CoNe Freiburg

IIF INSTITUT FÜR INFORMATIK FREIBURG

Systeme II

3. Sicherheit

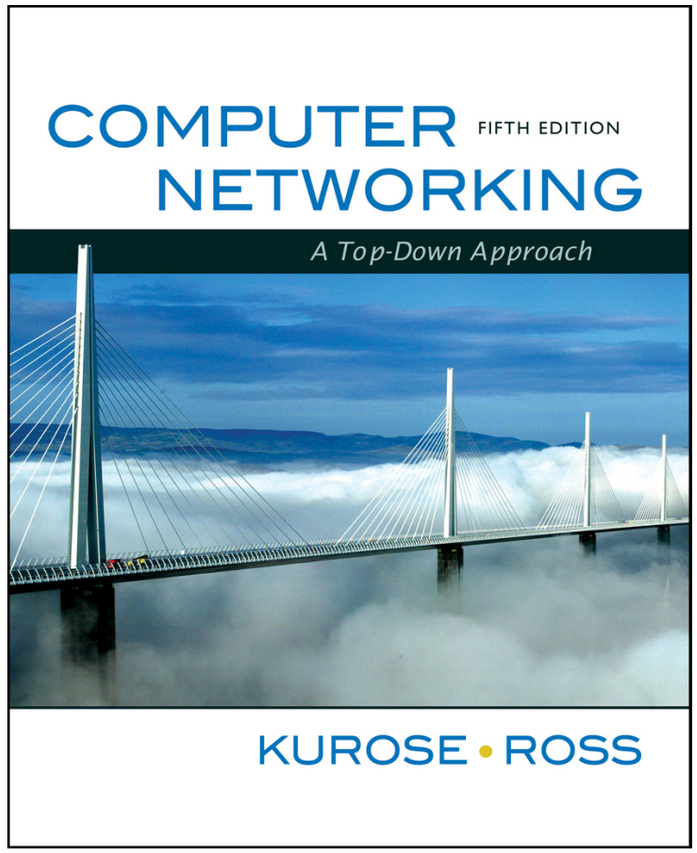
Thomas Janson°, Kristof Van Laerhoven*, Christian Ortolf°
Folien: Christian Schindelhauer°
Technische Fakultät
°: Rechnernetze und Telematik, *: Eingebettete Systeme
Albert-Ludwigs-Universität Freiburg
Version 24.04.2015

UNI FREIBURG

CoNe Freiburg

Sicherheit

- Folien und Inhalte aus
  - Computer Networking: A Top Down Approach 5th edition. Jim Kurose, Keith Ross Addison-Wesley, April 2009.
- Copyright liegt bei den Autoren Kurose und Ross



UNI FREIBURG

CoNe Freiburg

Ziele

- Grundlagen von Netzwerksicherheit
  - Kryptographie und deren vielfältige Einsatzmöglichkeiten
  - Authentifizierung
  - Message Integrity
- Sicherheit in der Praxis
  - Firewalls und Intrusion Detection
  - Sicherheit in Anwendungs-, Transport-, Vermittlungs- und Sicherungsschicht

UNI FREIBURG

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

CoNe Freiburg

Was ist Netzwerk-Sicherheit

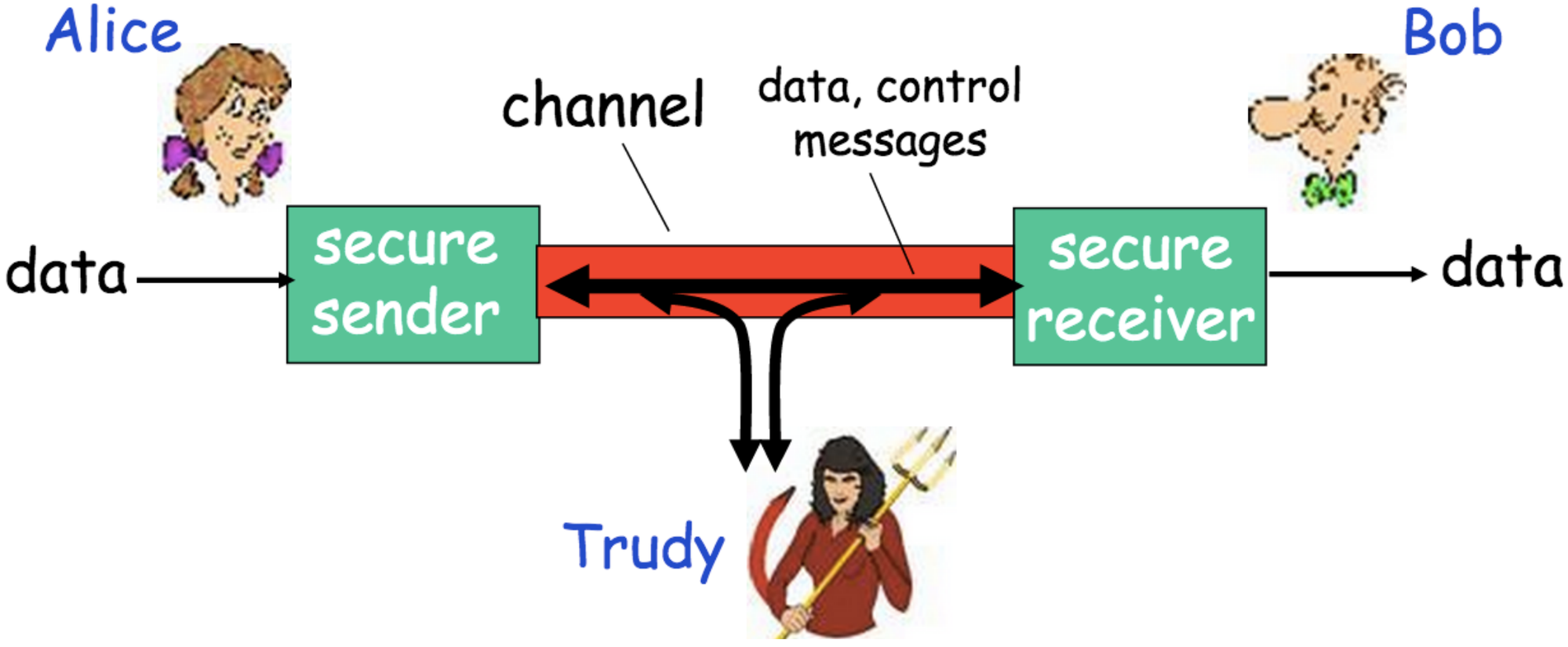
- Vertraulichkeit (Confidentiality)
  - Nur der Sender, gewünschter Empfänger sollte den Nachrichteninhalt „verstehen“
- Authentifizierung
  - Sender und Empfänger möchten sich ihrer Identität versichern
- Integrität (message integrity)
  - Sender und Empfänger wollen, dass eine Nachricht nicht unbemerkt verändert werden
    - bei der Übertragung oder später
- Zugriff und Verfügbarkeit
  - von Diensten

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

UNI FREIBURG

Freunde und Feinde: Alice, Bob und Trudy

- Standardnamen im Sicherheitsbereich
- Alice und Bob möchten „sicher“ kommunizieren
- Trude (In-Trude-r) möchte mithören, löschen, hinzufügen, verändern



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

CoNe Freiburg

Wer steckt hinter Alice und Bob

- Echte Menschen
- Web-Browser
- Online-Banking-Clients und Servers
- DNS-Servers
- Routers, die Routing-Tabellen austauschen
- etc.

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

UNI FREIBURG

CoNe Freiburg

Angriffsmethoden: Was kann ein böser Mensch so tun?

- Abhören (eavesdrop)
  - Nachrichten abfangen und lesen
- Einfügen von Nachrichten
  - Nachrichten werden in die bestehende Verbindung eingefügt
- Sich als jemand anders ausgeben (impersonation)
  - Quell-Adresse kann in einem Paket gefälscht werden
- Hijacking
  - Übernahme einer bestehenden Verbindung durch Ersetzen des Empfängers oder Senders
- Denial of Service
  - Dienst abschalten
    - durch Überlast oder direkten Angriff

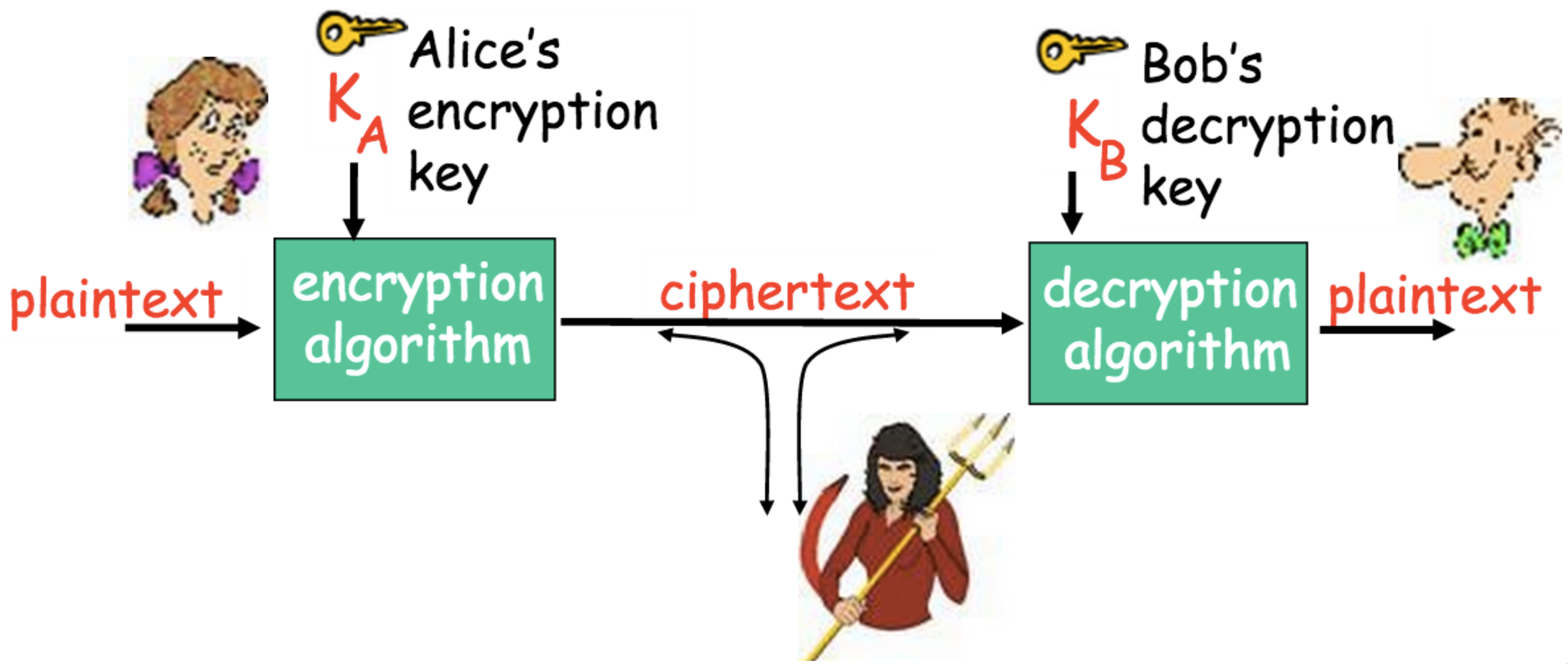
Computer Networking: A Top Down Approach
Jim Kurose, Keith Ross, Addison-Wesley, April 2009.

UNI FREIBURG

CoNe Freiburg

Ein kurzer Rundgang durch die Kryptographie

- m: Originalnachricht (message)
- $K_A(m)$: mit Schlüssel K_A verschlüsselte Nachricht
- $m = K_B(K_A(m))$



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

Einfache Verschlüsselung: Monoalphabetisch

- Ersetze jeden Buchstaben durch einen anderen
- Beispiel: Edgar Allen Poe „The Gold Bug“ (1843)

53‡‡†305))6*;4826)4‡.)4‡);806*;48†8
¶60))85;;]8*;:‡*8†83(88)5*†;46(;88*96
?;8)‡(;485);5*†2:*‡(;4956*2(5*—4)8
¶8*;4069285);)6†8)4‡‡;1(‡9;48081;8:8‡
1;48†85;4)485†528806*81(‡9;48;(88;4
(‡?34;48)4‡;161;:188;‡?;

- Jedes Symbol steht für einen Buchstaben:
5 3 ‡ ‡ † 3 0 5)) 6 * ; 4 8 2 6) 4 ‡ .) 4 ‡) ; 8 0 6 * ;
a g o o d g l a s s i n t h e b i s h o p s h o s t e l i n t

Einfache Verschlüsselung: Monoalphabetisch

- Ersetze jeden Buchstaben durch einen anderen

```
plaintext:   abcdefghijklmnopqrstuvwxyz
ciphertext:  mnbvcxzasdfghjklpoiuytrewq
```

E.g.:

```
Plaintext: bob. i love you. alice
ciphertext: nkn. s gktc wky. mgsbc
```

CoNe Freiburg

Polyalphabetische Verschlüsselung

- n monoalphabetische Schlüssel, $M_1,M_2,\ldots,M_n$
- Zyklus-Muster
  - e.g., n=4, M_1,M_3,M_4,M_3,M_2; M_1,M_3,M_4,M_3,M_2;
- Für jeden neuen Buchstaben aus den monoalphabetischen Schlüsseln einer ausgewählt
  - „aus“: a from M_1, u from M_3, s from M_4
  - Schlüssel: n Schlüsselverfahren und der Zyklus

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

CoNe Freiburg

Bruch einer Kodierung

- Cipher-text only Attack
  - nur mit verschlüsselten Text
  - Zwei Ansätze:
    - Durchsuche alle Schlüssel und teste ob sie einen vernünftigen Text produzieren
    - Statistische Analyse des Schlüssels
- Known Plaintext Attack
  - mit der Originalnachricht und dem verschlüsselten Text
- Chosen Plaintext Attack
  - Trudy wählt den Text und lässt Alice ihn verschlüsseln
  - Trudy erhält den verschlüsselten Text

UNI FREIBURG

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