**Hybride Verschlüsselung**

Definition: Bei der hybriden Verschlüsselung werden die symmetrischen Verschlüsselung und die asymmetrische Verschlüsselung kombiniert. Dies kombiniert die Vorteile der beiden Verschlüsselungsmethoden - Geschwindigkeit (symmetrische Verschlüsselung) und Sicherheit (asymmetrische Verschlüsselung).

Die Verschlüsselung der eigentlichen Daten erfolgt per symmetrischer Verschlüsselung. Allerdings wird für jede Datenübertragung/ jede Datei ein eigener Schlüssel generiert (session key), der per asymmetrischer Verschlüsselung dem/ den Kommunikationspartnern übermittelt bzw. der eigentlichen Nachricht angehängt wird. Da es sich bei einem Schlüssel nur um sehr wenige Daten (wenige hundert Bit - vgl. Schlüssellängen) handelt, fällt hier der Nachteil der langsamen asymmetrischen Verschlüsselung praktisch nicht ins Gewicht.

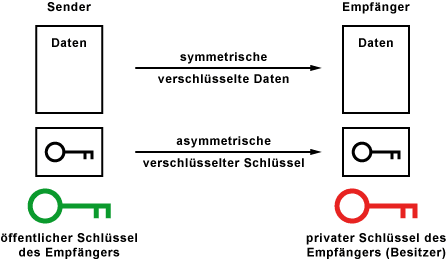


Bild 1: Prinzip hybrider Verfahren

Siehe auch: symmetrische Verschlüsselung, asymmetrische Verschlüsselung

Quellenverzeichnis:

Wikimedia Foundation Inc. und Andere auf wikipedia.org,

URL: <https://de.wikipedia.org/wiki/Computerwurm> (Stand: 26.04.2017)

Klaus Lipinski, Dipl.-Ing. (V.i.S.d.P.) auf ITwissen.info,

URL: <http://www.itwissen.info/Hybrid-Verschluesselung-hybrid-encryption.html> (Stand: 26.04.2017)

Patrick Schnabel auf Elektronik-Kompendium.de,

URL: <http://www.elektronik-kompendium.de/sites/net/1910141.htm> (Stand: 26.04.2017)

Gerhard Glaser auf Trojaner-und-Sicherheit.de,

URL: <http://www.trojaner-und-sicherheit.de/security/verschluesselung.htm> (Stand: 26.04.2017)

Bild 1: <http://www.elektronik-kompendium.de/sites/net/bilder/09080714.gif> (Stand: 26.04.2017)