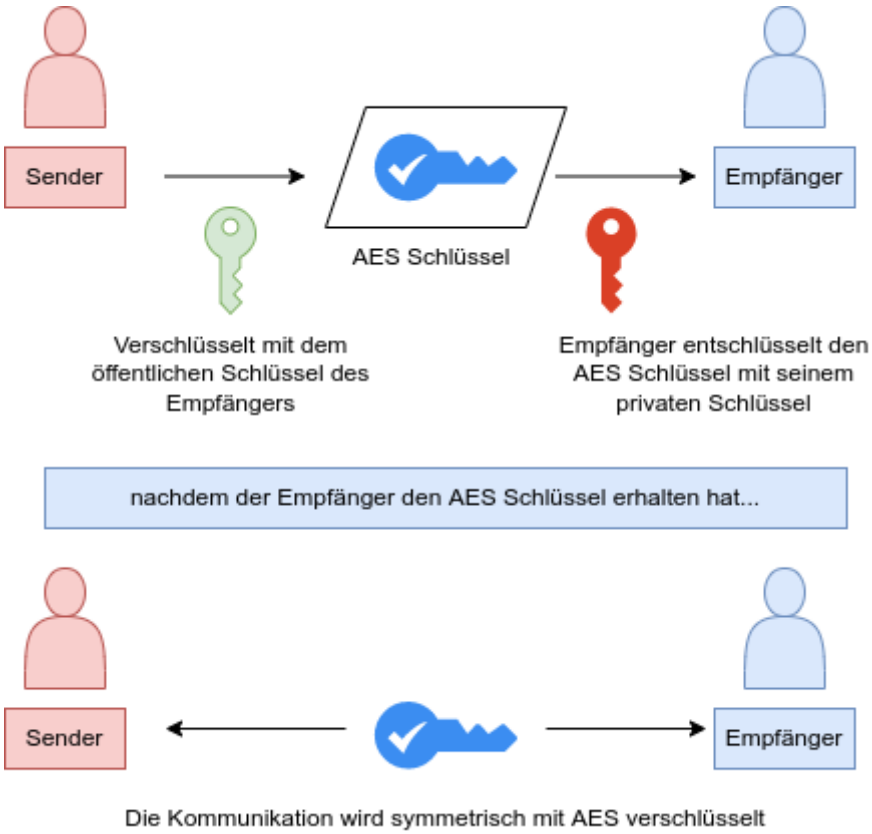
Hybride Verschlüsselung

RSA und andere Public-Key-Verschlüsselungsverfahren haben einen entscheiedenden Nachteil: Sie sind relativ **rechenaufwändig** und damit **langsam**. Eine RSA-Entschlüsselung ist etwa um den Faktor 1.000 langsamer als der gleiche Vorgang beim AES. Auch eine RSA-Verschlüsselung mit einer kleinen Primzahl ist noch deutlich aufwendiger als eine AES-Verschlüsselung.

Wenn längeren Nachrichten zudem auf einzelne Blöcke aufgeteilt werden müssen, die dann nacheinander verschlüsselt werden, schlagen solche Performanceprobleme unangehnehm zu Buche.

RSA und andere Public-Key-Verschlüsselungsverfahren werden daher in der Praxis fast nie verwendet, um ganze Nachrichten oder Kommunikationsvorgänge zu verschlüsseln. Meist wird damit lediglich ein Schlüssel (Sitzungsschlüssel) für ein symmetrisches Verfahren übermittelt, um damit den Rest der Kommunikation zu verschlüsseln. Also wird RSA in der Praxis häufig nicht als Verschlüsselungsverfahren, sondern als **Schlüsselaustauschverfahren** eingesetzt. Die gemeinsame Verwendung von asysmmetrischer und symmetrischer Verschlüsselung auf diese Weise wird **Hybridverfahren** genannt.



From:
https://www.info-bw.de/ -

Permanent link:
https://www.info-bw.de/faecher:informatik:oberstufe:kryptographie:hybrideverfahren:start?rev=1648744149

Last update: **31.03.2022 16:29**