4.2 Digitale Unterschriften

Wie oft haben Sie in der letzten Woche mit ihrem Namen ein Stück Papier unterschriebe, beispielsweise Schecks, Kreditkartenbelege, juristische Dokumente, Briefe, etc.? Mit ihrer Unterschrift stellen Sie sicher, dass Sie (und niemand anderes) den Inhalt des Dokuments bestätigt oder damit einverstanden ist.

Auch in der digitalen Welt benötigt man oft einen Hinweis auf den Erzeuger oder Besitzer eines Dokuments bzw. man möchte sein Einverständnis mit dem Inhalt eines Dokumentes deutlich machen. Eine *digitale Unterschrift* (engl. ***D**igital **S**ignature,* kurz *DS*) ist die kryptografische Technik, um dieses Ziel in der digitalen Welt zu erreichen. Genau wie bei handschriftlichen Signaturen sollten digitale Unterschriften *verifizierbar* und *fälschungssicher* sein. Die Signierung erfolgt mit dem RSA-Verfahren.

Ein Problem bei der Signierung von Daten mittels Verschlüsselung besteht darin, dass Ver- und Entschlüsselung zu rechenintensiv ist. Daher berechnet ein Hash-Algorithmus für eine Nachricht von beliebiger Länge einen „*Fingerabdruck*“ fester Länge. Der „*Fingerabdruck*“ wird mit dem *Private-Key* verschlüsselt und gilt als *digitale Unterschrift*. Der Empfänger des Dokumentes entschlüsselt die *digitale Unterschrift* mit dem *Public-Key* und überprüft, ob der Hash-Wert, den er selbst erstellt, mit dem entschlüsselten Wert übereinstimmt. Bei Übereinstimmung der Hash-Werte, ist die Integrität des Erzeugers der Nachricht gewährleistet (siehe Abbildung 8).

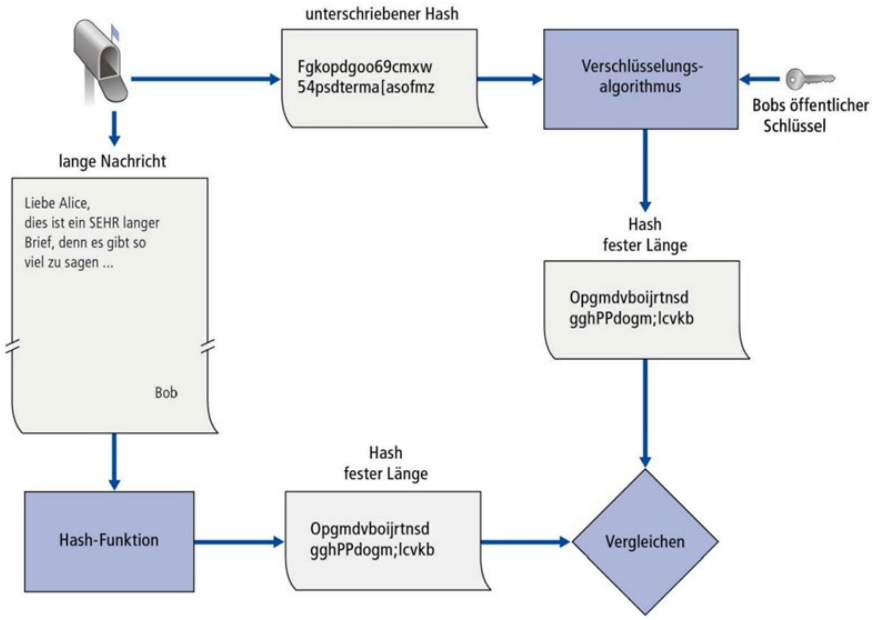

Abbildung 1: Überprüfung einer digital unterschriebenen Nachricht

Für eine *Public-Key*-Verschlüsselung ist es allerdings unbedingt erforderlich, den Nachweis der Authentizität durch digitale Zertifikate zu erwirken.

