ASYMMETRISCHE VERSCHLÜSSELUNG (Z. B. VIA PGP):

Bei der symmetrischen Verschlüsselung gibt es *einen* Schlüssel, mit dem eine Nachricht verschlüsselt und dann wieder entschlüsselt werden kann: derselbe Schlüssel verschlüsselt und entschlüsselt: Wenn man beispielsweise ein Zip-Archiv mit dem Passwort „Geheim123!“ verschlüsselt, dann kann es jeder öffnen, der ebendiesen Schlüssel „Geheim123!“ in die entsprechende Eingabeaufforderung eingibt.

Bei der asymmetrischen Verschlüsselung gibt es zwei unterschiedliche Schlüssel – ein Schlüsselpaar. Der eine Schlüssel dient zum Verschlüsseln einer Nachricht – der andere dient dazu, diese Nachricht wieder zu entschlüsseln. Man kann also nicht mit demselben Schlüssel verschlüsseln und entschlüsseln!

Das Schlüsselpaar bei der asymmetrischen Verschlüsselung besteht aus einem öffentlichen Schlüssel (*public key*) und einem privaten Schlüssel (*private key*). Beide Schlüssel werden zusammen erzeugt und gehören zusammen.
Der öffentliche Schlüssel wird veröffentlicht. Er ist öffentlich zugänglich: man kann ihn beispielsweise auf seiner Homepage für alle zugänglich hinterlegen.
Er dient dazu, eine Nachricht zu verschlüsseln. Ist eine Nachricht mit dem öffentlichen Schlüssel verschlüsselt worden, dann kann man diese Nachricht nicht mehr mit diesem öffentlichen Schlüssel entschlüsseln – das leistet nur der zugehörige private Schlüssel.
Der private Schlüssel wird geheim gehalten – man gibt ihn an niemanden weiter. Genau das ist das Besondere an diesem asymmetrischen Verfahren: bei der symmetrischen Verschlüsselung muss man seinen Schlüssel an alle Empfänger der Nachricht weitergeben, denn sonst können sie die Nachricht nicht entschlüsseln. Durch diese Weitergabe wird der Schlüssel aber unsicher: vielleicht verrät ihn jemand oder geht nicht sorgsam damit um? Vielleicht ist der Übertragungsweg dieses Schlüssels unsicher? – Weil bei der asymmetrischen Verschlüsselung der private Schlüssel nicht weitergegeben werden muss, ist es sicherer.

Wenn nun Mr. X an Mr. Y eine verschlüsselte Nachricht schicken möchte, dann verwendet er den öffentlichen Schlüssel von Mr. Y, den dieser auf seiner Homepage oder auf Nachfrage über einen ungesicherten E-Mail-Account gefahrlos zur Verfügung stellt. Die mit dem öffentlichen Schlüssel von Mr. Y verschlüsselte Nachricht mailt Mr. X nun an Mr. Y: er muss dazu keine Vorsichtsmaßnahen ergreifen: es ist egal, ob der E-Mail-Verkehr abgehört wird oder nicht, denn die Nachricht kann nur mit dem privaten Schlüssel von Mr. Y entschlüsselt werden. Wer die verschlüsselte Datei ohne den privaten Schlüssel von Mr. Y lesen möchte, bekommt nur wirre Zeichen zu sehen. Gelangt die Datei zu Mr. Y, dann kann er sie mit seinem privaten Schlüssel entschlüsseln. Und weil Mr. Y seinen privaten Schlüssel an niemanden weitergibt, kann einzig und alleine Mr. Y diese Nachricht lesen.

Man kann das Schlüsselpaar der asymmetrischen Kryptografie auch zur Signierung verwenden: Wenn ich möchte, dass eine Nachricht eindeutig mir als Autor zugeordnet werden soll, wenn ich also verhindern möchte, dass jemand in meinem Namen Nachrichten postet, dann kann ich meine Nachricht mit meinem privaten Schlüssel verschlüsselt veröffentlichen und gleichzeitig auf meinen öffentlichen Schlüssel auf meiner Homepage hinweisen. Nun kann jeder meine Nachricht mit meinem öffentlichen Schlüssel entschlüsseln – und weil diese Entschlüsselung nur funktioniert, wenn die Nachricht zuvor genau mit meinem privaten Schlüssel verschlüsselt worden ist, muss diese Nachricht eindeutig von mir stammen: ich habe meinen privaten Schlüssel nämlich keinem verraten und also kann nur ich alleine die Nachricht verschlüsselt haben, wenn sie sich mit meinem öffentlichen Schlüssel entschlüsseln lässt.
(Hier gibt es allerdings das Problem, dass jemand sich den öffentlichen Schlüssel kopieren könnte, er legt ihn auf seine Homepage und behauptet, es sei sein eigener öffentlicher Schlüssel: wenn der eigentliche Schlüsselbesitzer das nicht bemerkt, dann kann der Betrüger so tun, als sei er der Urheber der Nachricht – dagegen gibt es verschiedene Zertifizierungsmodelle)

- http://de.wikipedia.org/wiki/Asymmetrisches_Kryptosystem
- http://de.wikipedia.org/wiki/Pretty_Good_Privacy
- http://de.wikipedia.org/wiki/Public-Key-Infrastruktur