Sicherheit der USA gefährde
- der Quellcode wurde als Buch veröffentlicht, exportiert und von Freiwilligen abgetippt, um die Exportbestimmungen zu umgehen
- 1998 wurde der OpenPGP-Standard veröffentlicht
  - GnuPG ist eine Open-Source-Implementierung dieses Standards

# PGP-Schlüssel

- **Schlüsselpaar**: genau ein öffentlicher und privater Schlüssel passen zusammen

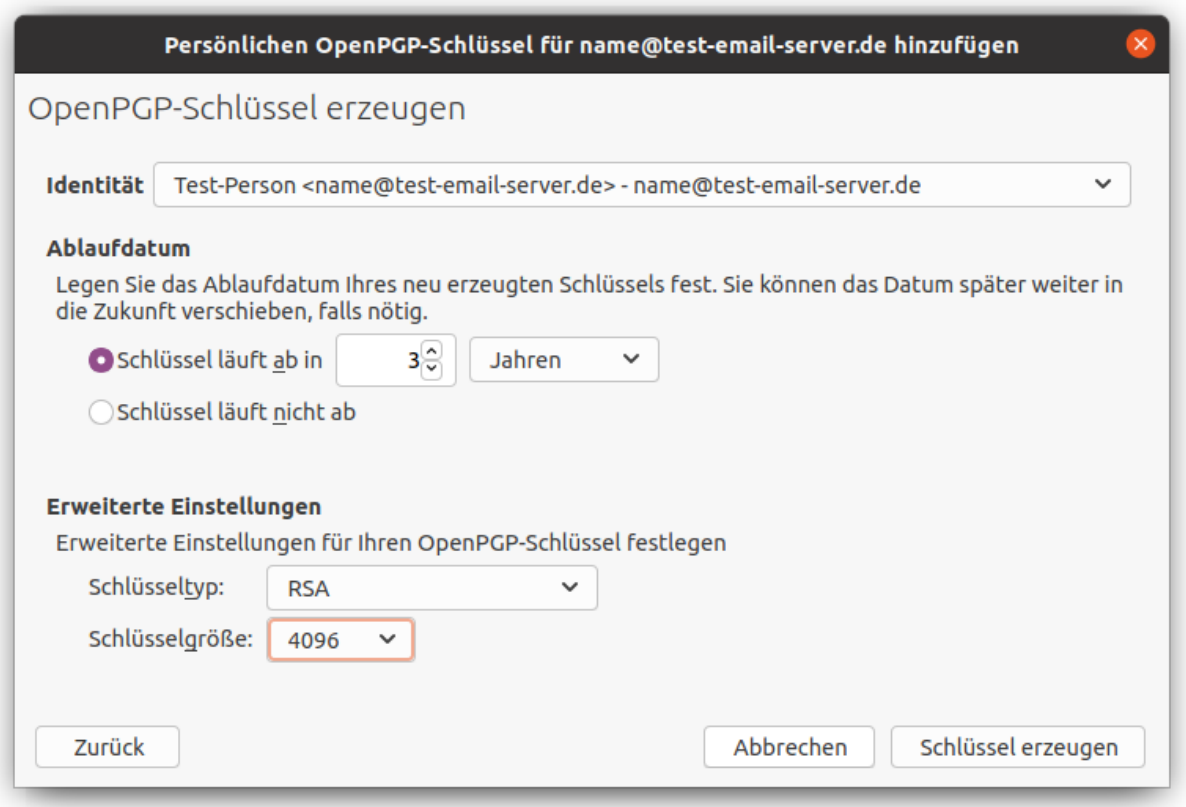
- **Öffentlicher Schlüssel**
  - zum Verschlüsseln
  - zum Überprüfen einer Signatur




- **Privater Schlüssel**
  - zum Entschlüsseln
  - zum Signieren

# PGP-Schlüsselpaar erzeugen

z. B. über die Schlüsselverwaltung im E-Mail-Programm Thunderbird:



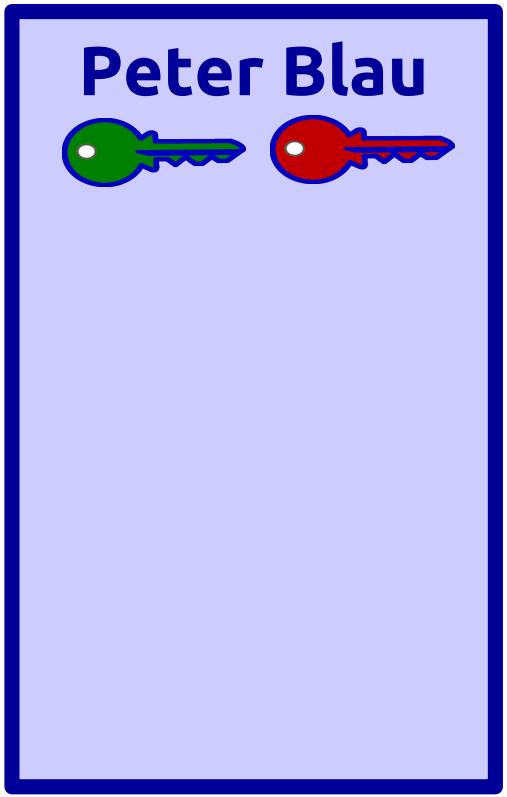
# Schlüsselaustausch

- nur die öffentlichen Schlüssel dürfen ausgetauscht werden
- die privaten Schlüssel müssen gut geschützt bleiben
- der Austausch der öffentlichen Schlüssel kann direkt (z. B. per USB-Stick), per E-Mail oder über einen **Schlüssel-Server** erfolgen
- wenn der Austausch nicht direkt erfolgt, sollte die Echtheit noch per Abgleich des Fingerabdrucks (Schlüssel-ID) per Telefon erfolgen

# Web of Trust

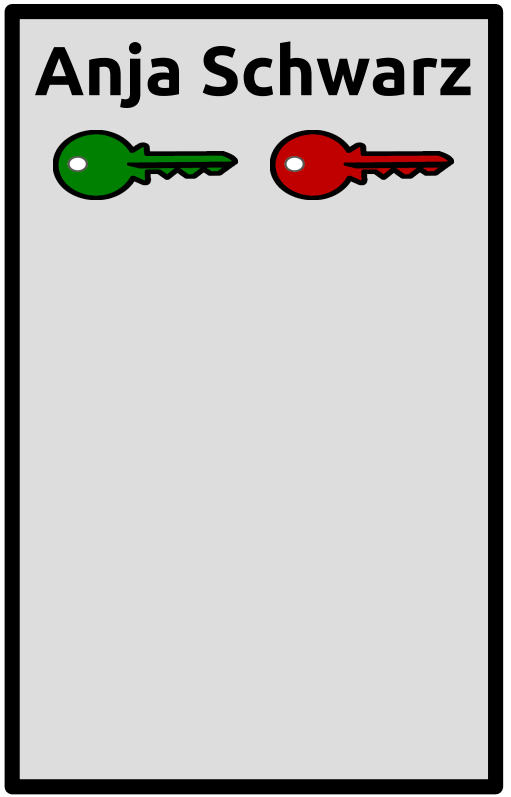
- es gibt keine zentrale Autorität, die alle Schlüssel verwaltet, sondern jede/r Teilnehmer/in entscheidet selbst, wem sie/er vertraut
- **direktes Vertrauen**
  - Schlüssel von Personen, die persönlich überprüft wurden
- **indirektes Vertrauen**
  - Schlüssel von Personen, die von Personen überprüft wurden, die wiederum persönlich überprüft wurden
- dadurch entstehen Vertrauensketten, die je nach Anzahl der Indirektionen weniger vertrauenswürdig werden

# Schlüsselaustausch, Ver- und Entschlüsselung

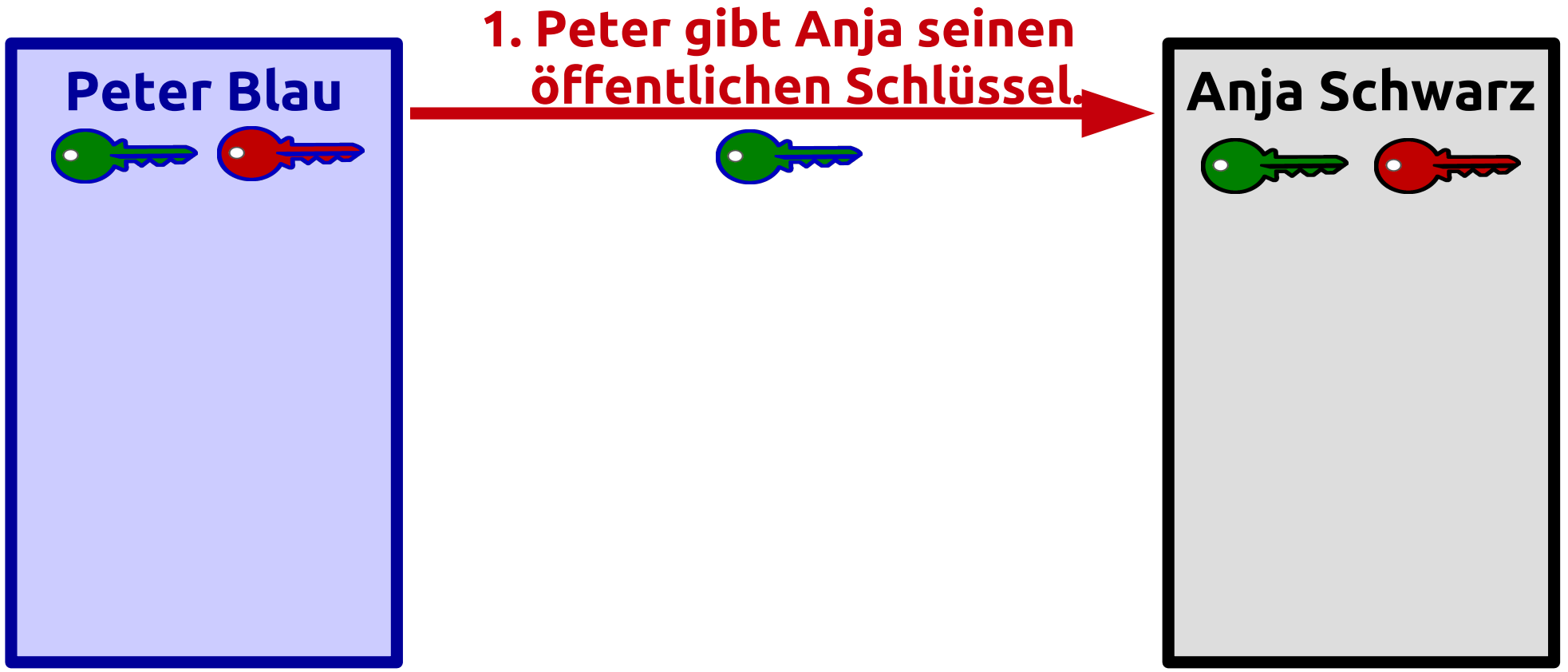



**Peter Blau und Anja Schwarz haben jeweils ein Schlüsselpaar.**

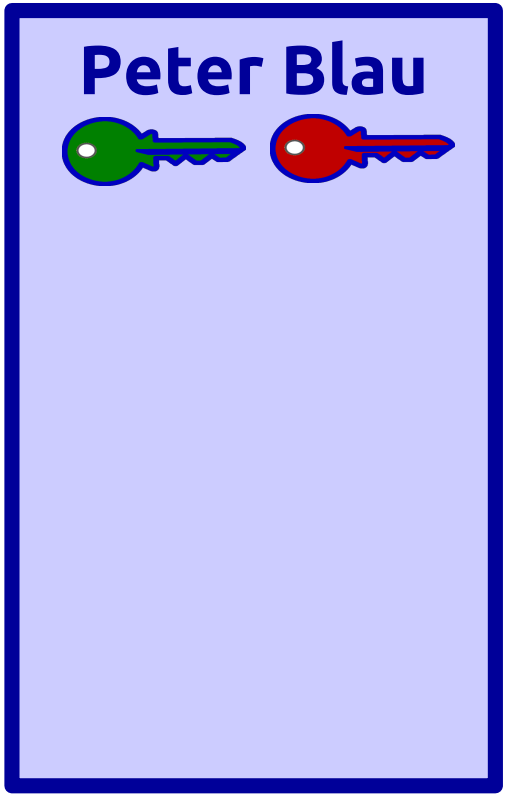
**Anja will eine verschlüsselte E-Mail an Peter schicken.**



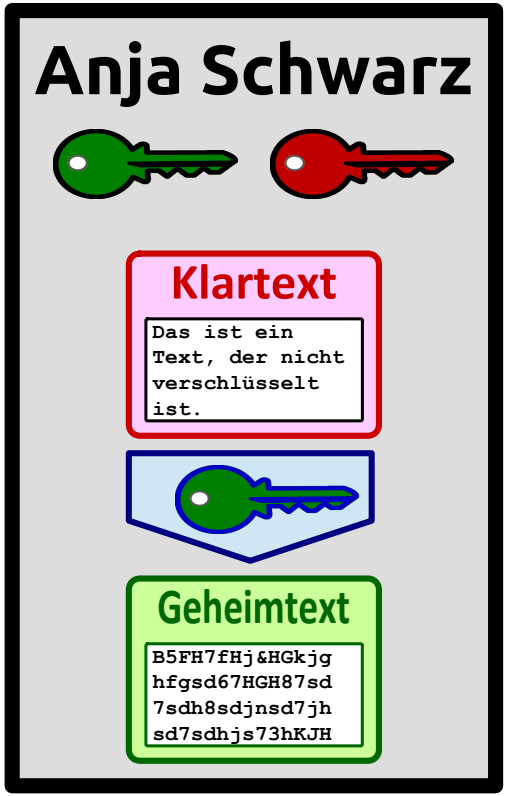
# Schlüsselaustausch, Ver- und Entschlüsselung



# Schlüsselaustausch, Ver- und Entschlüsselung

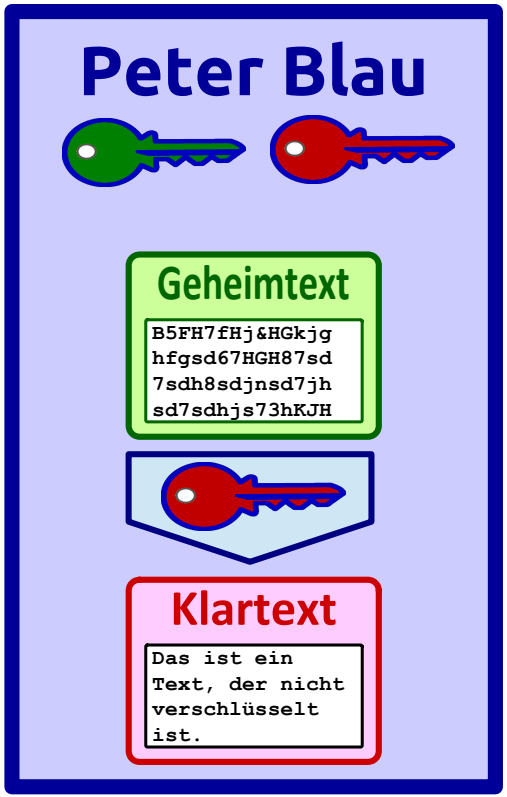



**2. Mit dem öffentlichen Schlüssel von Peter verschlüsselt Anja die E-Mail.**

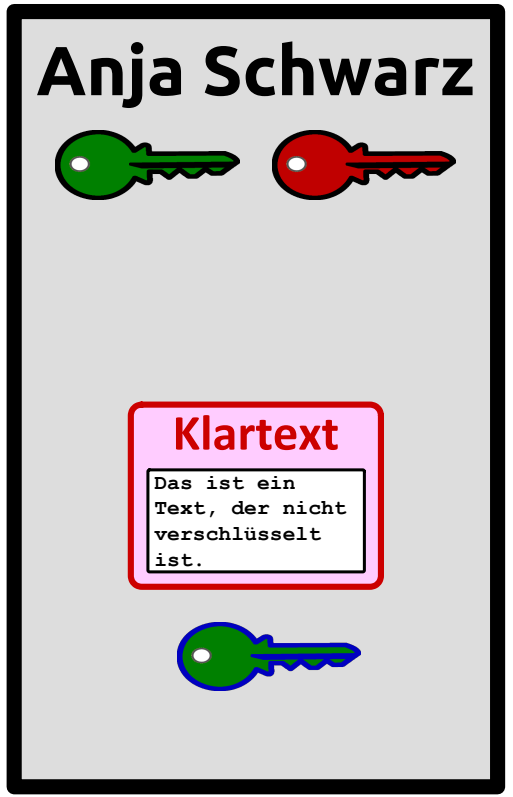


# Schlüsselaustausch, Ver- und Entschlüsselung

# Schlüsselaustausch, Ver- und Entschlüsselung




**4. Mit seinem privaten Schlüssel entschlüsselt Peter die E-Mail von Anja.**



# PGP-Verschlüsselung

- **Hybrides Verschlüsselungsverfahren**
  - asymmetrische Verschlüsselung, damit öffentliche und private Schlüssel eingesetzt werden können
  - symmetrische Verschlüsselung, damit es schneller geht und nur einmal für mehrere Empfänger/innen verschlüsselt werden muss
- **Schritte der Verschlüsselung**
  - Klartextdaten werden komprimiert (zur Reduktion der Größe und Erschwerung der Kryptoanalyse)
  - zufälliger Einmalschlüssel wird erzeugt und damit die komprimierten Klartextdaten symmetrisch verschlüsselt
  - der Einmalschlüssel wird mit dem öffentlichen Schlüssel der Zielperson asymmetrisch verschlüsselt
  - der verschlüsselte Einmalschlüssel und die verschlüsselten Daten werden zu einem Block zusammenfasst und per Base64-Codierung zu ASCII-Zeichen transformiert

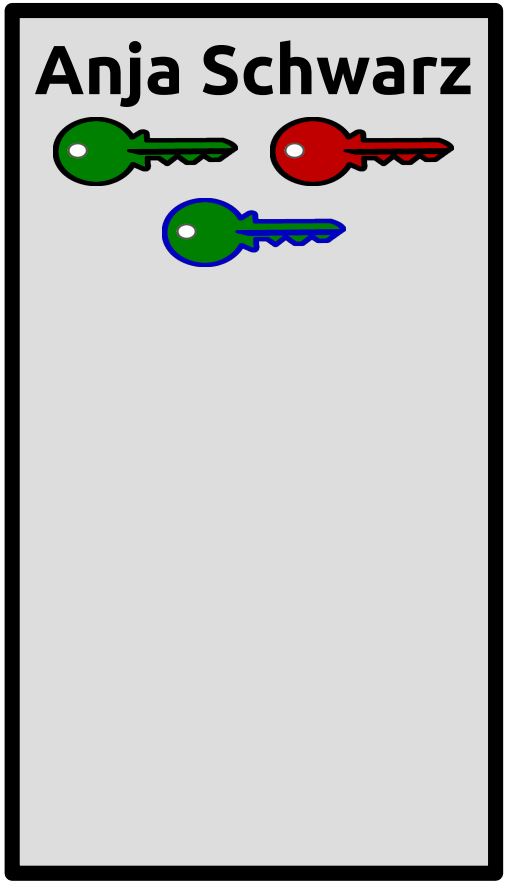
```
-----BEGIN PGP MESSAGE-----
Charset: utf-8
Version: GnuPG v1

hQMOA5o9kBAwakXiEAv/Sg8F4GJvD9O+IhR1z0I9P7RknaHJw8hdspL5JS10vHve
9oGAUYEgU+QYRbh9YYSUw8WK0fRmicom2j3LkFAU5EzzrKPBmgj56qSV+b/q8cC1
pevlRxx13HhyPurAF+PzJjSoGeZ9fV+RjowEV1POA+3qGj+M56cwD+Z1QK8GqwyF
srbcX+86YD0vPINWtbR1KpmZuu7S4x0oM6+EJx4iUQc7IYD2oTwLqpp2TPeHSL8/
FYNi6gKgDFY1ebn6UZl75WuWGE5ZcKrbVElz7s3L3LMD5q3c7FlavP8DA+x9ABio
x+EYFwl9HVVMhO92XAUsUC3nVVhmR3852wvyjUPYC96MylFa8g5N542vSvEqfsWE
Ek8ZYLNzNt4wQtGm0YmUzI/itVMEHDAx1qBSHaKMyq1rX+EAx8/9pWfKqroVSI+X
gRsbzW3qdP059YblSuAm6w8LkcGnPmcfzzB2klNjuckPTyUzzS2G/VlM+OEvLVvJ
IhGKeuresIStRLK9Lxb3C/4kxXtDEo3oBBzeGK9UhYTq2iU6Lpw2I5e0BHE79+kc
FerWNpFj363LwP9qjF8QhmyF6hzlBX4wlQJVL9FrO4wK2WM6cAn7KkMhyfPWGemr
risX2w9cHOVQlVm25k2+H8tRjoSh3Sy1J33ALUyY5K3eT8wEKceGh/8WBHOrSZrl
6aF7giRH+VUnkYwRM/SbjPSyN+va6XPEhpwwuFElIaSw/0MkzSfBBWj75/tRWbZo
3DD/KWMmtk/viLBVJpNsh6AiQrfO+7v32VrlG0B+j5b1qTqUU/LClXHGby/wz18G
wmTEkiwNa+0SVXwlyP+x6yYVpJ/MhS6CYeIY1QQ5pfbgmmwnSFJKo8FGjX9p5sW5
9mBEfimkhR4FmxKA6+GNNMxfrBxCzdIOBLtFonNB8PKb/K1gknM+HeDwcbF5sWcO
EUDMDLpj0+/+gY5exbbYnqiSwz4QFmlCsgJPEV1JWr2APdvQoGRxXtrS8V/fW5vL
9MeX5sWM4x52wRFSo6BrMx7umRq6NfhprFVee6osCQ6agW+AuI4Uds++
=P/9X
-----END PGP MESSAGE-----
```

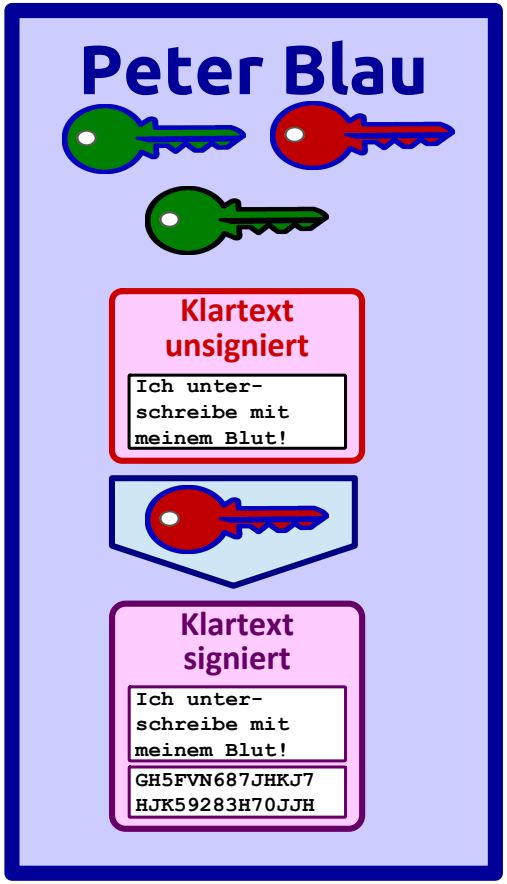
# Signieren und Signatur überprüfen


**Peter Blau und Anja Schwarz haben jeweils ein Schlüsselpaar und haben die öffentlichen Schlüssel schon ausgetauscht.**

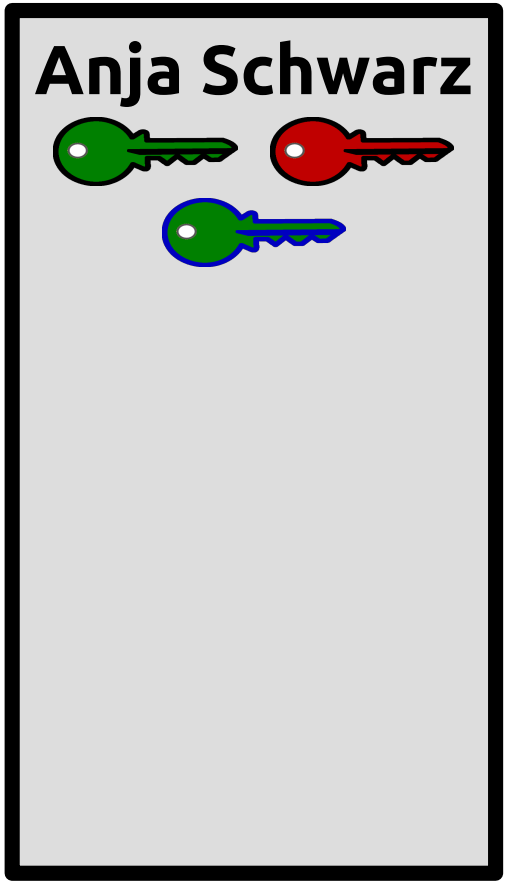
**Peter will eine signierte E-Mail an Anja schicken.**



# Signieren und Signatur überprüfen

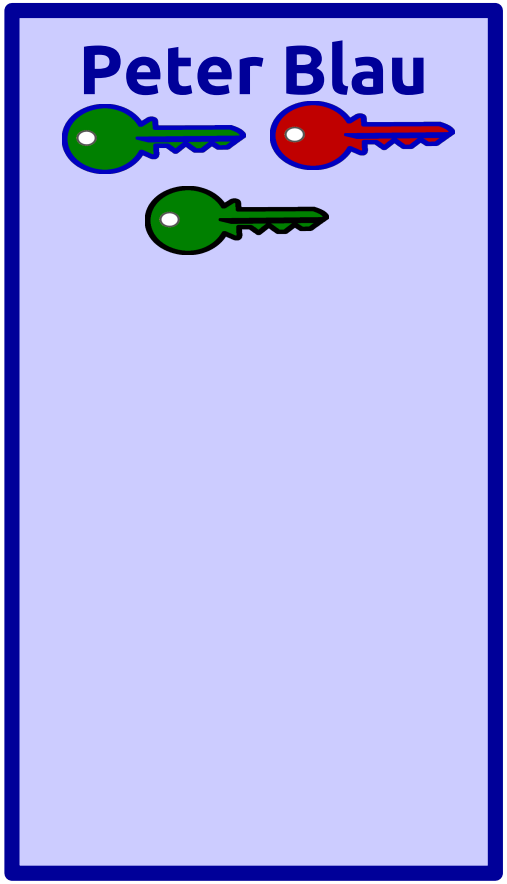



**1. Peter signiert die E-Mail mit seinem privaten Schlüssel.**

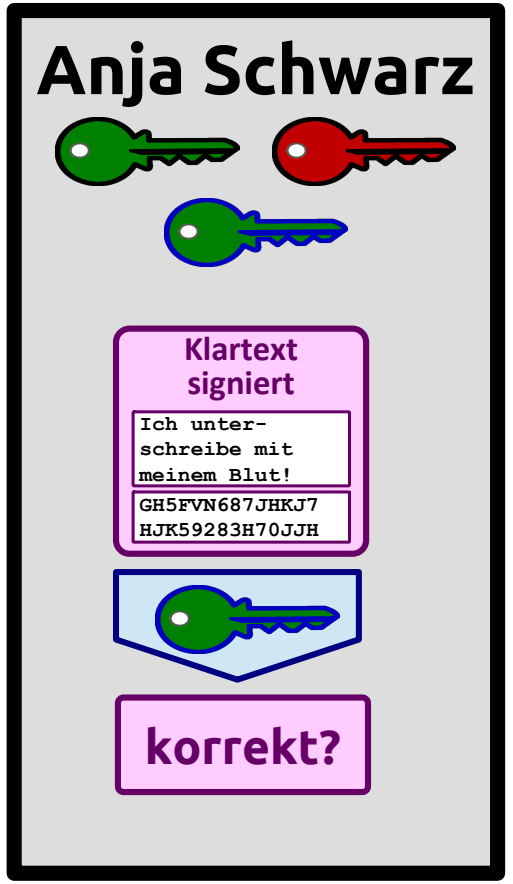


# Signieren und Signatur überprüfen

# Signieren und Signatur überprüfen




**3. Anja überprüft mit dem öffentlichen Schlüssel von Peter, ob die E-Mail tatsächlich von Peter signiert wurde.**



# PGP-Signaturen

wenn die Signatur zur E-Mail passt, dann ist gewährleistet, dass:

- die/der Signaturinhaber/in die E-Mail signiert hat
  ⇨ Authentizität
  ⇨ Nichtabstreitbarkeit
- die E-Mail nicht verändert wurde auf dem Transportweg
  ⇨ Integrität

Verschlüsselung und Signaturen können kombiniert werden.

# Beachten bei PGP

- der Betreff bei E-Mails wird in einigen PGP-Implementierungen  nicht verschlüsselt – nur der Inhalt der E-Mail!
- Passwort so wählen, dass es lang und komplex, aber zugleich gut zu merken ist
- niemals den privaten Schlüssel weitergeben

# S/MIME

- **S/MIME = Secure / Multipurpose Internet Mail Extension**
- wurde einige Jahre nach PGP in 1995 entwickelt
- bietet Verschlüsselung und Signaturen für E-Mails
- X.509-Zertifikate
- da PKCS #7 als Container der verschlüsselten und/oder signierten Daten genutzt wird, können viele verschiedene Verschlüsselungsverfahren eingesetzt werden, solange es asymmetrische Verfahren sind
- ist in vielen kommerziellen E-Mail-Programmen schon direkt enthalten (z. B. in Outlook)

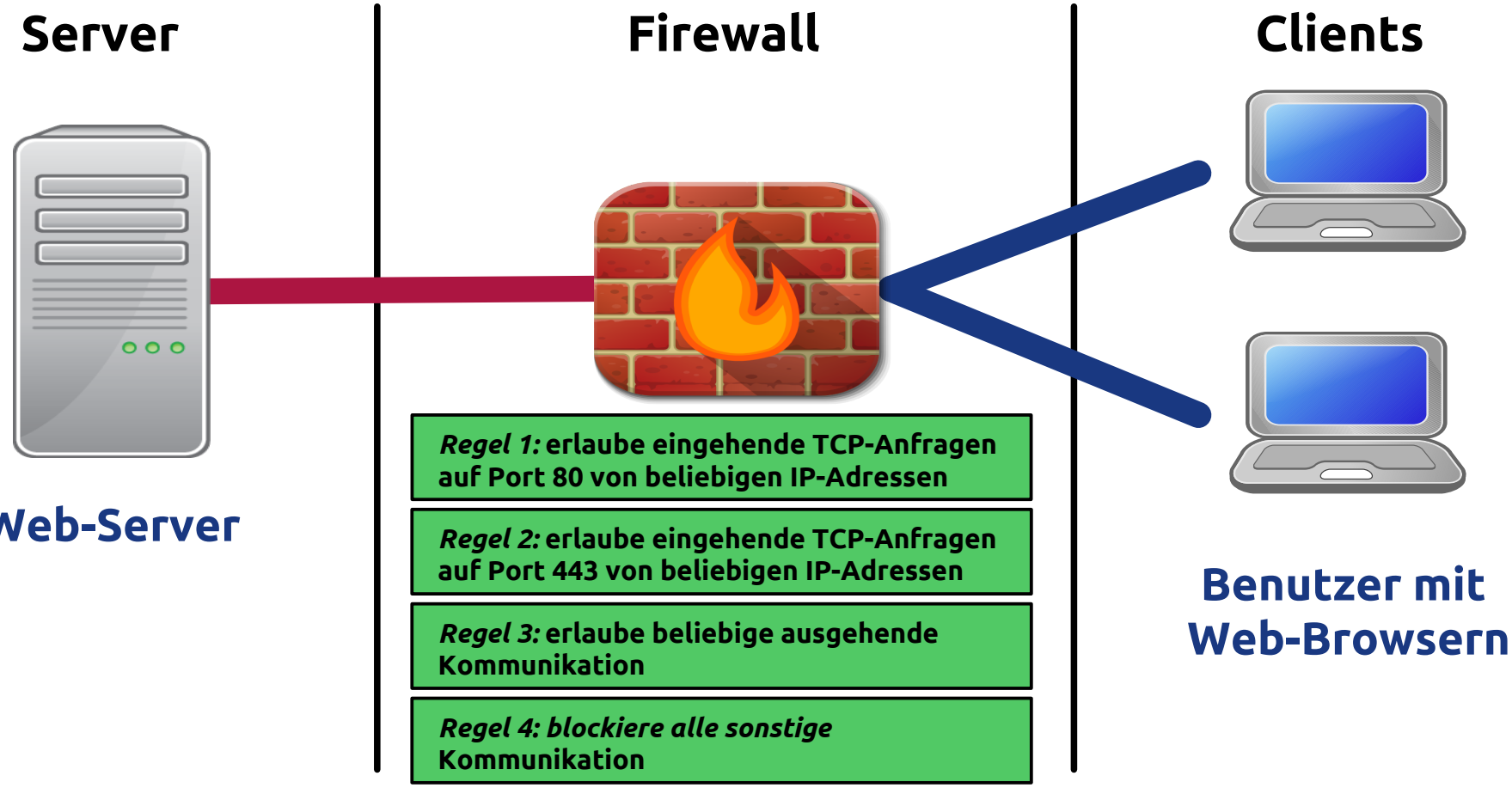
# Firewalls

- eine Firewall ist eine Schnittstelle zwischen dem externen Netzwerk und einem geschützten Bereich
- die Firewall beschränkt den Datenverkehr zwischen dem externen Netzwerk und dem geschützten Bereich
- zwei Arten
  - Paketfilter
  - Proxies
- Firewalls arbeiten richtungsabhängig
  - Firewalls für in den geschützten Bereich eingehenden Verkehr
  - Firewalls für aus dem geschützten Bereich ausgehenden Verkehr

# Paketfilter-Firewall

- die Aufgabe des Paketfilterns wird meist von einem Router übernommen – kann aber auch einfach Software auf einem Computer sein
- filtert eingehende und ausgehende Daten-Pakete
- verwirft/erlaubt Pakete abhängig von
  - IP-Adresse des Senders und/oder Empfängers
  - Protokoll (TCP, UDP, ICMP)
  - Port des Senders und/oder Empfängers
  - Eingangsnetzwerkkarte / Ausgangsnetzwerkkarte
- Beispiele: Fritzbox, Windows-Firewall

# Paketfilter-Firewall



# Proxy-Firewall

- wird zwischen Client und Server eingefügt
- arbeitet als Server und als Client
- ist Protokoll-spezifisch - für jeden Dienst ist ein eigener Proxy erforderlich, z.B. HTTP, SMTP, NNTP
- da es Protokoll-spezifisch ist, kann es auch die Semantik der Daten verstehen und entsprechend auch nach Inhalten filtern und auch spezielle Funktionen übernehmen – z. B. Verschlüsselung oder Authentifizierung

# Web Application Firewall (WAF)

- Proxy-Firewall, die den Zugriff auf eine spezielle Web-Anwendung schützt
- kennt die Internas der Webanwendung und kann die Netzwerkkommunikation somit sehr genau nach problematischen Daten durchsuchen (z.B. um SQL-Injection- oder Cross-Site-Scripting-Angriffe zu verhindern)
- ist oft hinter einer allgemeinen Firewall nachgelagert

# TLS-Interception

- Zum Schutz von Daten in Netzwerken wird immer öfters TLS eingesetzt, d.h. die Nutzdaten sind verschlüsselt und nur eine Paketfilter-Firewall kann die Netzwerkkommunikation überwachen/kontrollieren.
- TLS-Interception ist eine Technologie, um
  1. die verschlüsselten Daten abzufangen und zu entschlüsseln,
  2. die Daten zu kontrollieren und
  3. die guten Daten erneut verschlüsseln und weiterzuleiten.
- keine echte Ende-zu-End-Verschlüsselung mehr

# Netzwerksegmentierung

- in größeren Organisationen wird das interne Netzwerk oft in weitere Teil-Netzwerke (Segmente) unterteilt
- zwischen den Segmenten sind Firewalls zwischengeschaltet, die kontrollieren, dass nur berechtigte Daten zwischen den Segmenten ausgetauscht werden
- oft wird auch ein Segment speziell für die Systeme eingerichtet, die mit dem Internet verbunden werden – diese Segmente werden als Demilitarized Zone (DMZ) bezeichnet, weil sie die Systeme weniger schützen, als die Systeme die nur im internen Netz sind