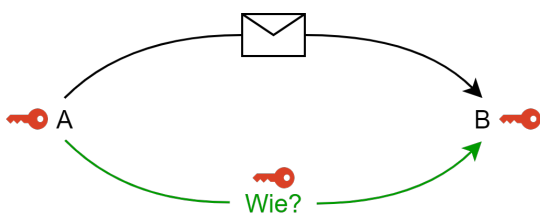


Symmetrische & Asymmetrische Verschlüsselung

→ Verschlüsselung dient dazu, dass eine gesendete Nachricht nicht so leicht ausgelesen werden kann, falls sie abgefangen wird.

Beispiel: Alice möchte Bob eine verschlüsselte Nachricht zukommen lassen.

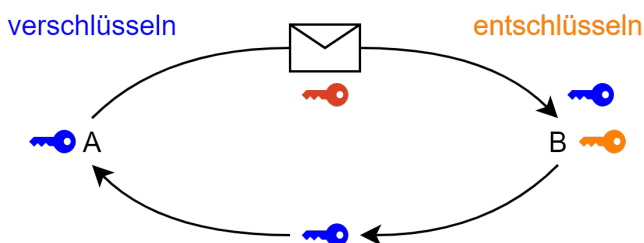
1. Die Nachricht wird symmetrisch verschlüsselt, da mit symmetrischer Verschlüsselung große Datenmengen schnell verschlüsselt werden können.



Um die Nachricht zu ver- und entschlüsseln, wird ein

symmetrischer Schlüssel verwendet. Diesen muss Alice Bob zukommen lassen. Das nennt man **das Schlüsselaustauschproblem**.

2. Der symmetrische Schlüssel wird asymmetrisch verschlüsselt um das Schlüsselaustauschproblem zu lösen.



Um den **symmetrischen Schlüssel** zu

verschlüsseln, verwendet Alice den **öffentlichen Schlüssel** von Bob. Die Nachricht wird versendet. Zum Entschlüsseln verwendet Bob **seinen privaten Schlüssel**. Den öffentlichen Schlüssel erhält Alice vorher von Bob. Zum Beispiel per E-Mail.

Diese Kombination der symmetrischen Verschlüsselung und asymmetrischen

Verschlüsselung nennt sich **hybride Verschlüsselung**.

Revision #3

Created 19 January 2022 10:28:31 by Martin Tienken

Updated 28 February 2022 13:32:01 by Martin Tienken