Elektronische Unterschrift - *Digitale Signatur*

Eine digitale Signatur übernimmt die Funktion einer „Unterschrift“ in einem Dokument.
Die Unterschrift beweist, dass das Dokument von einer bestimmten Person stammt.
Wie eine klassische Unterschrift muss damit die digitale Signatur eindeutig und überprüfbar sein, d.h. es muss sich feststellen lassen, ob sie von einer bestimmten Person stammt ->Authentizität.

➔ *Prüfung der Authentizität einer Nachricht*

Hashwert als Signatur

Die digitale Signatur darf nicht fälschbar sein, d.h. ihre Integrität muss gewährleistet werden. In der Digitaltechnik kann das durch einen sog. Hashwert erreicht werden.
Der Hashwert wird über ein mathematisches Verfahren unter Einbeziehung aller vorhandenen Daten (Bits) einer Nachricht (eines Dokuments) erzeugt.
Der Hash stellt einen sog. CRC (CyclicRedundantCheck) dar mit dem u.a. auch zwei große, ähnliche Dateien auf Gleichheit überprüft werden können. Anstatt jeweils die beiden Dateien Zeichen für Zeichen durchzusehen, reicht es, die beiden Hash-Werte der Dateien miteinander zu vergleichen.

➔ Prüfung der Integrität einer Nachricht oder Datei

Damit bindet der Hash die Daten einer Nachricht an die Signatur genauso wie das Papier eines unterschriebenen Dokuments die Unterschrift an den Text bindet.

In der Kryptografie werden Hashverfahren zum Signieren von Dokumenten oder zum Erzeugen von Einweg-Verschlüsselungen verwendet (z.B. MD5, SHA-1).

Ein, mit einem private Key, verschlüsselter Hashwert stellt somit im eigentlichen Sinn die „Digitale Signatur“ dar. In der Kryptographie wird ein derartiger verschlüsselter Hashwert auch *Message Authentication Code* (MAC) genannt.

Um digital vorliegende Dokumente unterschreiben zu können, d.h. um ihre Authentizität und Integrität nachweisen zu können wird die *Digitale Signatur* verwendet.

Abbildung-1: Digitale Signatur ohne Verschlüsselung des Dokuments

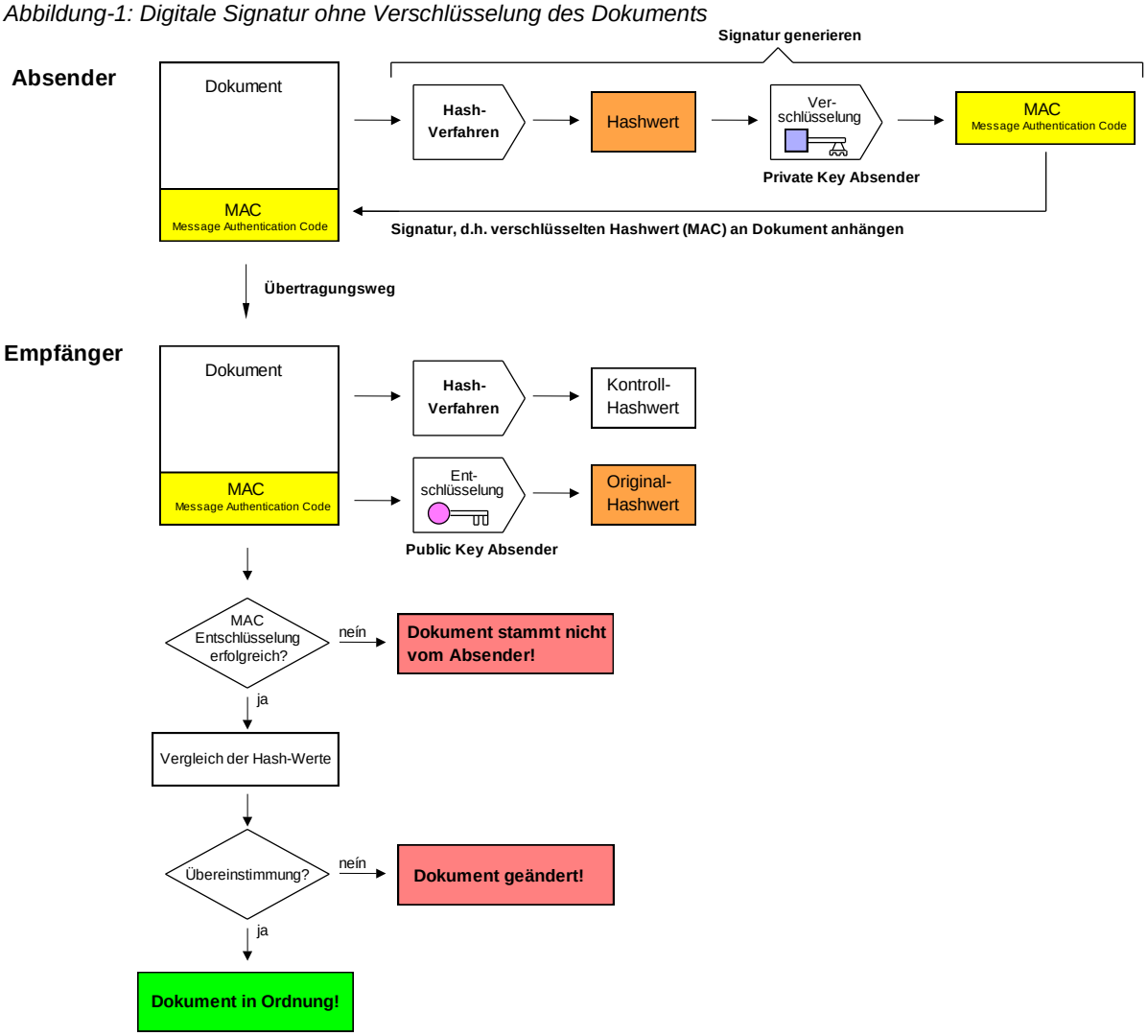
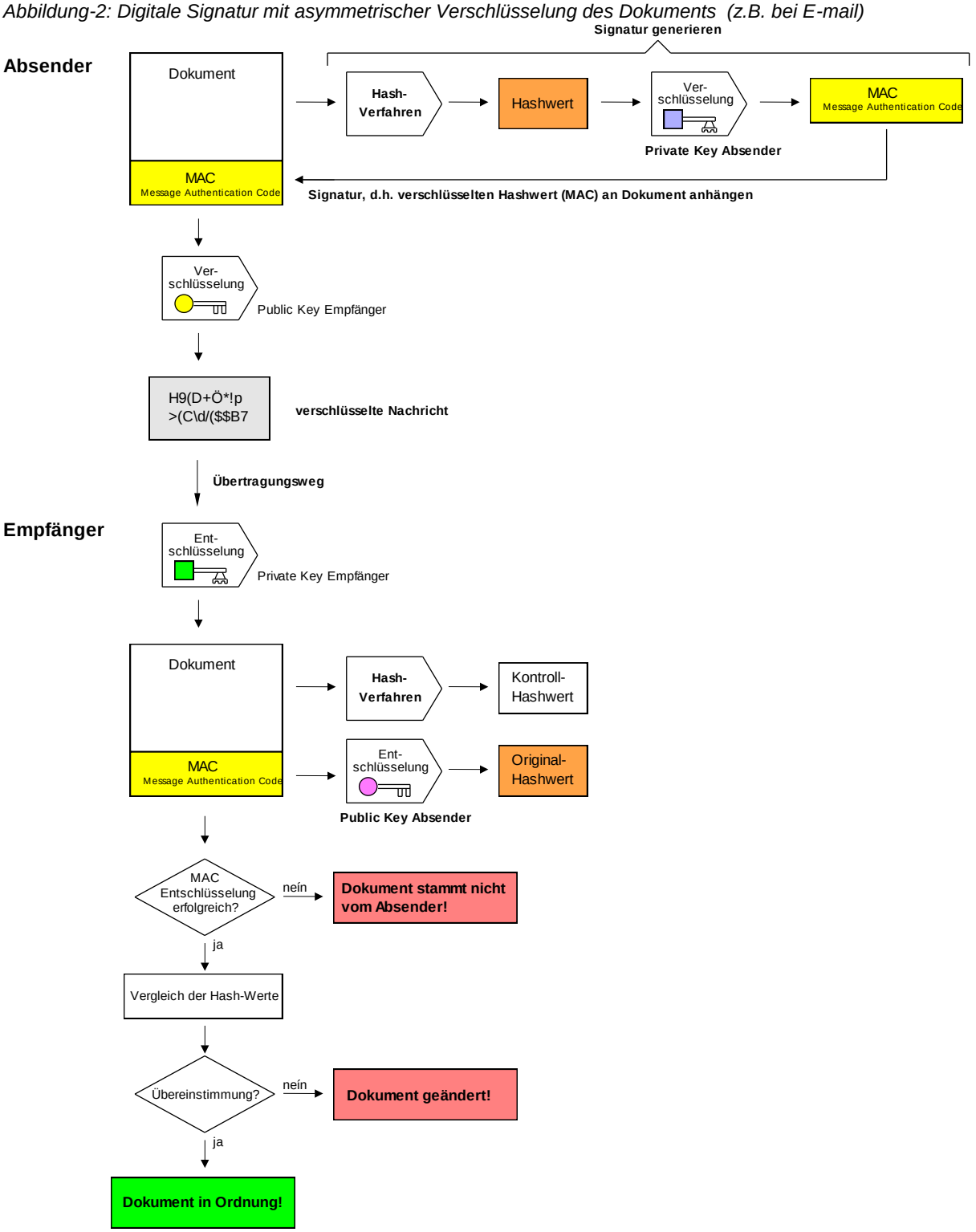


Abbildung-2: Digitale Signatur mit asymmetrischer Verschlüsselung des Dokuments (z.B. bei E-mail)



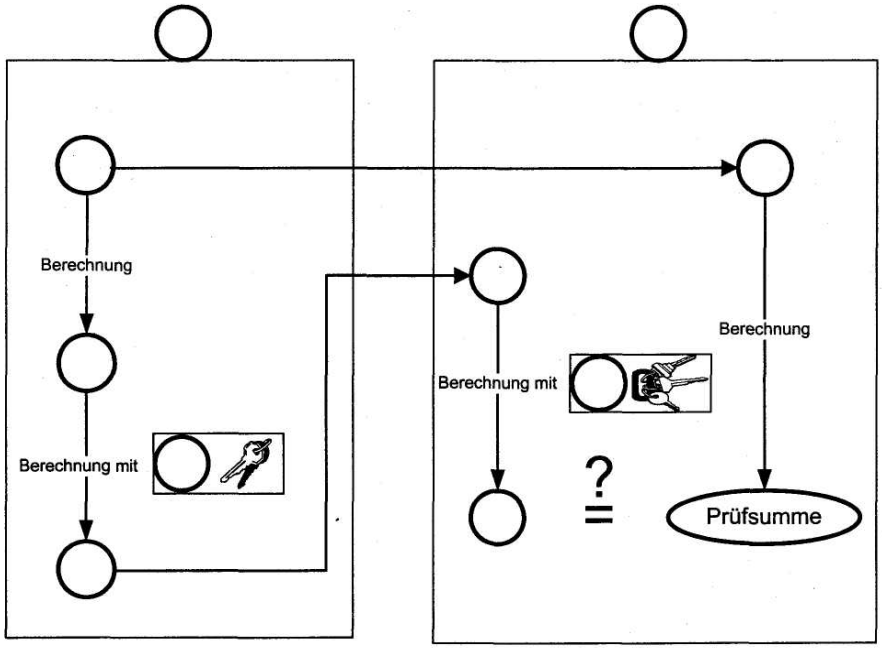
Aufgaben

1.) Beschreiben Sie in Ihren eigenen Worten, wie die digitale Signatur von Dokumenten in den beiden Varianten funktioniert. Stellen Sie deutlich heraus, welche Schlüssel wo zum Einsatz kommen.

2.) (APr-KQ) Tragen Sie in unten stehendes Schaubild zur digitalen Signatur die Ziffern 1 bis 7 der folgenden Bezeichnungen an den entsprechenden Stellen ein.

1 Dokument
2 Empfänger
3 Privater Schlüssel
4 Signatur
5 Absender
6 Prüfsumme (Hash Code)
7 Öffentlicher Schlüssel

Hinweis:
Alle Ziffern werden mindestens einmal benötigt.



3.) (APr-FQ) Bei der Konfiguration von Systemen treffen Sie auf die Begriffe MD5 und RSA.
Nennen Sie den jeweiligen Einsatzzweck dieser Verfahren.

4.) Generieren Sie von einer beliebigen Datei MD5- und SHA1-Hashes. z.B. mit **`fsum`** von www.slavasoft.com/. Ändern Sie mit einem Hexeditor (z.B. **`HxD`** von www.mh-nexus.de/) ein beliebiges Byte der Datei und generieren Sie die Hashwerte erneut. Was fällt auf?