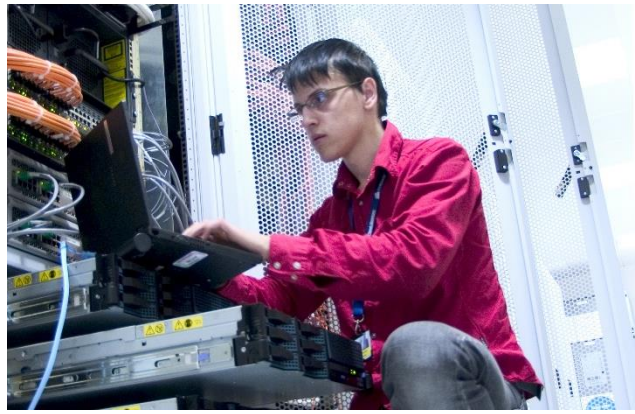
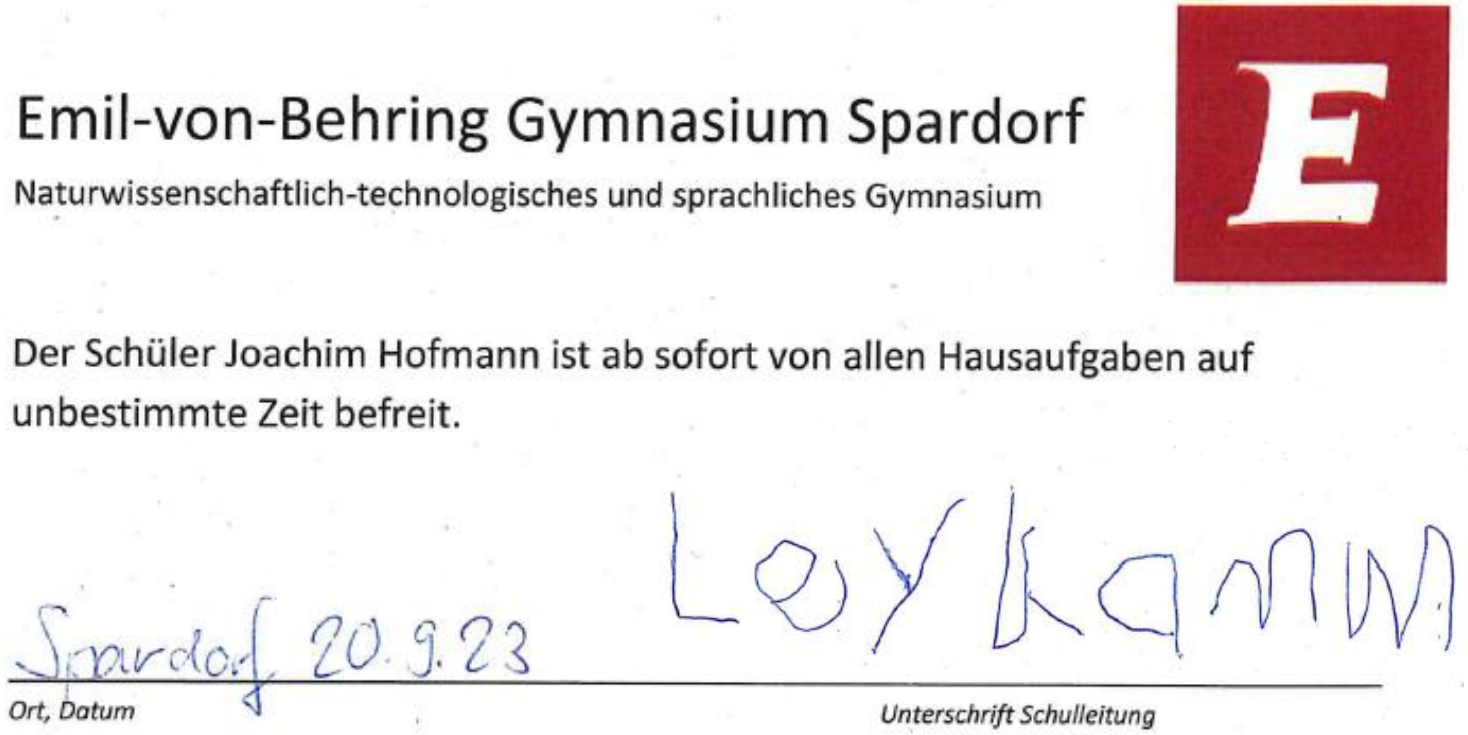
EMIL-VON-BEHRING GYMNASIUM

Codierung und Verschlüsselung
Digitales Signieren, kryptographische Hashfunktion & Zertifikate



Weitere Ziele der Kryptographie

- Mit RSA haben wir ein kryptographisch sicheres Verschlüsselungssystem. Das heißt, dass keine unbefugte Person unserer Nachrichten lesen kann, aber es gibt noch mehr Ziele, die die Kryptographie sicherstellen sollte. Beispiel:



Emil-von-Behring Gymnasium Spardorf

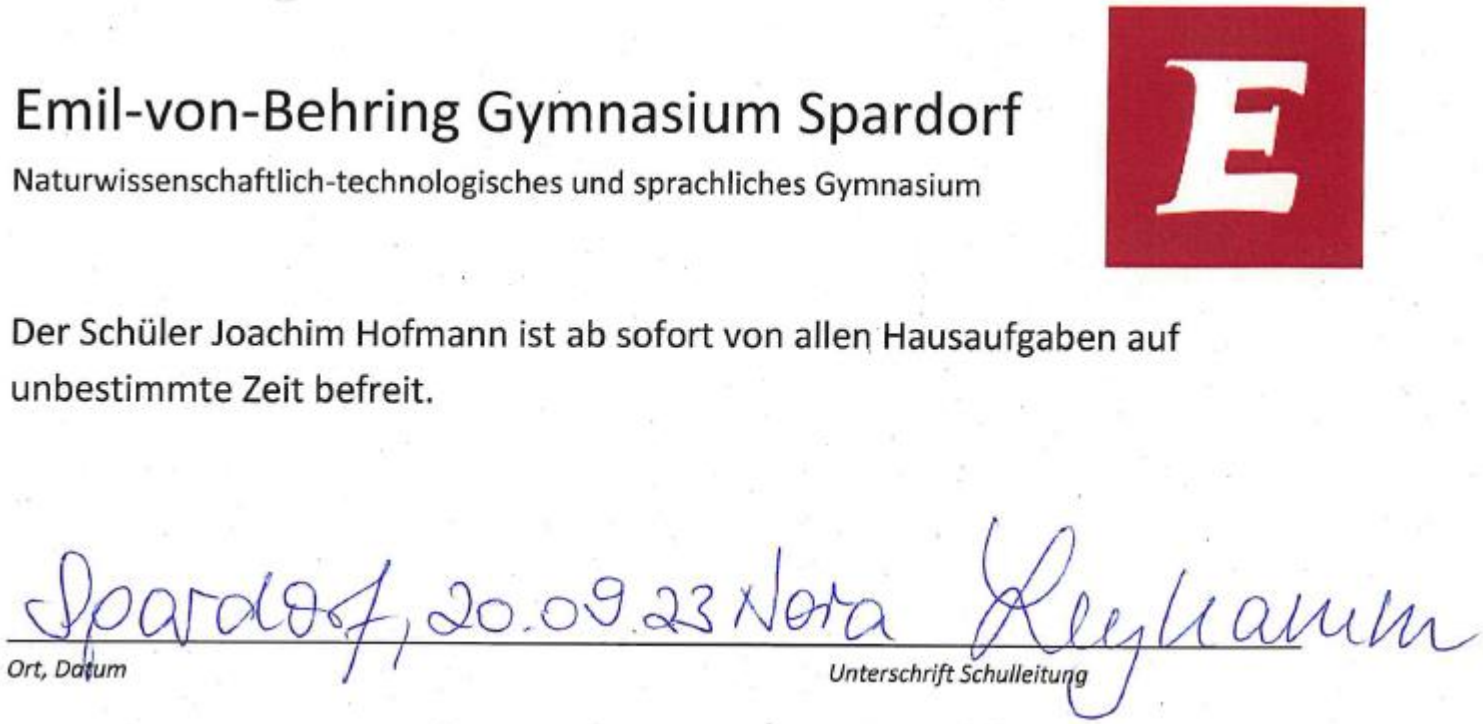
Naturwissenschaftlich-technologisches und sprachliches Gymnasium

Der Schüler Joachim Hofmann ist ab sofort von allen Hausaufgaben auf unbestimmte Zeit befreit.

Spardorf 20.9.23 — Ort, Datum

Leykamm — Unterschrift Schulleitung

Wie schaut es jetzt aus?



Emil-von-Behring Gymnasium Spardorf

Naturwissenschaftlich-technologisches und sprachliches Gymnasium

Der Schüler Joachim Hofmann ist ab sofort von allen Hausaufgaben auf unbestimmte Zeit befreit.

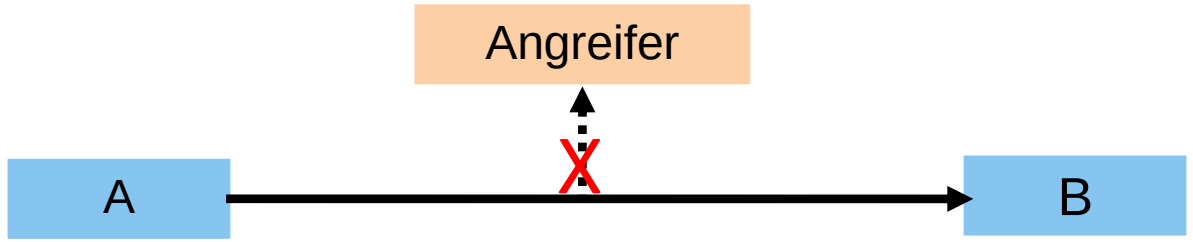
Spardorf, 20.09.23 Nora Keylmann

Ort, Datum *Unterschrift Schulleitung*

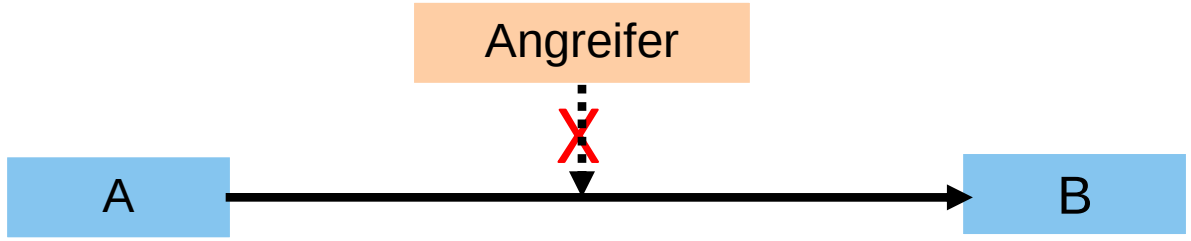
- Diese Unterschrift ist im Vergleich zur Vorherigen echt und vertrauenswürdig.

Ziele der Kryptographie – Nachricht von A an B

- **Vertraulichkeit**: Nur B kann die Nachricht lesen.



- **Integrität**: Die Nachricht ist vollständig und unverändert.



- **Authentizität**: B weiß sicher, dass der Absender A ist.

Authentisierung bezeichnet das Nachweisen einer Identität. **Authentifizierung** bezeichnet die Prüfung dieses Identitätsnachweises auf seine Authentizität.

Caesar vs. RSA

Kryptosystem	Caesar	RSA
Vertraulichkeit		
Integrität		
Authentizität		

Caesar vs. RSA

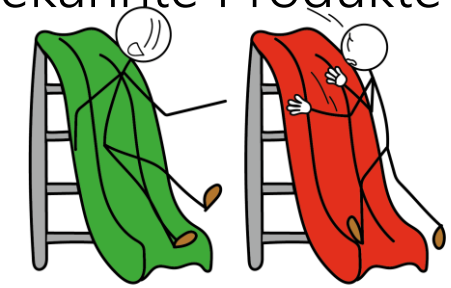
Kryptosystem	Caesar	RSA
Vertraulichkeit	Nein, zu leicht zu knacken.	
Integrität	Nein, Nachricht kann verändert werden und neue Inhalte dazugeschrieben werden.	
Authentizität	Nein, jeder kann mit Caesar verschlüsseln	

Caesar vs. RSA

Kryptosystem	Caesar	RSA
Vertraulichkeit	Nein, zu leicht zu knacken.	Ja, da nur B den privaten Schlüssel hat
Integrität	Nein, Nachricht kann verändert werden und neue Inhalte dazugeschrieben werden.	Nein, denn der Angreifer kann an bestimmten Stellen die Werte ändern z. B. Überweisung
Authentizität	Nein, jeder kann mit Caesar verschlüsseln	Jaein, man könnte mit dem privaten Schlüssel verschlüsseln und der andere kann mit dem öffentlichen Schlüssel entschlüsseln → Nachteil: jeder kann entschlüsseln

Hashfunktionen – Einwegfunktionen

- Unter einer Einwegfunktion versteht man in der Informatik eine mathematische Funktion, die ressourcensparend zu berechnen, aber sehr schwer umzukehren ist.
- Das «sehr schwer» im obigen Satz bedeutet genau dasselbe wie in der folgenden Aussage: «Ein gutes Passwort ist nicht unmöglich zu erraten, aber sehr schwer.» Das Problem besteht in beiden Fällen nicht darin, dass der Lösungsweg (=Algorithmus) unbekannt ist, sondern darin, dass das Finden/Berechnen der Lösung schlicht zu lange braucht. Wie lange genau, hängt von der Rechengeschwindigkeit ab – das ist aber wenig relevant, weil weder Millionen noch Milliarden von Jahren als angemessene Zeit für das Erraten eines Passworts oder für das Knacken einer Verschlüsselung gelten können.
- Analog zu einer mathematischen Einwegfunktion können wir uns auch ein Kuchenrezept vorstellen. Es ist nahezu unmöglich vom Kuchen zurück auf alle einzelnen Zutaten und deren exakte Mengen zu schließen.
- Trotz aufwendiger Analysen wurde es bislang nicht geschafft, bekannte Produkte wie Coca Cola oder auch die Big Mac Sauce zu kopieren.



Hashfunktionen – Einwegfunktion

- Grundlegende Idee von Hashfunktionen ist eine beliebig große Eingabe eindeutig auf eine Zahl in einem begrenzten Zahlenbereich abzubilden
  Beispiel: Summe der ASCII-Codes mod 26:
  - H(„HALLO“) = „H“ + „A“ + „L“ + „L“ + „O“ mod 26 = (72 + 65 + 76 + 76 + 79) mod 26 = 4
  - → Die 4 ist so eine Art Prüfsumme für das Wort Hallo
  - Falls die Nachricht “HALLO” dann z. B. Zu “HELLO” verändert wird, passt die Prüfumme 4 nicht mehr zur Nachricht → HELLO mit 4 empfangen → Test: H(“HELLO”) = 8 ≠ 4 → Nachricht wurde verändert
- Einwegeigenschaft: Ich denke an ein Wort und sage dir, dass bei meinem Wort die Summe der ASCII-Codes 14 ist. Welches Wort hatte ich mir gedacht? → ggf. Programm benutzen
  - Mögliche Wörter: B, INFO, …
  - → Warum ist es bei einem Angriffsszenario so schlecht, dass so viele Wörter denselben Hashwert 14 haben?

Kryptographische Hashfunktionen – Zusammenfassung

Natürlich ist die Summe des ASCII-Codes mod 26 keine kryptographisch sichere Hashfunktion, denn viele Wörter bilden dieselben Wert.

Aber sie veranschaulicht das Prinzip der Einwegfunktion und das Abbilden auf fester Länge.

Eigenschaften von kryptographische Hashfunktion:

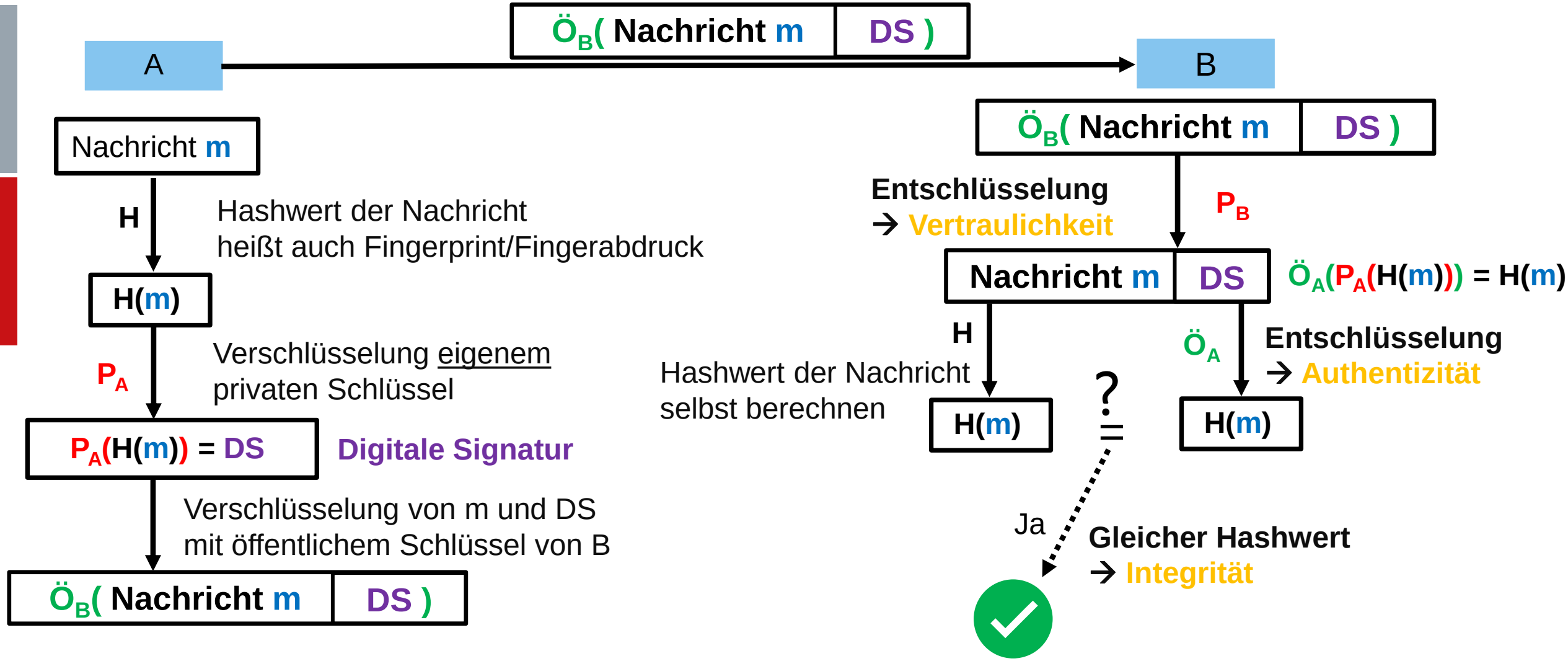
- $h: \Sigma^* \rightarrow \Sigma^n$ → Sie bildet beliebig lange Zeichenketten auf Zeichenketten fester Länge ab
- Einwegeigenschaft, also nur sehr schwer umkehrbar
- Kollisionsresistenz (Eindeutigkeit)
  - Schwach kollisionsresistent: Zu gegebenem Text kann nahezu kein weiterer Text gefunden werden, der auf denselben Hashwert abbildet.
  - Stark kollisionsresistent: Es können überhaupt keine zwei Texte gefunden werden, die auf denselben Hashwert abbilden.
- Beispiele für kryptographische Hashfunktionen: https://emn178.github.io/online-tools/sha256.html

Übung

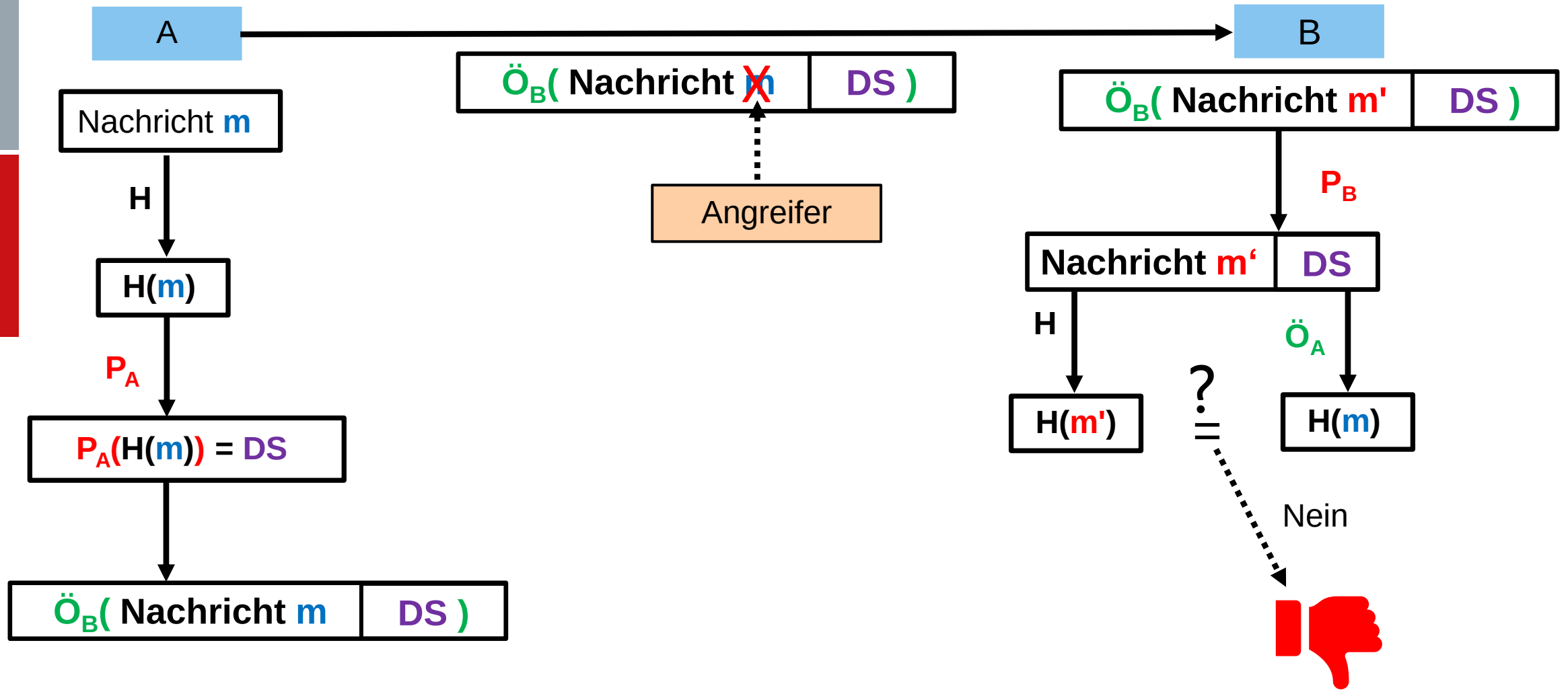
- Such dir einen Partner.
- Denk dir ein Wort aus und generiere den sha-256-Hashwert der Nachricht. https://emn178.github.io/online-tools/sha256.html
- Schicke **Klartextnachricht** und **Hashwert** (z. B. per Chat in mebis oder Teams) an deinen Partner.

- Überprüfe, ob der empfangene Hashwert mit dem Hashwert der Klartextnachricht übereinstimmt.

Digitales Signieren von Nachrichten + Verschlüsselung

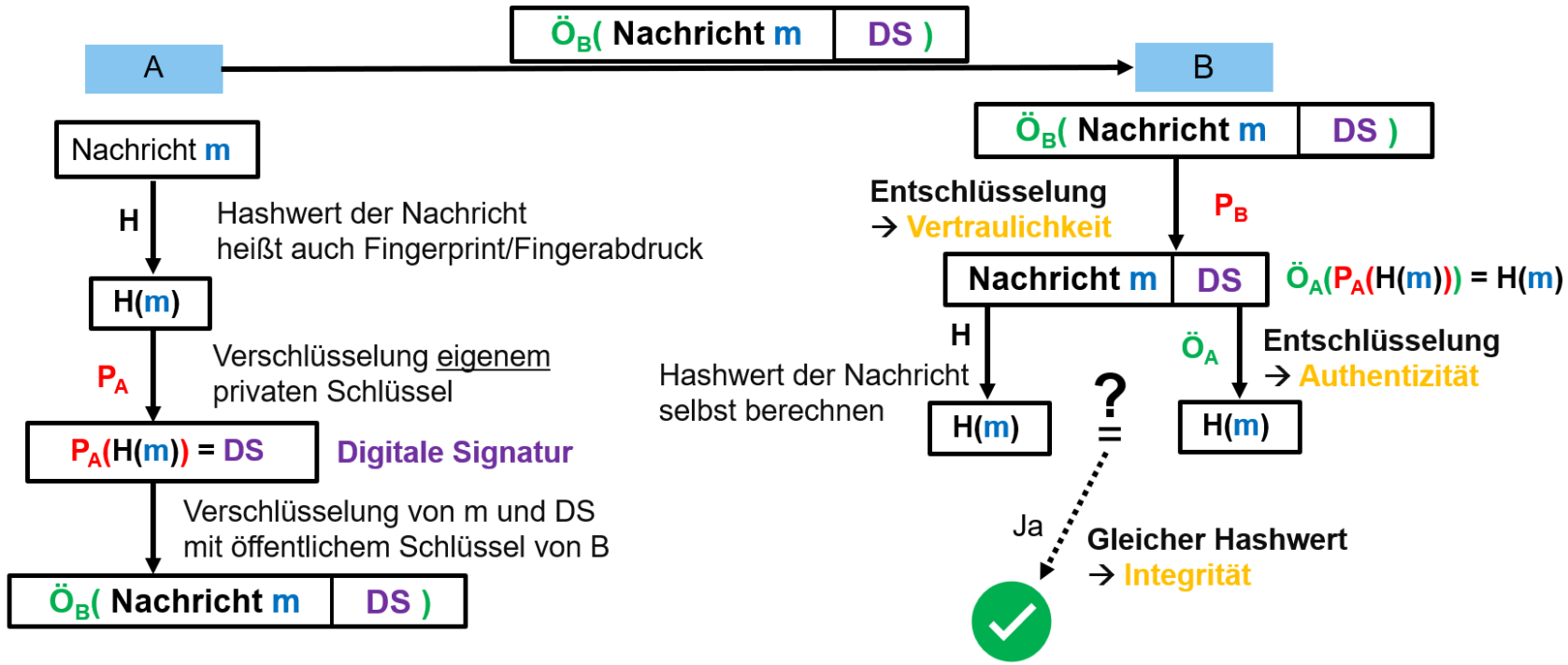


Digitales Signieren von Nachrichten + Verschlüsselung



Zertifikate

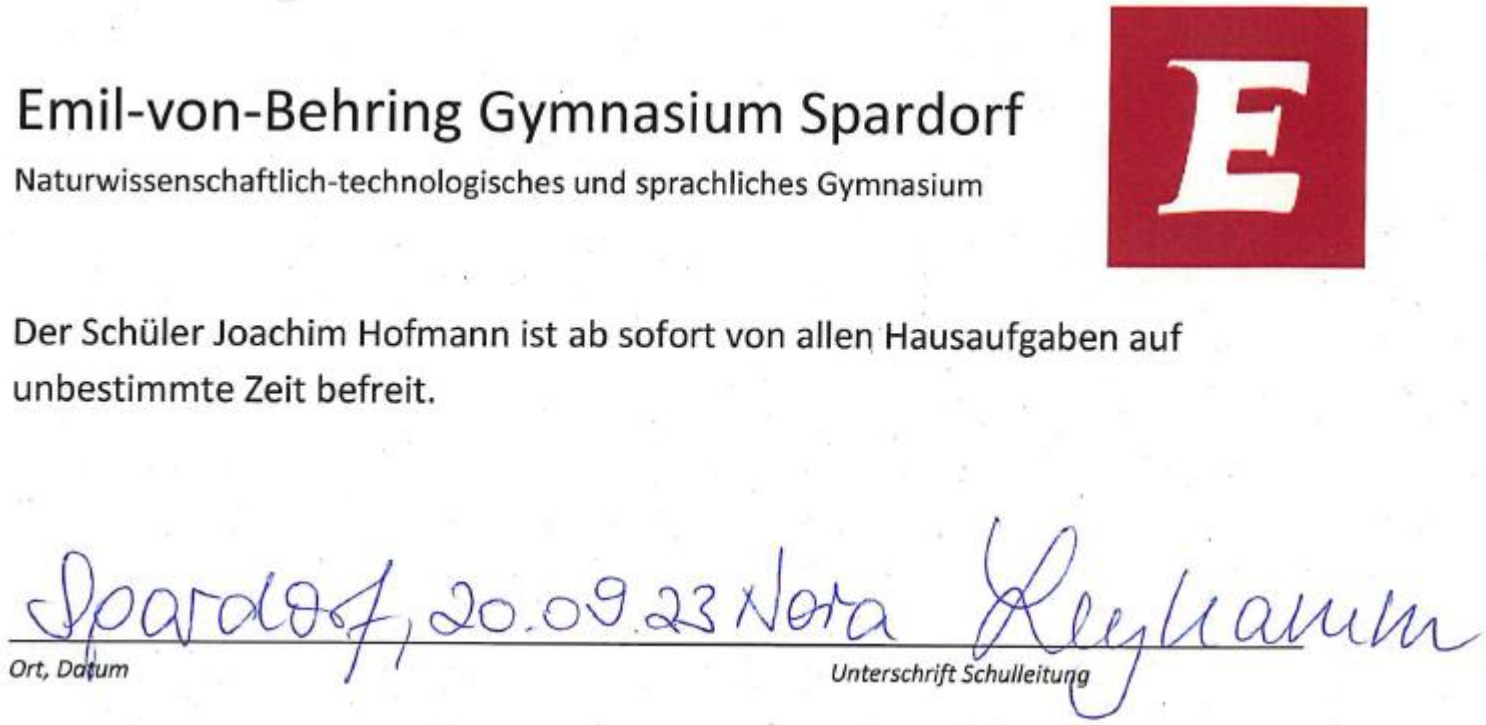
Ist dieses System jetzt komplett sicher oder gibt es eine Schwachstelle?



→ Indem man die Schlüssel ausgibt, die nicht sicher sind oder man selbst einen „Generalschlüssel" besitzt! → Dagegen gibt es (Signatur-)Zertifikate. Diese werden von offiziellen Zertifizierungsstellen ausgestellt, um die Gültigkeit und Vertrauenswürdigkeit des Signierenden zu bestätigen.

Zertifikate

Würdet ihr als Lehrer eine solche Befreiung einfach akzeptieren?



Emil-von-Behring Gymnasium Spardorf

Naturwissenschaftlich-technologisches und sprachliches Gymnasium

Der Schüler Joachim Hofmann ist ab sofort von allen Hausaufgaben auf unbestimmte Zeit befreit.

Spardorf, 20.09.23 Nora Leykamm

Ort, Datum

Unterschrift Schulleitung

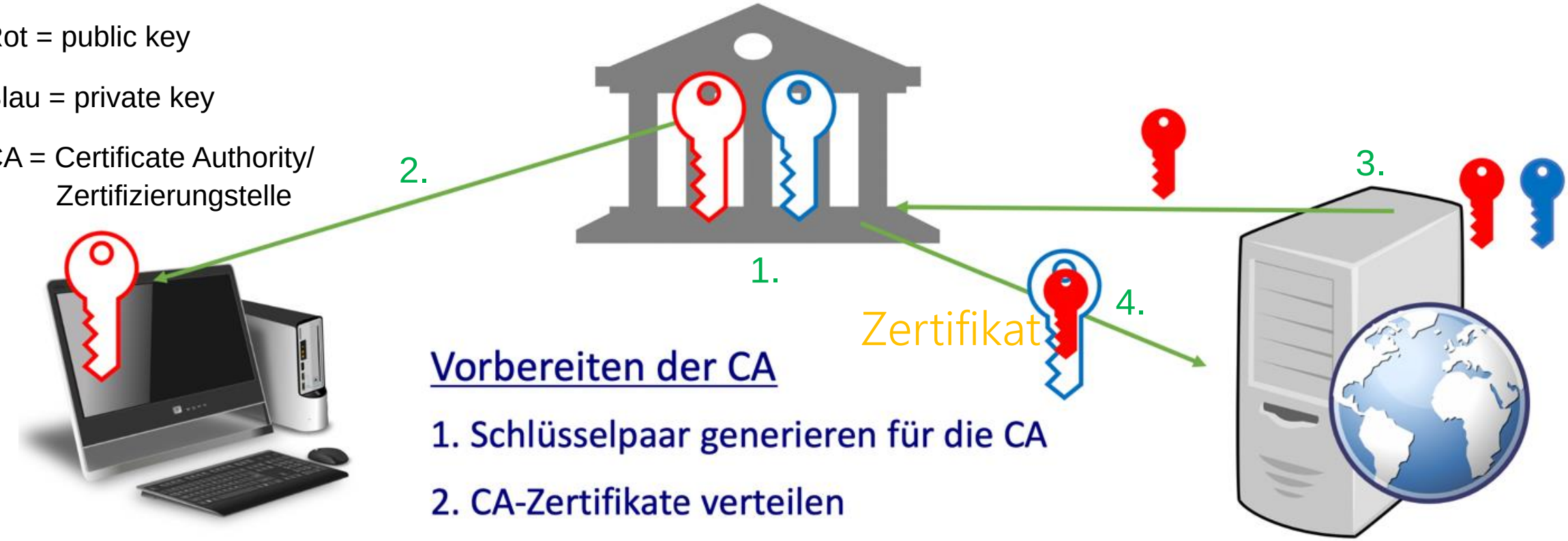
- Eher nicht, da würde man mal bei der Schulleitung nachfragen! → Sprich: man überprüft diese Befreiung bzw. lässt man sie sich zertifizieren! → Frau Leykamm: ja, das war ich!

Zertifikatsausstellung

Rot = public key

Blau = private key

CA = Certificate Authority/
Zertifizierungstelle



Vorbereiten der CA

1. Schlüsselpaar generieren für die CA
2. CA-Zertifikate verteilen

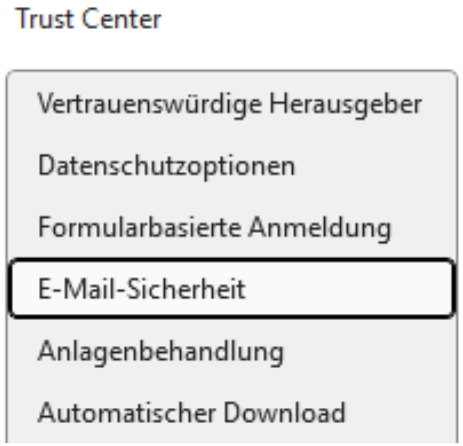
Vorbereiten des Webservers

3. Schlüsselpaare für den Webserver generieren
4. Zertifizierung des Webservers (→ CA)

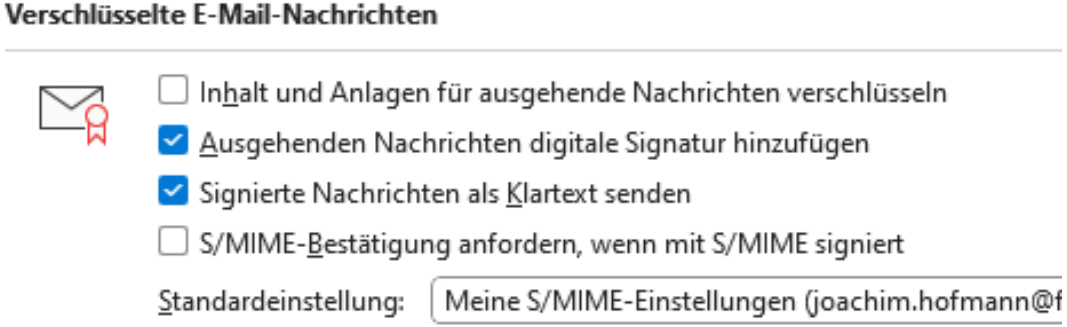
Zertifikate

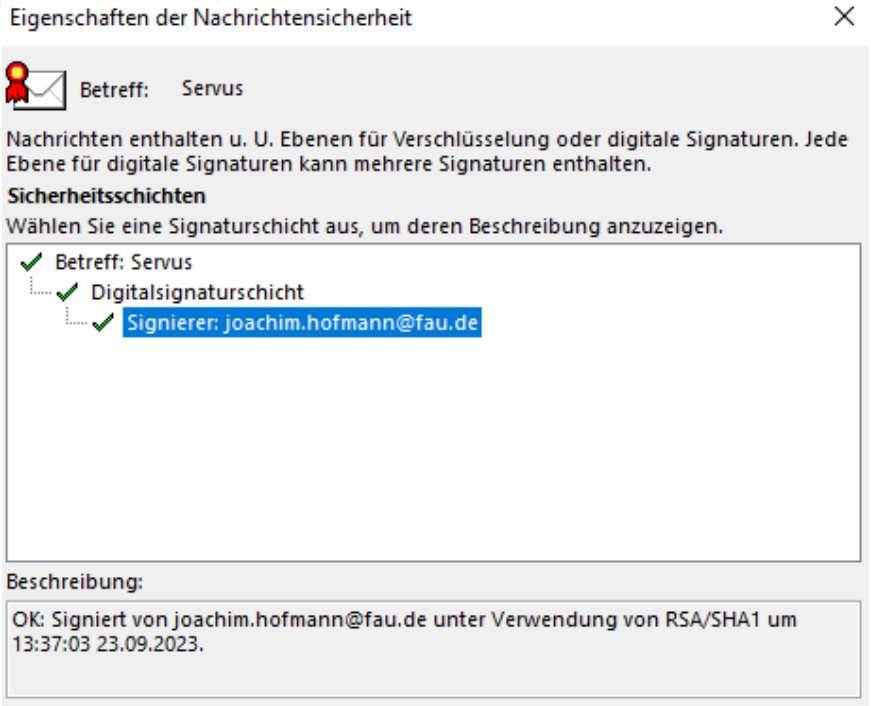
- Man kann sich also seinen public key zertifizieren lassen.
  → Public-Key-Zertifikate
- Dabei ist das Zertifikat an z. B. die E-Mail-Adresse bzw. an die Domain (joachimhofmann.org) gebunden und ist für andere E-Mail-Adressen bzw. Domains nicht nutzbar.
- Zertifikate kommen an verschiedenen Stellen zum Einsatz:
  - E-Mail
  - Webserver
  - Login (Client-Zertifikat als Variante für eine 2-Faktor-Authentisierung)

Digitales Signieren von E-Mails mit Zertifikaten



[E-Mail-Verschlüsselung in der Praxis vom BSI]





- Damit kann ein Empfänger sich sicher sein, dass die Mail vom wirklich von meiner E-Mail-Adresse stammt.

- Warum verschlüssle ich meine aber E-Mails meist nicht?
  - Asymmetrische Verschlüsselung ist bei langen Nachrichten zeitintensiv! → siehe RSA
  - Fast niemand verschlüsselt Mails, weil es standardmäßig nicht vorgesehen war.
  - Man kennt von vielen Empfängern nicht den Schlüssel, da es anders bei bei Threema keinen zentralen Server gibt, der alle public keys verwaltet.

Webzertifikate

Zertifikat

www.evbg.de | R3 | ISRG Root X1

Inhabername

Allgemeiner Name: www.evbg.de

Ausstellername

Land: US
Organisation: Let's Encrypt
Allgemeiner Name: R3

Gültigkeit

Beginn: Tue, 15 Aug 2023 07:30:17 GMT
Ende: Mon, 13 Nov 2023 07:30:16 GMT

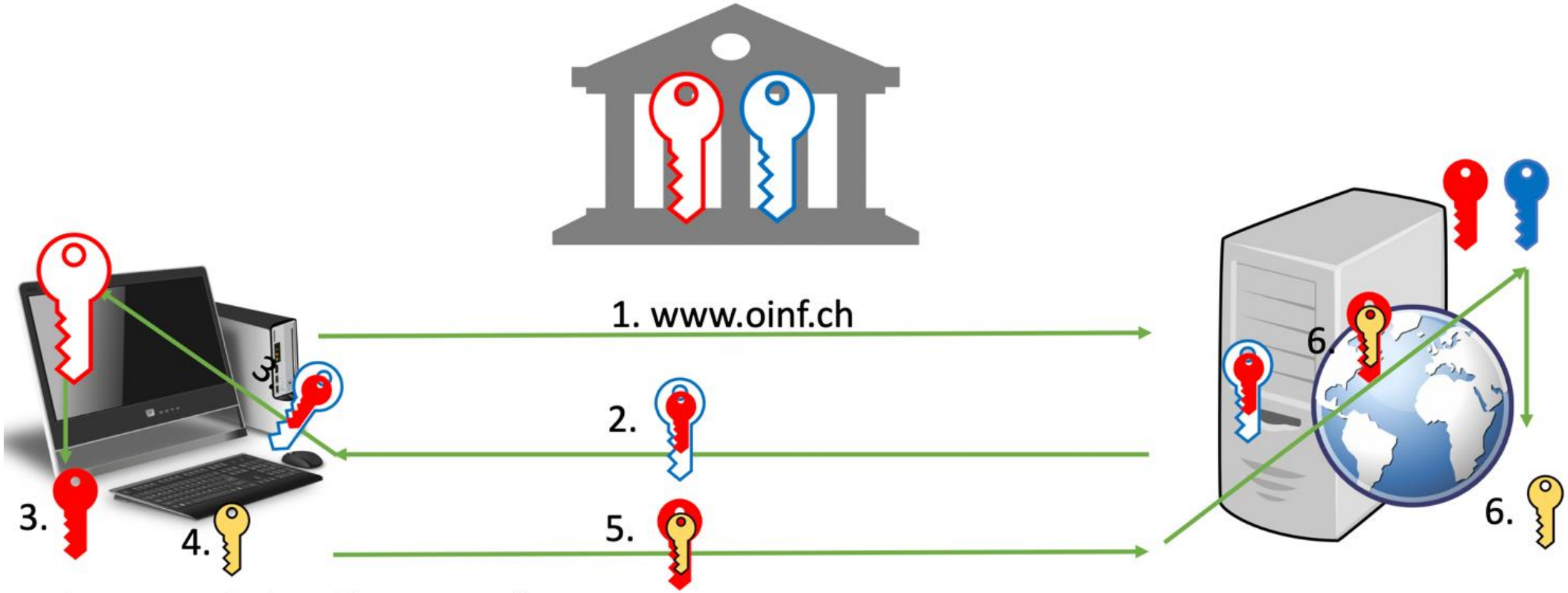
Alternative Inhaberbezeichnungen

DNS-Name: www.evbg.de

Öffentlicher Schlüssel - Informationen

Algorithmus: RSA
Schlüssellänge: 4096
Exponent: 65537
Modulus: AD:BD:30:78:DD:1C:B6:32:8A:0F:B8:5D:2B:C4:2F:54:77:86:78:32:3D:2C:8A:EE:CE:0...

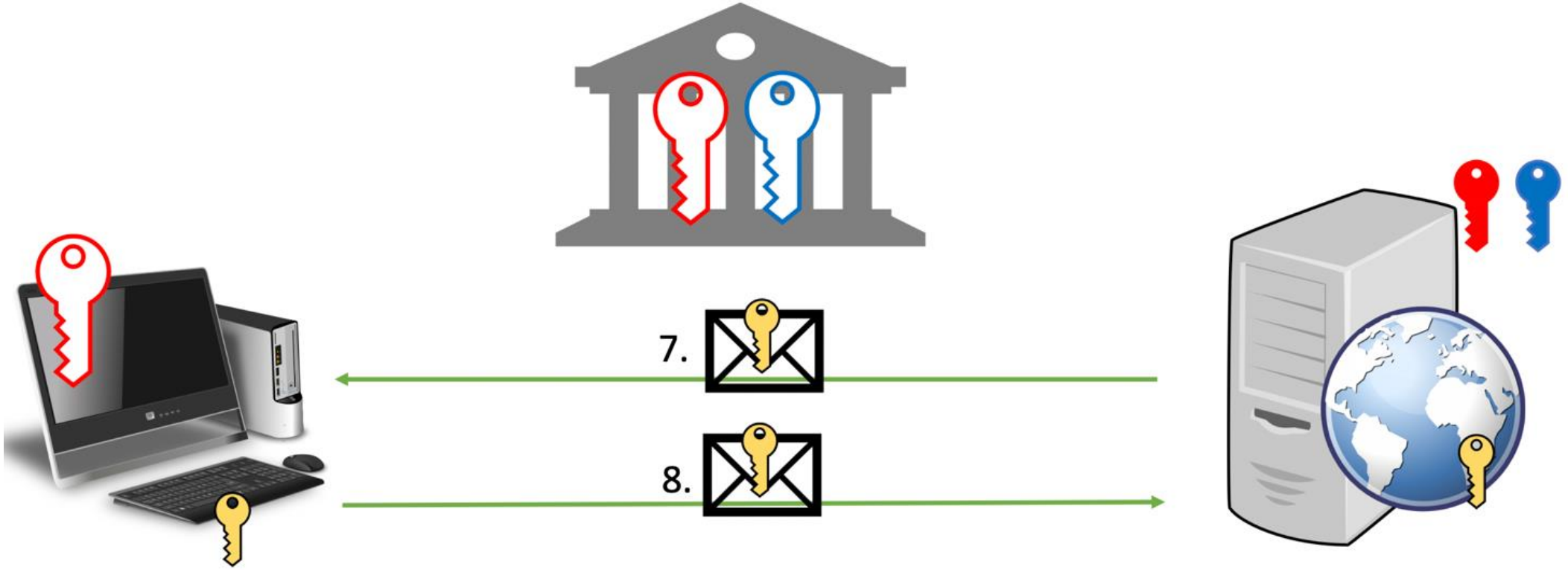
Wie funktioniert ein Webseitenaufruf?



Asymmetrischer Sitzungsaufbau

1. Aufbau der Verbindung
2. Übertragen des Webserver-Zertifikats
3. Prüfen der Signatur des Zertifikats anhand des von der CA hinterlegten Schlüssels
4. Generieren eines (symmetrischen) Sitzungsschlüssels
5. Senden des Sitzungsschlüssels in verschlüsselter Form
6. Entschlüsseln des Sitzungsschlüssels

Wie funktioniert ein Webseitenaufruf?



Symmetrischer SSL-Tunnel

7. Symmetrische Ver- und Entschlüsselung

8. Symmetrische Ver- und Entschlüsselung

Weshalb verwenden wir einen «Symmetrischen Schlüssel»?

- Jeder Client müsste auch ein Zertifikat besitzen bzw. zumindest ein Schlüsselpaar
- Ver- und Entschlüsselung ist weniger rechenintensiv