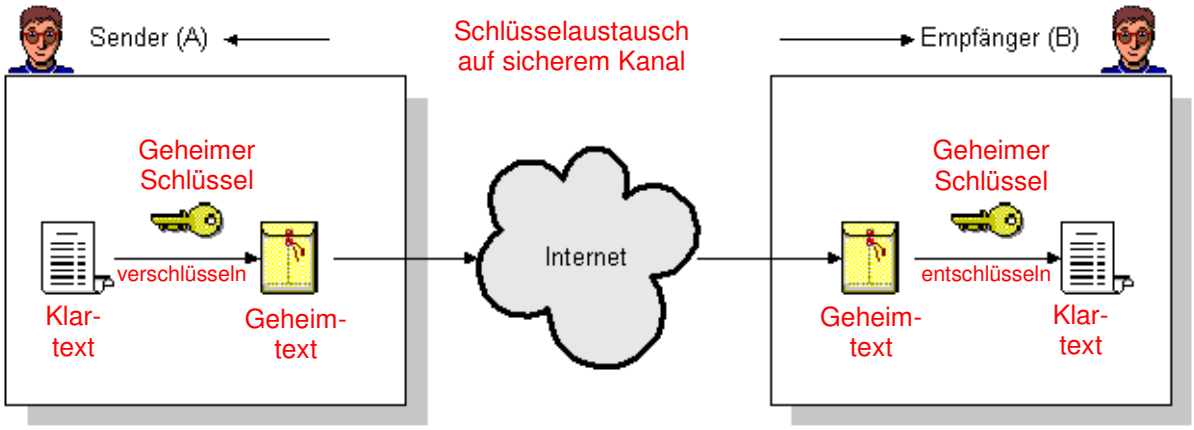
Symmetrische und asymmetrische Verschlüsselung

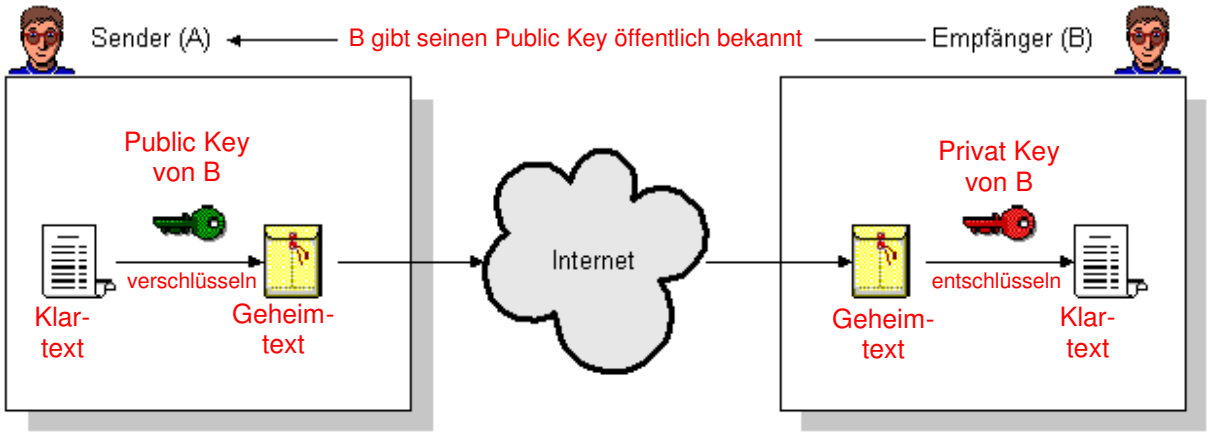
Schema der symmetrischen Verschlüsselung



Definition der symmetrischen Verschlüsselung

Bei der symmetrischen Verschlüsselung kennen und benutzen Sender und Empfänger für die Ver- und Entschlüsselung einer Nachricht den gleichen geheimen Schlüssel. Das Hauptproblem hierbei ist, dass sich Sender und Empfänger auf den gleichen geheimen Schlüssel einigen, ohne dass ihn ein Dritter erfährt.

Schema der asymmetrischen Verschlüsselung



Definition der asymmetrischen Verschlüsslung

Das Konzept der asymmetrischen Verschlüsselung wurde 1976 von Whitfield Diffie und Martin Hellman vorgeschlagen, um das Problem zu lösen, dass bei symmetrischer Verschlüsselung der geheime Schlüssel zwischen den Kommunikationspartnern ausgetauscht werden muss. Jeder Beteiligte hat zwei Schlüssel, einen öffentlichen (Public Key) und einen privaten (Privat Key). Der Public Key wird veröffentlicht und der Privat Key bleibt geheim. Die Notwendigkeit eines gemeinsamen Geheimnisses zwischen Sender und Empfänger ist damit verschwunden. Jede Kommunikation verwendet nur öffentliche Schlüssel, private Schlüssel werden nie übertragen. Jeder, der eine wichtige Information versenden will, chiffriert mit dem öffentlichen Schlüssel des Empfängers. Nur der Empfänger kann den geheimtext mit seinem Privat Key entschlüsseln. Eine Entschlüsselung mit dem Public Key ist nicht möglich!