Technische Bedingungen wirksamer Verschlüsselung

Dr. Sebastian Pape

Lehrstuhl Mobile Business and Multilateral Security
Goethe Universität Frankfurt am Main

18. November 2016 DGRI-Jahrestagung Frankfurt

Agenda

1	Grundlagen
2	Überwachungsmaßnahmen
3	Seitenkanalattacken
4	Zusammenfassung

Limitierung

“Anybody who asserts that a problem is readily solved by encryption, understands neither encryption nor the problem.”

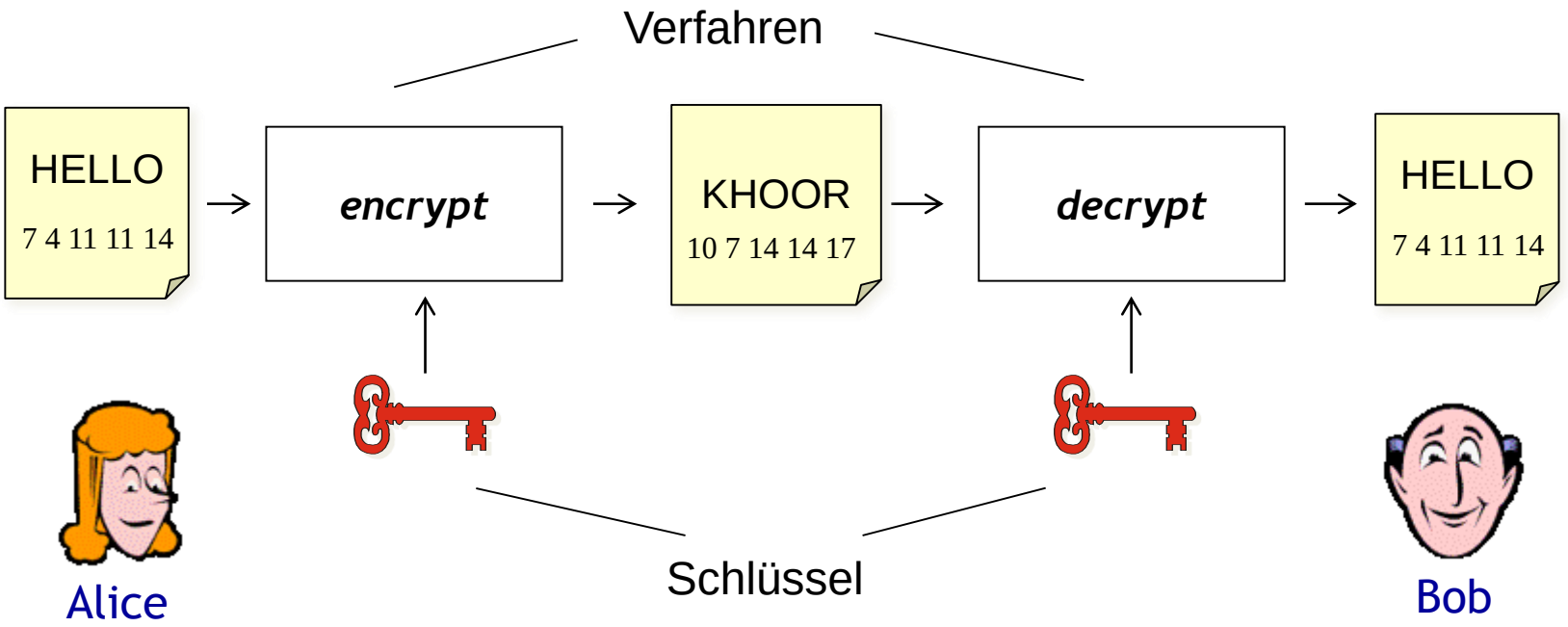
Roger Needham

Butler Lampson

[ToHell 2003]

[Marshall Symposium 1998] [Randell 2004]

Alice und Bob



[J. Buchmann: Lecture Public Key Infrastrukturen, FG Theoretische Informatik, TU-Darmstadt]

Kerkhoffs Prinzip

Auguste Kerckhoff (1835 – 1903)

[Wikipedia]

Die Sicherheit eines Verschlüsselungs-verfahrens sollte auf der Geheimhaltung des Schlüssels beruhen.

- Algorithmus geheim zu halten schwer (Reverse-Engineering)
- Algorithmus nicht leicht ersetzbar
- Peer-Review möglich
- Hintertüren / Vertrauen

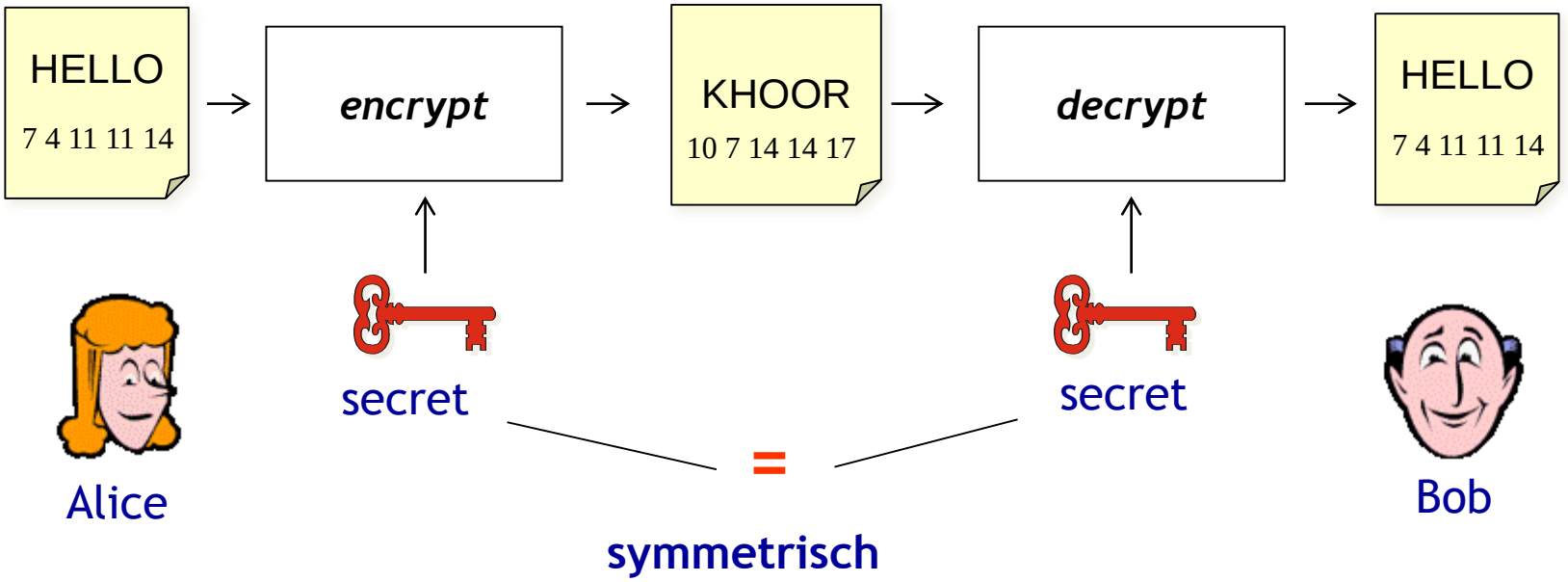
Advanced Encryption Standard (AES):

- Öffentliche Ausschreibung
- Expertenmeinungen

A5/1, A5/2 (GSM), Mifare (Chipkarten):

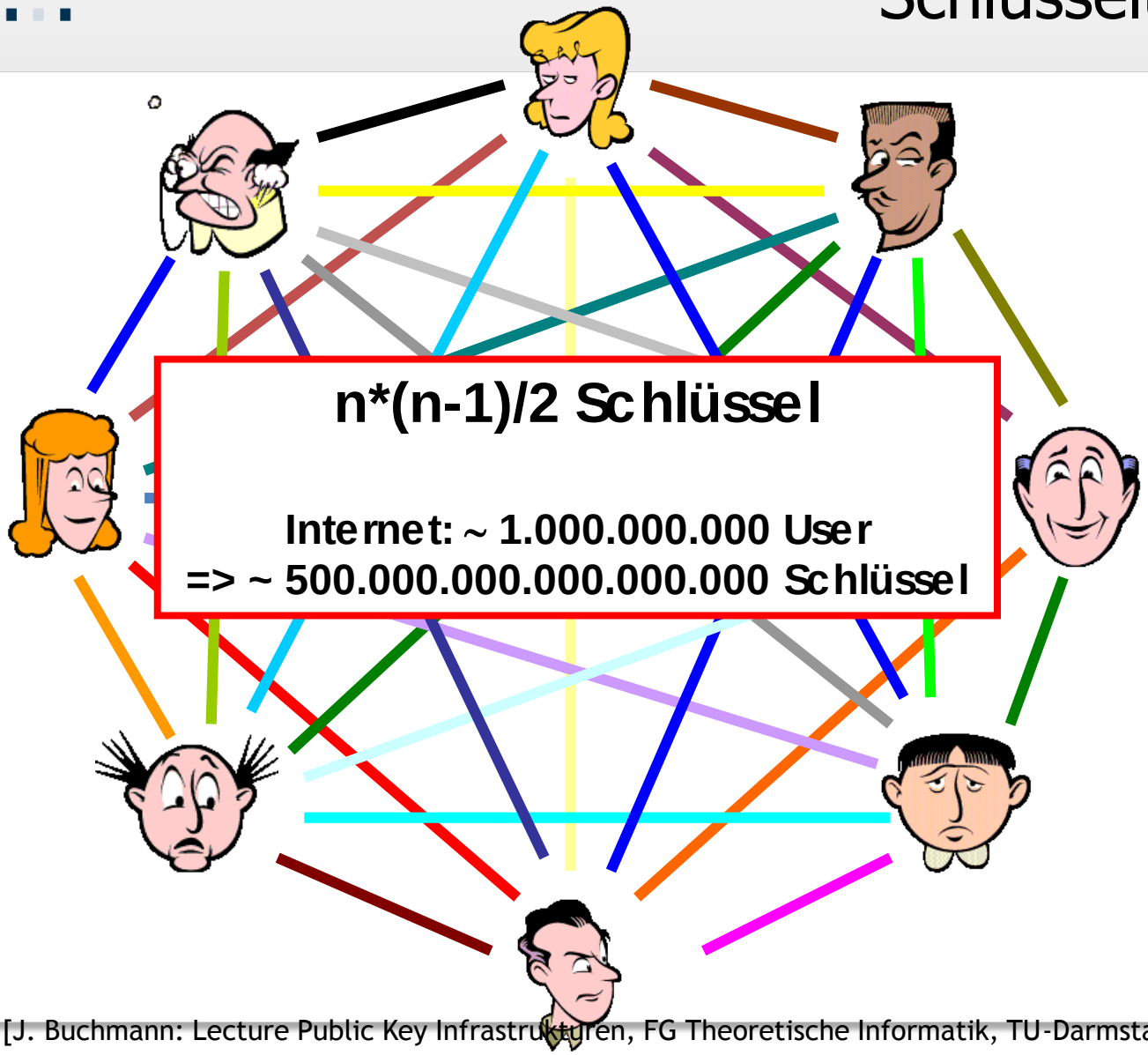
- Offen gelegt und gebrochen

Symmetrische Verschlüsselung



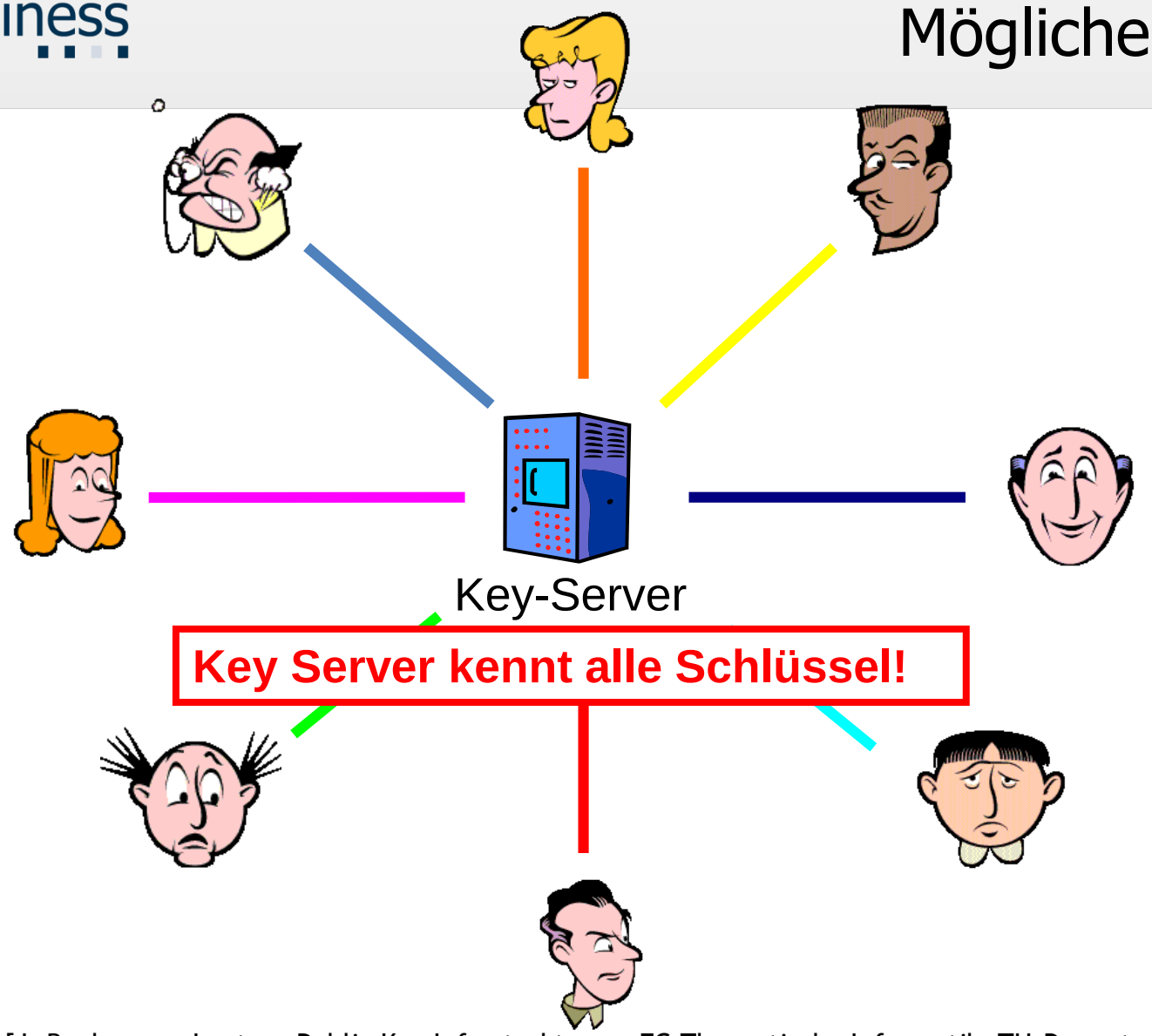
[J. Buchmann: Lecture Public Key Infrastrukturen, FG Theoretische Informatik, TU-Darmstadt]

Problem Symmetrischer Verschlüsselung: Schlüsseltausch



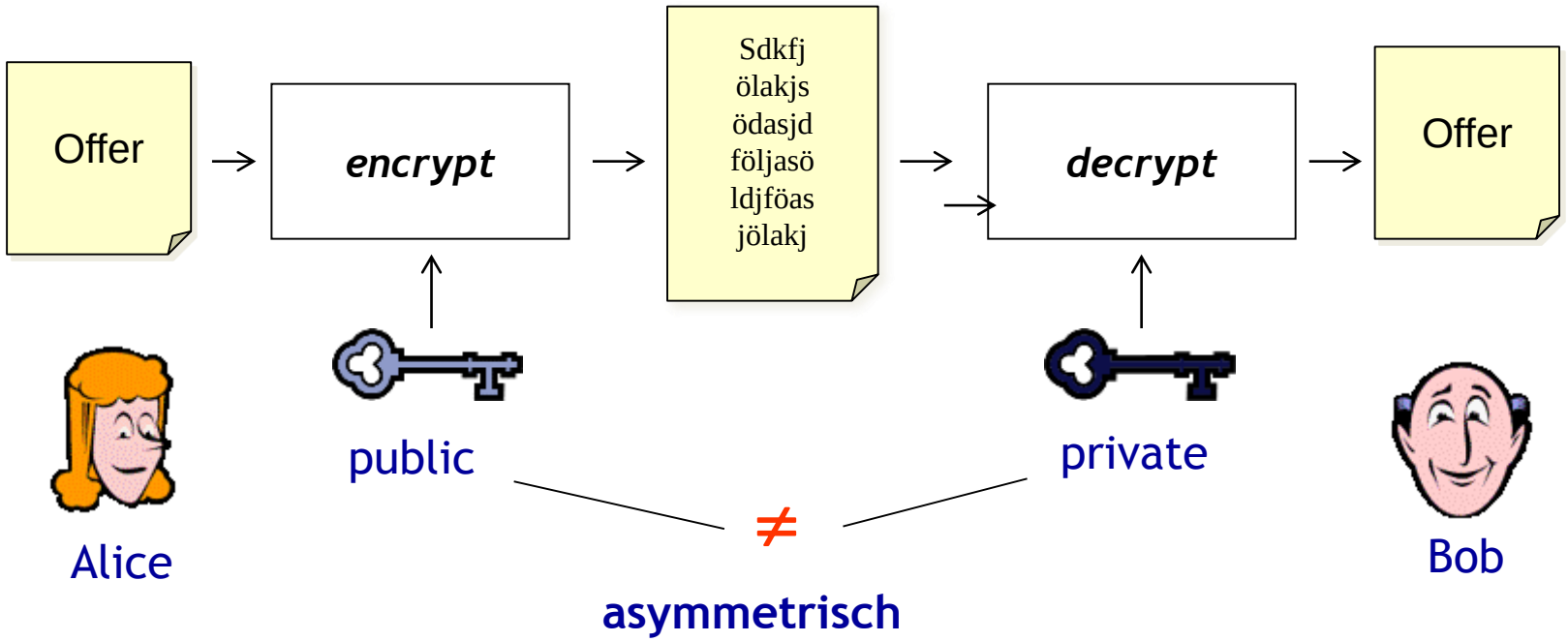
[J. Buchmann: Lecture Public Key Infrastrukturen, FG Theoretische Informatik, TU-Darmstadt]

Symmetrische Verschlüsselung: Mögliche Lösung



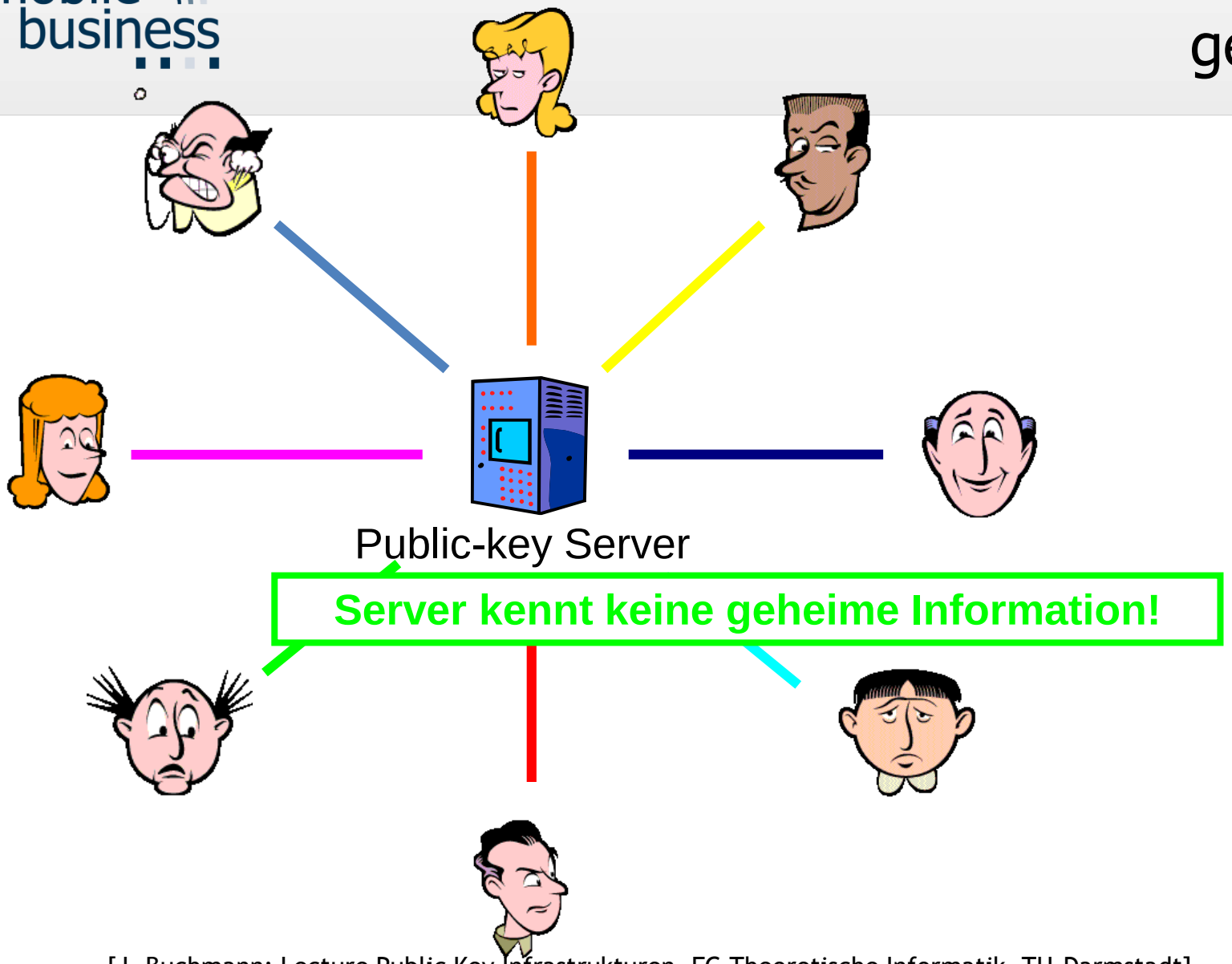
[J. Buchmann: Lecture Public Key Infrastrukturen, FG Theoretische Informatik, TU-Darmstadt]

Public Key Verschlüsselung



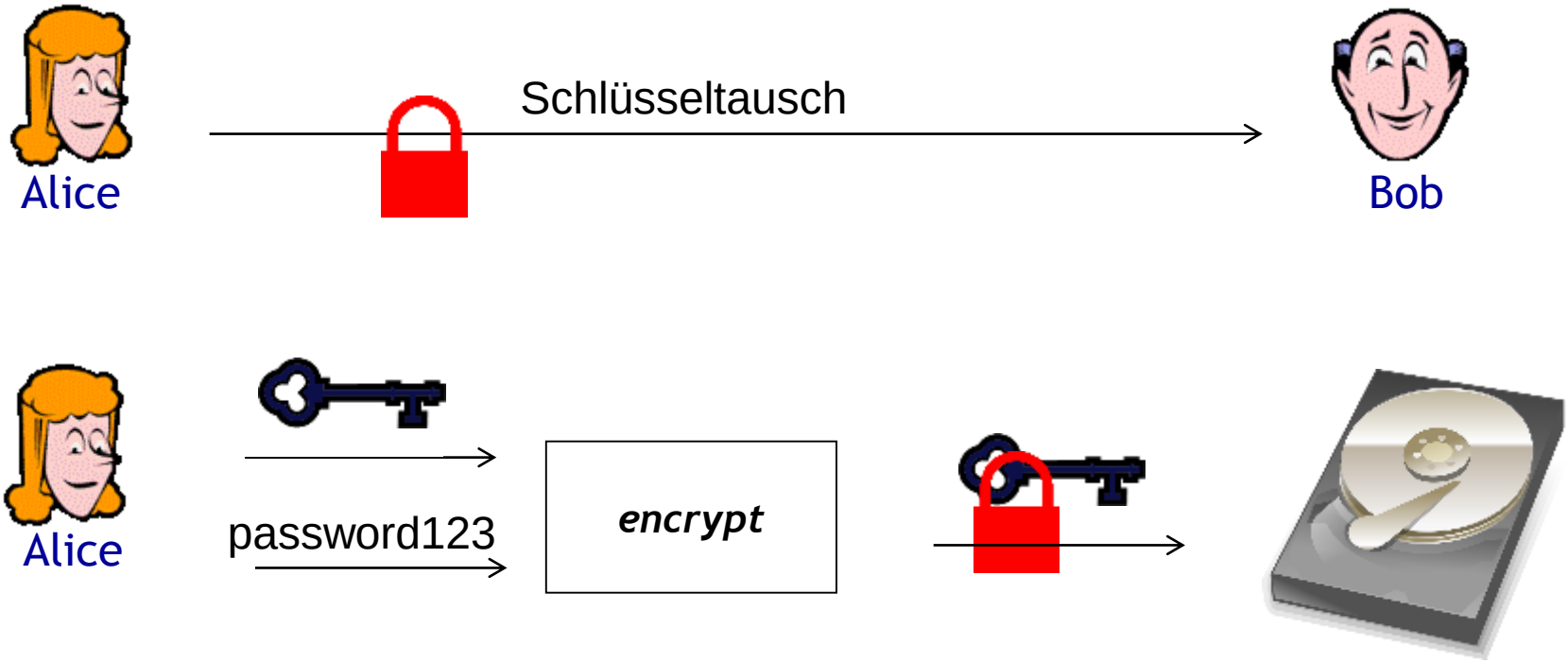
[J. Buchmann: Lecture Public Key Infrastrukturen, FG Theoretische Informatik, TU-Darmstadt]

Schlüsseltausch gelöst!

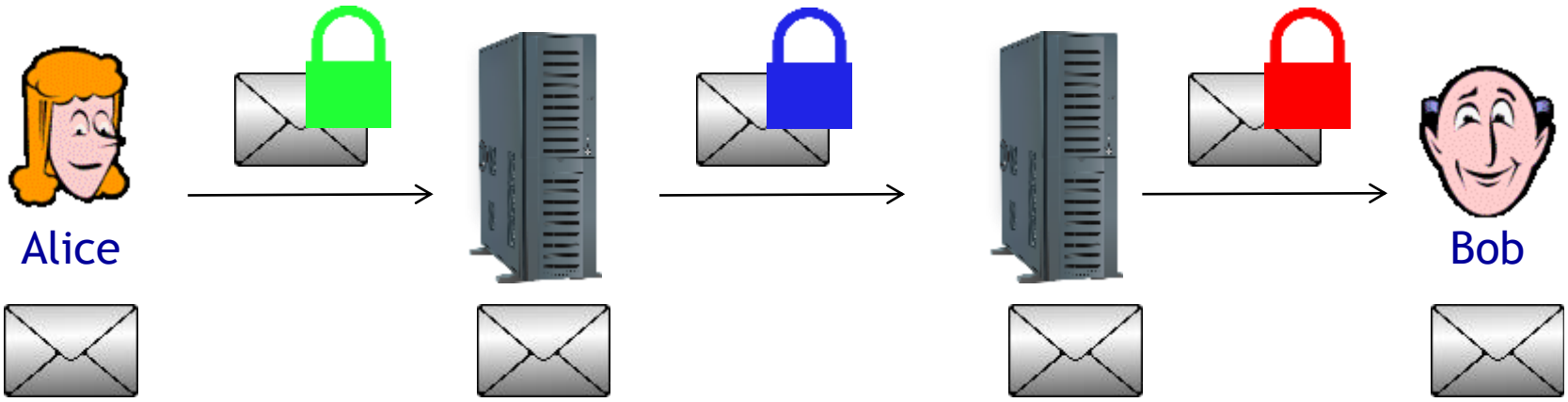


[J. Buchmann: Lecture Public Key Infrastrukturen, FG Theoretische Informatik, TU-Darmstadt]

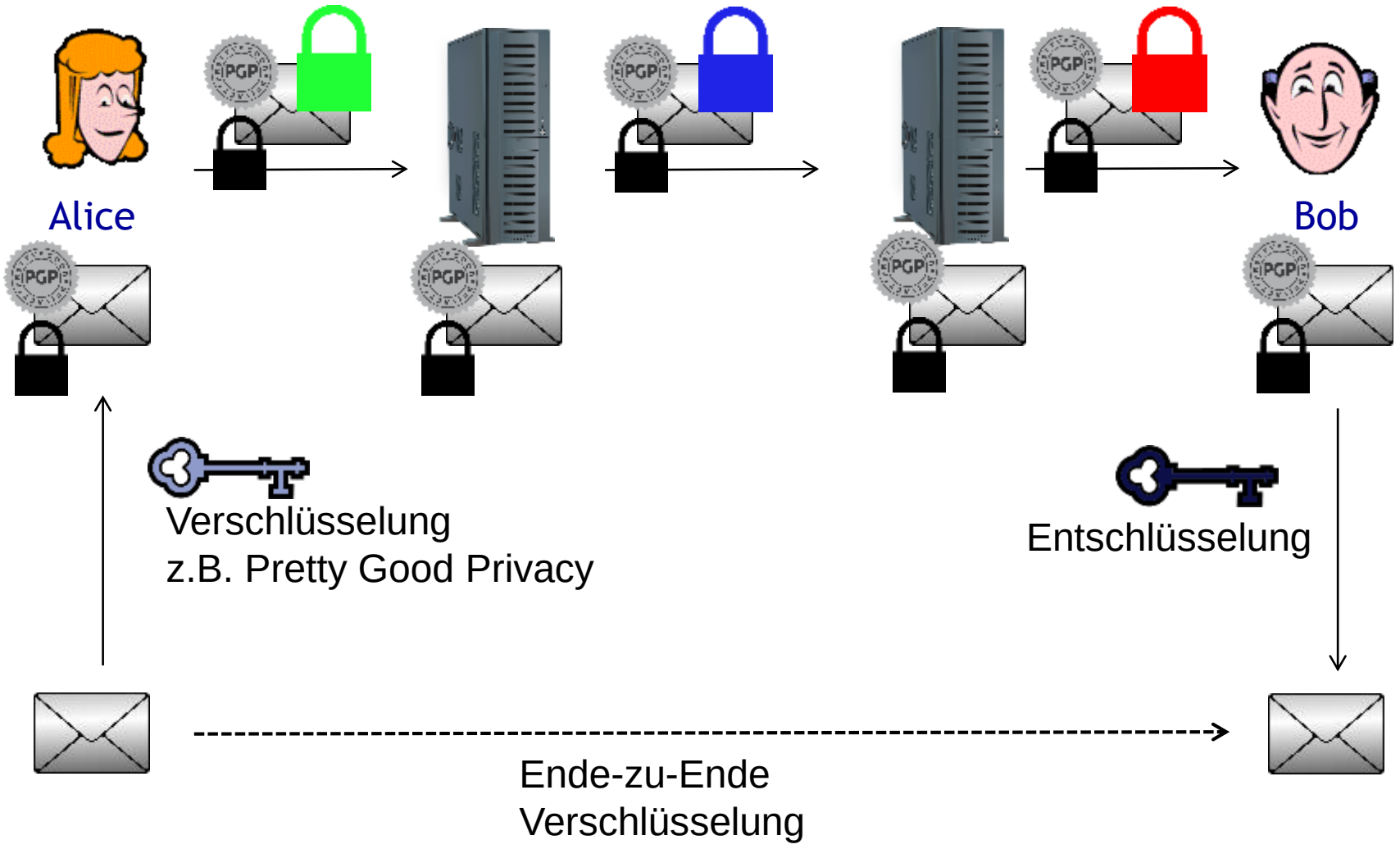
Speicherung und Austausch der Schlüssel



Ende-zu-Ende Verschlüsselung
Beispiel: Email

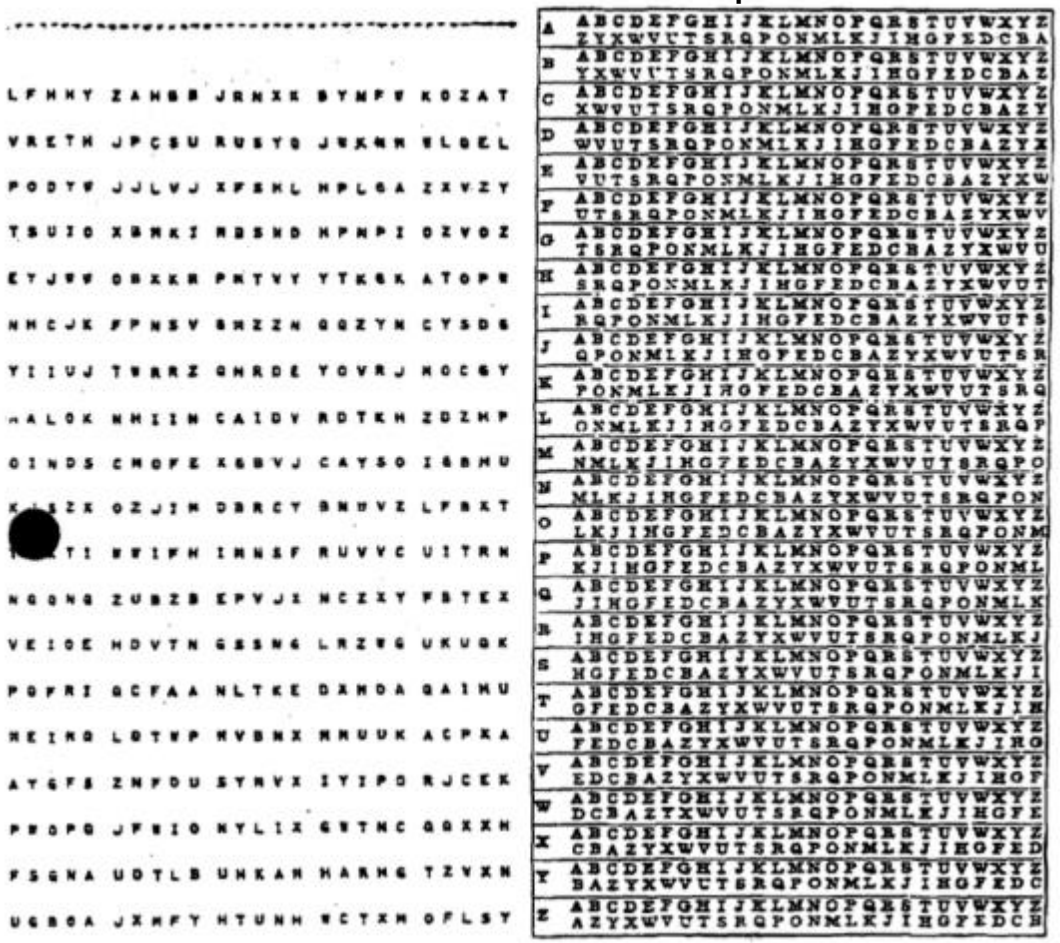


Ende-zu-Ende Verschlüsselung
Beispiel: Email



Nachweisbarkeit der Sicherheit?

One-Time Pad / Vernam Cipher



[National Security Agency (NSA), 1973]

- Traditionelle Sicherheits“beweise“: Reduktion auf angenommen schweres Problem
- One-Time Pad
  - Sicher
  - Voraussetzung: Schlüssel hat selbe Länge wie Nachricht
  - Schlüssel muss vorher (sicher) ausgetauscht werden

mobile business

Agenda

1. Verschlüsselung
2. Überwachungsmaßnahmen
3. Seitenkanalattacken
4. Zusammenfassung

Anwendungsbeispiele





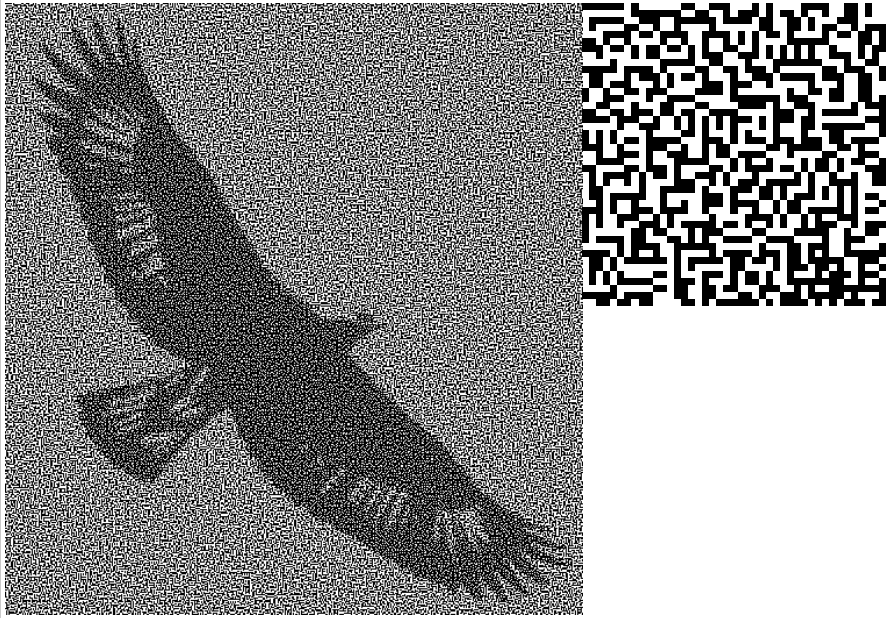

Kryptographie ist ein Werkzeug

Ziel: Nur für „die Guten“ einsetzbar

Umsetzung?

Verschlüsselungsverbot

- Halten sich Kriminelle daran?
- Kontrollierbarkeit

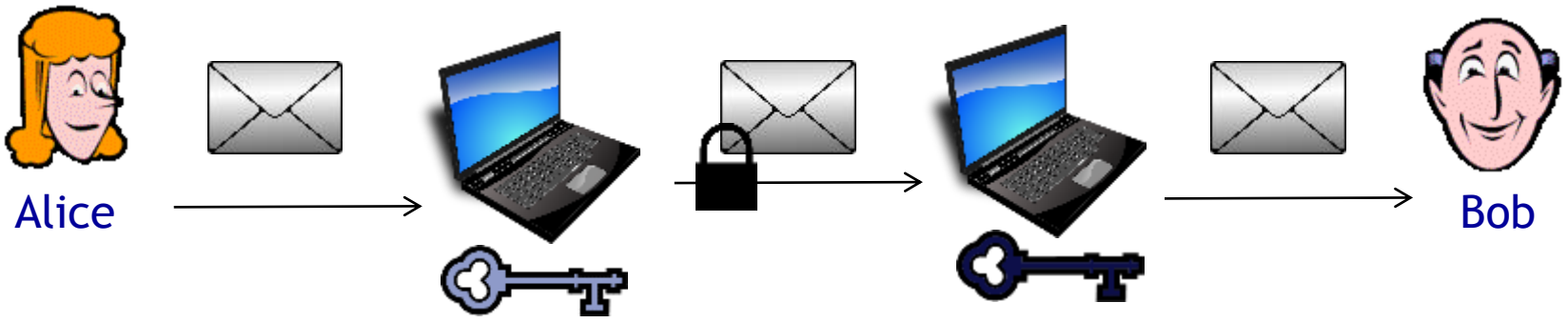


[Borchert]

Steganographie

- Linguistisch
- Geheimsprache / Jargon
  z.B. „Stoff“ = „Drogen“
- Technisch in Bildern, Audio, Video

(überwachte) Schlüsselhinterlegung



Hinterlegung

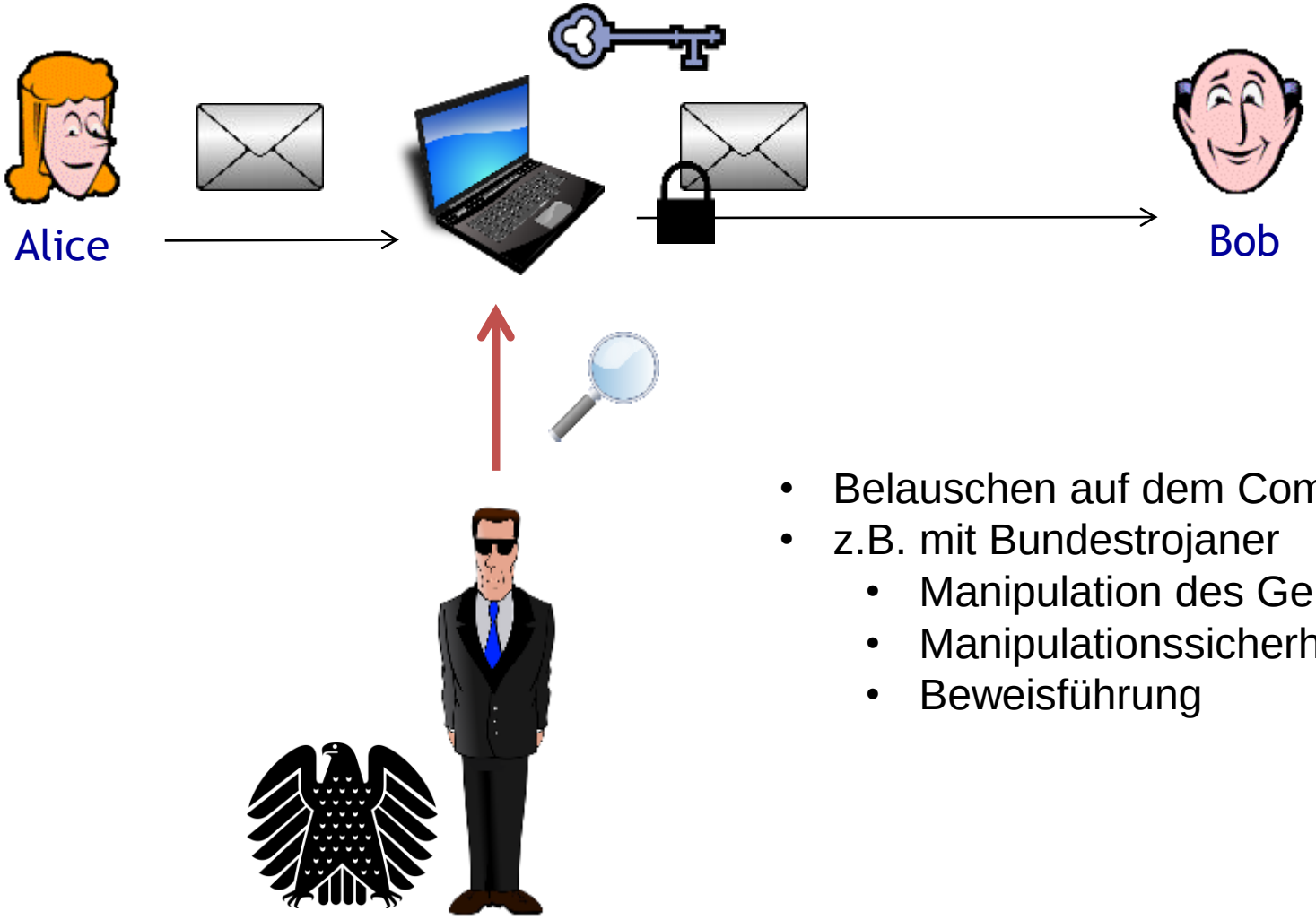
- Zentrale Instanz
- Durchsetzung kompliziert
  - Mehrfachverschlüsselung
  - Steganographie
  - Überwachung „richtiger Schlüssel“?

Hintertüren

- Schwächen in Implementierung
- Schwächen in Algorithmus bzw. bei der Parameterwahl

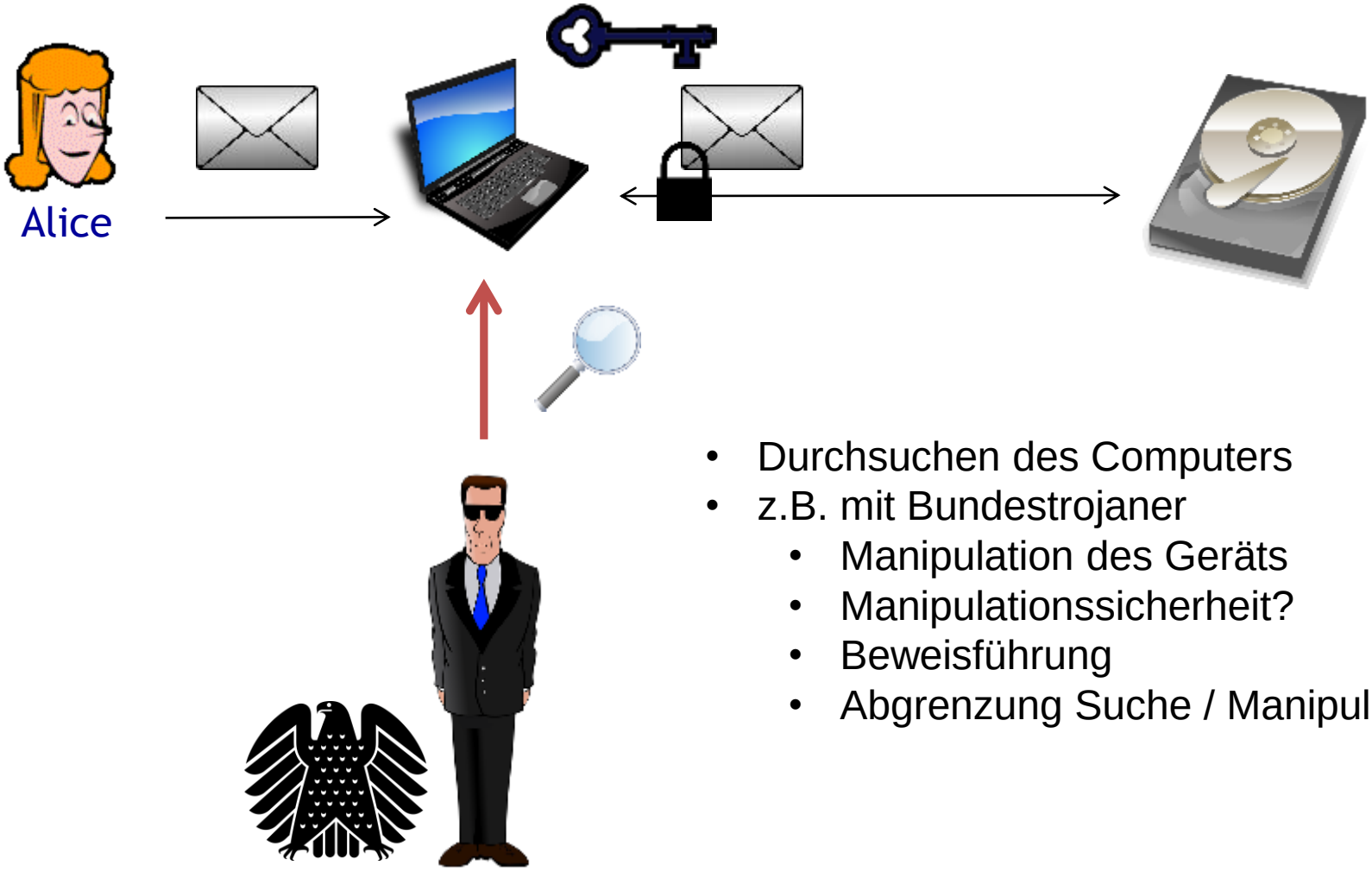
- Beispiel: Dual EC_DRBG (NSA), Standardisierung NIST 800-90, Parameterwahl folgte mit dem Ziel das grundlegende mathematische Problem zu vereinfachen

QuellenTKÜ



- Belauschen auf dem Computer
- z.B. mit Bundestrojaner
  - Manipulation des Geräts
  - Manipulationssicherheit?
  - Beweisführung

Onlinedurchsuchung



- Durchsuchen des Computers
- z.B. mit Bundestrojaner
  - Manipulation des Geräts
  - Manipulationssicherheit?
  - Beweisführung
  - Abgrenzung Suche / Manipulation

Agenda

1	Grundlagen
2	Überwachungsmaßnahmen
3	Seitenkanalattacken
4	Zusammenfassung

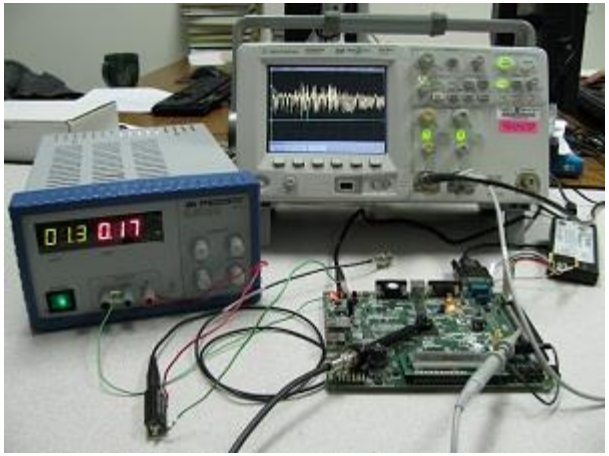
Seitenkanalangriffe I

Ein sicherer Kryptoalgorithmus bedeutet noch nicht, dass seine Implementierung auch sicher ist.

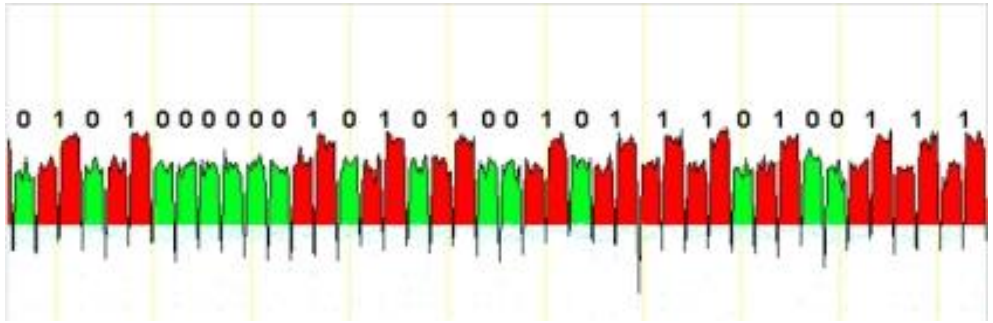
[Tromer]

Seitenkanalangriffe II

Seitenkanäle: Zeit, Strom, Geräusche, Strahlung, ...



[CESCA]



[Goodwill]

- Andere Daten (Seitenkanal) liefern Informationen
- Schluss auf Werte der Berechnung möglich

mobile business

Agenda

1	Grundlagen
2	Überwachungsmaßnahmen
3	Seitenkanalattacken
4	Zusammenfassung

Zusammenfassung

Kryptographie:

- Nicht trivial einsetzbar
- Keine Universallösung
- Aktuelle Systeme nicht beweisbar sicher

Einsatz von Kryptographie / Steganographie:

- Schwer überwachbar
- Schwer kontrollierbar

Mögliche Lösung(?): Überwachung durch Seitenkanalangriffe.

- Aufwändig
- Schwer zu verhindern

Deutsche Telekom Chair of Mobile Business & Multilateral Security

Dr. Sebastian Pape
Goethe University Frankfurt
Theodor-W.-Adorno-Platz 4
60629 Frankfurt, Germany

Phone +49 (0)69 798 34668
Fax +49 (0)69 798 35004

E-Mail: sebastian.pape@m-chair.de
WWW: www.m-chair.de