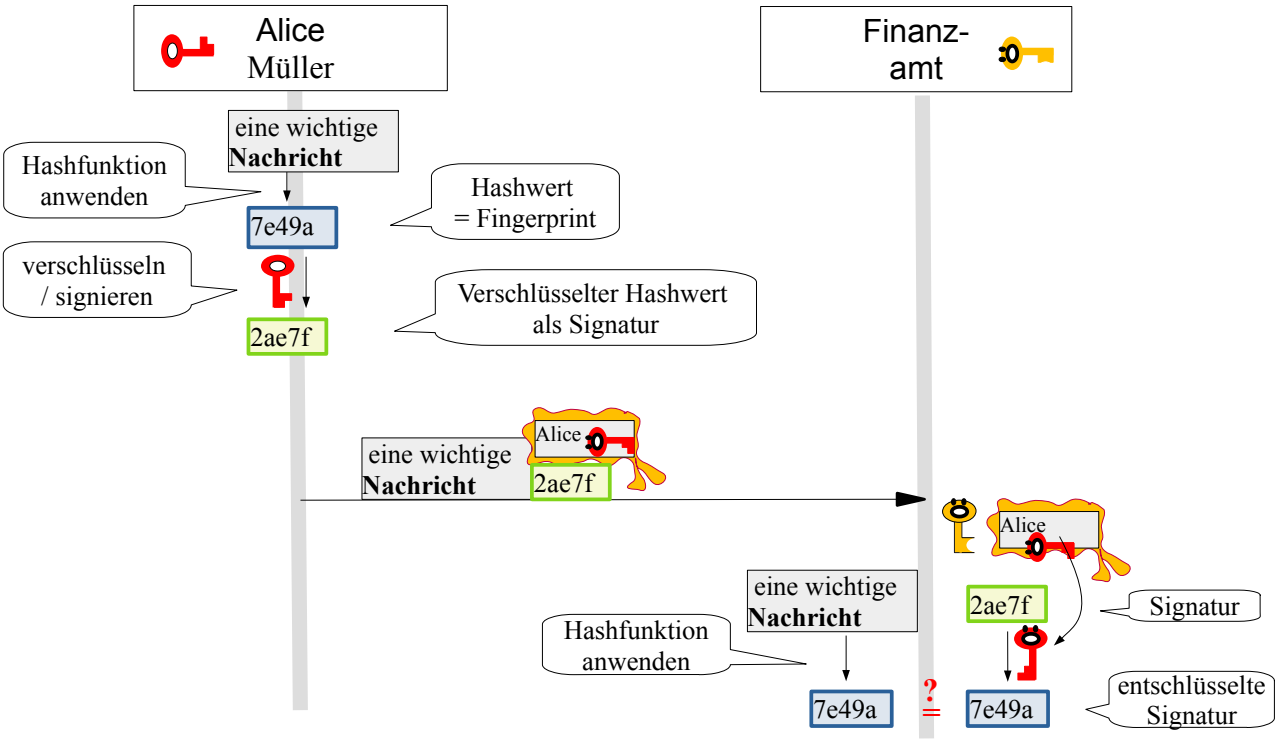
IuD: Digitale Signatur

Frau Müller verschlüsselt ihre Steuererklärung mit dem öffentlichen Schlüssel des Finanzamts, von dem sie das Zertifikat erhalten hat. Damit ist die Nachricht vertraulich und kann nicht mitgelesen werden. Aber wie kann das Finanzamt sicher sein, dass die Steuererklärung tatsächlich von Frau Müller stammt?

> Wikipedia: „Ein […] digitales Signaturverfahren ist ein asymmetrisches Kryptosystem, bei dem ein Sender mit Hilfe eines geheimen Signaturschlüssels (dem Private Key) zu einer digitalen Nachricht (d.h. zu beliebigen Daten) einen Wert berechnet, der ebenfalls digitale Signatur genannt wird. Dieser Wert ermöglicht es jedem, mit Hilfe des öffentlichen Verifikationsschlüssels (dem Public Key) die nichtabstreitbare Urheberschaft und Integrität der Nachricht zu prüfen. Um eine mit einem Signaturschlüssel erstellte Signatur einer Person zuordnen zu können, muss der zugehörige Verifikationsschlüssel dieser Person zweifelsfrei zugeordnet sein.“ [1]



Aufgaben

1. *a) Beschreibe den Ablauf und setze ihn in Zusammenhang mit der Definition von Wikipedia.*

   Hinweis: Eine kryptographische *Hashfunktion* erzeugt eine Art Fingerabdruck der eigentlichen Nachricht: Einen Text, der viel kürzer ist als die Nachricht, und aus dem man die ursprüngliche Nachricht nicht wieder herleiten kann. Es ist auch quasi unmöglich (zumindest sehr sehr schwer), eine andere Nachricht mit dem gleichem Fingerabdruck zu generieren.

b) Erläutere, wie das Finanzamt erkennt, ob die Nachricht tatsächlich von Alice Müller stammt?

c) Analysiere, was sich ändern würde, wenn Mal entweder die Nachricht oder die Signatur manipuliert?

d) In obigem Diagramm wird die eigentliche Nachricht öffentlich lesbar übertragen. Ändere

1 *https://de.wikipedia.org/wiki/Digitale_Signatur, abgerufen 20.1.20*

den Ablauf so ab, dass auch die Nachricht verschlüsselt übertragen wird.

e) Recherchiere, wo Signaturen verwendet werden. Gib mind. zwei Anwendungsbereiche an.

2. Signieren einer Nachricht - ohne Zertifikat (Chat-Tool)

a) Schicke eine digital unterschriebene Nachricht an eine/mehrere andere Personen. Schreibe eine Nachricht. Durch Rechtsklick auf die Nachricht kannst du eine Signatur erzeugen. Auch die Signatur lässt sich durch Ziehen eines Schlüssels verschlüsseln.

Verwendeter Schlüssel: _____

b) Wenn du eine digital unterschriebene Nachricht erhältst, ist die Signatur verschlüsselt. Entschlüssele die Signatur. Überprüfe durch Rechtsklick auf die Nachricht die Signatur.

Verwendeter Schlüssel: _____

3. Versenden einer verschlüsselten und signierten Nachricht – ohne Zertifikat (Chat-Tool)

a) Verschicke eine Nachricht, die nicht von dritten gelesen werden kann und bei der sichergestellt ist, dass du der Absender bist. Notiere die Reihenfolge der Schritte und die verwendeten Schlüssel.

4. Signieren und Verschlüsseln – mit Zertifikat (Chat-Tool)

Diesmal werden die Schlüssel vor dem Versenden von der Zertifizierungsstelle auf den Namen des Schlüsselbesitzers zertifiziert. Klicke dazu im Schlüsselspeicher mit der rechten Maustaste (Schlüssel-Name-Paar zertifizieren).

Wenn du einen Schlüssel erhältst, darfst du ihn erst dann in deinen Schlüsselspeicher aufnehmen, wenn du seine Signatur geprüft hast. Lasse dazu den öffentlichen Schlüssel der Zertifizierungsstelle (rechte Maus auf den Schlüsselspeicher) anzeigen und nutze ihn zur Überprüfung der Signatur.

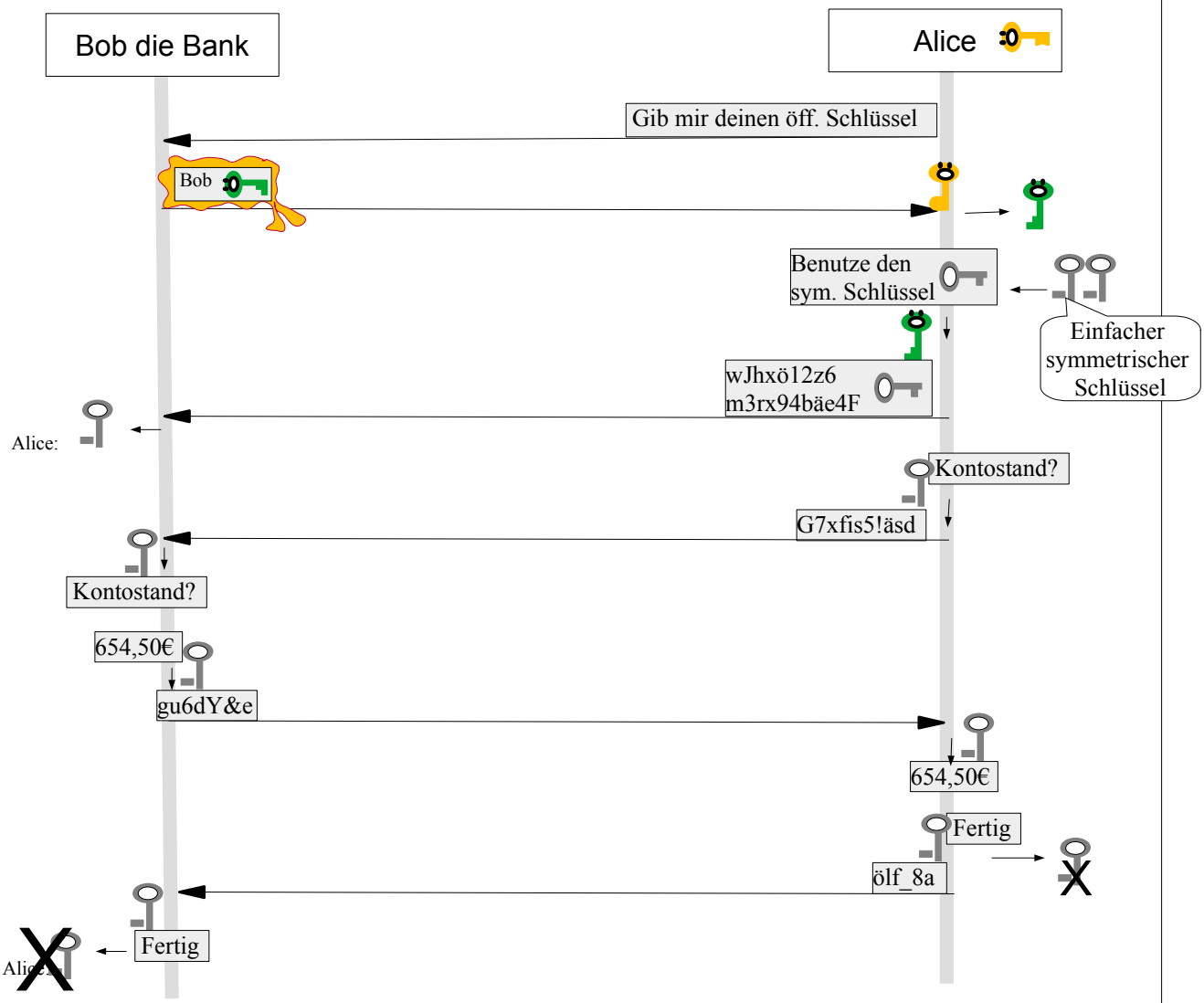
a) Spielt die Szenarien aus Aufgabe 2 und 3 erneut durch und analysiert dabei, ob der Man-in-the-Middle nun noch eine Chance auf einen Angriff hat.

5. *Bei einer sicheren Kommunikation über eine Internetseite geschieht Folgendes (siehe Diagramm)*

   a) Erläutere den Ablauf.

   b) Begründe, warum zu einem symmetrischen Schlüssel gewechselt wird.

   c) Analysiere, ob die Kommunikation sicher ist.



6. *Wie sieht ein Zertifikat ‚in echt' aus?*

Gehe dazu auf eine Internetseite mit verschlüsselter Kommunikation (https://….) und lasse dir das Zertifikat anzeigen. Je nach Browser findest du es z.B. so:

Firefox: *Klicke auf das Schloss-Symbol inks der Adresszeile → Verbindung sicher → weitere Informationen → Zertifikat anzeigen.*

Chrome: Je nach Version: *kleines grünes Schloss links der Adresszeile.* Oder: *rechts der Adresszeile die drei Punkte anklicken → weitere Tools → Entwicklertools (oder F12) → Sicherheit → Zertifikat anzeigen → Details.*

Internet Explorer: *Menü: Datei → Eigenschaften → Zertifikate → Zertifizierungspfad → Zertifikat*

anzeigen → Details.

a) Informiere dich über die Inhalte eines Zertifikats.

b) Erläutere, warum das Zertifikat nicht verschlüsselt, sondern für jeden lesbar ist.

c) Erläutere, was ein Fingerabdruck ist. (steht ganz unten im Zertifikat) Was bedeutet dort z.B. SHA-256?

7. *In deinem Browserfenster erscheint die Meldung*
   „Das Zertifikat ist nicht bekannt. Möchten Sie es trotzdem akzeptieren?“
   Erläutere, was das bedeutet und analysiere, welche Gefahren bestehen.

8. *Informiere dich im Internet, welche Probleme trotz Zertifikaten auftreten können. Beschreibe einen Fall genauer.*

9. *SHA-256-Hashfunktion*

Öffne das Chat-Tool und schreibe eine Nachricht und erzeuge deren Hashwert (rechte-Maus-Klick). Experimentiere mit der Hashfunktion:

- *Schreibe dieselbe Nachricht noch einmal und ändere nur ein einziges Zeichen ab (am besten hast du sie vorher kopiert). Wie ändert sich dadurch der Fingerabdruck?*
- *Wie ändert sich der Hashwert, wenn du die Nachricht komplett änderst?*
- *Kann es zu demselben Hashwert verschiedene Ausgangstexte geben? Begründe.*
- *Versuche, einen Text zu schreiben, der zu diesem Hashwert passt: q07mlqBHI2*

Fasse zusammen, welche Eigenschaften eine kryptographische Hashfunktion hat.

10. *Recherchiere nach aktuell verwendeten Hashfunktionen.*

11. *Bei einer sicheren Informiere dich über PGP-Systeme (Pretty good Privacy).*

12. *Informiere dich über das Web of Trust. (Z.B. bei inf-schule.de)*