Vorab

- Kein Kryptoprofi, korrigiert mich gern
- wenn ich zu schnell bin, sagt Bescheid

Ich

- Fabian Blechschmidt (@Fabian_ikono)
- blechschmidt@fabian-blechschmidt.de
- PHP seit 2004
- Freelancer seit 2008
- Magento seit 2011
- Certified Magento Developer
- spielt gerne, aktuell mit
  - OWASP TOP10
  - Sicherheit
  - Passwörter

Verschlüsselungsverfahren

eine kleine Einführung

Verschlüsselung

Die Verschlüsselung ist die Umsetzung einer verständlichen Information in eine unverständliche: die Umsetzung eines Klartextes in einen Geheimtext.
[...]

(ITWissen)

Ich wollte keine Definition aus der Wikipedia, aber das ist zu detailliert wenn ihr mich fragt

Vertraulichkeit

Kann niemand sonst die Nachricht lesen

Authentizität

Reden die richtigen miteinander

Integrität

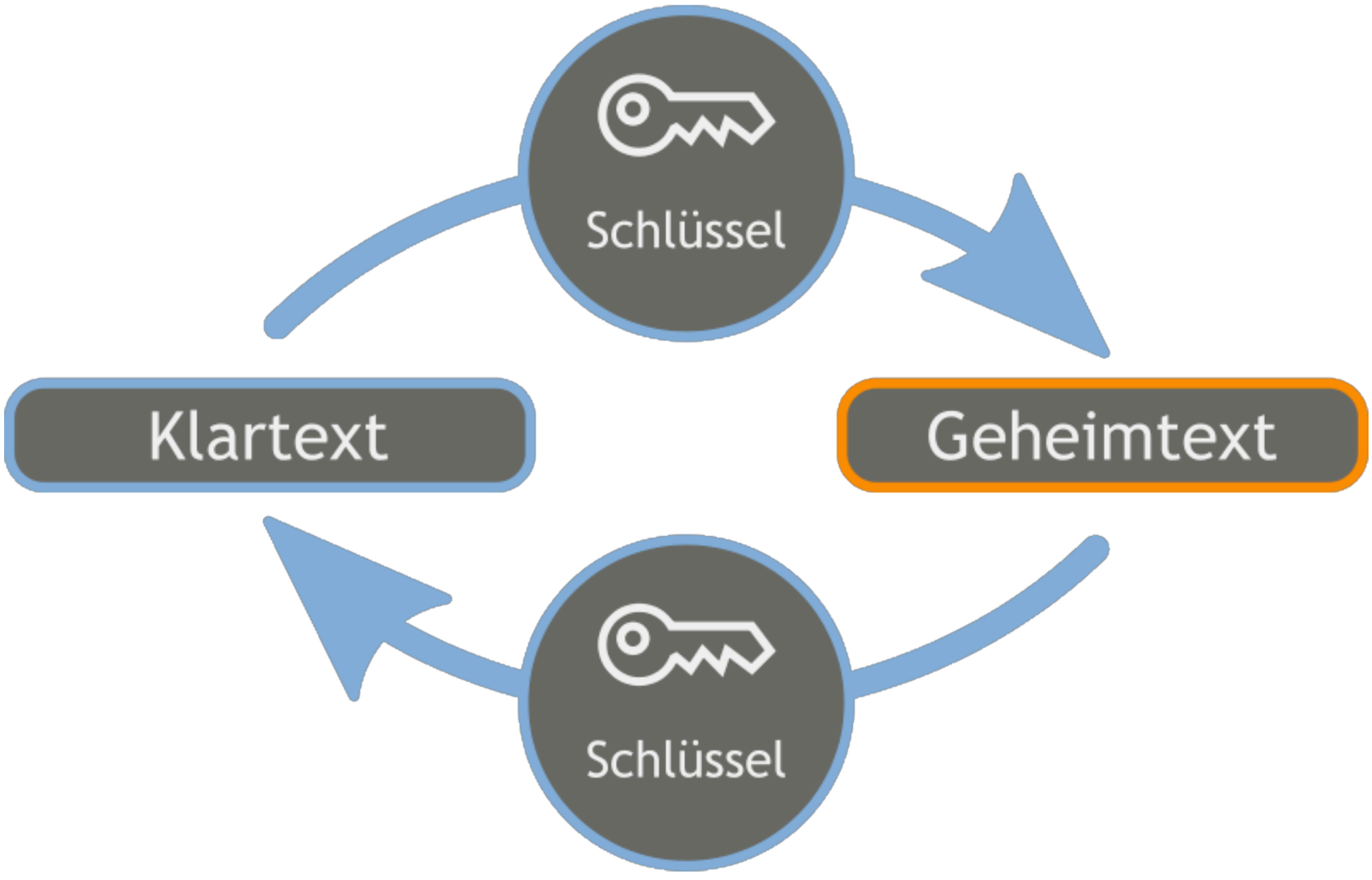
Daten verfälschen/ändern/löschen

Symmetrische und asymmetrische Verschlüsselung

Symmetrische Verschlüsselung

Schlüssel gleich

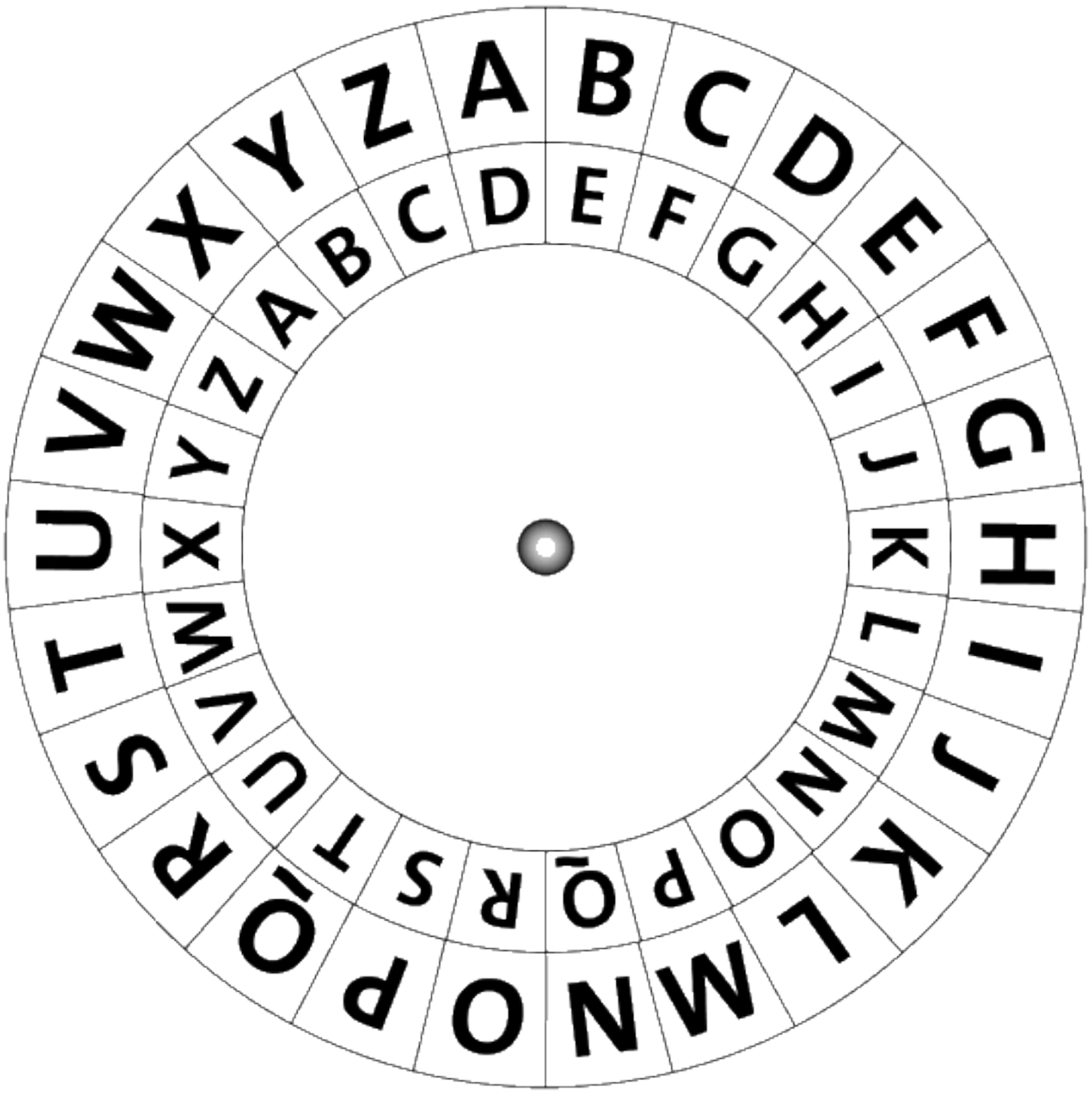
Schlüssel gleich heißt man muss nicht nur die Nachricht übertragen, sondern auch die Schlüssel. Früher geschah das über einen Boten, aber der braucht halt seine Zeit



http://commons.wikimedia.org/wiki/File:Orange_blue_symmetric_cryptography_de.svg

Cäsar Chiffre

einfachstes Beispiel



http://kickundklick.fh-trier.de/Kryptographie/Kryptobilder/caesar-scheibe%2001.gif

Kennt man aus der Mickey Mouse oder der Ypps

Vertraulichkeit, Authentizität,(Integrität)?

nur gemeinsam

Asymmetrische Verschlüsselung

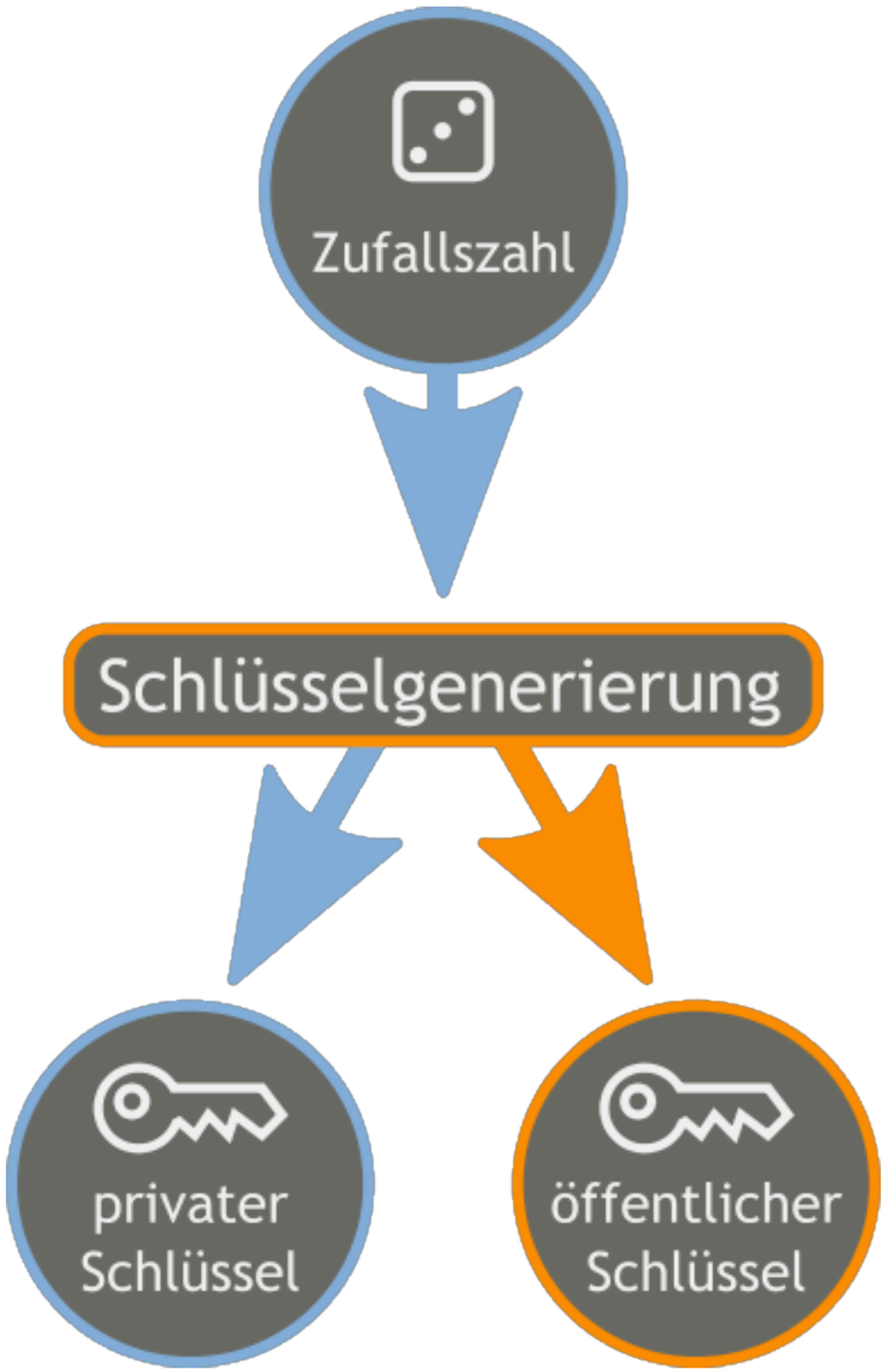
Mathematische Probleme

Leicht lösbar in eine Richtung, aber verdammt schwer in die andere

Primzahlzerlegung/Multiplikation

$$x * y = 1233625093$$

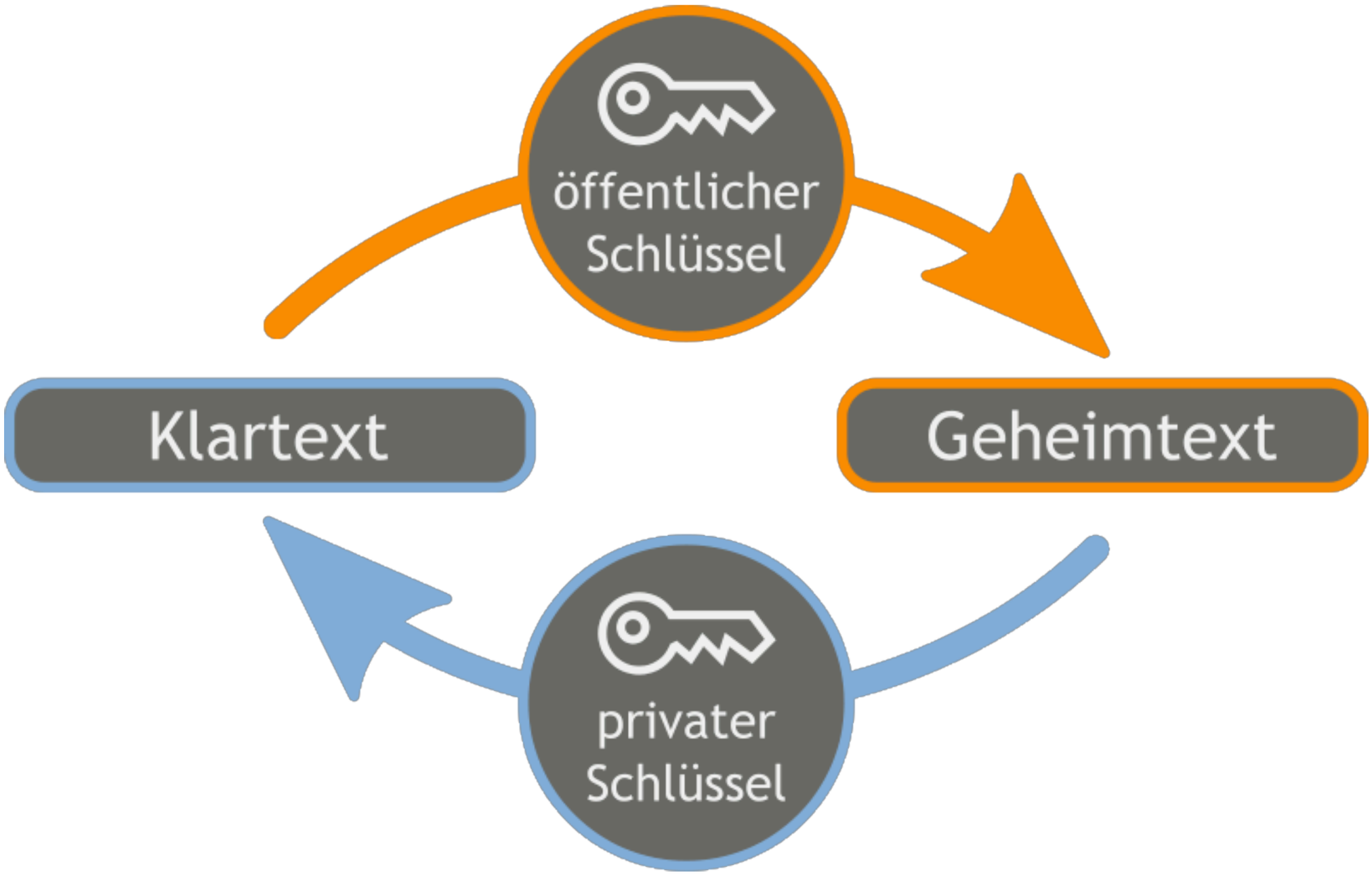
$$35117 \times 35129 = 1233625093$$



http://commons.wikimedia.org/wiki/File:Orange_blue_public_private_keygeneration_de.svg

Schlüssel technisch gleich

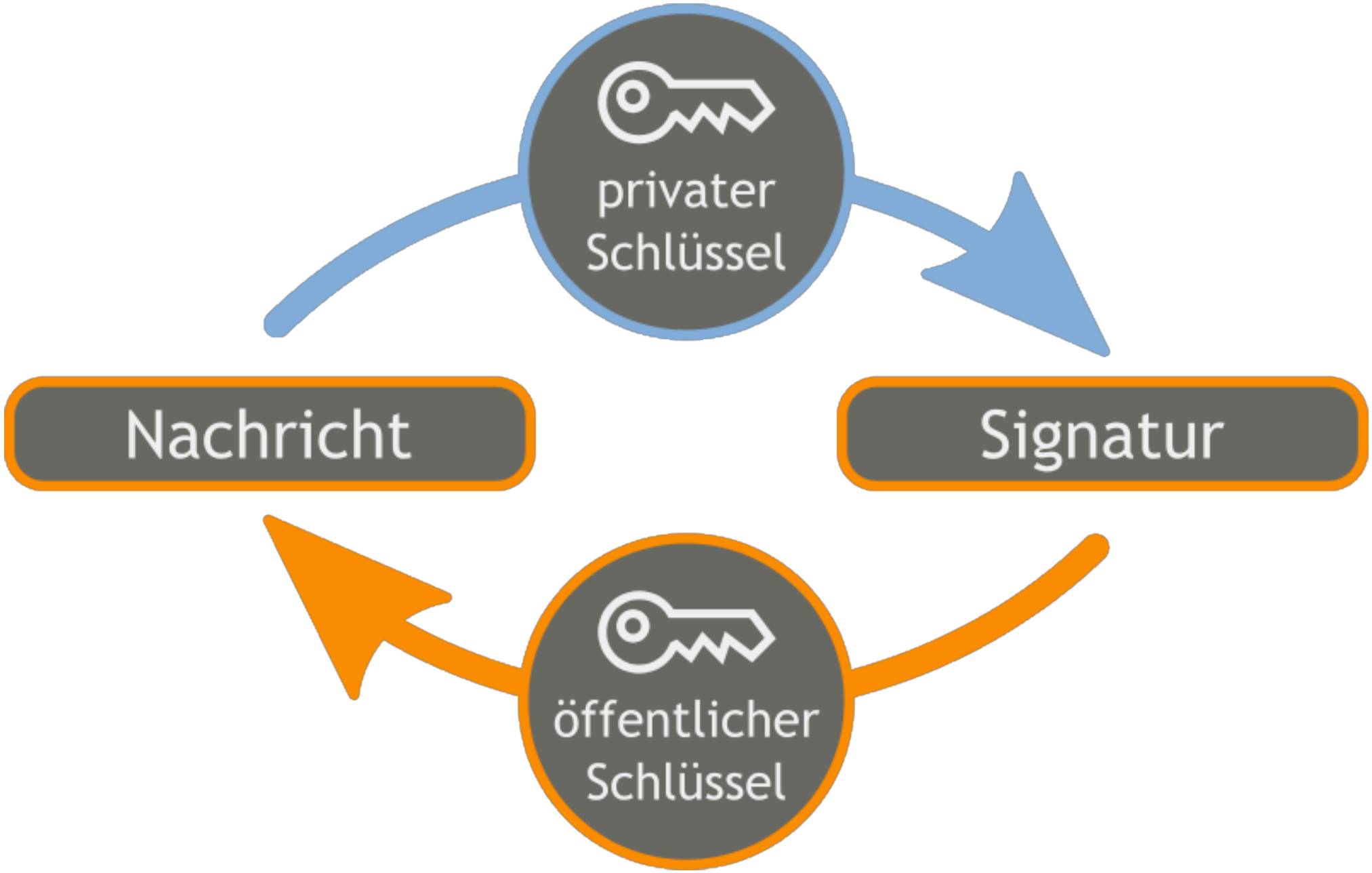
Öffentlicher und Privater Schlüssel sind technisch gleich und austauschbar.



http://commons.wikimedia.org/wiki/File:Orange_blue_public_key_cryptography_de.svg

Vertraulichkeit, Authentizität,(Integrität)?

Authentizität (Signieren)



http://commons.wikimedia.org/wiki/File:Orange_blue_digital_signature_de.svg

Signieren, Verschlüsseln

vs.

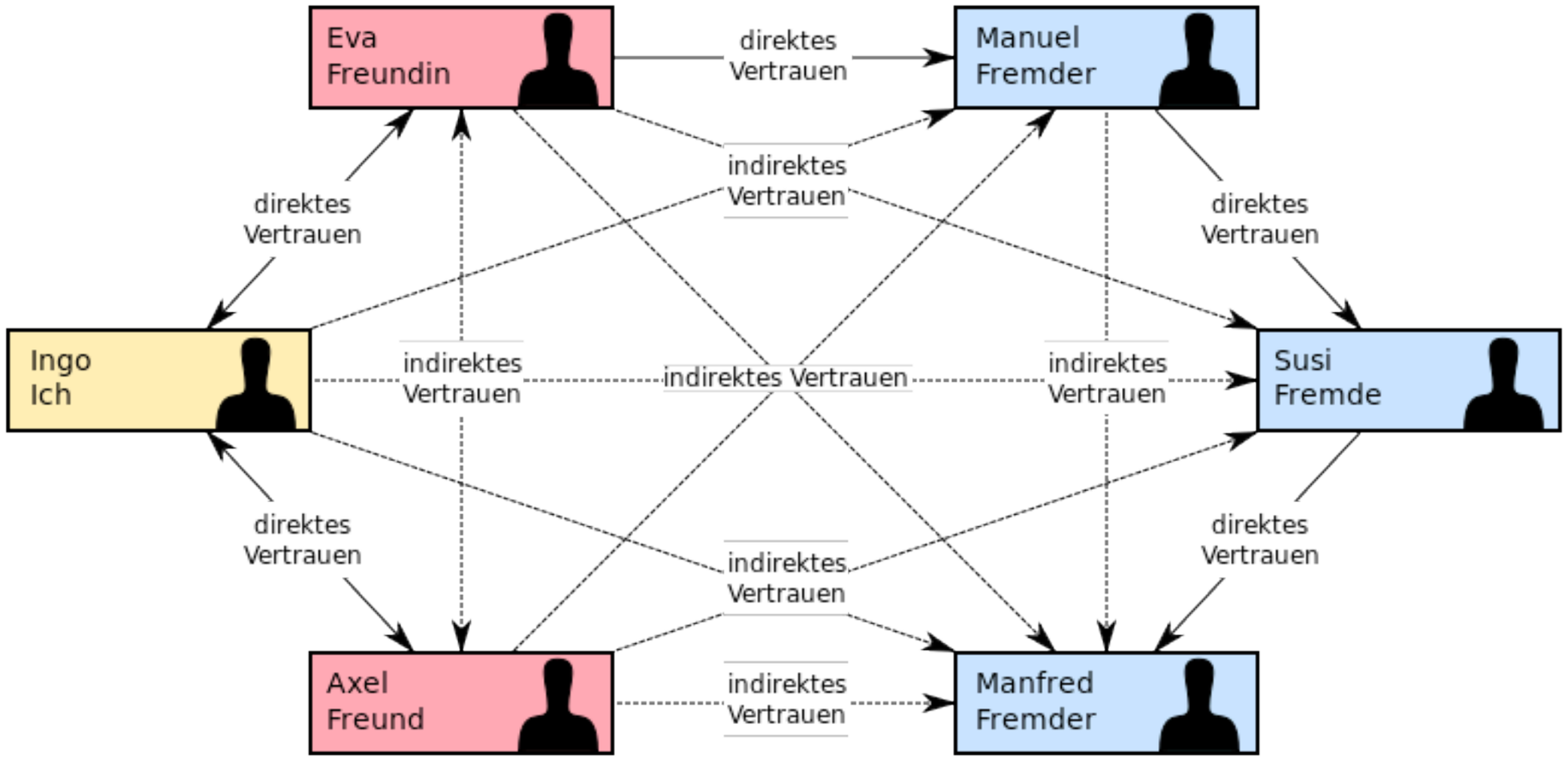
Verschlüsseln, Signieren

Soll jeder wissen, das Alice Bob eine Nachricht geschrieben hat oder nicht?

PGP - Pretty Good Privacy

http://de.wikipedia.org/w/index.php?title=Datei:Hybrid_2_encrypt.png&filetimestamp=20091221155404

Web of Trust



http://commons.wikimedia.org/wiki/File:Web_of_Trust.svg

TLS -Transport Layer Security

certificate authority (CA)

Zertifizierungsstelle für digitale Zertifikate

Zertifikat: unterschriebener öffentlicher Schlüssel

Revoke

Transportverschlüsselung

vs.

Inhaltsverschlüsselung

Verschlüsselung - praktisch

- E-Mail Verschlüsselung
  - Enigmail (Thunderbird)
  - GPG4O, outlook-privacy-plugin (Outlook)
- Festplattenverschlüsselung
  - TrueCrypt
- InstantMessaging
  - OTR
  - RetroShare

Danke! Fragen?

Präsentation

- http://www.ikonoshirt.de/stuff/13-03-28 Kryptosysteme.pdf