# Integrität und Authentizität mit digitaler Unterschrift sicherstellen


Durch Verschlüsseln mit Alices öffentlichem Schlüssel kann Bob Alice Nachrichten senden, die nur Alice wieder entschlüsseln kann. Allerdings kann JEDE(R) eine solche Nachricht verfassen - die Integrität der Nachricht (Wurde die Nachricht im Nachhinein verändert?) und die Authentizität des Absenders (Stammt die Nachricht wirklich von Bob?) bleiben also ungeklärt. Doch bietet die asymmetrische Kryptographie auch für diese Herausforderung eine elegante Lösung: Eine so genannte "Hash-Funktion" liefert für eine bestimmte Folge von Zeichen immer denselben Wert. Verändert man auch nur ein Zeichen der Folge, fügt man ein Zeichen hinzu oder entfernt man ein Zeichen, so ergibt sich stets ein anderer Hashwert. Du kannst die Entwicklung des Hashwerts beim Verfassen einer Nachricht im Feld Hashwert verfolgen!

Sende ich nun den Hashwert meiner Nachricht zusätzlich zur eigenen Nachricht, so kann der Empfänger den Hashwert der empfangenen Nachricht berechnen und das Ergebnis mit dem der Nachricht beigefügten ursprünglichen Nachricht vergleichen - jegliche Veränderung lässt sich so auf einen Blick feststellen!

Doch könnte jemand, der die Nachricht auf dem Kommunikationsweg verändert auch den Hashwert verändern, so dass der zur veränderten Nachricht passt - die Veränderung bleibt unbemerkt! Auch könnte die Nachricht nach wie vor von jemand ganz anderem verfasst worden sein, der den passenden Hashwert ermittelt und angehängt hat. Um zu zeigen, dass Bob und kein anderer als er genau diese Nachricht verfasst hat, verschlüsselt er den Hashwert mit seinem eigenen privaten Schlüssel. Aus dem Hashwert wird die "digitale Unterschrift" - auch "**digitale Signatur**" genannt. Nun kann jeder mit Bobs öffentlichem Schlüssel den Hashwert der Nachricht wieder entschlüsseln - es ist aber eindeutig belegt, dass die Signatur nur mit Bobs privatem Schlüssel erstellt worden sein kann.

Damit das Vertrauen in die digitale Unterschrift bestehen bleibt, müssen alle Teilnehmer gut auf ihre privaten Schlüssel aufpassen. In Programmen, die solche Schlüssel verwalten, werden die Dateien, in denen ein privater Schlüssel gespeichert ist, deshalb oft selbst mit einer Passworteingabe vor unbefugtem Benutzen des Schlüssels geschützt!

**Aufgabe:**

Öffne die Animation „Integrität und Authentizität mit digitaler Unterschrift sicherstellen“ und sende eine digital signierte Nachricht an Alice:

- Verschlüssle dazu zunächst die Nachricht mit Alices öffentlichem Schlüssel! (Anleitung siehe „Vertraulichkeit durch asymmetrische Kryptologie herstellen“)
- Kopiere den Hashwert der verschlüsselten Nachricht als Signatur, indem Du im Bereich von Bobs Computer auf den Knopf "V" klickst.
- Verschlüssle nun den Hashwert mit Bobs eigenem privaten Schlüssel: Klicke erst auf das Tresor-Symbol ( ) um Bobs privaten Schlüssel und dann auf den Knopf "Schlüssel auf Signatur anwenden" unterhalb des Signatur-Eingabefelds!
- Versende die Nachricht an Alice (Knopf "<<") und wechsle in die Rolle von Alice!
- Überprüfe in der Rolle von Alice zunächst Integrität und Authentizität der Nachricht, indem Du die erhaltene Signatur mit Bobs öffentlichem Schlüssel entschlüsselst: Klicke erst auf das Webseiten-Symbol ( ) um Bobs öffentlichen Schlüssel und dann auf den Knopf "Schlüssel auf Signatur anwenden" unterhalb des Signatur-Eingabefelds im Bereich von Alices Computer! Stimmt der Hashwert der verschlüsselten Nachricht mit der entschlüsselten Signatur überein? Dann kann die Nachricht in dieser Form nur von Bob sein!
- Entschlüssle nun die eigentliche Nachricht mit Alices privatem Schlüssel! (Anleitung siehe „Vertraulichkeit durch asymmetrische Kryptologie herstellen“)