# Vertraulichkeit mit asymmetrischer Kryptographie herstellen


Eine E-Mail lässt sich bekanntlich nicht mit einem Vorhängeschloss verschließen. Die in der zweiten Hälfte des 20. Jahrhunderts entwickelte **asymmetrische Kryptographie** ermöglicht es, Ver- und Entschlüsseln von Zahlen und Texten mit zwei verschiedenen Schlüsseln zu realisieren, so dass man nicht mehr geheime Schlüssel austauschen muss. Weil dieses Verfahren aufwendiger ist als symmetrische Verschlüsselung, wird es meist benutzt, um Schlüssel für eine symmetrische Verschlüsselung auf einem sicheren Weg auszutauschen. Viele Online-Shops und Online-Banking-Portale nutzen dieses Verfahren, um die Daten ihrer Kunden zu schützen.

Öffne die Animation „*Vertraulichkeit durch asymmetrische Kryptologie herstellen*“, mit der Du das Prinzip der asymmetrischen Kryptographie mit öffentlichen und privaten Schlüsseln kennen lernst!

Wenn die Animation geladen wird bist Du in der Rolle von Bob. Bob hat zwei Schlüssel: den vom Webseiten-Symbol ( ) umgeben **öffentlichen Schlüssel**, den er im Internet veröffentlicht hat, und den vom Tresor-Symbol ( ) umgeben **privaten Schlüssel**, den er sicher verwahrt und niemand anderem mitteilt. Über das Internet kann Bob auch den öffentlichen Schlüssel von Alice lesen, den sie dort veröffentlicht hat.

Will Bob Alice nun eine geheime Nachricht schreiben, die nur Alice wieder entschlüsseln kann, so sollte er seine Nachricht mit dem öffentlichen Schlüssel von Alice verschlüsseln. Helfe Bob dabei:

- Klicke dazu zunächst auf das Webseiten-Symbol ( ), das den öffentlichen Schlüssel von Alice umgibt, um diesen Schlüssel in die Felder "anzuwendender Schlüssel" auf Bobs Computer zu kopieren!
- Klicke dann im Bereich von Bobs Computer auf den Knopf "Schlüssel auf Nachricht anwenden", um die Nachricht mit dem zuvor kopierten Schlüssel zu verschlüsseln!
- Klicke nun im Bereich von Bobs Computer auf den Knopf "<<", um die verschlüsselte Nachricht über das Internet an Alice zu versenden!

Nun ist Alice am Zug, sie möchte die Nachricht von Bob entschlüsseln:

- Klicke auf den Knopf "Alice" oben links, um in die Rolle von Alice zu wechseln!
- Klicke dann auf das Tresor-Symbol ( ), das den privaten Schlüssel von Alice umgibt, um den privaten Schlüssel in die Felder "anzuwendender Schlüssel" auf Alices Computer zu laden!
- Klicke nun im Bereich von Alices Computer auf den Knopf "Schlüssel auf Nachricht anwenden", um die Nachricht mit dem zuvor kopierten Schlüssel zu entschlüsseln!

Die Nachricht ist ausgetauscht, ohne dass der Klartext im Internet zu lesen war. Im Unterschied zu symmetrischen Verfahren mussten Alice und Bob jedoch niemals ihre geheimen Schlüssel austauschen!

**Aufgaben:**

1. Alice möchte Bob - und nur Bob und nicht ihren Eltern, deren Computer sie benutzt! - den Namen ihrer neuen Lieblingsband mitteilen. Zeige was Alice und Bob machen, so dass Bob die Nachricht von Alice auf sicherem Wege erfährt!

   *Hinweis:* Diese Simulation unterstützt nur die Verschlüsselung von Kleinbuchstaben, Punkt und Komma – Zahlen sollten daher ausgeschrieben werden!

2. Verfasse einen Lexikon-Eintrag, der erklärt, wie mit asymmetrischer Kryptographie Ver- und Entschlüsseln kann, ohne vorher geheime Informationen austauschen kann!
3. *für Schnelle:* Könnte es Sinn machen, eine Nachricht mit dem privaten Schlüssel zu verschlüsseln?