



IT-Sicherheit

02 Kryptographische Primitiven

Gerrit.Kalkbrenner@hwr-berlin.de

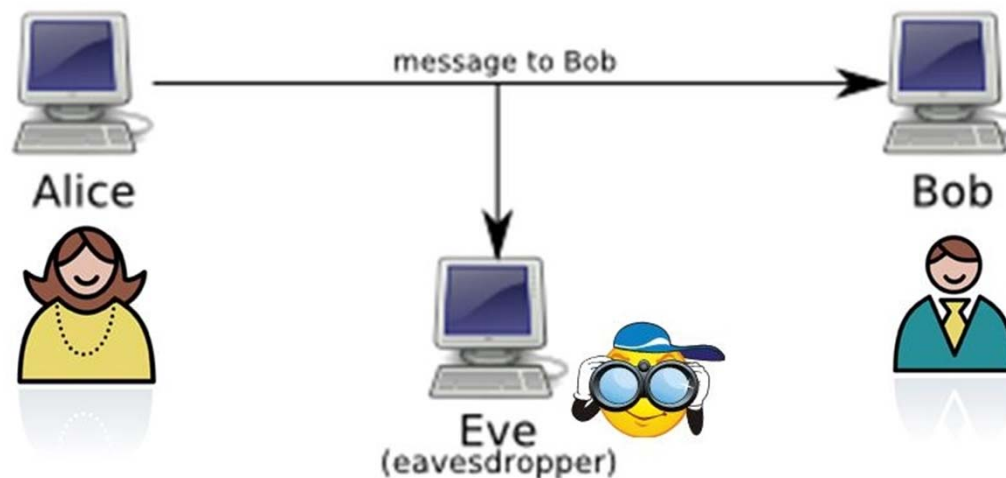


Baukasten für kryptographische Funktionen

- Kryptographische Funktionen schaffen nicht per se Sicherheit!
- Aber mit ihrer Hilfe kann ein sicheres System konstruiert werden.

Vertrauliche Nachrichten

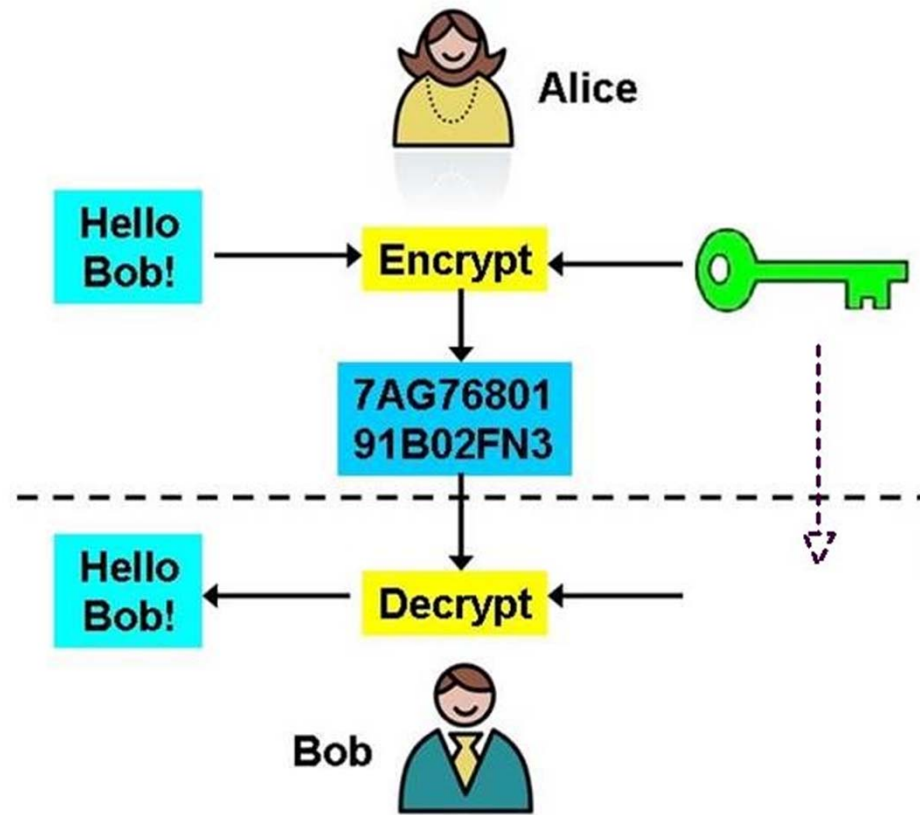
- Soll nur von vertrauten Personen gelesen werden



- Symmetrischer Verschlüsselungsalgorithmus
- Chiffre

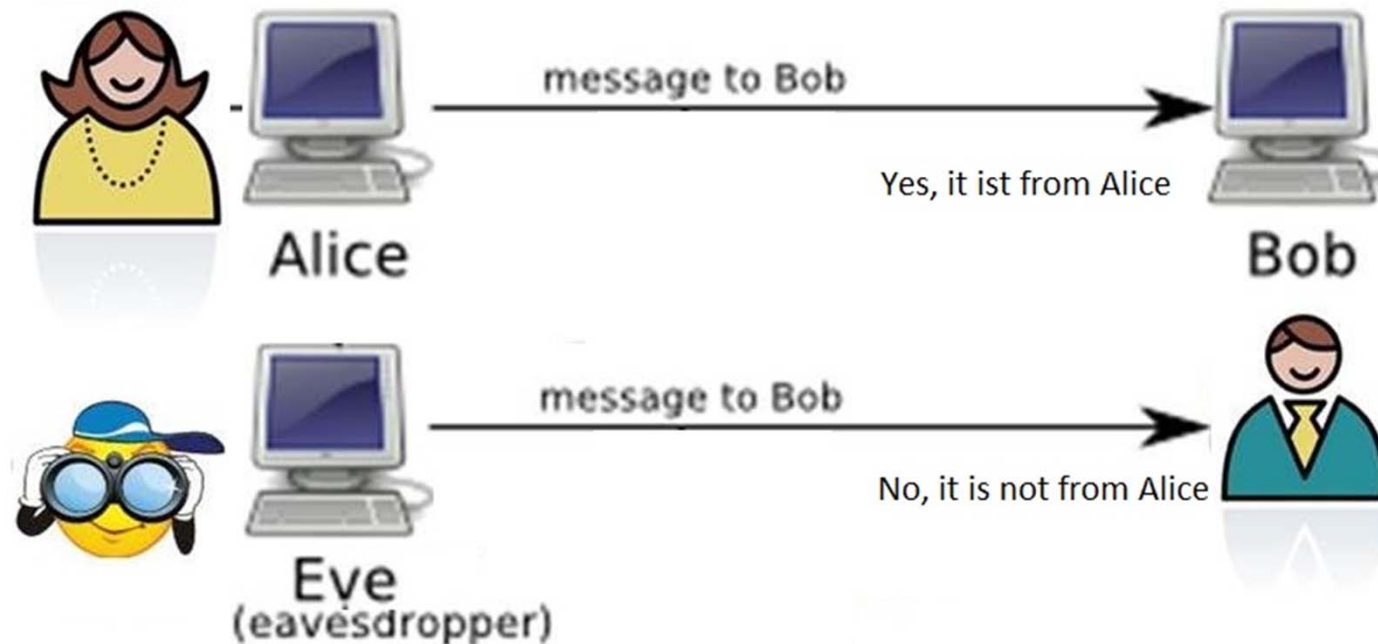
Vertrauliche Nachrichten

- Zwei zentrale Funktionen: Encrypt, Decrypt



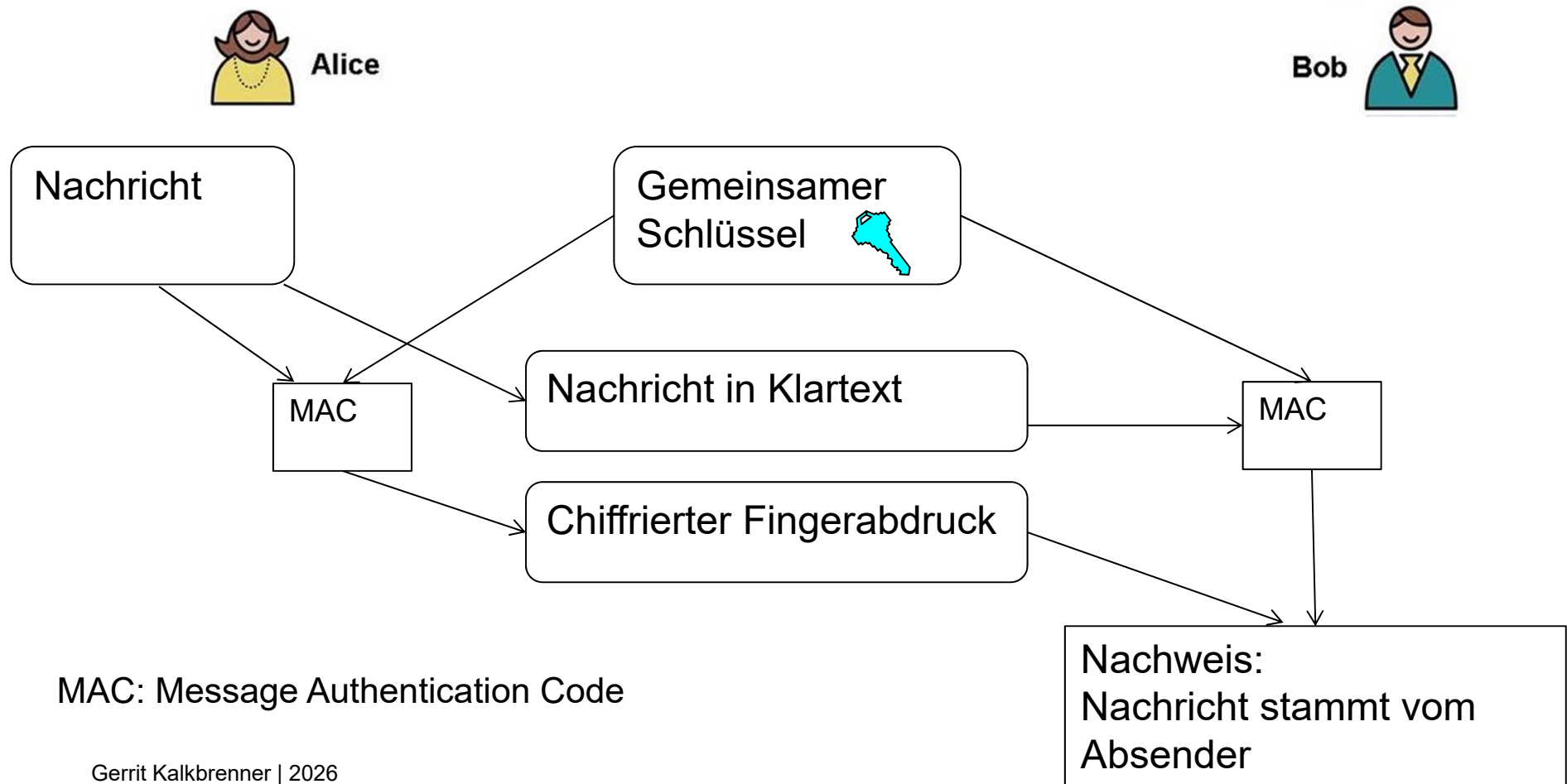
Authentische Nachrichten

- Stammt eine Nachricht wirklich vom angegebenen Absender



Authentische Information

MAC: Message Authentication Code





Schlüssel-Austausch

- Gemeinsamer Schlüssel!
- Wie kommen wir zu einem gemeinsamen Schlüssel? (ein gemeinsames Geheimnis)
- Problem war lange Zeit schwer zu lösen!
- Erst in den 1970er Jahren wurde die asymmetrische Kryptografie erfunden.
- → Diffie-Hellman



gemeinsamen Geheimnis: Diffie-Hellman



Alice

Gemeinsame Form



Bob



Privater
Schlüssel

Privater
Schlüssel



+



=



Öffentliche Schlüssel



=



+



Austausch



+



=



Gemeinsames Geheimnis



=



+





RSA: asymmetrische Verschlüsselung

- Auf die Erfindung von Diffie-Hellman folgte RSA
- Schlüsselpaar: einer zum verschlüsseln
einer zum entschlüsseln
- RSA = Ron Rivest, Adi Shamir, Leonard Adelman
- Flexibler als Diffie-Hellman



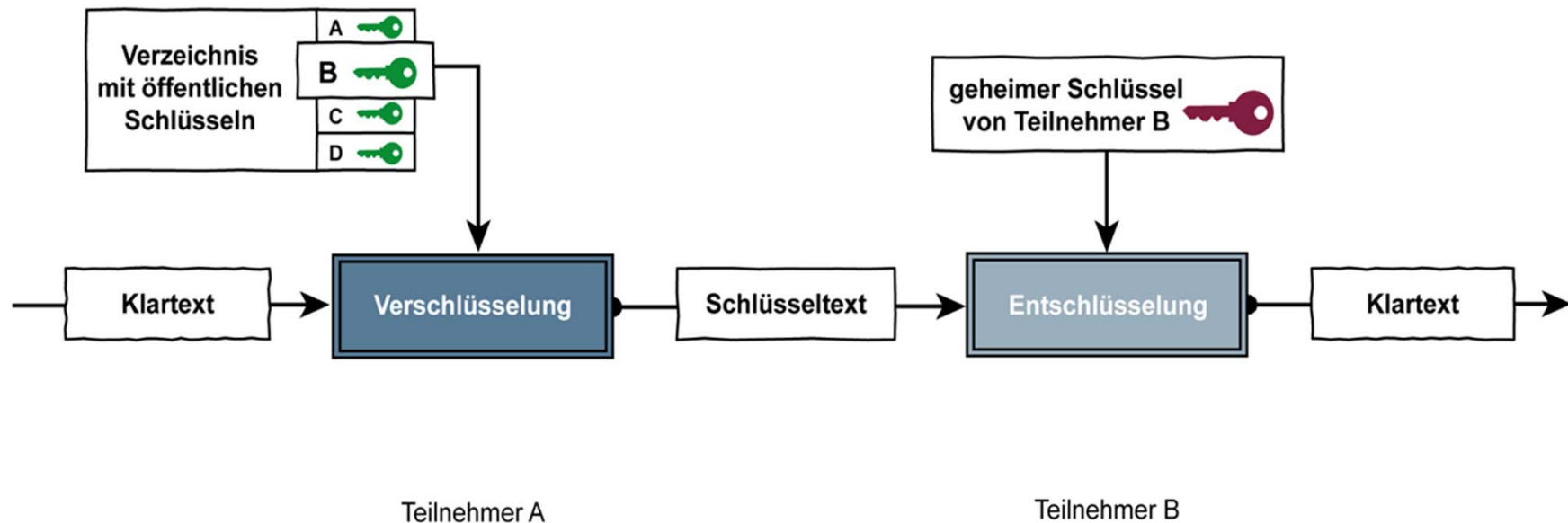
RSA: asymmetrische Verschlüsselung

- Schlüsselpaar
- bietet 2 Funktionen:
 - Verschlüsseln / Entschlüsseln
 - Signieren / Signatur Prüfen



RSA: asymmetrische Verschlüsselung

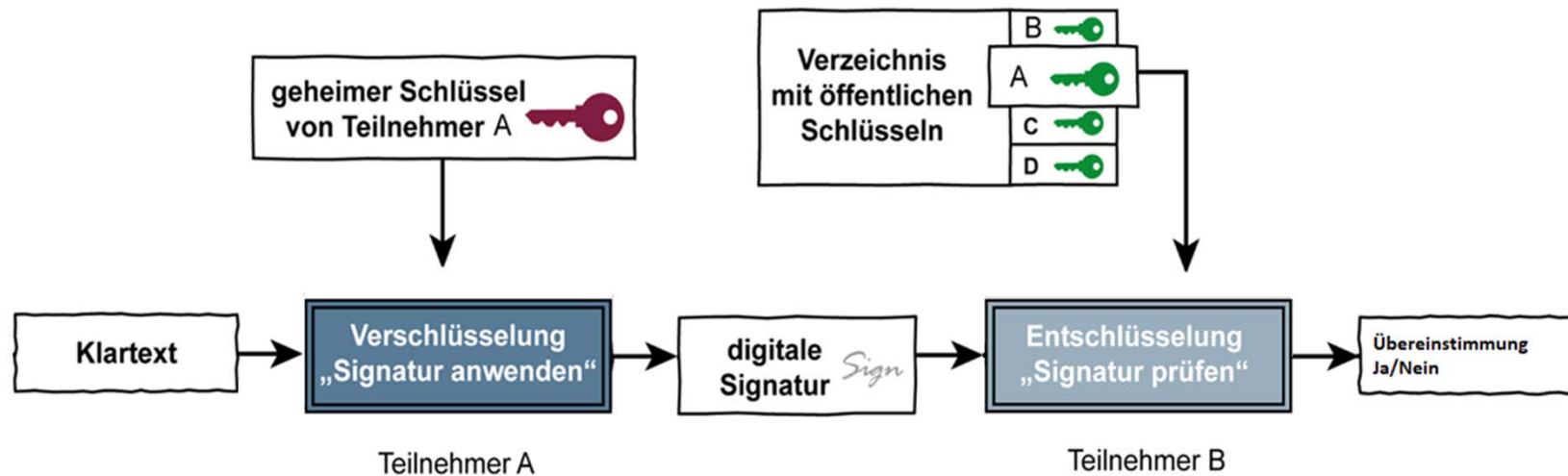
- Funktion 1: Verschlüsseln und Entschlüsseln





RSA: asymmetrische Verschlüsselung

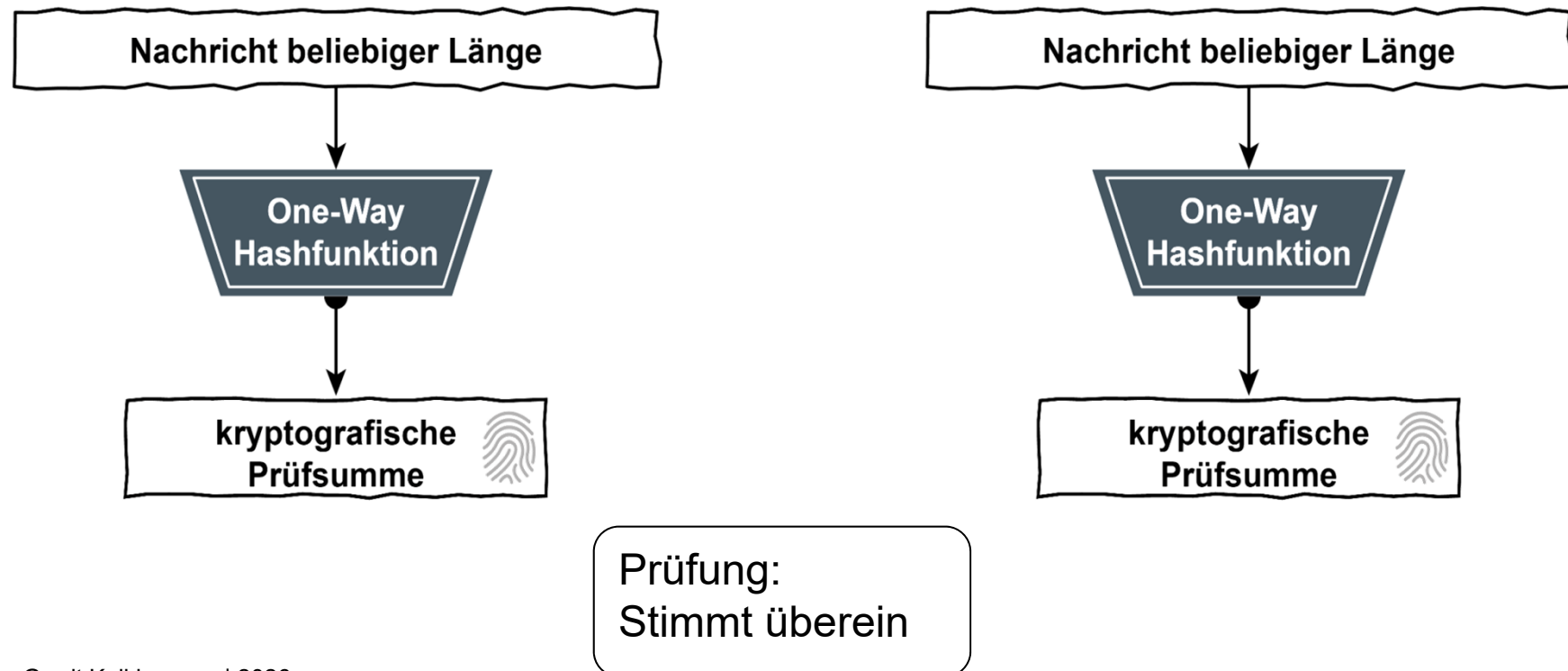
- Funktion 2: Signieren und Signatur Prüfen





Fingerabdruck

Kryptographische Hash-Funktionen





- Das war es!
- Mehr braucht man nicht!