CoNe Freiburg

Nachrichtenintegrität

- Erlaubt den Komunikationspartnern die Korrektheit und Authentizität der Nachricht zu überprüfen
  - Inhalt ist unverändert
  - Urheber ist korrekt
  - Nachricht ist keine Wiederholung
  - Reihenfolge der Nachrichten ist korrekt
- Message Digests

Computer Networking: A Top Down Approach
Jim Kurose, Keith Ross, Addison-Wesley, April 2009.

UNI FREIBURG

CoNe Freiburg

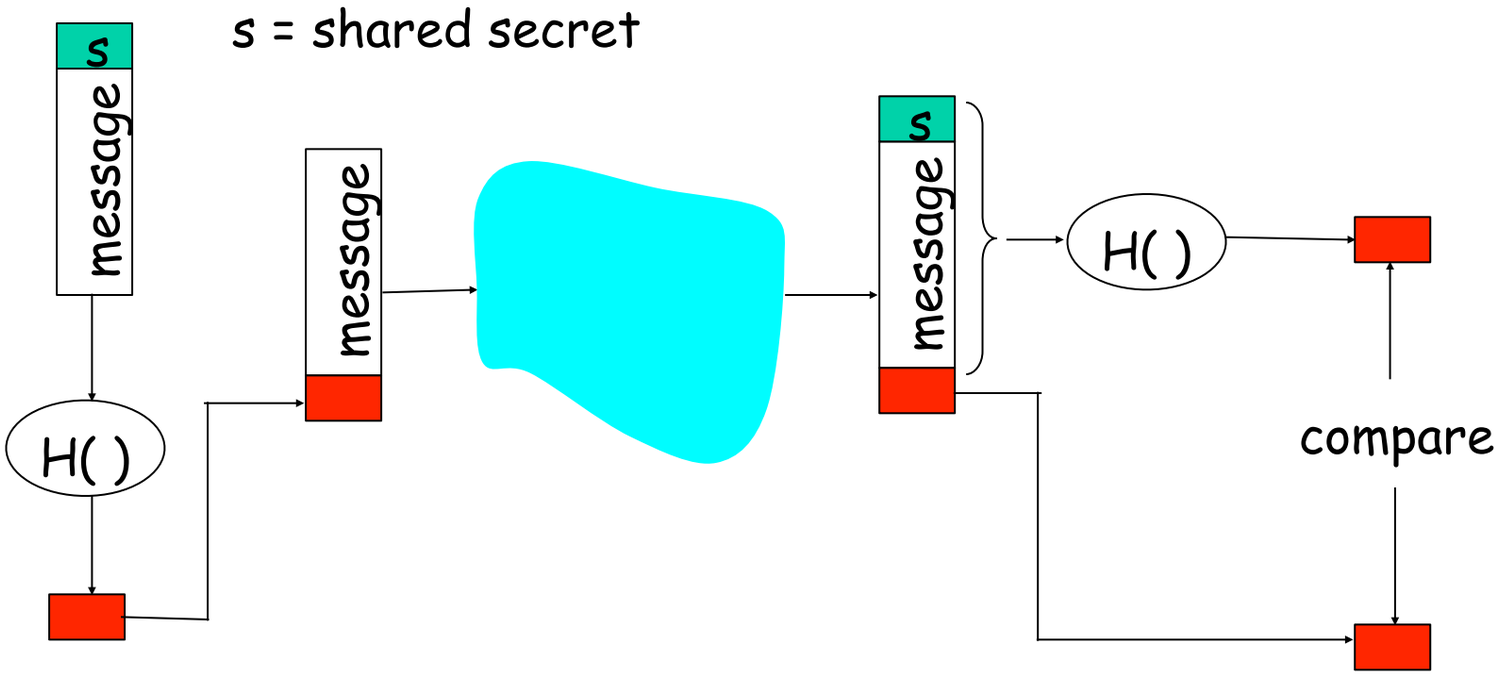
Kryptographische Hash-Funktion

- z.B. SHA-1, SHA-2, MD5
- Ein kryptographische Hash-Funktion h bildet einen Text auf einen Code fester Länge ab, so dass
  - h(text) = code
  - es unmöglich ist einen anderen Text zu finden mit:
    - h(text‘) = h(text) und text ≠ text‘
- Mögliche Lösung:
  - Verwendung einer symmetrischen Kodierung

- MD5 ist sehr verbreitet (RFC 1321)
  - berechnet 128-bit Nachricht
  - unsicher
- SHA-1 auch gebräuchlich
  - US standard [NIST, FIPS PUB 180-1]
  - 160-bit Message Digest
  - nicht mehr als sicher angesehen
- SHA-2
  - SHA-256/224
  - SHA-512/384
  - bis jetzt (2015) als sicher angesehen
- SHA-3
  - 2012 veröffentlicht

CoNe Freiburg

Message Authentication Code (MAC)



- Authentifiziert Absender
- Überprüft Nachrichtenintegrität
- Keine Verschlüsselung
- “keyed hash”
- Notation: MDm = H(s || m) ; sende m || MDm

Computer Networking: A Top Down Approach
Jim Kurose, Keith Ross, Addison-Wesley, April 2009.

CoNe Freiburg

HMAC (Keyed-Hash Message Authentication Code)

- Populärer MAC-Standard
- Sicher gegen Anhängen von Nachrichten

$$HMAC_K(N) = H\Big((K \oplus opad) \,||\, H\big((K \oplus ipad) \,||\, N\big)\Big)$$

  - Nachricht N
  - geheimer Schlüssel K
  - Konstante opad und ipad
- Erhöht Sicherheit gegen angreifbare Hash-Codes
  - wird in TLS und IPsec verwendet

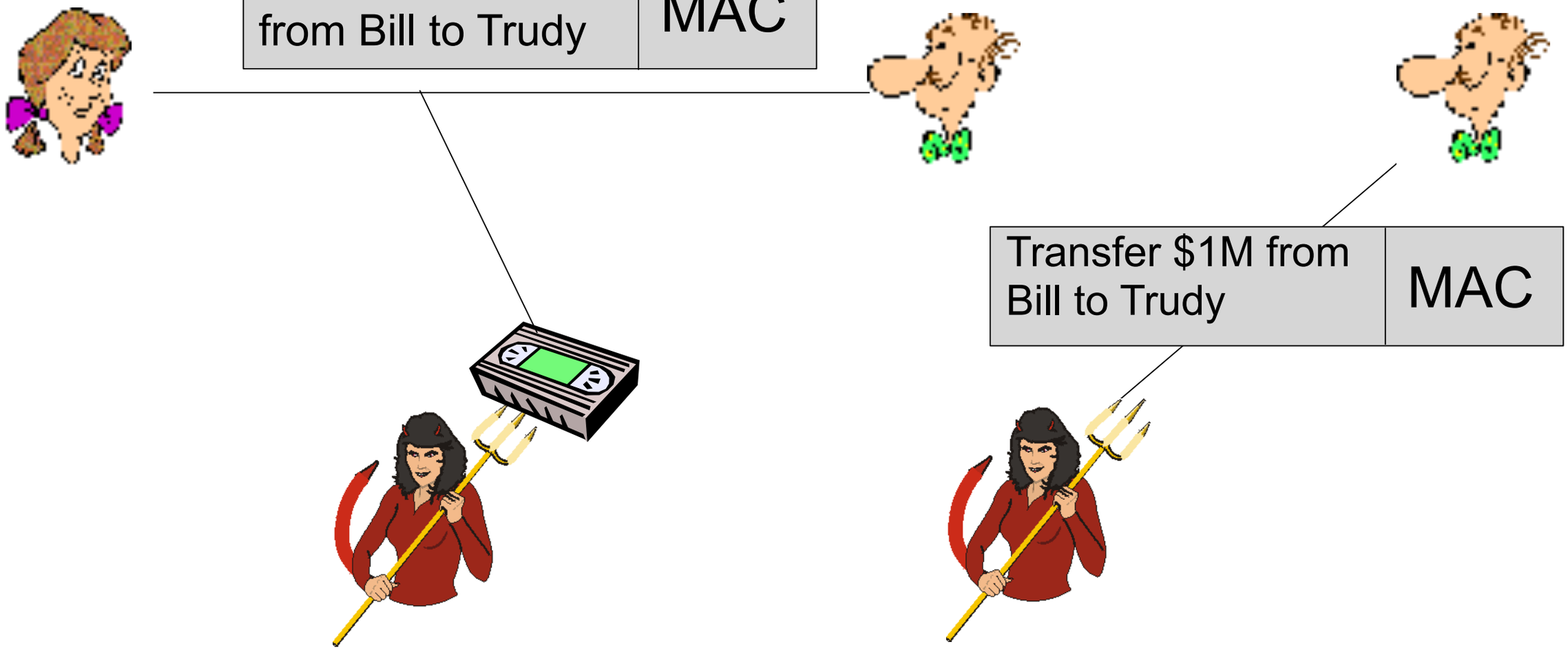
CoNe Freiburg

Authentifizierung der Endpunkte

- Versicherung, dass der Kommunikationspartner korrekt ist
- Angenommen Alice und Bob haben ein gemeinsames Geheimnis, dann gibt MAC eine Authentifizeirung der Endpunkte
  - (end-point authentication)
  - Wir wissen, dass Alice die Nachricht erzeugt hat
  - Aber hat sie sie auch abgesendet?

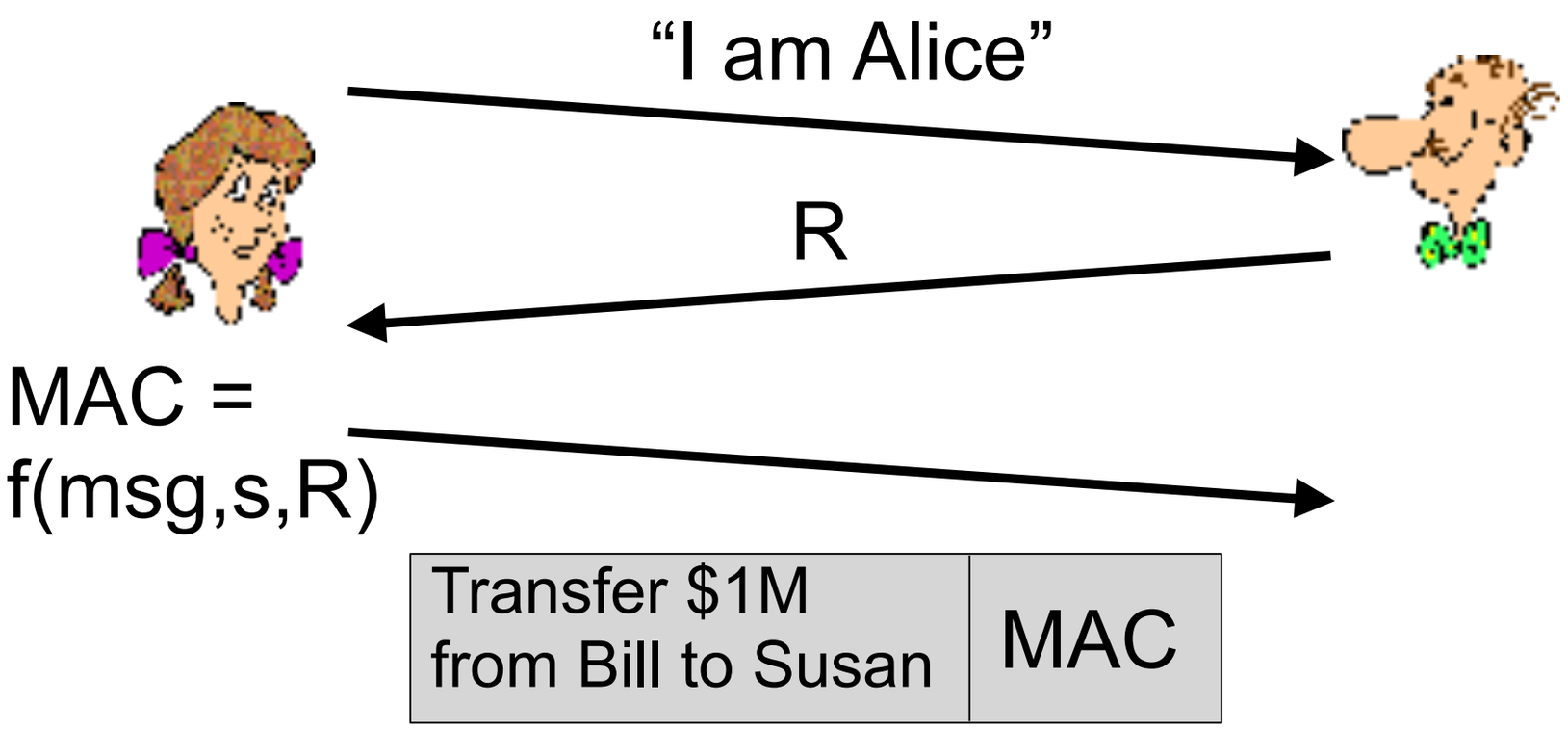
Playback-Attacke

MAC = f(msg,s)



CoNe Freiburg

Verteidigung gegen die Playback-Attacke: nonce (use only once)



Computer Networking: A Top Down Approach
Jim Kurose, Keith Ross, Addison-Wesley, April 2009.

CoNe Freiburg

Digitale Unterschriften

- Kryptographischer Algorithmus analog zu handgeschriebenen Unterschriften
  - nur sicherer
- Absender (Bob) unterschreibt digital das Dokument
  - bestätigt seine Urheberschaft
- Ziel ist ähnlich wie MAC
  - aber mit Hilfe von Public-Key-Kryptographie
  - verifizierbar, nicht fälschbar:
    - Empfänger (Alice) kann anderen beweisen, dass Bob und sonst niemand das Dokument unterschrieben hat

Computer Networking: A Top Down Approach
Jim Kurose, Keith Ross, Addison-Wesley, April 2009.

CoNe Freiburg

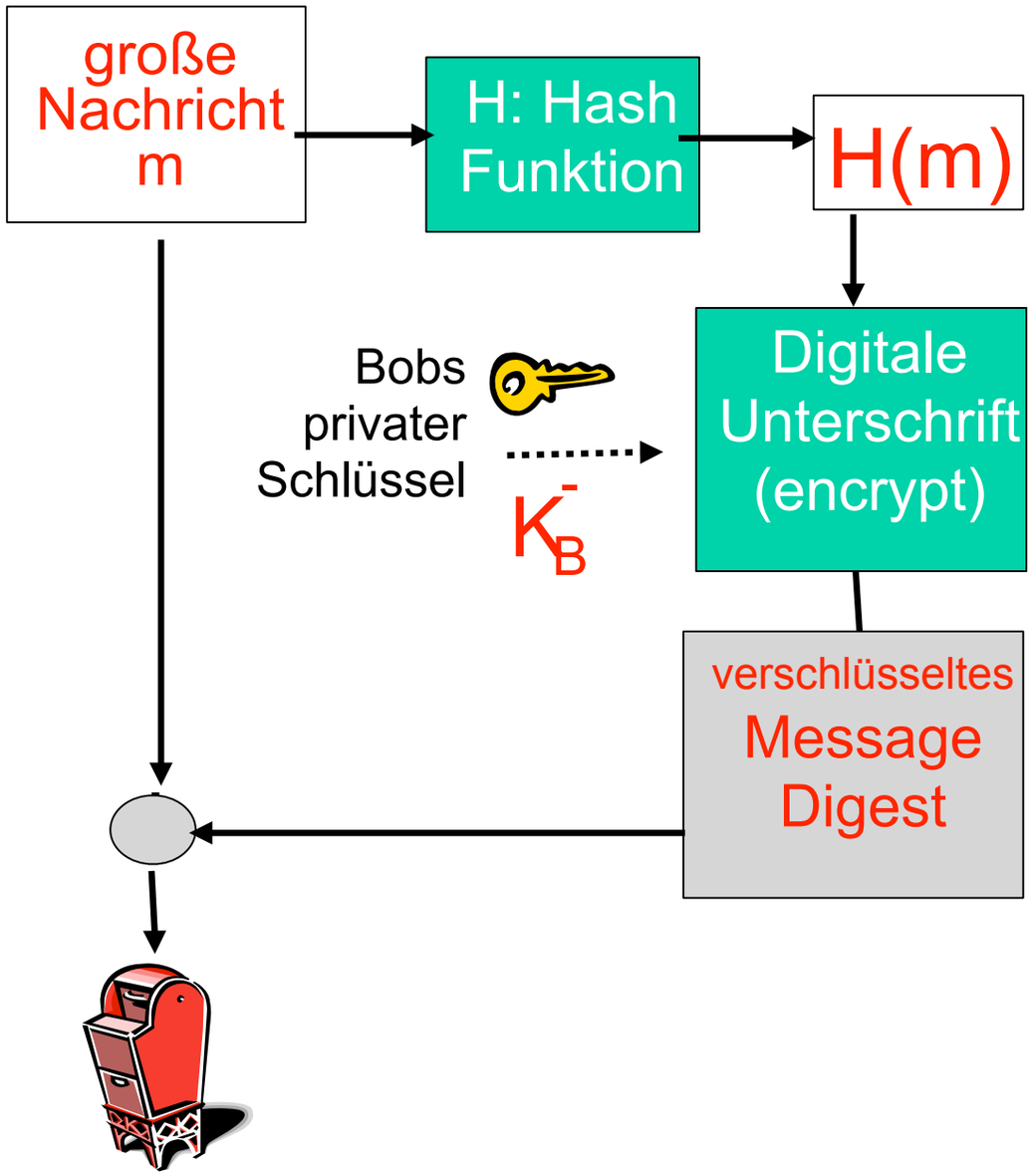
Elektronische Unterschriften

- Digitale Signaturen
  - Unterzeichner besitzt einen geheimen Schlüssel
  - Dokument wird mit geheimen Schlüssel unterschrieben
  - und kann mit einem öffentlichen Schlüssel verifiziert werden
  - Öffentlicher Schlüssel ist allen bekannt
- Beispiel eines Signaturschemas
  - m: Nachricht
  - Unterzeichner
    - berechnet h(text) mit kryptographischer Hashfunktion
    - und veröffentlicht m und
      signatur = g(privat, h(text)), für die Entschlüsselungsfunktion g
  - Kontrolleur
    - berechnet h(text)
    - und überprüft f(offen, signatur) = h(text), für die asymmetrische Verschlüsselungsfunktion g

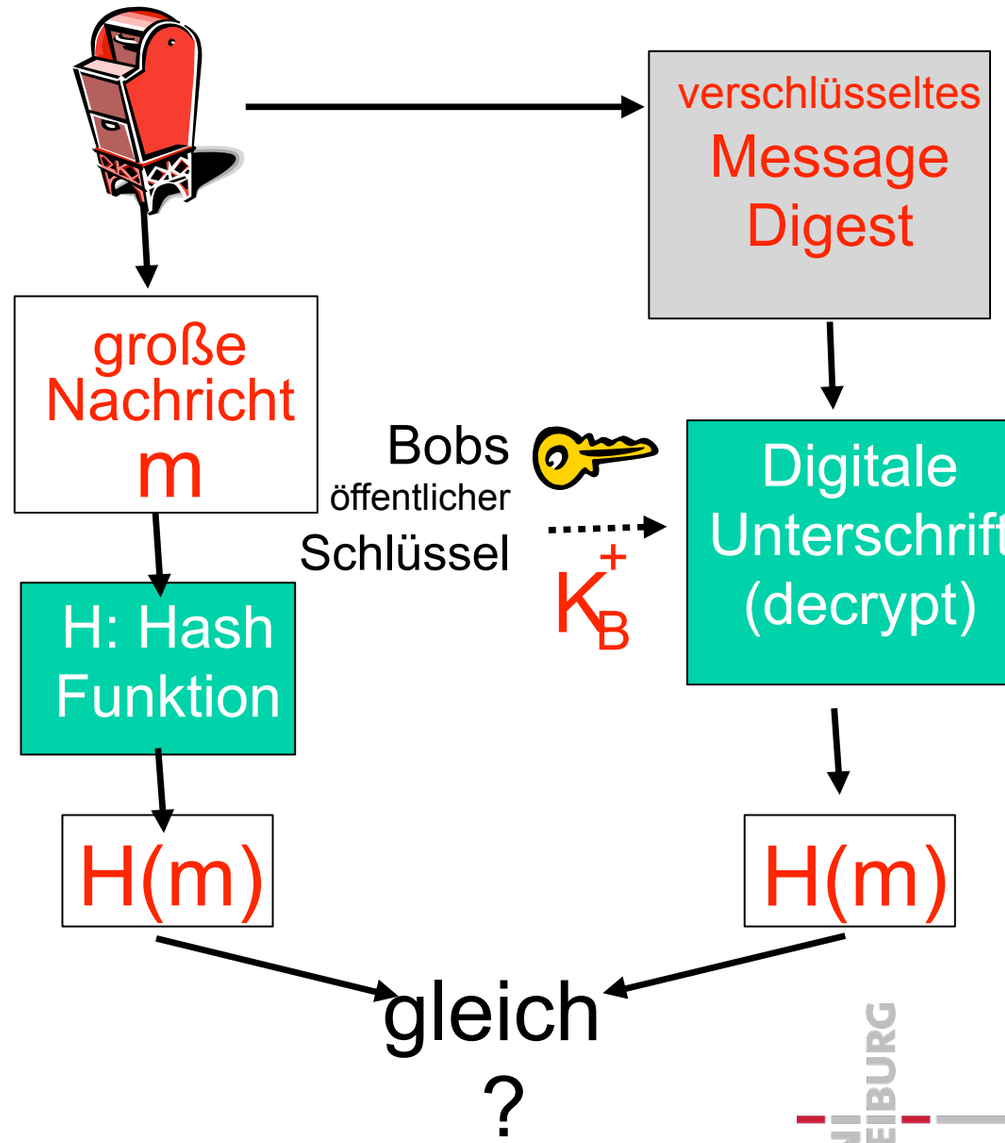
UNI FREIBURG

Digitale signature = signiertes Message Digest

Bob sendet eine digital unterschriebene Nachricht



Alice überprüft die Unterschrift und die Korrektheit der Nachricht



CoNe Freiburg

Digitale Unterschrift

- Angenommen Alice erhält
  - die Nachricht m
  - mit digitaler Unterschrift $K^-_B(m)$
- Alice überprüft m
  - mit den öffentlichen Schlüssel von Bob
  - Ist $K^+_B(K^-_B(m)) = m$?
- Falls $K^+_B(K^-_B(m)) = m$
  - dann hat jemand Bobs geheimen Schlüssel
- Alice verifiziert daher, dass
  - Bob hat m unterschrieben
  - Niemand anders hat m unterschrieben
  - Bob hat m und nicht m‘≠m unterschrieben
- Unleugbarkeit
  - Alice kann mit m und der Unterschrift vor Gericht gehen und beweisen, dass Bob m unterschrieben hat

UNI FREIBURG

CoNe Freiburg

Public-key Zertifizierung

- Motivation: Trudy spielt Bob einen Pizza-Streich
- Problem:
  - Trudy bestellt per e-mail: „Liebe Pizzeria, schick mir bitte vier Pepperoni-Pizza. vielen Dank Bob“
  - Trudy unterschreibt mit einem privaten Schlüssel
  - Trudy sendet die Bestellung zur Pizzeria
  - Trudy sendet der Pizzeria den öffentlichen Schlüssel, behauptet aber er gehöre Bob
  - Die Pizzeria überprüft die Unterschrift
  - Aber Bob mag gar keine Pepperoni