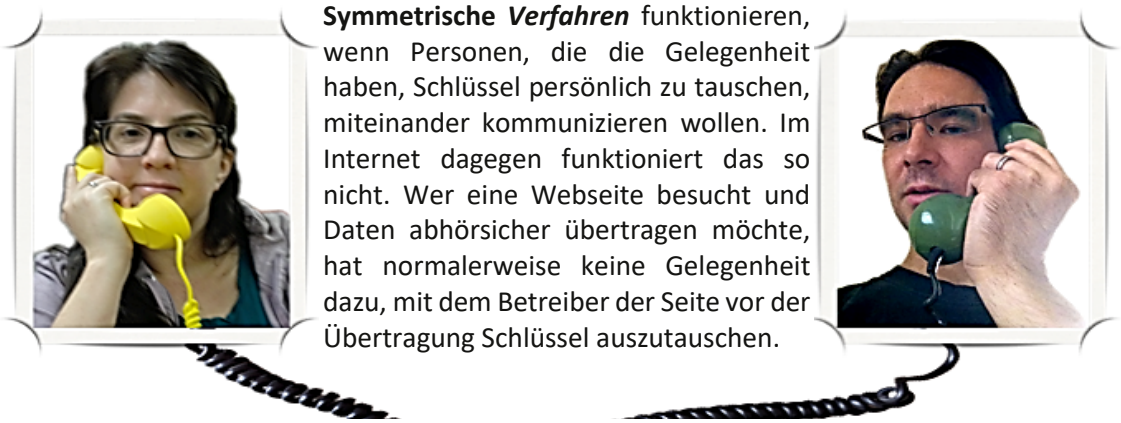
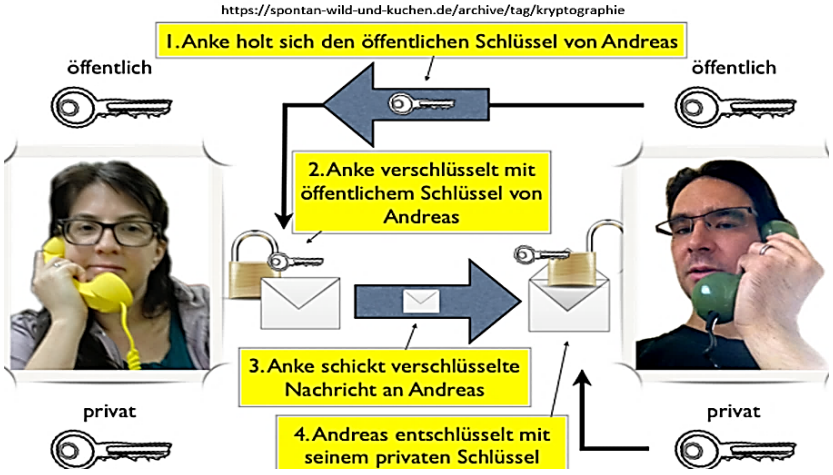
Praktische Anwendung assymetrischer Verschlüsselungen - Zertifikate



Symmetrische *Verfahren* funktionieren, wenn Personen, die die Gelegenheit haben, Schlüssel persönlich zu tauschen, miteinander kommunizieren wollen. Im Internet dagegen funktioniert das so nicht. Wer eine Webseite besucht und Daten abhörsicher übertragen möchte, hat normalerweise keine Gelegenheit dazu, mit dem Betreiber der Seite vor der Übertragung Schlüssel auszutauschen.

Asymmetrische Verschlüsselungsverfahren arbeiten mit zweigeteilten Schlüsseln. Der Schlüssel, der zum Chiffrieren einer Nachricht verwendet wird, ist ein anderer als der, mit dem die Nachricht entschlüsselt werden kann. Da es mit ersterem Schlüssel nicht möglich ist, einen Geheimtext wieder zu dechiffrieren, ist er öffentlich. Nur der zweite Schlüssel muss geheim gehalten werden und nur der Empfänger kennt ihn. Es entfällt die Notwendigkeit, einen n Schlüssel über einen sicheren Kanal auszutauschen. Dafür nutzt man den auf **Einwegfunktionen** basierenden **RSA-Algorithmus**.



Ende zu Ende Verschlüsselung
Die Verbindung ist sicher, wenn die Nachricht beim Sender verschlüsselt und beim Empfänger wieder entschlüsselt wird, die Nachricht also auf der ganzen Strecke verschlüsselt bleibt.

Anwendungen:
HTTPS, WhatsApp, Threma

Wie kann Anke sicher sein, dass der öffentliche Schlüssel von Andreas wirklich ihm gehört und nicht heimlich von einem Bösewicht ersetzt wurde? Das nennt man **Man-in-the-Middle-Attack.**
Wir wollen z.B. Online-Banking betreiben, haben den öffentlichen Schlüssel der Bank und senden unsere Überweisungsdaten. Um uns zu täuschen, könnte ein Angreifer unsere Anfrage und die Antwort der Bank mithören, um im entscheidenden Moment, wenn wir eine Überweisung tätigen, seine eigene Kontonummer und einen höheren Betrag einzusetzen.
Wir brauchen also eine Garantie, dass der öffentliche Schlüssel echt ist. Die Lösung besteht darin, dass eine dritte Stelle, der sowohl Anke als auch Andreas (die Bank) vertrauen, den öffentlichen Schlüssel von Andreas (der Bank) digital signiert, also **Zertifikat** erstellt hat, das die Echtheit garantiert.

Wenn man mal bei einer Webseite, die mit HTTPS beginnt, auf der Adresszeile des Browsers an die richtige Stelle klickt, bekommen wir die wichtigsten Informationen eines solchen Zertifikats angezeigt.