IuD: Digitale Signatur - Lösung

Aufgaben:

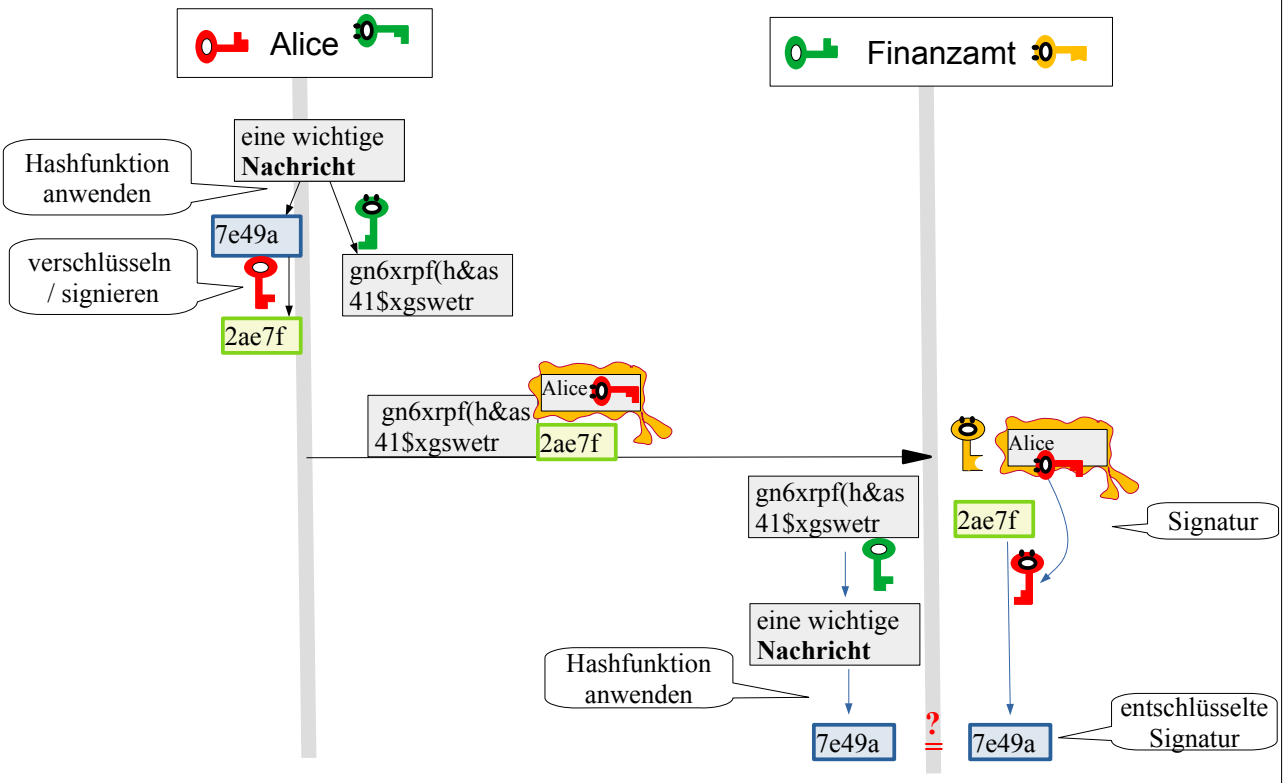
1. a) Es wird nicht die komplette Nachricht verschlüsselt, sondern nur ein kleiner Teil, der Fingerabdruck der Nachricht. Dazu wird mit einer sogenannten Hash-Funktion ein Hash-Wert berechnet. Das ist der Fingerabdruck der Nachricht. Nur auf diesen (viel kleineren) Hash-Wert wird der privaten Schlüssel angewendet. Das Ergebnis ist die Signatur. Die Signatur wird zusammen mit der Nachricht an den Empfänger geschickt. Das Zertifikat mit dem öffentlichen Schlüssel schickt Alice gleich mit. Der Empfänger trennt die Nachricht von der Signatur. Auf die Nachricht wendet er die Hash-Funktion an und erzeugt den Fingerabdruck der Nachricht. Parallel dazu wendet er auf die Signatur den öffentlichen Schlüssel aus dem Zertifikat an und erhält den Fingerabdruck der Nachricht. Diese beiden Fingerabdrücke vergleicht er. Sind sie gleich, stammt die Nachricht tatsächlich von Alice.

b) Die Nachricht stammt tatsächlich von Alice, wenn der Hashwert der Nachricht und die entschlüsselte Signatur gleich sind.

c) Wenn Mal entweder die Nachricht ändert oder die Signatur, dann sind Hashwert der Nachricht und entschlüsselte Signatur nicht gleich.

d) s.u.

e) Signaturen werden überall dort verwendet, wo eine elektronische Unterschrift eine Unterschrift auf Papier ersetzen soll. Z.B. Anträge bei Behörden, Steuererklärung beim Finanzamt, Firmen, die anderen Firmen Rechnungen stellen,… Aber auch um z.B. Dateien fälschungssicher aufzubewahren.



2. Signieren einer Nachricht: (Aufgabe mit Chat-Tool)

a) Verwendeter Schlüssel: mein privater Schlüssel

b) Verwendeter Schlüssel: öffentlicher Schlüssel des Senders

c) Nein, das ist nicht möglich.

3. Versenden eine verschlüsselten und signierten Nachricht: (Aufgabe mit Chat-Tool)

Signatur erzeugen und mit meinem privaten Schlüssel verschlüsseln.

Die Nachricht mit dem öffentlichen Schlüssel des Empfängers verschlüsseln.

4. Nein er hat keine Chance. (Aufgabe mit Chat-Tool)

5. a) Alice stellt die Anfrage an Bobs Internetseite, dass sie kommunizieren will. Bob sendet ihr sein Zertifikat. Alice Browser verifiziert das indem er den öffentlichen Schlüssel der CA anwendet und merkt sich Bobs öffentlichen Schlüssel. Es wird eine Nachricht an Bob geschickt mit einem einfachen symmetrischen Schlüssel. Die folgende Kommunikation findet mit diesem symmetrischen Schlüssel statt. Wenn die Seite verlassen wird , wird der Schlüssel wieder gelöscht.

b) Die Verschlüsselung mit einem symmetrischen Schlüssel ist viel schneller als mit dem asymmetrischen Schlüssel.

c) Ja, weil ein Angreifer den symmetrische Schlüssel zwar theoretisch mit brute force knacken kann, aber praktisch nicht genug Zeit dazu hat.

6. a) Wesentlichen Inhalte eines Zertifikats sind z.B. :

Inhaber: ...
Aussteller: ...
Gültigkeit von … bis ...
öff. Schlüssel: Algorithmus: ...RSA
Schlüssellänge: ...2048
Exponent: ...65537
Modulus: ...B1:89:9E:….
SerienNr: ...
Fingerabdrücke: ...SHA-256: 82:A7:0D:58:….
Schlüsselverwendung: ...digitale Signatur, key Encrypment
...

b) Die gängigen Browser beinhalten diesen öffentlichen Schlüssel und zeigen das Zertifikat bereits „entschlüsselt“ also verifiziert an. Weiterhin ist das Zertifikat kein Geheimnis, sondern für jeden zugänglich. Die Verschlüsselung dient nur der Authentifizierung und soll sicherstellen, dass es tatsächlich von der Zertifizierungsstelle ausgestellt wurde.

c) Ein Fingerabdruck ist ein Text, der viel kürzer ist als die eigentlichen Nachricht und die Nachricht eindeutig „repräsentiert“. Aus dem Fingerabdruck kann man die ursprüngliche Nachricht (praktisch) nicht wieder herleiten. Das ist ähnlich einem menschlichen Fingerabdruck. SHA-256 ist der Name eines standardisierten Hashalgorithmus (Hashfunktion), mit dem man einen solchen Fingerabdruck erzeugen kann.

7. Es ist nicht sicher, ob das Zertifikat tatsächlich vom angegebenen Absender stammt. Es

könnte auch abgelaufen sein (‚gültig bis' wurde überschritten).

Es könnte also sein, dass der Eigentümer versäumt hat, sein Zertifikat verlängern zu lassen, dann würde zunächst keine Gefahr bestehen. Es könnte sich aber auch um ein gefälschtes Zertifikat handeln. Akzeptiert man es, ist jegliche Aktivität, die auf diesem Zertifikat beruht, nicht nur nicht sicher, sondern täuscht eine falsche Sicherheit vor.

8. Zertifikate werden auch von kommerziellen Stellen ausgegeben. Man kennt die Zertifizierungsstelle oft nicht, muss ihr aber vertrauen. Relevante Fragestellungen sind:

Welche Verfahren wurden bei der Ausstellung verwendet? Wie sicher ist das (für meine Anwendung)?

Wie genau prüft die Zertifizierungsstelle die Identität des Zertifikatseigentümers?

Wenn ein Zertifikat gesperrt wird, dann muss diese Sperrinformation an alle gelangen, die das Zertifikat verwenden könnten. Wer aktualisiert/prüft Sperrlisten?

u.s.w. Siehe dazu auch [1].

9. Hashfunktion

- Der Hashwert ändert sich wesentlich, unabhängig davon, ob nur ein einzelnes Zeichen geändert wird oder der ganze Text. Der Hashwert ist immer gleich lang.
- Weil der Hashwert kürzer sein kann als der Ursprungstext, muss es Hashwerte mit mehreren Ausgangstexten geben.
- Es ist quasi unmöglich, zu einem Hashwert einen Ausgangstext zu erfinden.

10. Der SHA-2, *secure hash algorithm*, wird aktuell zu Verwendung empfohlen.[2]

11. Ein PGP-System ist ein hybrides System, bei dem die Nachricht mit einem zufällig erzeugten (symmetrischen) Schlüssel verschlüsselt wird. Nur dieser Schlüssel wird asymmetrisch verschlüsselt und zusammen mit der Nachricht verschickt. Vorteil: schneller, weniger aufwendig. PGP-Syteme basieren häufig auf dem Web of Trust. (siehe z.B. Wikipedia [3])

12. Bob hat Alice Schlüssel und hat sichergestellt, dass es wirklich der Schlüssel von Alice ist. Das kennzeichnet er auf dem Schlüsselserver. Carl möchte nun Alice Schlüssel haben, kennt sie aber nicht. Er sieht auf dem Schlüsselserver, dass Bob den Schlüssel von Alice als echt gekennzeichnet hat. Da es Bob kennt und vertraut, vertraut er auch Alice Schlüssel. So entsteht ein Netzwerk von Vertrauensbeziehungen. (Siehe z.B. inf-schule [4] oder genauer: Wikipedia [5])

1 *https://de.wikipedia.org/wiki/Public-Key-Zertifikat (abgerufen, 27.3.20)*

2 *https://de.wikipedia.org/wiki/SHA-2, (abgerufen 03.01.2020)*

3 *https://de.wikipedia.org/wiki/Pretty_Good_Privacy (28.3.20)*

4 *https://www.inf-schule.de/kommunikation/kryptologie/sicherheitsinfrastruktur/konzept_weboftrust (28.3.20)*

5 *https://de.wikipedia.org/wiki/Web_of_Trust (28.3.20)*