CoNe Freiburg

IIF INSTITUT FÜR INFORMATIK FREIBURG

Systeme II

7. Sicherheit

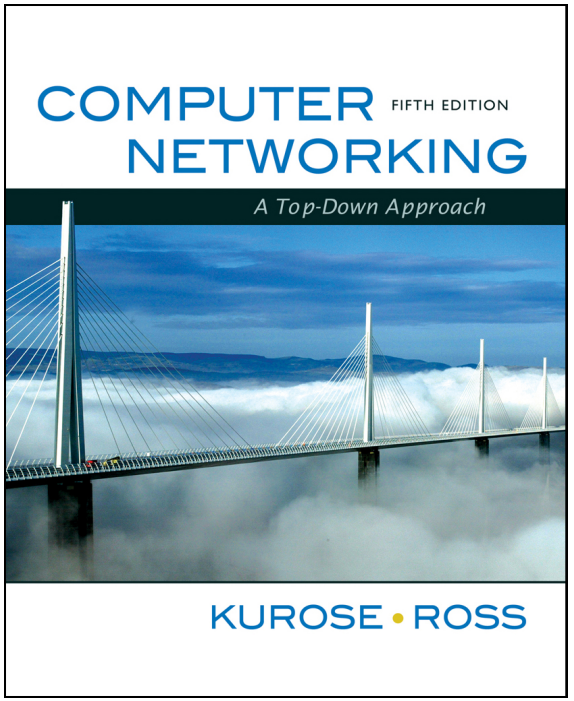
Christian Schindelhauer
Technische Fakultät
Rechnernetze und Telematik
Albert-Ludwigs-Universität Freiburg
(Version 14.07.2014)

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

CoNe Freiburg

Was ist Netzwerk-Sicherheit

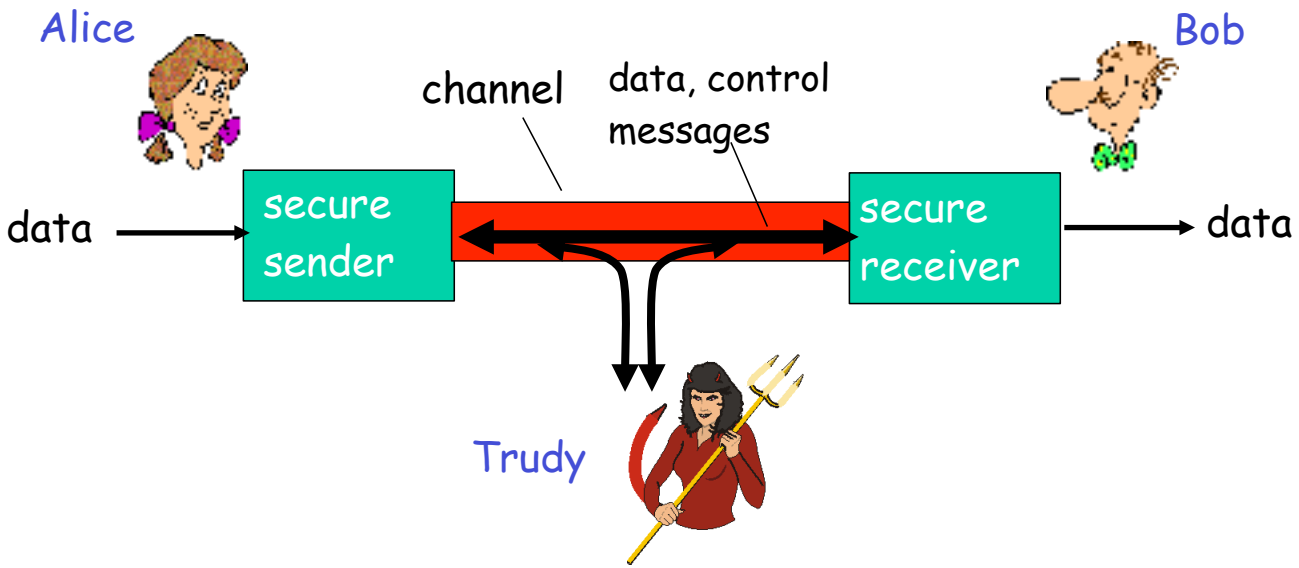
- Vertraulichkeit (Confidentiality)
  - Nur der Sender, gewünschter Empfänger sollte den Nachrichteninhalt „verstehen“
- Authentifizierung
  - Sender und Empfänger möchten sich ihrer Identität versichern
- Integrität (message integrity)
  - Sender und Empfänger wollen, dass eine Nachricht nicht unbemerkt 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



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.

CoNe Freiburg

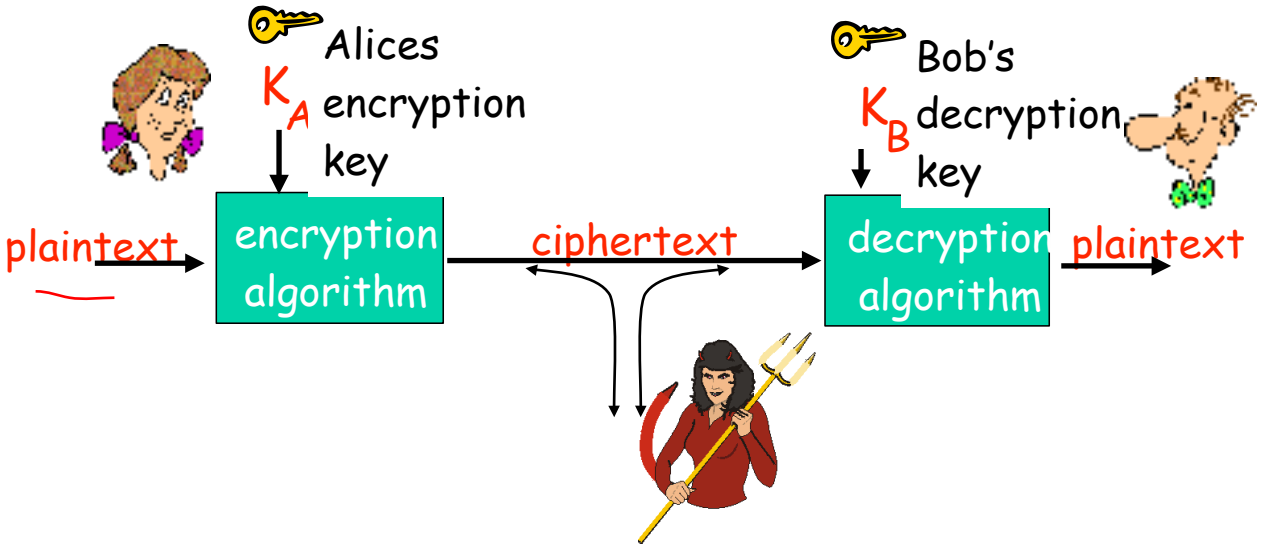
Was kann ein böser Mensch so tun?

- 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

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.

UNI FREIBURG

CoNe Freiburg

Einfache Verschlüsselung

- Monoalphabetischer Schlüssel
  - ersetze jeden Buchstaben durch einen anderen
- Beispiel: Edgar Allen Poe „The Gold Bug“
  - 53305))6*;4826)4)4;806*;488¶60))85;1-(;:*8-83(88)5*
  - ;46(;88*96*?;8)*(;485);5*2:*(;4956*2(5*-4)8¶8*;40692
  - 85);)68)4;1(9;48081;8:81;4885;4)485528806*81(9;48;
  - (88;4(?34;48)4;161;:188;?;
- Jedes Symbol steht für einen Buchstaben:
  - 8 = e
  - ; = h
  - ...

UNI FREIBURG

CoNe Freiburg

Einfache Verschlüsselung

- Monoalphabetischer Schlüssel
  - 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

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

CoNe Freiburg

Methoden der Kryptographie

- Geheime Schlüssel sind die Sicherheitsgrundlage
  - Der Algorithmus ist bekannt
    - außer bei „security by obscurity“
- Public-Key-Cryptography
  - verwendet zwei Schlüssel
  - ein geheimer und ein öffentlicher Schlüssel
- Symmetrische Kryptographie
  - beide Seiten verwenden den selben geheimen Schlüssel
- Hash-Funktion
  - Ohne Schlüssel und ohne Geheimnis

CoNe Freiburg

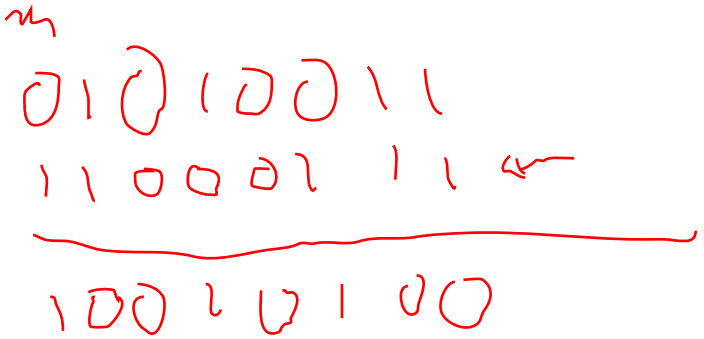
Chiffrierungstypen

- Stromchiffrierer (stream cipher)
  - verschlüsselt bitweise
- Blockchiffre, Blockverschlüsselung (block ciphers)
  - Originaltext wird in gleichgroße Blöcke unterteilt
  - Jeder Block wird einzeln kodiert

CoNe Freiburg

Stream Ciphers

- Kombiniere jedes Bit eines Schlüsselstroms (key stream) mit dem Original bit
  - m(i) = i-tes Bit der Nachricht
  - ks(i) = i-tes Bit des Key Streams
  - c(i) = i-tes bit des verschlüsselten Texts



- Verschlüsselung
  - c(i) = ks(i) + m(i) (mod 2)
    = ks(i) ⊕ m(i)
- Entschlüsselung
  - m(i) = ks(i) ⊕ c(i)

CoNe Freiburg

RC4 Stream Cipher

- RC4 ist ein populärer Streamchiffrierer
  - ausführlich analysiert und als sicher angesehen
  - Schlüssellänge: von 1 bis 256 Bytes
  - wird in WEP für 802.11 verwendet
  - kann in SSL verwendet werden

CoNe Freiburg

Quell-Code RC4

```
k[]: gegebene Schlüssel-Zeichenfolge der Länge 5 bis 256 Byte
L := Länge des Schlüssels in Byte
s[]: Byte-Vektor der Länge 256
 Für i = 0 bis 255
   s[i] := i
 j := 0
 Für i = 0 bis 255
   j := (j + s[i] + k[i mod L]) mod 256
   vertausche s[i] mit s[j]
```

```
klar[]: gegebene Klartext-Zeichenfolge der Länge X
schl[]: Vektor zum Abspeichern des Schlüsseltextes
 i := 0
 j := 0
 Für n = 0 bis X-1
   i := (i + 1) mod 256
   j := (j + s[i]) mod 256
   vertausche s[i] mit s[j]
   zufallszahl := s[(s[i] + s[j]) mod 256]
   schl[n] := zufallszahl XOR klar[n]
```

- Aus Wikipedia
  - http://de.wikipedia.org/wiki/Rc4

UNI FREIBURG

CoNe Freiburg

Block-Chiffre

- Nachrichten werden in Blöcken von k bits verschlüsselt
  - z.B. 64-bit Blöcke
- Injektive Abbildung um den Quelltext in den k-bit verschlüsselten Text umzuwandeln
- Beispiel k=3:

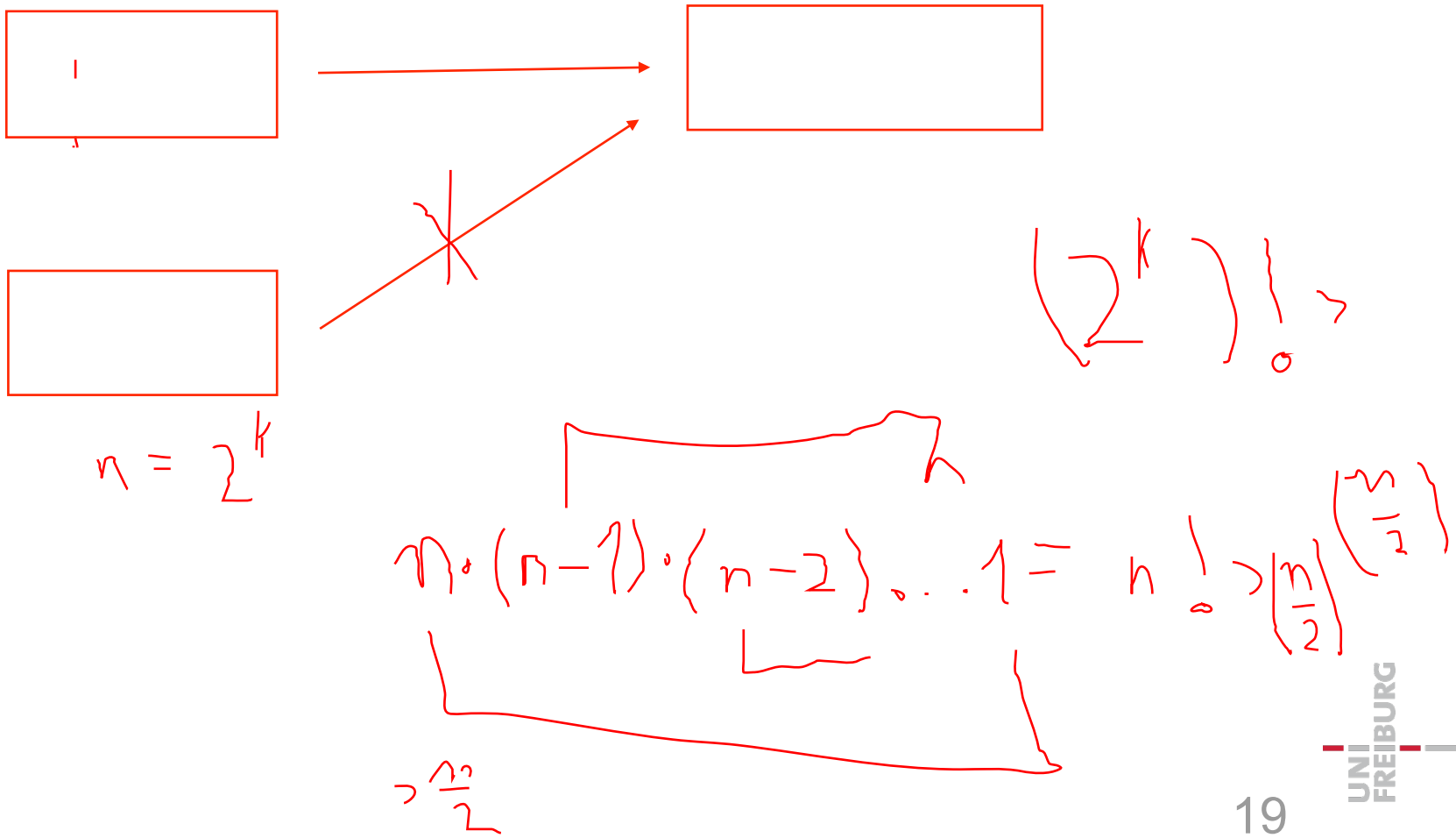
input	output
000	110
001	111
010	101
011	100

input	output
100	011
101	010
110	000
111	001

CoNe Freiburg

Block-Chiffre

- Wie viele mögliche Abbildungen gibt es für k-Bit Block-Chiffre?



UNI FREIBURG

CoNe Freiburg

Block-Chiffre

- Wie viele mögliche Abbildungen gibt es für k-Bit Block-Chiffre?
  - Im allgemeinen: $2^k!$
  - riesig für k=64
  - und absolut sicher, wenn man sie zufällig auswählt
- Problem:
  - Die meisten dieser Abbildungen benötigen große Tabellen um sie zu berechnen
- Lösung
  - Statt einer Tabelle, verwendet man eine Funktion, die diese Tabelle simuliert
  - Dadurch verliert man möglicherweise wieder die Sicherheit