E-Mailverschlüsselung mit OpenPGP

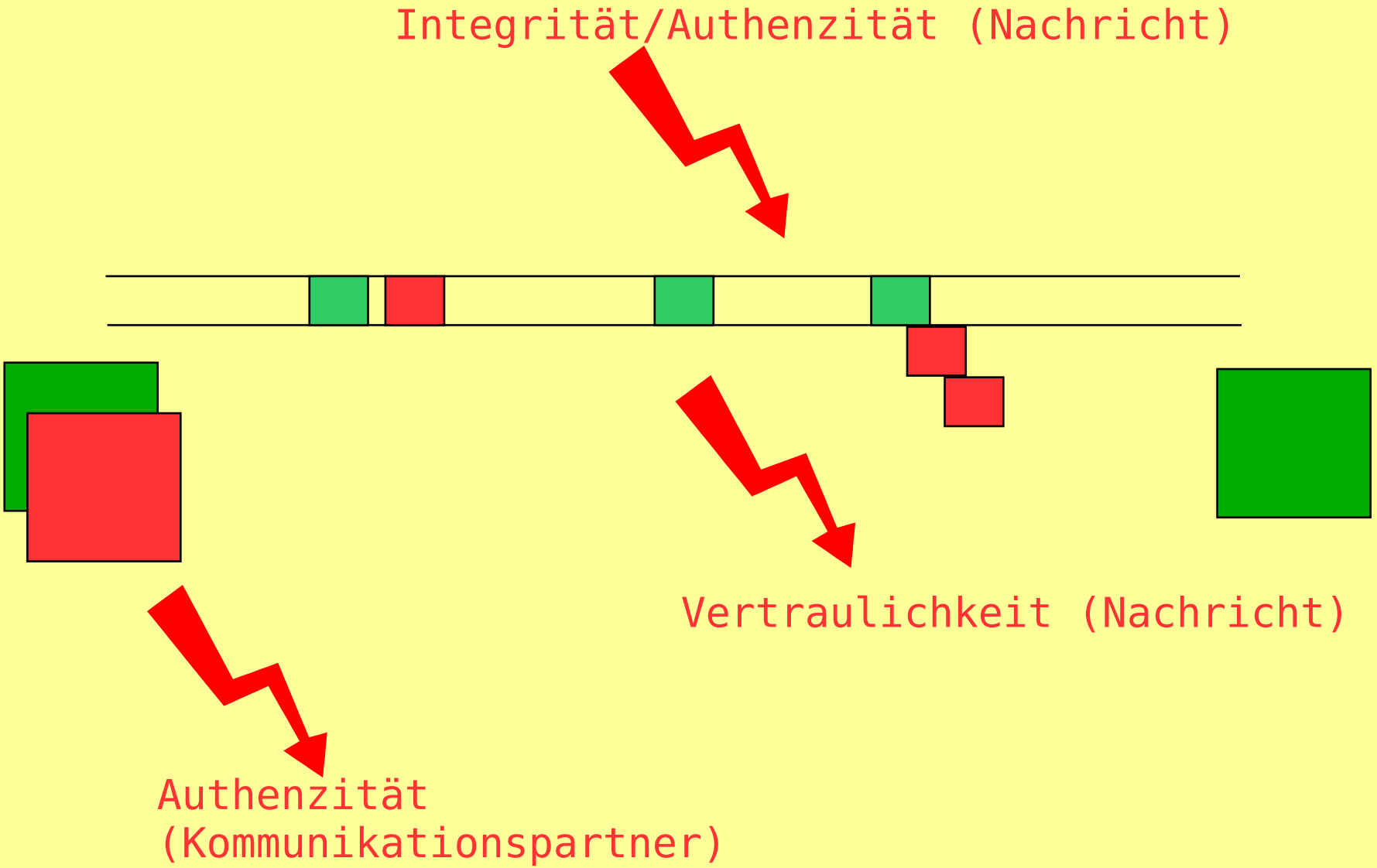
Christoph Thielecke - u15119@hs-harz.de

Inhalt

- Verschlüsselung – Wozu?
- Schutz vor Bedrohungen
- Funktionsweise PGP
- Programme rund um E-Mail Verschlüsselung
- Demonstration

Verschlüsselung - Wozu?

Bedrohungen der Netzkommunikation



Schutz vor Bedrohungen bei E-Mail

Authenzität der Kommunikationspartner
+
Vertraulichkeit der Nachricht
+
Integrität/Authenzität der Nachricht
+
E-Mail
+
Open Source

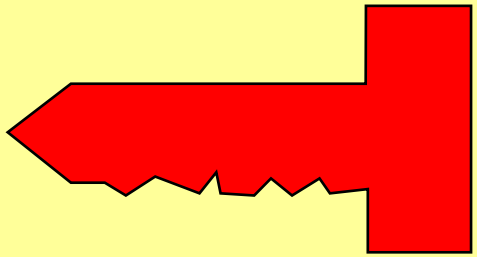
=

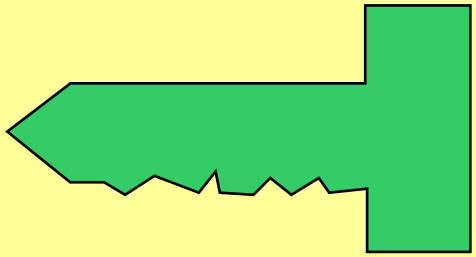
GnuPG

Funktionsweise PGP I

Erzeugung Schlüsselpaar

Privater Schlüssel



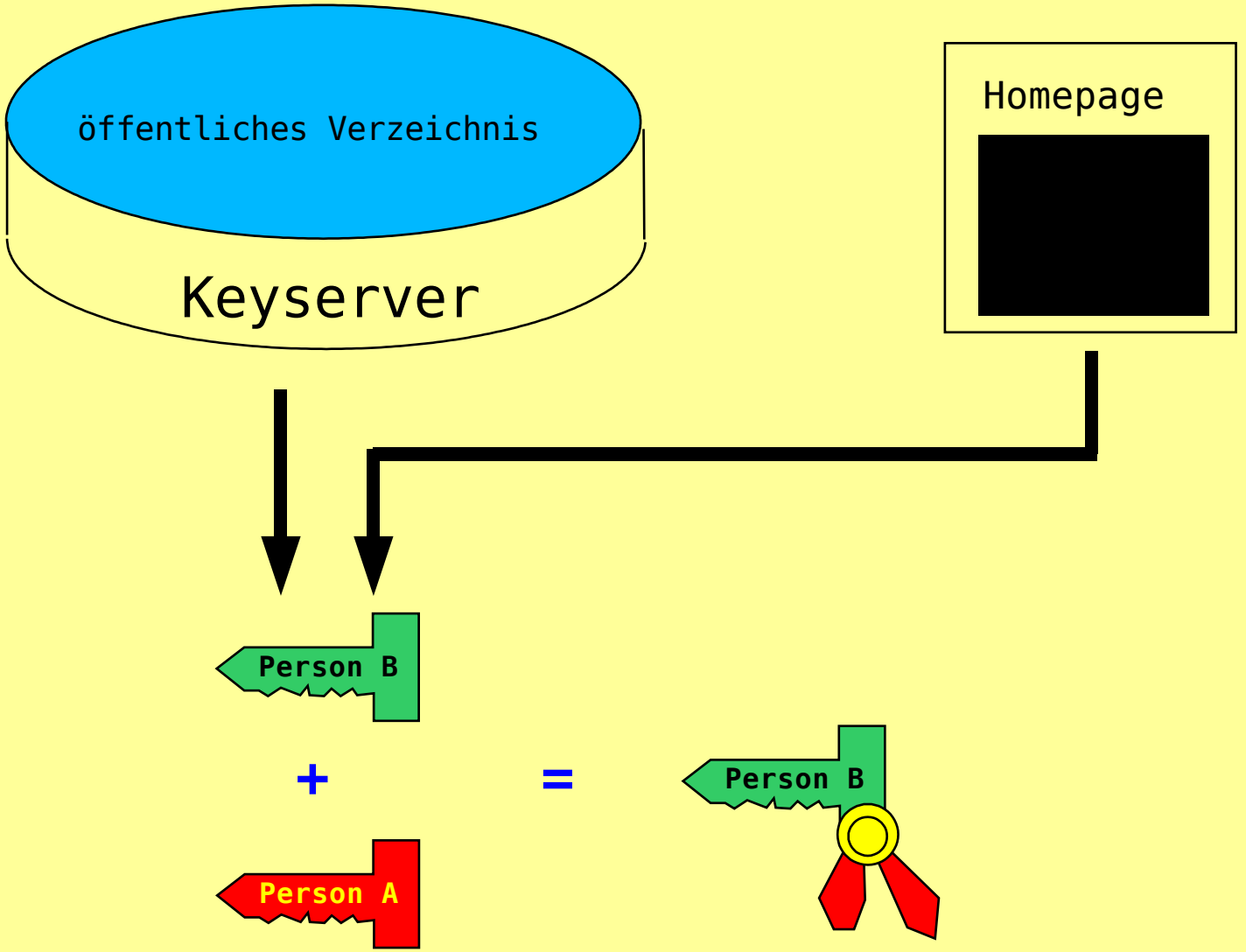


Öffentlicher Schlüssel

Privaten Schlüssel nur für Besitzer zugänglich aufbewahren!
Öffentlichen Schlüssel auf Homepage oder Keyserver publizieren!

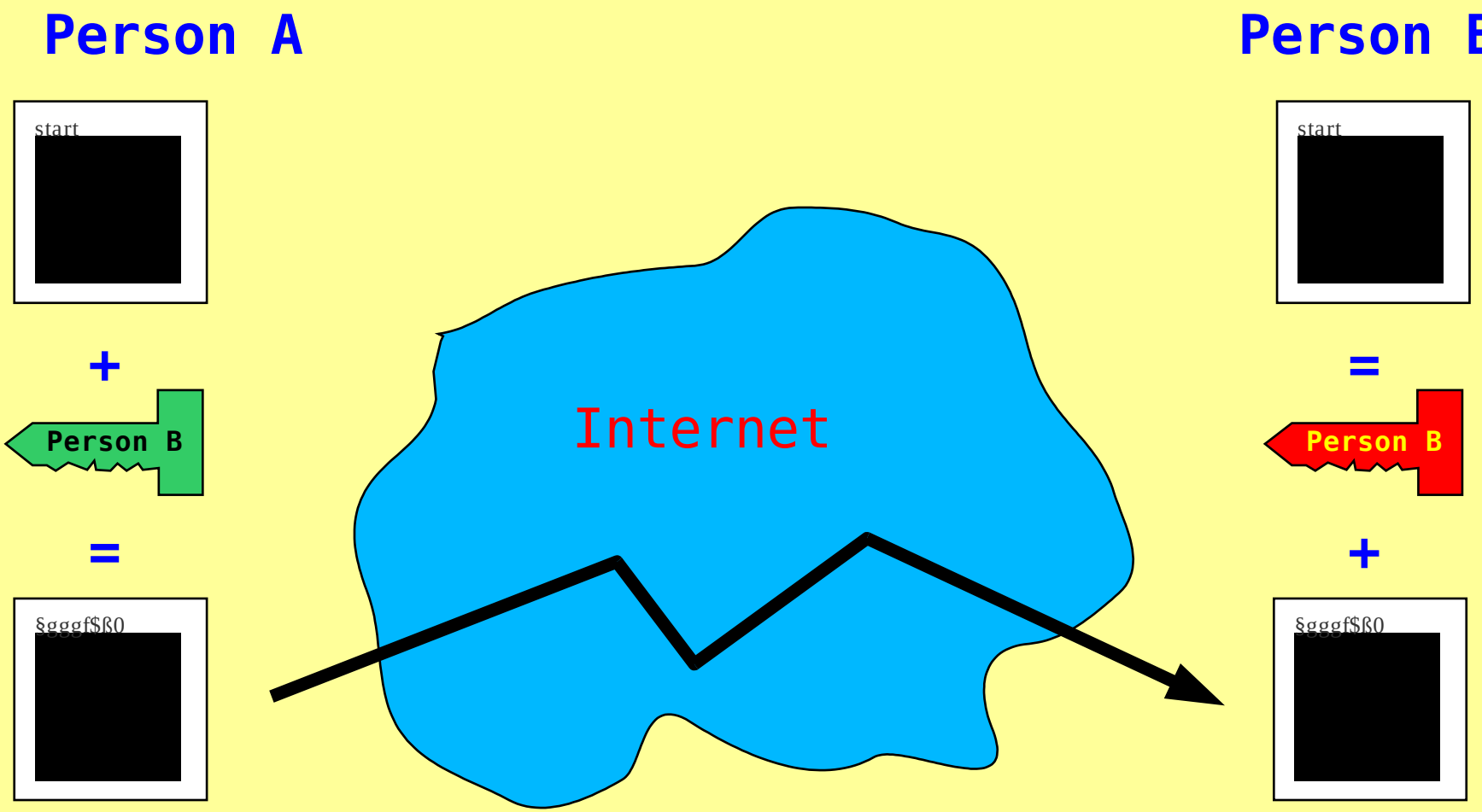
Funktionsweise PGP II

Schlüsselimport



Funktionsweise PGP III

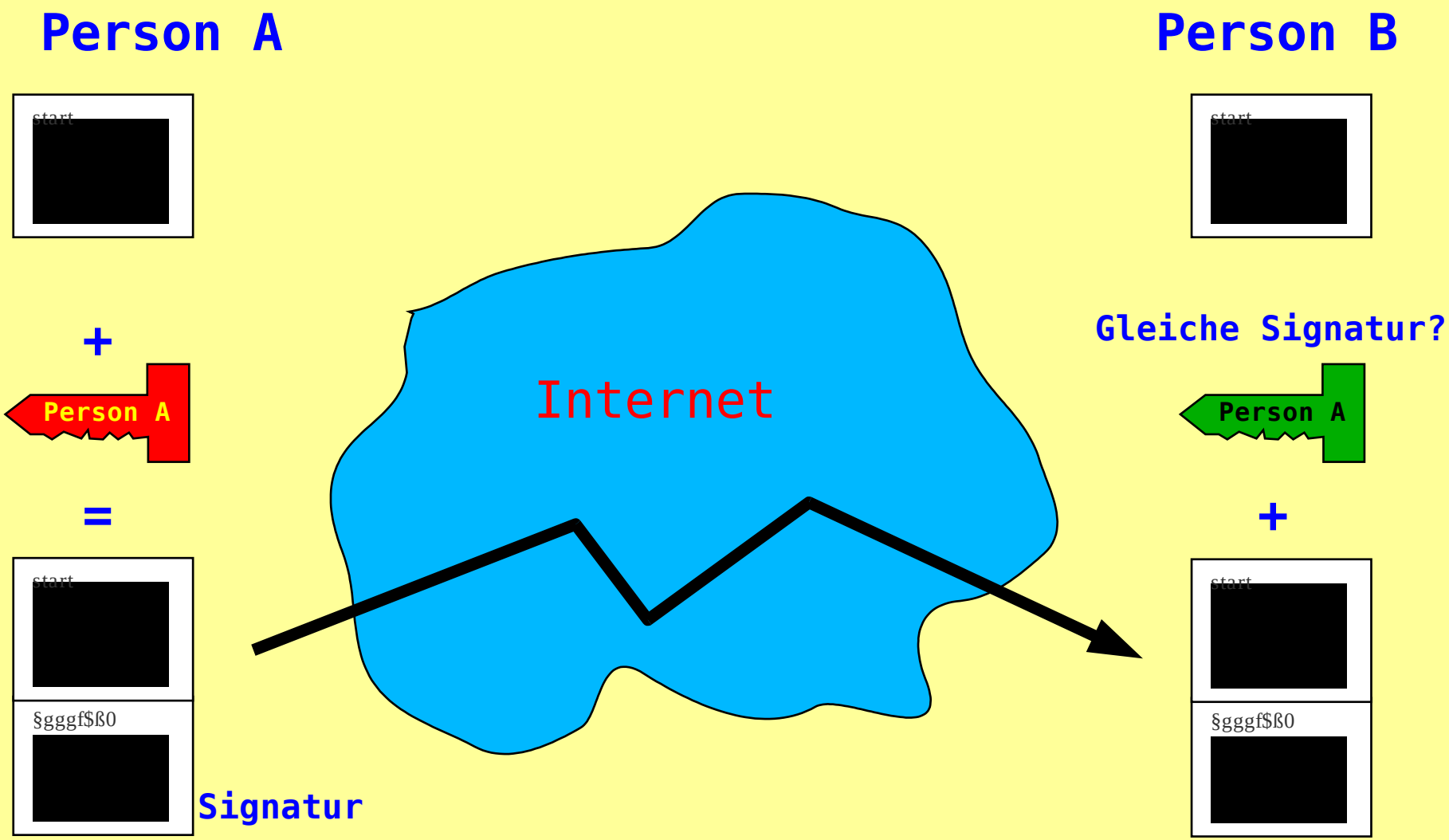
Verschlüsselung/Entschlüsselung einer Nachricht



Schlüsselauthenzität privat/über Keyserver sicherstellen!

Funktionsweise PGP II

Signierung/Prüfung einer Nachricht auf Intigrität



Schlüsselauthenzität privat/über Keyserver sicherstellen!

Programme rund um Verschlüsselung

Schlüsselverwaltung:

- Kgpg – KDE-Frontend
- GnomePGP – GNOME-Frontend
- GPG Keys

Verschlüsseln/Entschlüsseln

- Enigmail – Verschlüsselung für Mozilla
- Kmail
- Sylpheed
- Evolution