Symmetrische und asymmetrische Verschlüsselung (Einführung)

Arj / Sept-2015

Wenn etwas geheim oder
vertraulich sein soll,
schützen wir es
vor neugierigen Blicken!

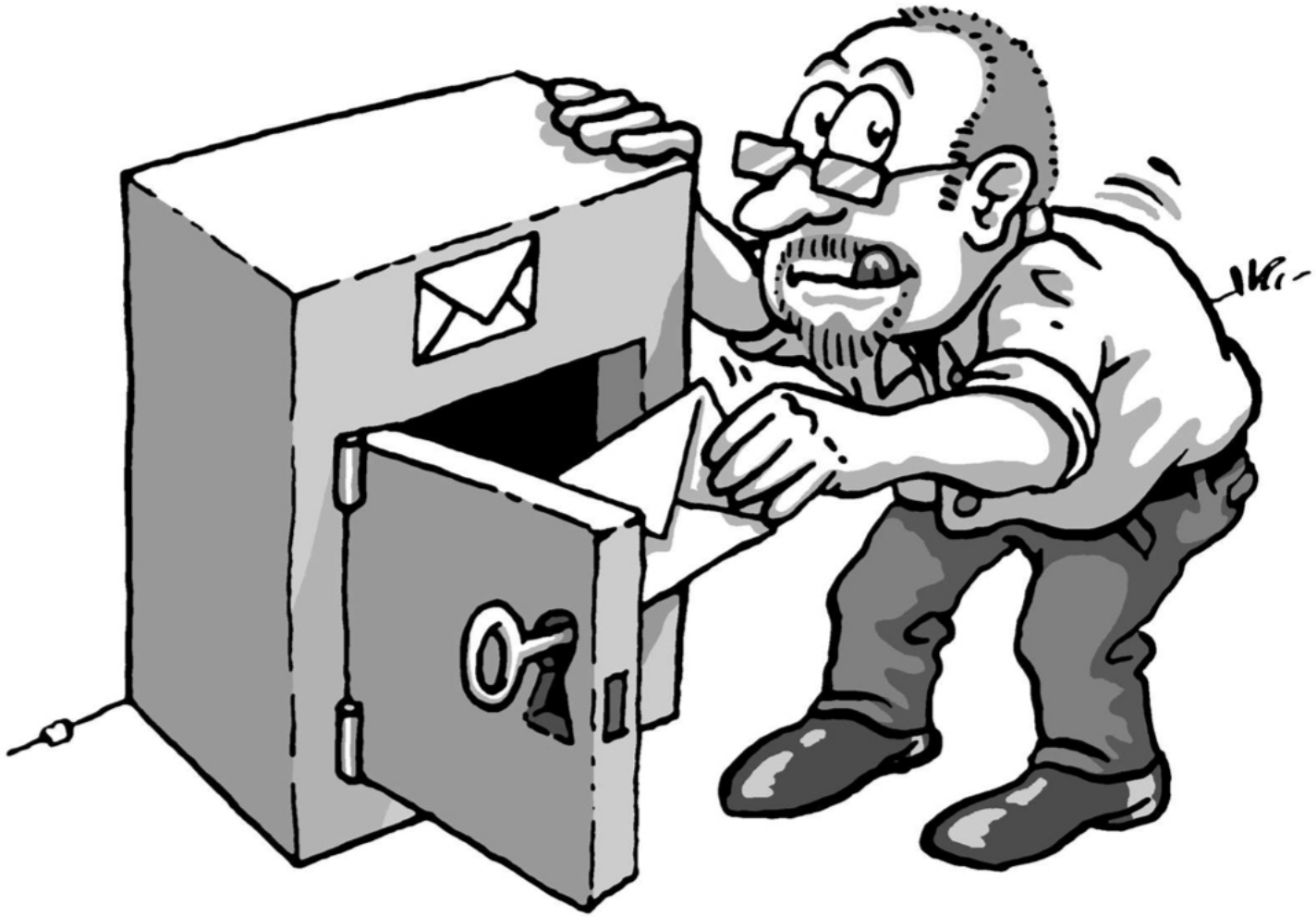
... oder man schliesst es
ein, mit einem Schlüssel,
den man sicher aufbewahrt!

Aber:

Fällt der Schlüssel in
falsche Hände,
ist's um die Geheim-
haltung geschehen!

Dieser Schlüssel ist also
genau so geheim,
wie die damit
verschlüsselte Botschaft!

Verschlüsselt und Entschlüsselt wird
mit demselben Schlüssel



Das Problem ist nur der sichere Schlüsseltausch...

... damit der Adressat, und nur dieser,
auf seine Mitteilung zugreifen kann!

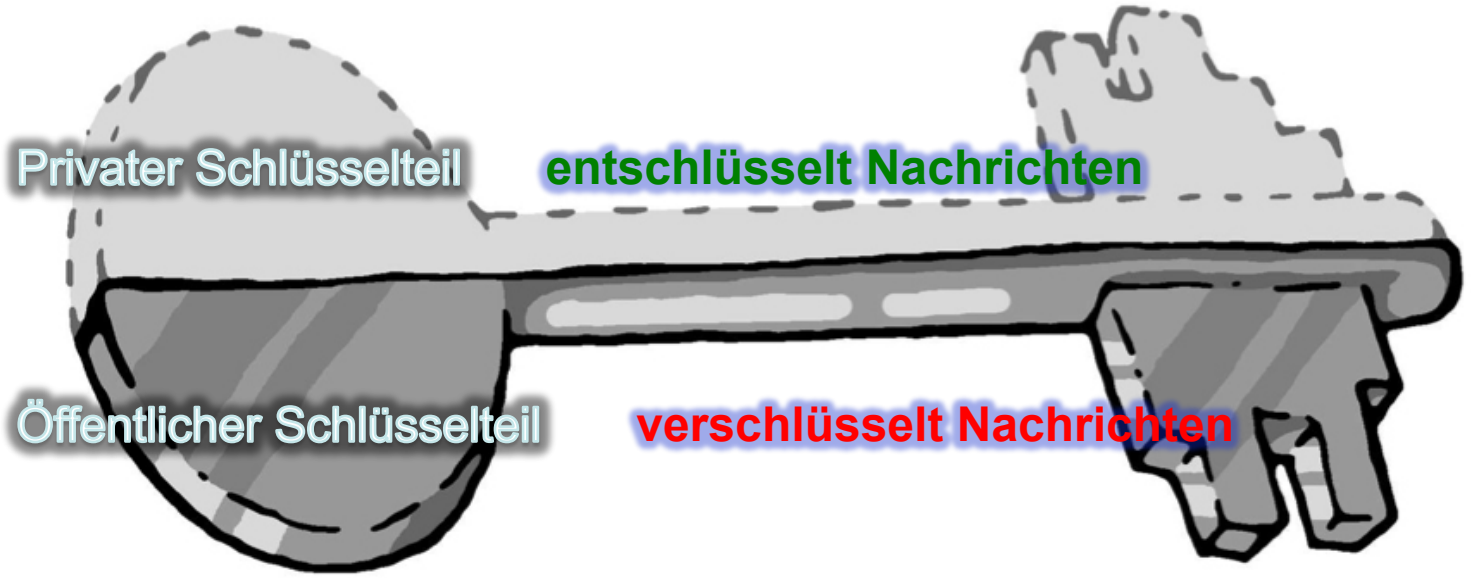
Das Verschlüsseln und Entschlüsseln der Botschaft mit demselben Schlüssel birgt Gefahr, weil:

- der Schlüssel wie auch die Botschaft geheim bleiben sollten
- der Schlüssel auf geheimen Weg dem Empfänger der Botschaft mitgeteilt werden muss
- und man bei dieser Gelegenheit auch gleich die geheime Botschaft austauschen könnte!

Man nennt dies symmetrische Verschlüsselung!

Der andere Ansatz: Ein zweiteiliger Schlüssel

Man nennt dies asymmetrische Verschlüsselung!



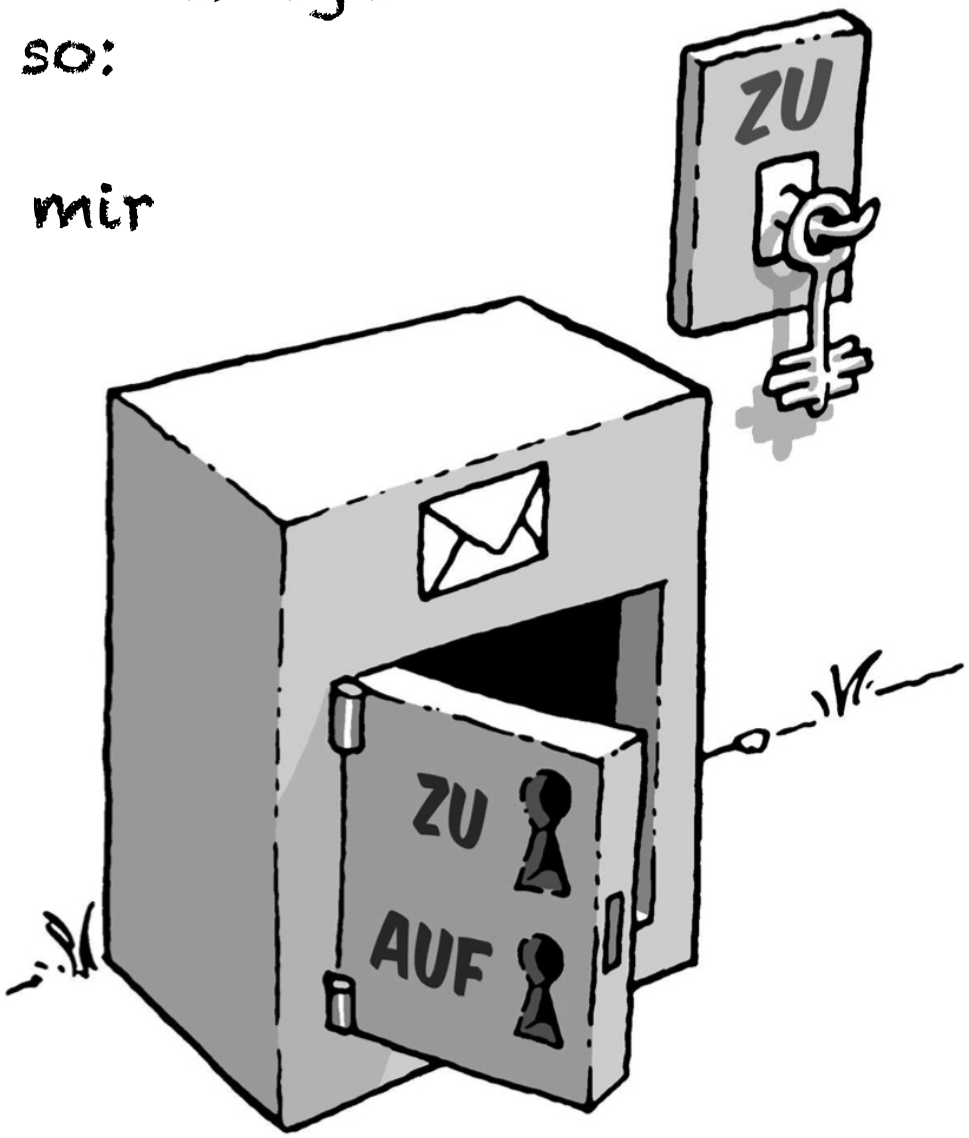
Das heisst:

Der öffentliche Schlüssel einer Person (Public-Key) kann von allen eingesehen werden.

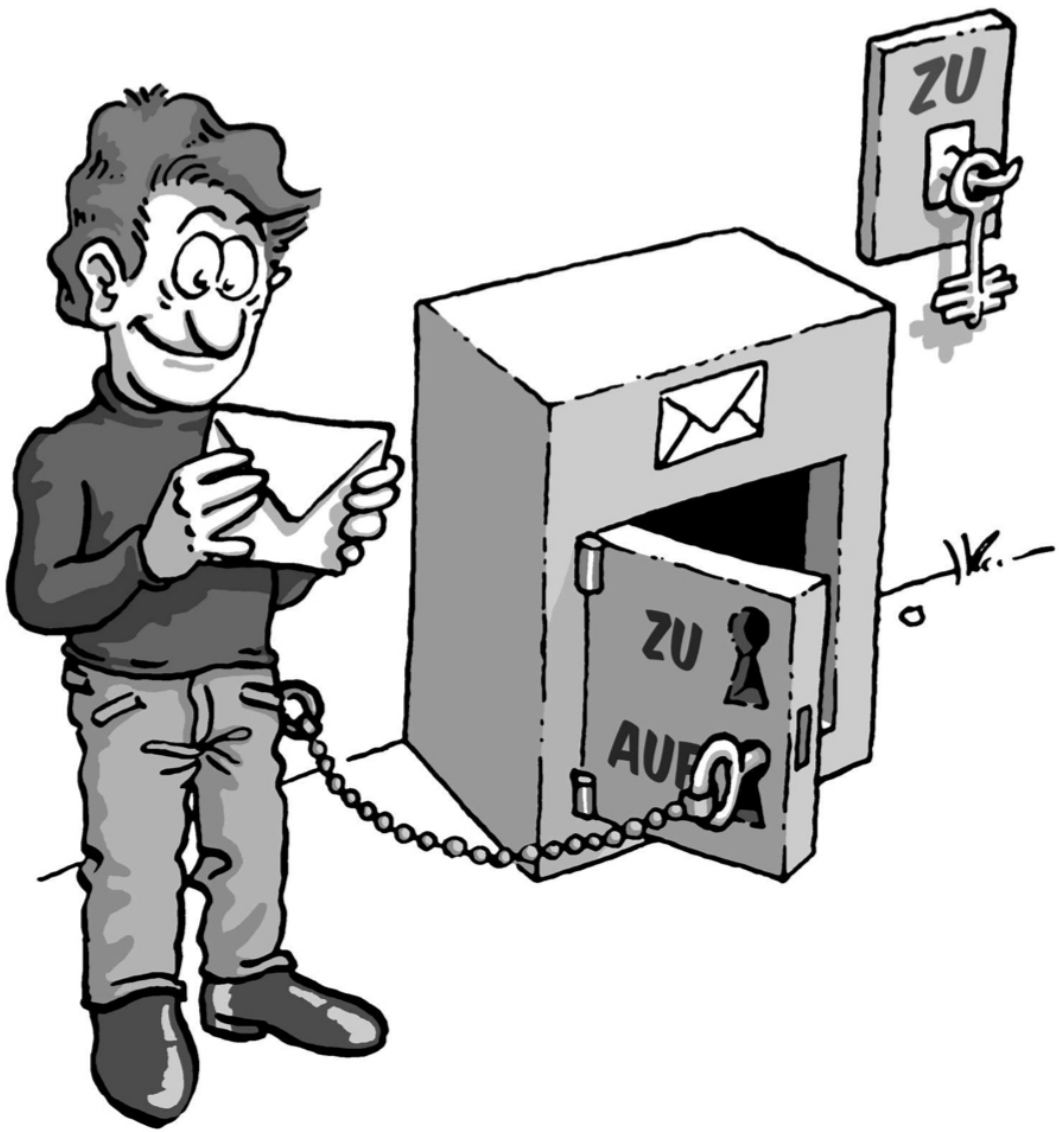
Wobei der private Schlüssel dieser Person (Private-Key) von ihr geheim gehalten wird.

Eine Botschaft zu hinterlegen funktioniert also so:

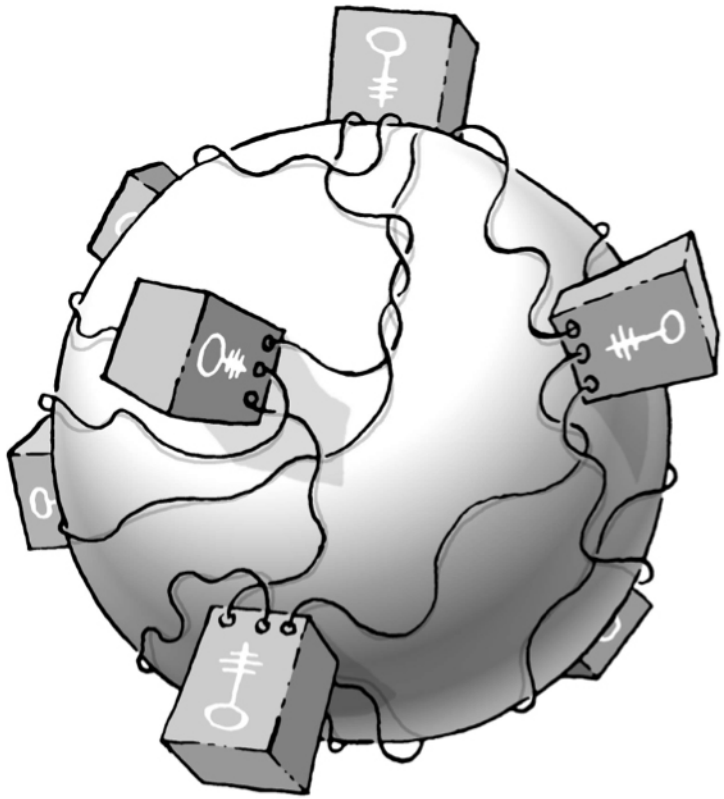
- Jederman kann mir eine Botschaft hinterlegen!
- Damit diese Botschaft auch geheim bleibt, schliesst der Absender den Safe mit meinem öffentlichen Schlüssel zu!



Nur ich, mit meinem privaten (geheimen) Schlüssel kann den Safe öffnen und die Botschaft lesen!



Wo erhalte ich den Public-Key einer Person, die nicht grad um die Ecke wohnt?



Nicht an der Frittenbude gegenüber sondern von global vernetzten Keyservern!

Dabei gelangen wir schon zur nächsten Hürde:
Wer garantiert mir die Echtheit von auf
Key-Servern hinterlegten Public-Keys?

Von X.509-Zertifizierungsstellen oder
Web-of-Trust oder PGP-Zertifizierungsstellen.