Informatik der digitalen Medien

Ergänzungs-Studienangebot der Mediendidaktik für Lehramtstudenten

Dr. rer. nat. Harald Sack
Institut für Informatik
FSU Jena

WInersemester 2005/2006

http://www.informatik.uni-jena.de/~sack/WS0506/infod.htm

Informatik der digitalen Medien

3. Internet und WWW (6)

Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Informatik der digitalen Medien

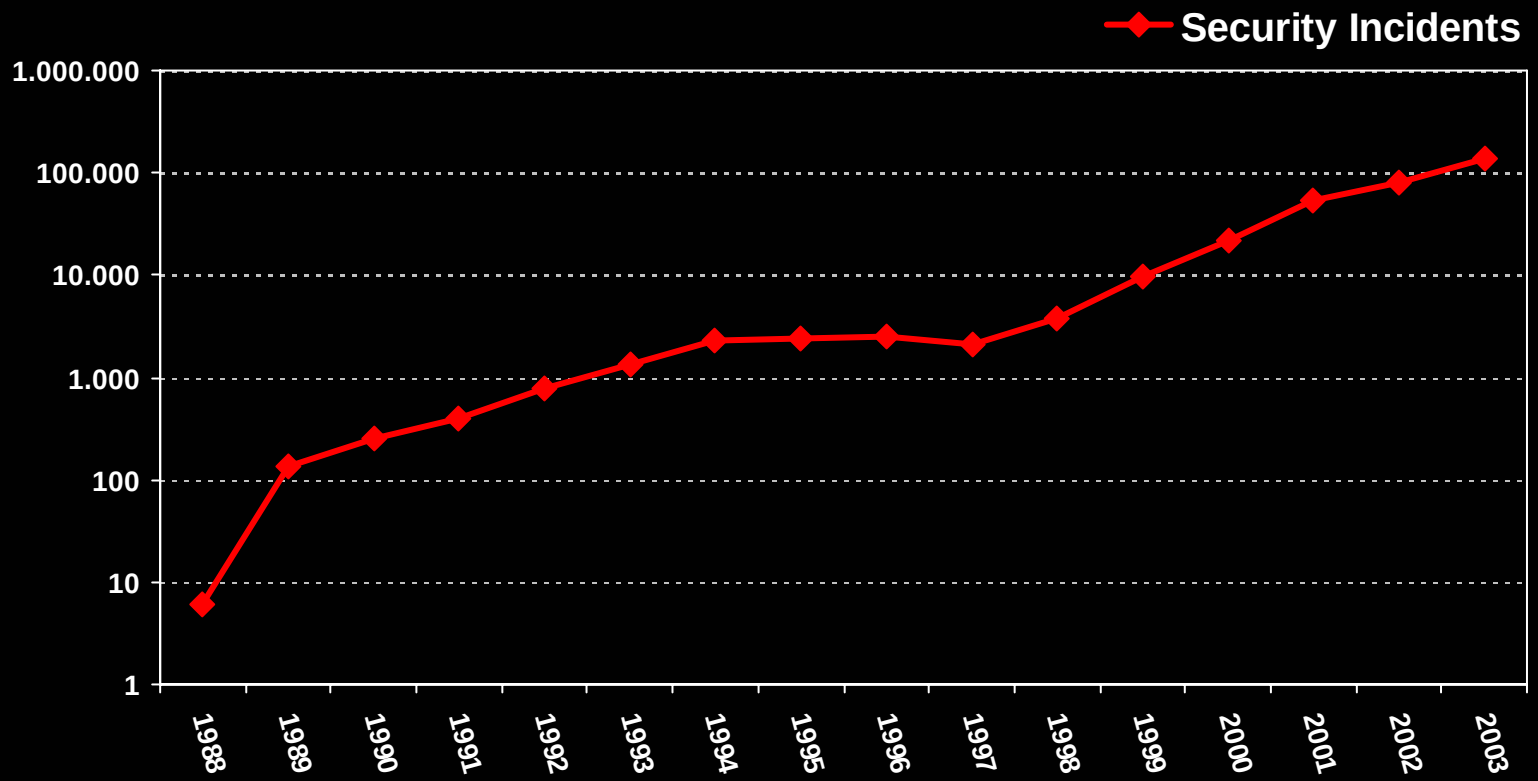
3. Internet und WWW (6)

- Grundlagen der Kryptografie
  - Sicherheitsziele
  - Kurze Geschichte der Kryptografie
  - Symmetrische Schlüsselverfahren
  - Verfahren mit öffentlichem Schlüssel
  - Digitale Signaturen
  - Zertifikate und Sicherheitsinfrastrukturen

Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

- **Grundlagen der Kryptografie**
  - Bekannt gewordene Sicherheitszwischenfälle im Internet



Informatik der digitalen Medien
Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Informatik der digitalen Medien

3. Internet und WWW (6)

- Grundlagen der Kryptografie
  - **Sicherheitsziele**
  - Kurze Geschichte der Kryptografie
  - Symmetrische Schlüsselverfahren
  - Verfahren mit öffentlichem Schlüssel
  - Digitale Signaturen
  - Zertifikate und Sicherheitsinfrastrukturen

Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

- Grundlagen der Kryptografie
  - **Sicherheitsziele**

Cast……

Alice (Sender)

Trudy

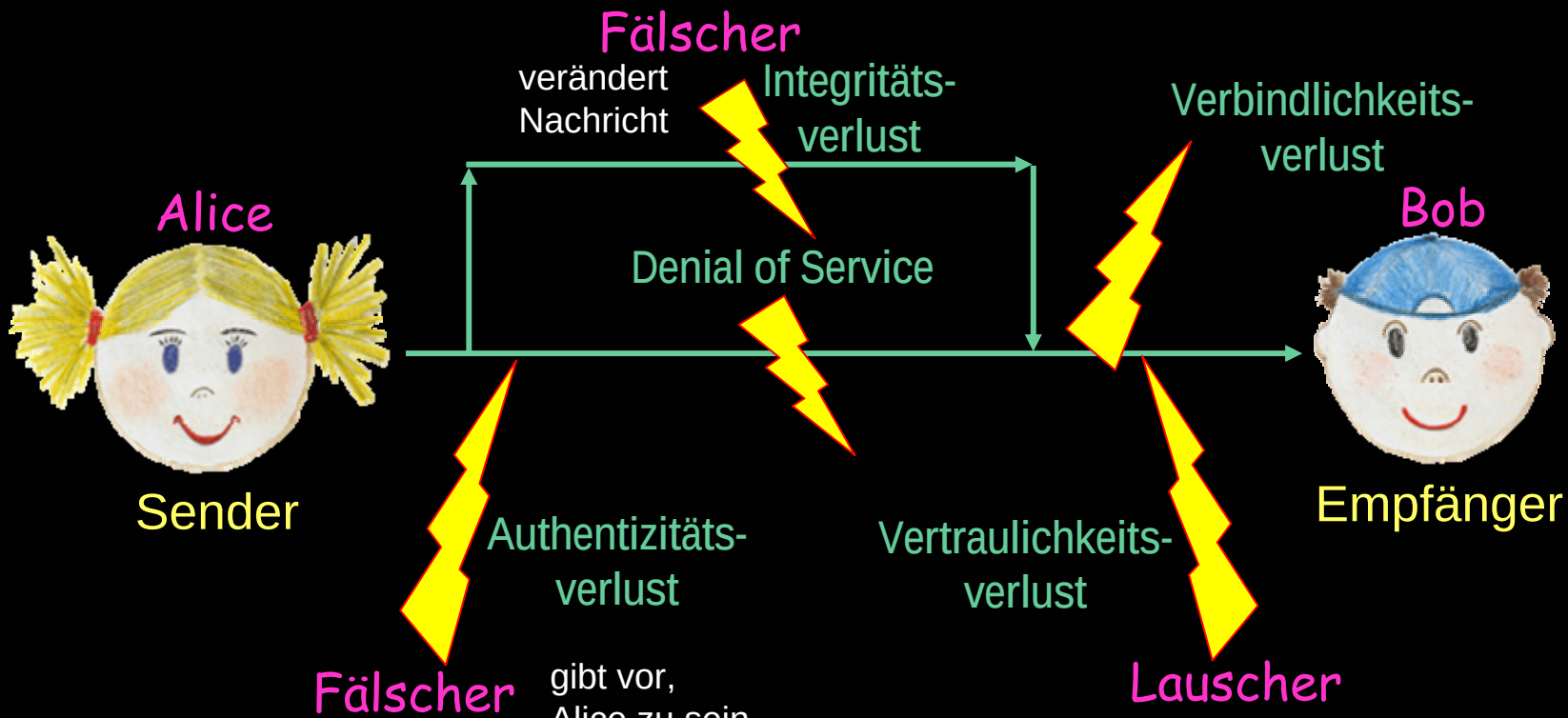
(Eindringling,Lauscherin, Fälscherin, etc..)

Bob (Empfänger)

Informatik der digitalen Medien
Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

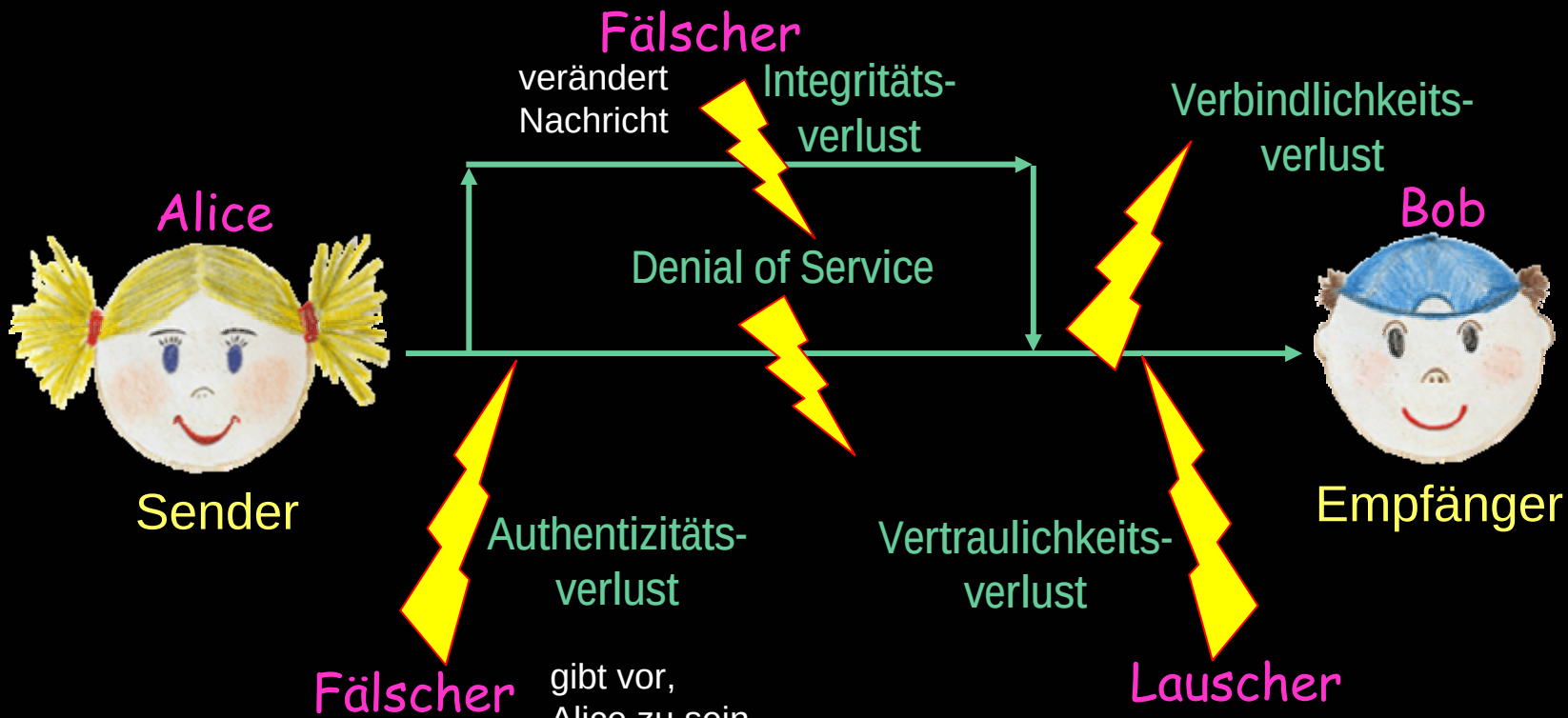
- Grundlagen der Kryptografie
  - **Sicherheitsziele**
    - „sicher ist, dass nichts sicher ist….und selbst das nicht.“



Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

- Grundlagen der Kryptografie
  - **Sicherheitsziele**
    - „sicher ist, dass nichts sicher ist….und selbst das nicht.“



Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

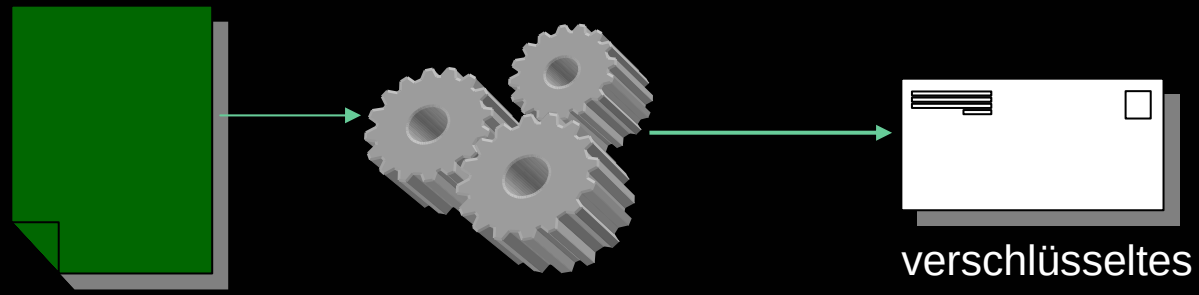
Internet und WWW (6)

- **Sicherheitsziele**
  - **Verfügbarkeit**
    Die zuverlässige Funktionstüchtigkeit der zur Kommunikation verwendeten Medien darf nicht gestört werden können
  - **Datenintegrität**
    Die übertragene Nachricht muss den Empfänger im Originalzustand erreichen und darf nicht verändert werden
  - **Vertraulichkeit**
    Der Inhalt der übermittelten Nachricht darf nur für Sender und Empfänger, nicht für unbefugte Dritte lesbar sein.
  - **Authentifikation**
    Der Empfänger muss sich darauf verlassen können, dass der Absender der Nachricht diese auch tatsächlich verfasst hat
  - **Autorisation**
    Es muss sichergestellt werden, dass niemand anderes als der designierte Empfänger einer Nachricht die Berechtigung hat, diese zu lesen.

Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

- Grundlagen der Kryptografie
  - **Sicherheitsziele**
    - Geheimhaltung durch Verschlüsselung
      - Um eine Nachricht zu verschlüsseln benötigt man dazu ein geeignetes Verfahren



      - **Problem**:
        Wird das Verfahren bekannt, muss man sich ein neues ausdenken (kompliziert)

Informatik der digitalen Medien
Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

- Grundlagen der Kryptografie
  - **Sicherheitsziele**
    - Geheimhaltung durch Verschlüsselung
      - Besser ist ein Verfahren, das auf einfache Weise, **Variationsmöglichkeiten** der durchzuführenden Verschlüsselung bietet
      - Die Parameter zur Einstellung der Variationsmöglichkeiten werden als **Schlüssel** bezeichnet

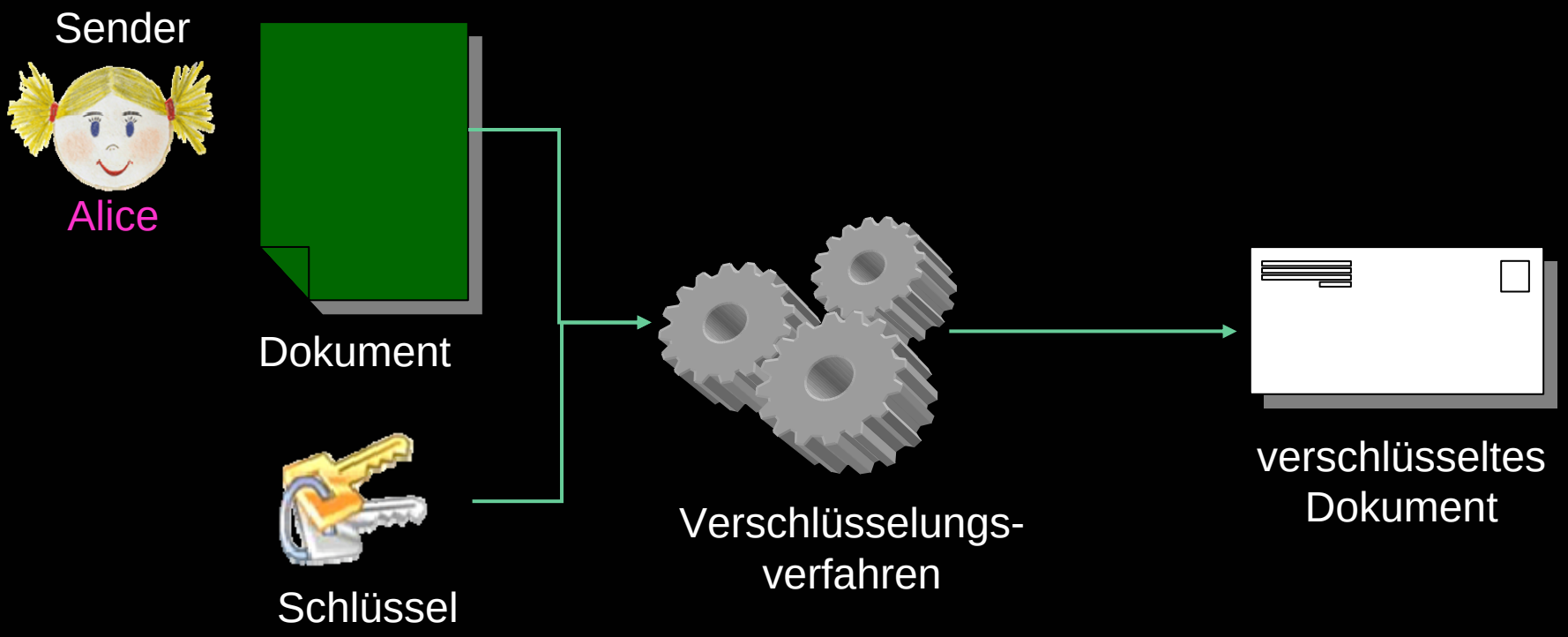
Schlüssel

      - **Vorteil:**
        Verfahren kann bekannt sein, nur der jeweilige **Schlüssel muss geheim gehalten werden**

Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

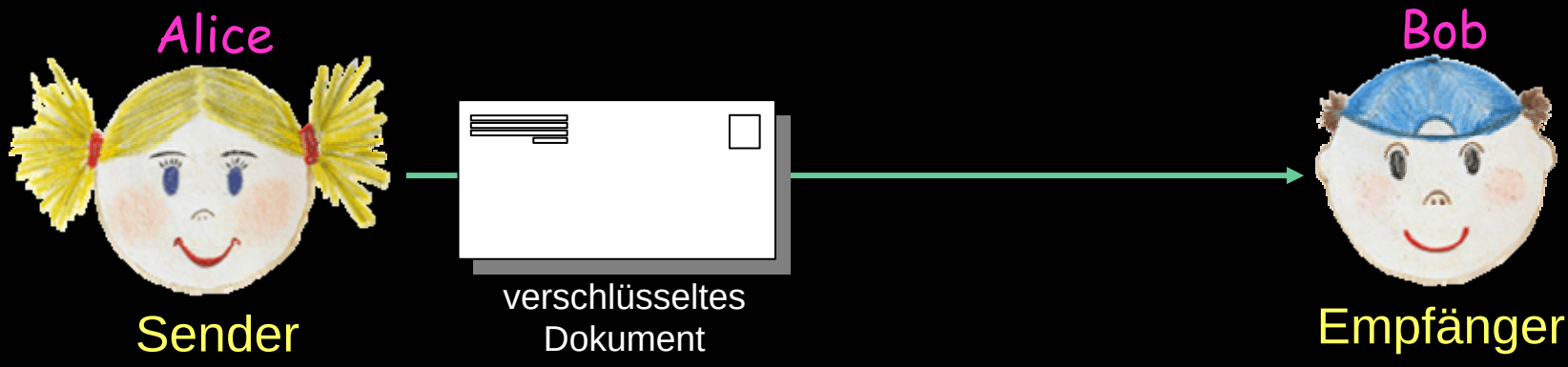
- Grundlagen der Kryptografie
  - **Sicherheitsziele**
    - Geheimhaltung durch Verschlüsselung



Informatik der digitalen Medien
Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

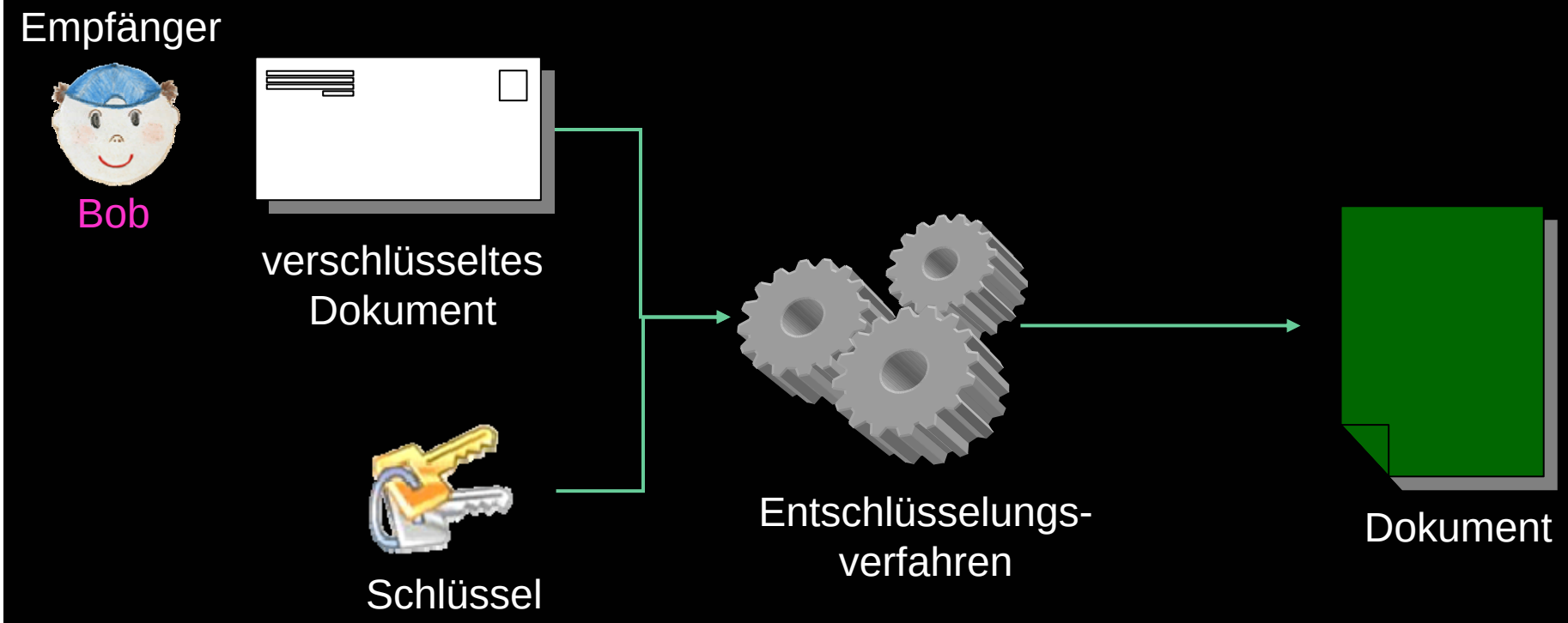
Internet und WWW (6)

- Grundlagen der Kryptografie
  - **Sicherheitsziele**
    - Übermittlung verschlüsselter Nachrichten



Internet und WWW (6)

- Grundlagen der Kryptografie
  - **Sicherheitsziele**
    - Geheimhaltung durch Verschlüsselung



Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Informatik der digitalen Medien

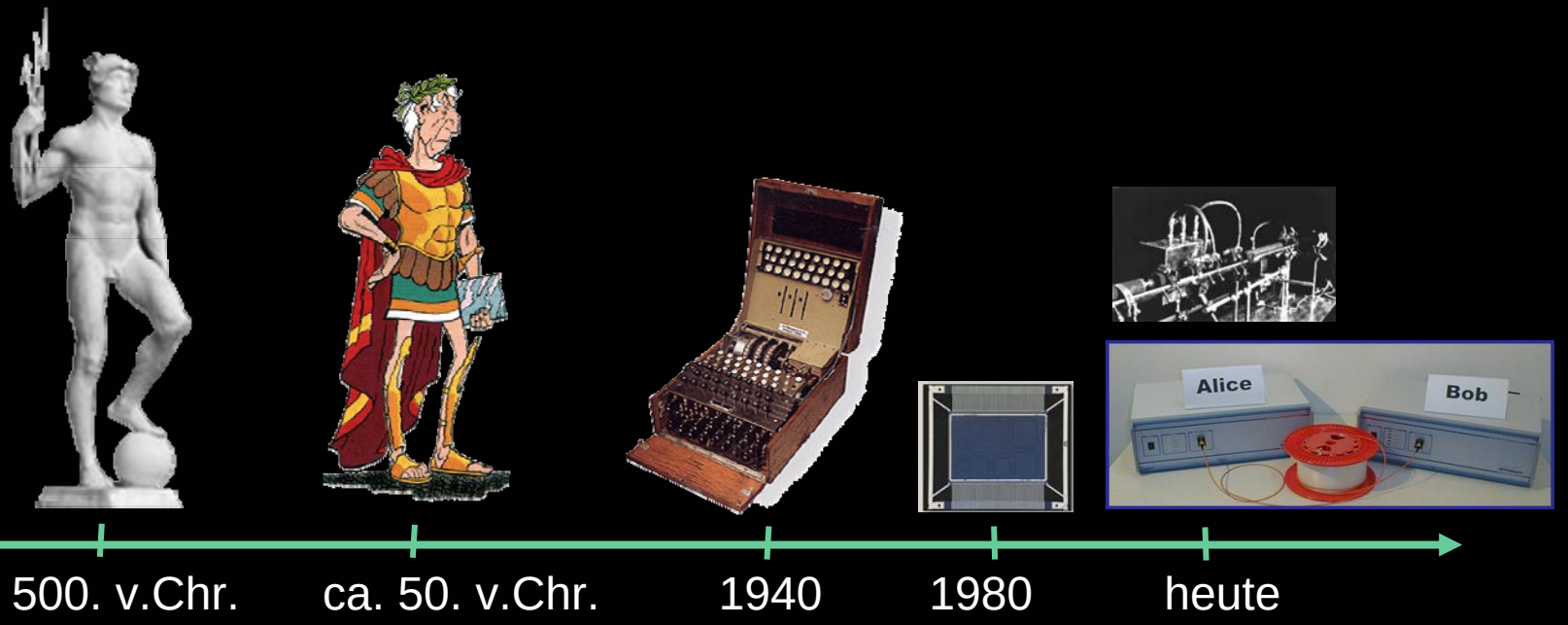
3. Internet und WWW (6)

- Grundlagen der Kryptografie
  - Sicherheitsziele
  - **Kurze Geschichte der Kryptografie**
  - Symmetrische Schlüsselverfahren
  - Verfahren mit öffentlichem Schlüssel
  - Digitale Signaturen
  - Zertifikate und Sicherheitsinfrastrukturen

Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

- Grundlagen der Kryptografie
  - **Kurze Geschichte der Kryptografie**
    - Überblick



Internet und WWW (6)

- Kurze Geschichte der Kryptografie
  - **Die griechische Skytale**
    - **Transpositionschiffre**
      - Im 5. Jhd. v. Chr. verschlüsselten die Spartaner Nachrichten mit Hilfe der Skytale
      - **Position** der Einzelzeichen wird nach einem festen Schema **vertauscht**

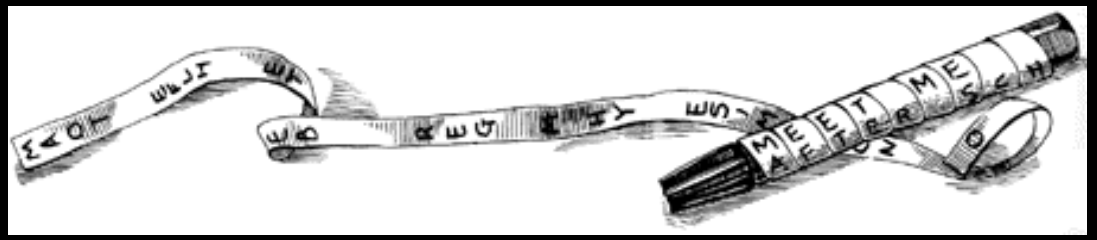
Klartext	DAS IST EIN GEHEIMNIS
Leerzeichen löschen	DASISTEINGEHEIMNIS
verschlüsseln	DEEAIISNMIGNSEITHS

Entschlüsselung

DEEAIISNMIGNSEITHS

DEEAIISNMIGNSEITHS

DEEAIISNMIGNSEITHS



Informatik der digitalen Medien
Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

- Kurze Geschichte der Kryptografie
  - **Cäsar‘s Verschlüsselung**
    - **Substitutionschiffre**
      - im 1. Jhd. v. Chr. nutzte Gaius Julius Cäsar ein einfaches Ersetzungsverfahren als Verschlüsselung
      - jedes **einzelne Zeichen** wird nach festem Schema durch ein anderes Zeichen **ersetzt**

Gaius Julius Cäsar
(100—44 v. Chr.)

Klartext ROMANI ITE DOMUM

Verschlüsselung verschiebe alle Buchstaben um drei Buchstabenwerte weiter

Chiffrat URPDQL LWH GRPXP

A→D
B→E
C→F
D→G
E→H
…

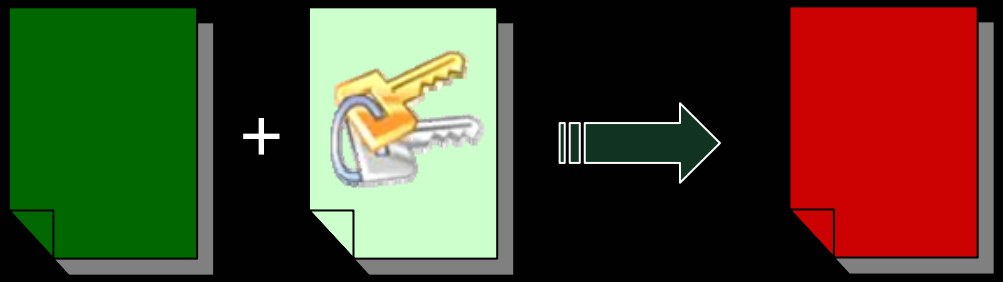
Informatik der digitalen Medien
Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

- Kurze Geschichte der Kryptografie
  - **One Time Pad**
    - wähle einen Schlüssel, der
      - nur **ein einziges Mal** zum Verschlüsseln einer einzigen Nachricht genutzt wird und
      - **genauso lang** ist, wie die Nachricht selbst
    - verknüpfe jedes einzelne Zeichen der Nachricht mit einem Zeichen des Schlüssels

Blaise de Vigenère (1523-1596)

Gilbert Vernam, 1917



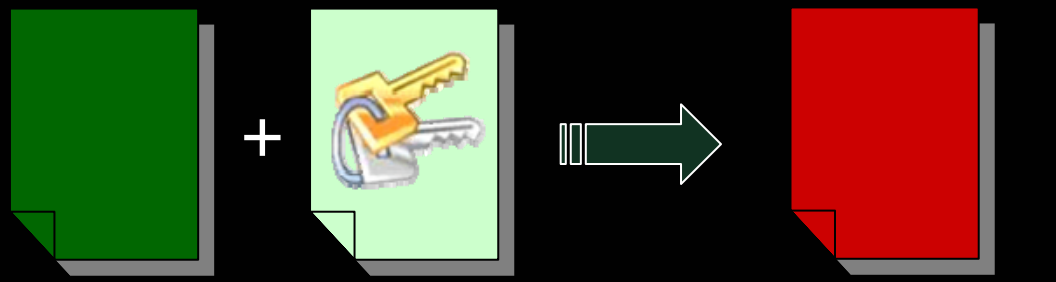
Nachricht Schlüssel verschlüsselte Nachricht

Einfachstes und nachweislich sicheres Verfahren

Informatik der digitalen Medien
Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

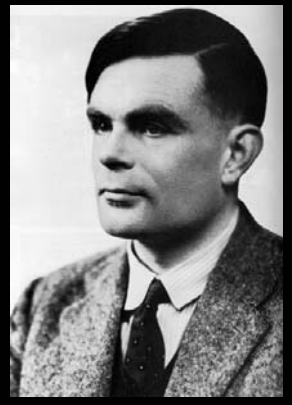
- Kurze Geschichte der Kryptografie
  - **One Time Pad**



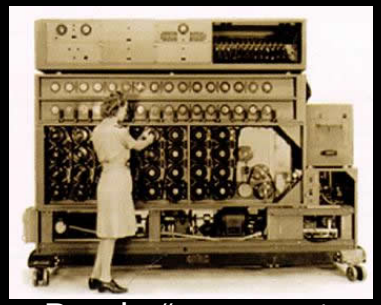
- **Merke**: je **länger** und je **zufälliger** der gewählte **Schlüssel**, desto **schwieriger** ist das Verfahren zu „knacken“!

Internet und WWW (6)

- Kurze Geschichte der Kryptografie
  - **Verschlüsselungsmaschinen**
    - Kombination von Transpositionen und Substitutionen mit dynamisch wechselndem Schlüssel
    - Abfolge und Parameter werden durch **geheimen Schlüssel** bestimmt
    - Berühmtestes Beispiel:
      - **Enigma**
        verschlüsselte Funksprüche der deutschen Wehrmacht im 2. Weltkrieg



Alan Turing
(1916-1954)



„Bombe“ – zur automatischen Entschlüsselung

Enigma - Maschine

Informatik der digitalen Medien
Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

- Kurze Geschichte der Kryptografie
  - **Offene Geheimnisse – öffentliche Schlüssel**
    - Wie komplex die Verschlüsselungsverfahren auch sind, alle hängen bislang von einem **sicheren Austausch der** verwendeten **Schlüssel** ab

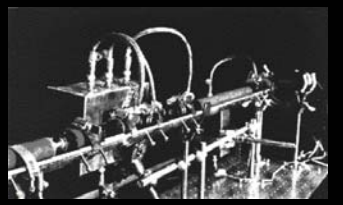
Whitfield Diffie
Martin Hellmann
Ralph Merkle
(1976)

- **Idee:**
  - Gibt es ein Verfahren zur Verschlüsselung, das ohne Austausch eines geheimen Schlüssels auskommt?
- Kommunikation mit **öffentlichen Schlüsseln**
  - **öffentlicher Schlüssel** zum Verschlüsseln (kann von jedem genutzt werden)
  - **geheimer Schlüssel** zum Entschlüsseln (bleibt beim Besitzer)

Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

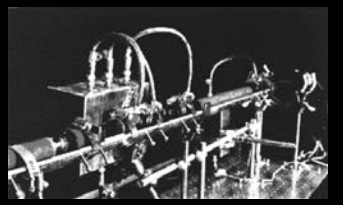
- Kurze Geschichte der Kryptografie
  - **Quantenkryptografie**
    - Absolut sicheres Verschlüsselungsverfahren
    - Nutzt Effekte der **Quantentheorie** aus:
      - in Quantentheorie kann sich ein Elementarteilchen **gleichzeitig in verschiedenartigen Zuständen** befinden (Superposition)
      - erst eine Messung des Zustands legt diesen fest



⇒ Lauscher kann erkannt werden, da er um zu Lauschen eine Messung durchführen muss!

Informatik der digitalen Medien
Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

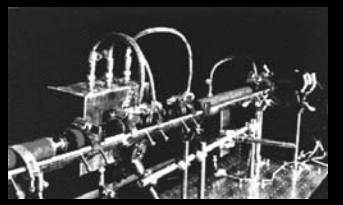


- Kurze Geschichte der Kryptografie
  - **Quantenkryptografie**
    - Einfachstes Beispiel: **Quantenzufallsgenerator**
      - Nutze „**verschränkte**“ Elementarteilchen, d,h.
      - Zwei Teilchen (Quanten) wurden gemeinsam erzeugt und befinden sich in einem „verschränktem“ Superpositions-Zustand
      - Wird der Zustand eines Teilchens durch Messung festgelegt, nimmt das andere („verschränkte“) Teilchen automatisch – und auch über größere Distanzen (Quantenfernwirkung) denselben Zustand an
      - Nutze Effekt, um ein sicheres und absolut zufälliges **One-Time-Pad** zu erzeugen

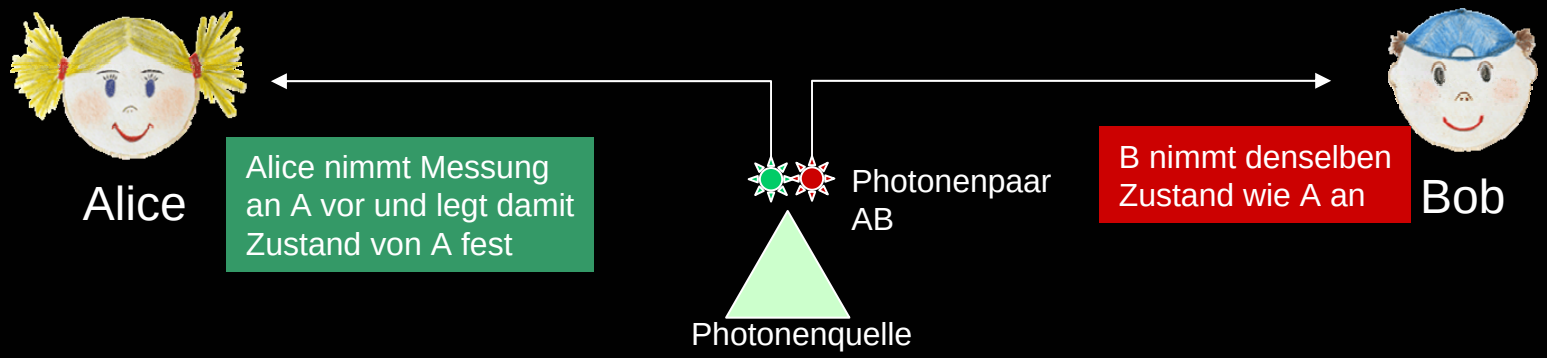
Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

- Kurze Geschichte der Kryptografie
  - **Quantenkryptografie** (stark vereinfacht…)
    - Einfachstes Beispiel: **Quantenzufallsgenerator**



1. Erzeuge Photonenpaar AB, A wird an Alice und B an Bob geschickt
2. Sobald Alice eine Messung an A durchführt, nimmt A – und damit auch B -- einen bestimmten Zustand an
3. Zustand bleibt bis zur Messung völlig unbestimmt (perfekter Zufallsgenerator)



Informatik der digitalen Medien
Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Informatik der digitalen Medien

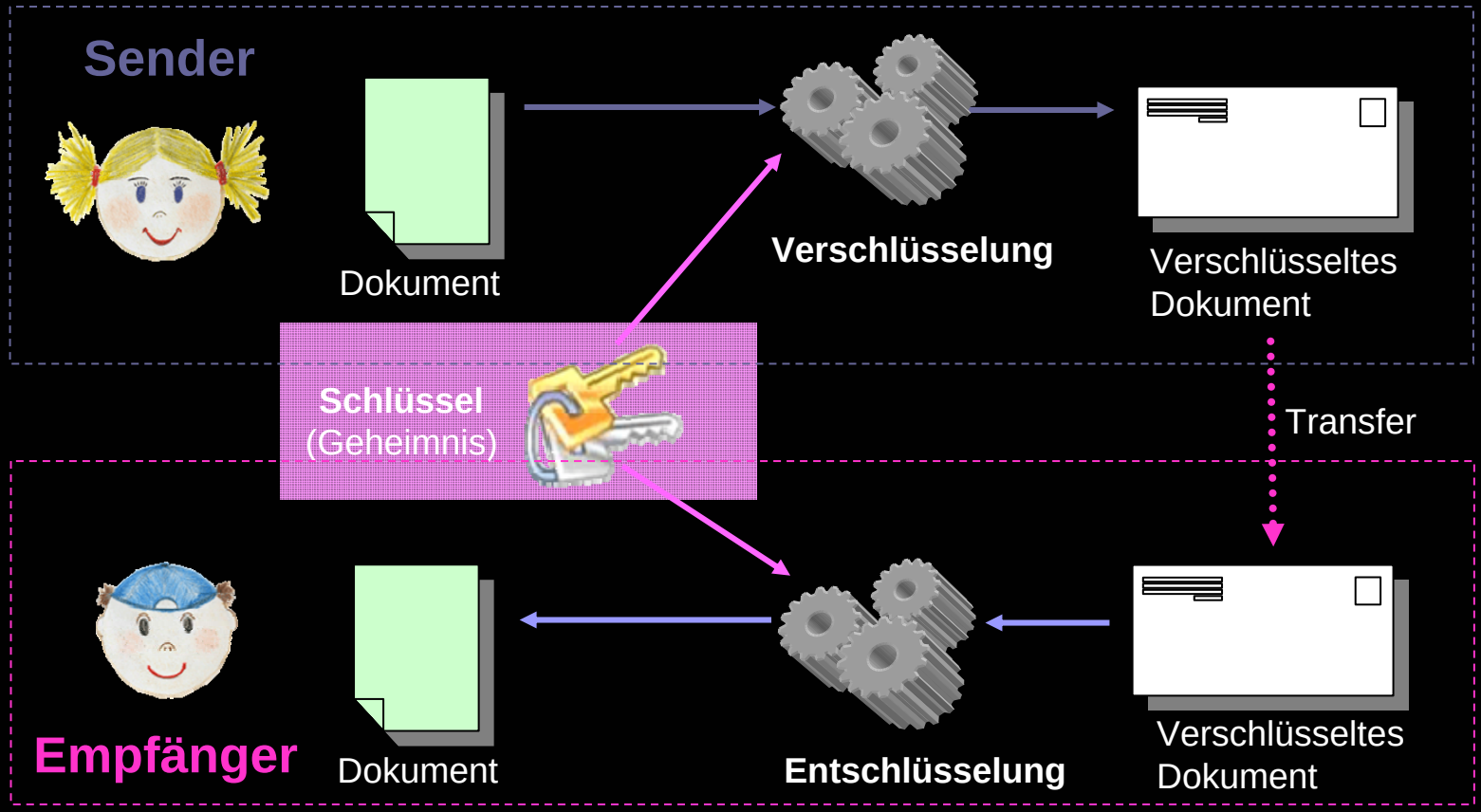
3. Internet und WWW (6)

- Grundlagen der Kryptografie
  - Sicherheitsziele
  - Kurze Geschichte der Kryptografie
  - **Symmetrische Schlüsselverfahren**
  - Verfahren mit öffentlichem Schlüssel
  - Digitale Signaturen
  - Zertifikate und Sicherheitsinfrastrukturen

Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

- Grundlagen der Kryptografie
  - **Symmetrische Verschlüsselungsverfahren**



Informatik der digitalen Medien
Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

- Grundlagen der Kryptografie
  - **Symmetrische Verschlüsselungsverfahren**
    - Sender und Empfänger verwenden einen **identischen Schlüssel**, der nur jeweils den beiden bekannt ist
    - Verschlüsselungsverfahren kann allgemein bekannt sein
    - **Problem:**
      - Sender und Empfänger müssen den jeweils verwendeten Schlüssel zuvor austauschen
      - der Schlüsselaustausch muss geheim gehalten werden!

Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

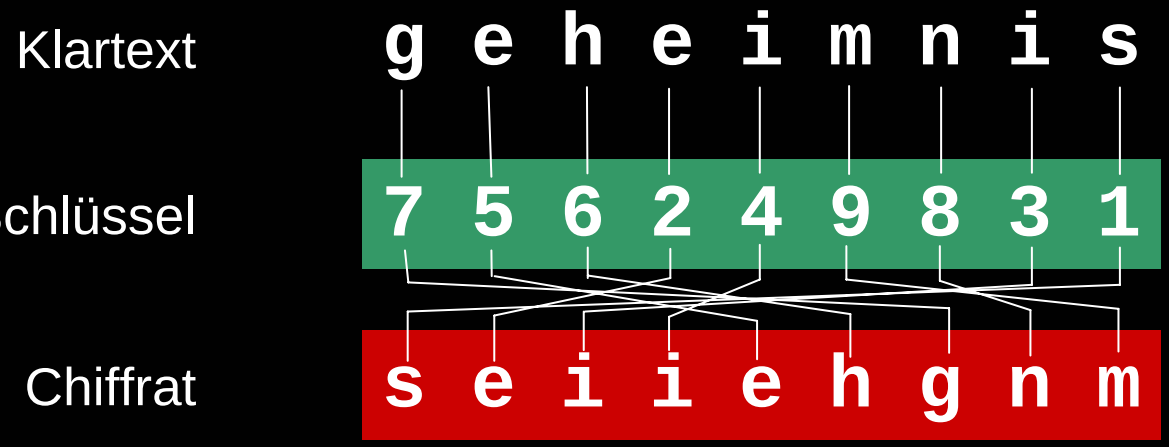
Internet und WWW (6)

- **Symmetrische Verschlüsselungsverfahren**
  - Kryptografische Verfahren mit symmetrischem Schlüsselaustausch
    - Transpositionschiffre
    - Substitutionschiffre
    - Einwegchiffre
    - Blockchiffre und Stromchiffre
    - DES-Verschlüsselung

Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

- Symmetrische Verschlüsselungsverfahren
  - **Transpositionschiffre**
    - verändert die **Position** der einzelnen Zeichen einer Nachricht
    - **k**-stelliger Schlüssel gibt an, wie k Zeichen der Original-nachricht **permutiert** werden sollen



Informatik der digitalen Medien
Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

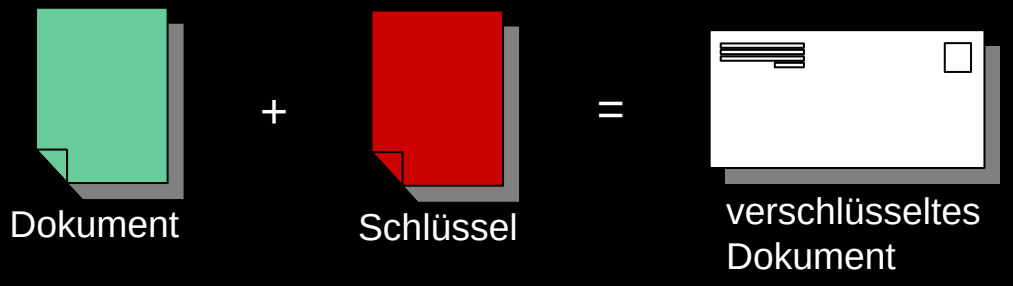
- Symmetrische Verschlüsselungsverfahren
  - **Substitutionschiffre**
    - ältestes bekanntes Verschlüsselungsverfahren
    - jedes Zeichen einer Nachricht wird durch einen anderen Buchstaben des Alphabets **ersetzt**
    - zwischen Originalzeichen und Chiffratzeichen besteht eine eineindeutige Zuordnung

Klartext	g e h e i m n i s	
Schlüssel	a b c d e f g h i j …	Alphabet
	e f g h i j k l m n …	Substitut
Chiffrat	k i l i m q r m w	

Informatik der digitalen Medien
Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

- Symmetrische Verschlüsselungsverfahren
  - **Einwegchiffre**
    - prinzipiell nicht zu brechen
    - erzeuge (zufälligen) **Schlüssel**, der die **gleiche Länge** besitzt wie die zu übertragende Nachricht = „**One-Time-Pad**“
    - verknüpfe jedes Einzelzeichen der Originalnachricht mit jedem Einzelzeichen des Schlüssels zum Chiffrat



Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

- Symmetrische Verschlüsselungsverfahren
  - **Einwegchiffre**
    - Bsp.:
      - Klartext und Schlüssel als Bit-Folge gegeben
      - Verknüpfung erfolgt über XOR

XOR-Funktion

a	b	a XOR b
0	0	**0**
0	1	**1**
1	0	**1**
1	1	**0**

Klartext **10110100110110010110**

Schlüssel **10100010010101111001**

Chiffrat **00010110100011101111**

Informatik der digitalen Medien
Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

- Symmetrische Verschlüsselungsverfahren
  - **Einwegchiffre**
    - Bsp.:
      - um den Originaltext wieder zu erhalten führt der Empfänger dieselbe XOR-Operation mit Schlüssel und Chiffrat aus

XOR-Funktion

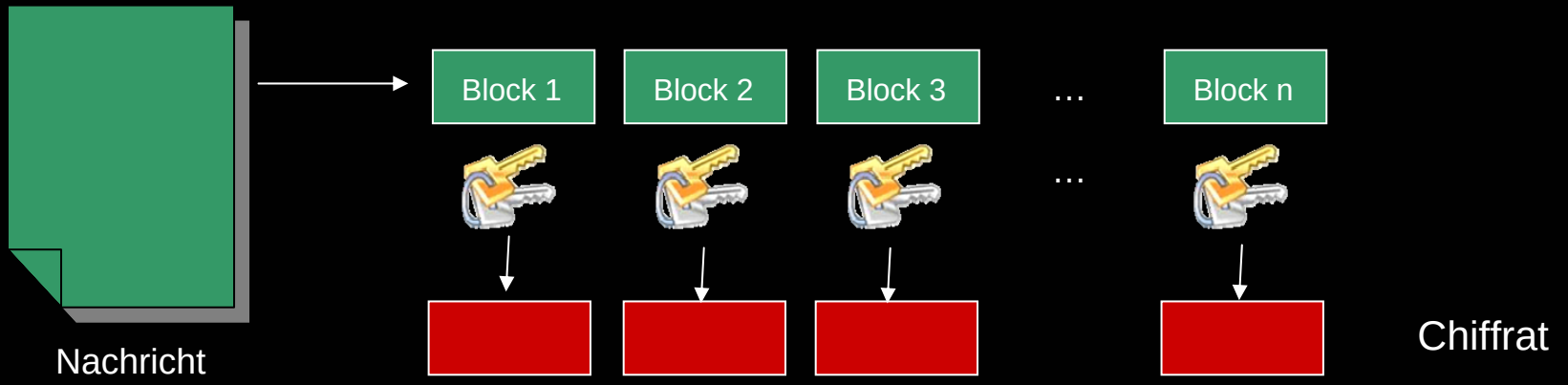
a	b	a XOR b
0	0	**0**
0	1	**1**
1	0	**1**
1	1	**0**

Chiffrat	**00010110100011101111**
Schlüssel	**10100010010101111001**
Klartext	**10110100110110010110**

Informatik der digitalen Medien
Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

- Symmetrische Verschlüsselungsverfahren
  - **Blockchiffre**
    - die zu verschlüsselnde Nachricht wird in einzelne **Blöcke fester Länge zerlegt**
    - jeder Block wird mit demselben Schlüssel fortlaufend verschlüsselt
    - alle verschlüsselten Blöcke bilden gemeinsam das Chiffrat



Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

- Symmetrische Verschlüsselungsverfahren
  - **Stromchiffre**
    - die zu verschlüsselnde Nachricht wird wird als **Strom aus Einzelzeichen** aufgefasst
    - der Strom der Originalzeichen wird mit einem Einmal-Schlüssel gleicher Länge Zeichen für Zeichen verschlüsselt

Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

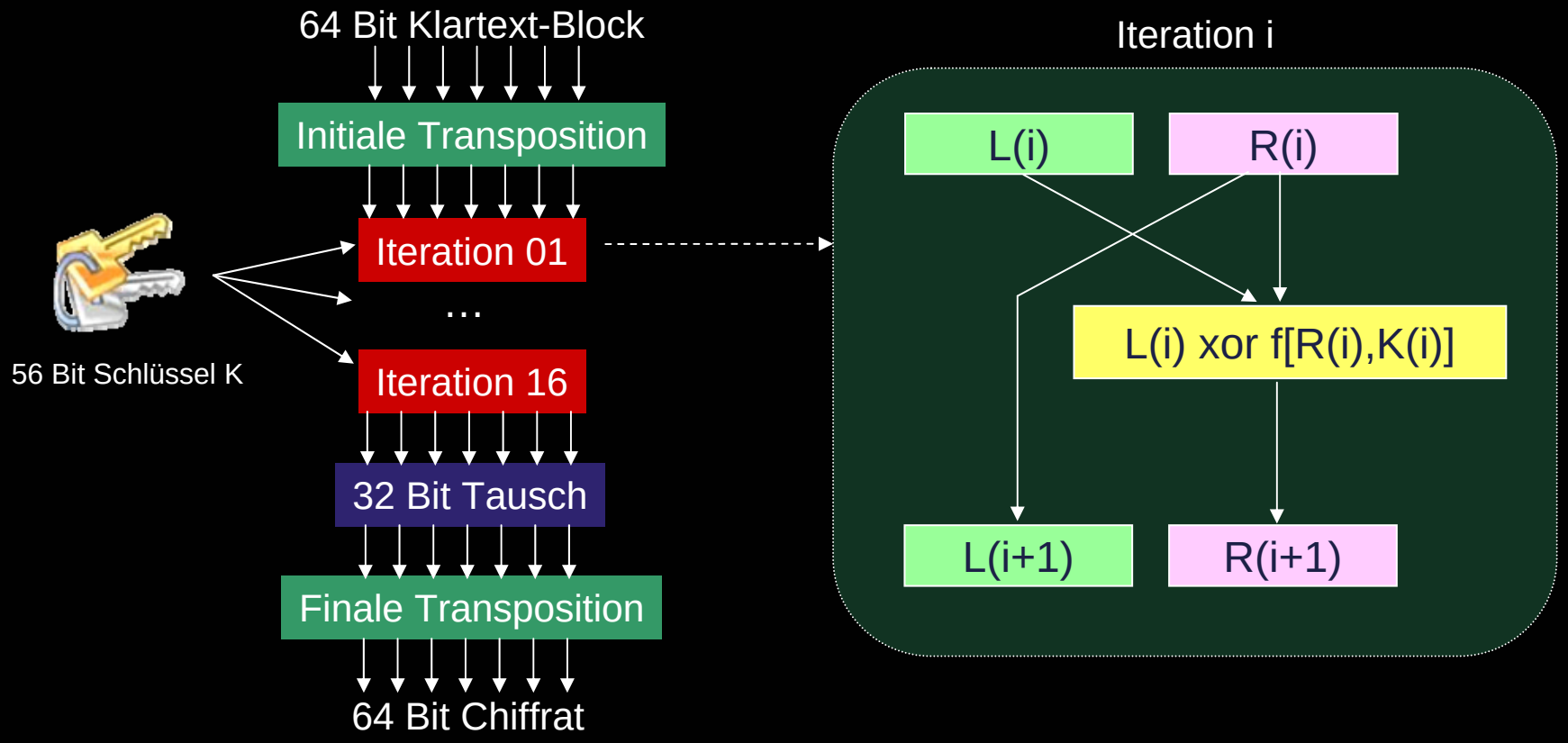
Internet und WWW (6)

- Symmetrische Verschlüsselungsverfahren
  - **DES – Data Encryption Standard**
    - symmetrisches Block-Verschlüsselungsverfahren
    - 1977 veröffentlicht
    - 1993 für kommerzielle Nutzung aktualisiert
    - Blocklänge = 64 Bit
      (=Schlüssellänge, effektiv aber nur 56 Bit genutzt)
    - nutzt Transpositions- und Substitutionsverfahren, die in insgesamt 19 Iterationen auf die zu verschlüsselnde Nachricht angewendet werden

Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

- Symmetrische Verschlüsselungsverfahren
  - **DES – Data Encryption Standard**



Informatik der digitalen Medien
Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

- Symmetrische Verschlüsselungsverfahren
  - **DES – Data Encryption Standard**
    - 1997 RSA startet **DES Challenge**
      10.000$ für denjenigen, der es schafft, DES zu knacken
    - nach knapp 4 Monaten konnte ein mit DES verschlüsselter Text entschlüsselt werden
    - Heute kann eine DES-Nachricht innerhalb **weniger Stunden** entschlüsselt werden
    - Daher: **Triple-DES**
      - mehrfache Anwendung von DES hintereinander mit verschiedenen Schlüsseln

Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Informatik der digitalen Medien

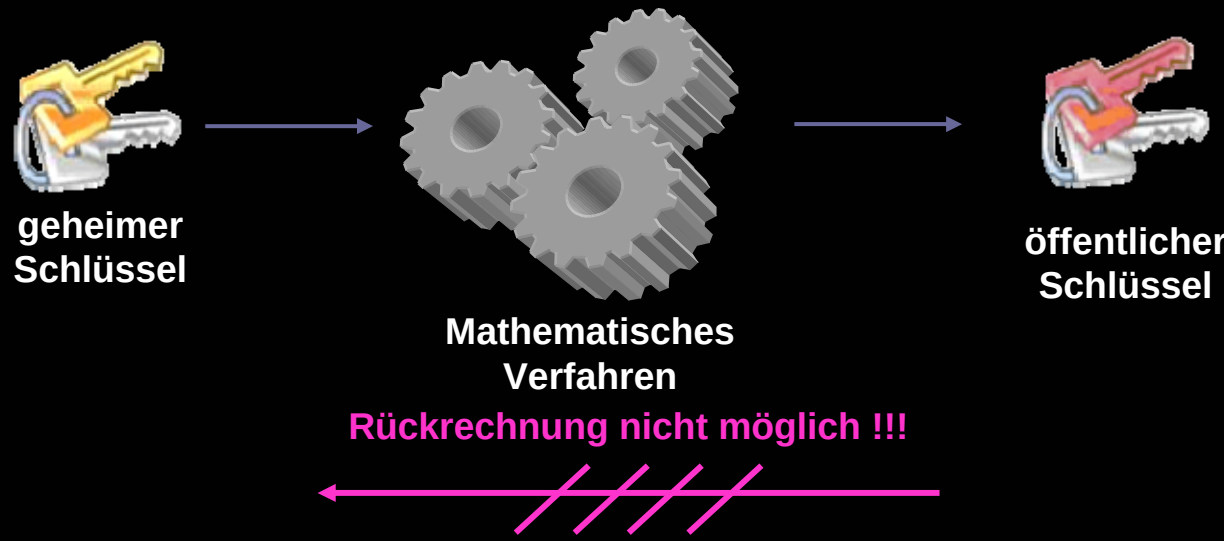
3. Internet und WWW (6)

- Grundlagen der Kryptografie
  - Sicherheitsziele
  - Kurze Geschichte der Kryptografie
  - Symmetrische Schlüsselverfahren
  - **Verfahren mit öffentlichem Schlüssel**
  - Digitale Signaturen
  - Zertifikate und Sicherheitsinfrastrukturen

Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

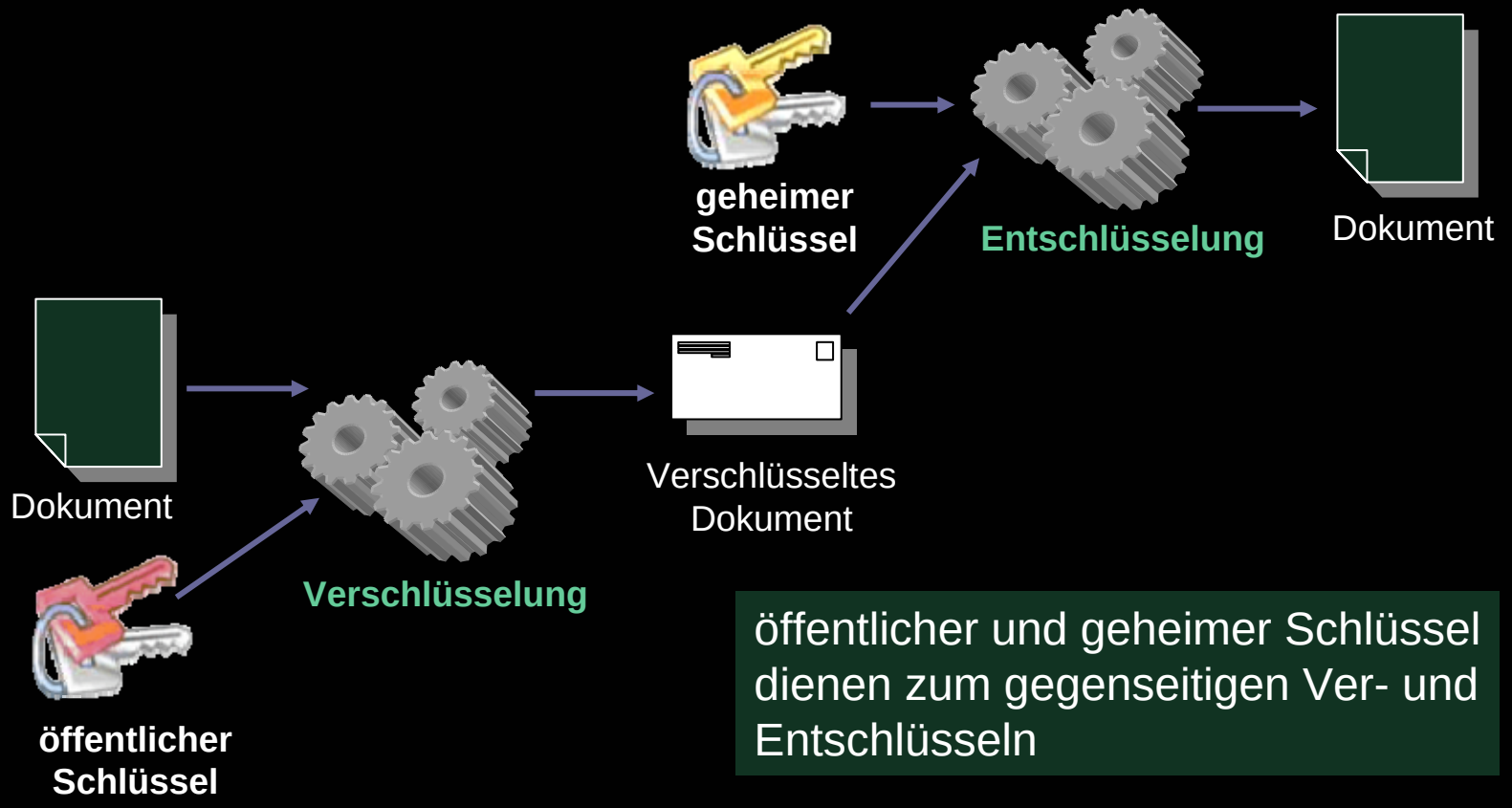
- Grundlagen der Kryptografie
  - **Verfahren mit öffentlichem Schlüssel**
    - Problem bei symmetrischen Verfahren ➔ Schlüsselaustausch
    - Ist es möglich, **ohne** einen geheimen **Schlüsselaustausch** auszukommen?
    - Voraussetzung dazu sind **mathematische Einwegfunktionen**



Informatik der digitalen Medien
Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

- Grundlagen der Kryptografie
  - **Verfahren mit öffentlichem Schlüssel**

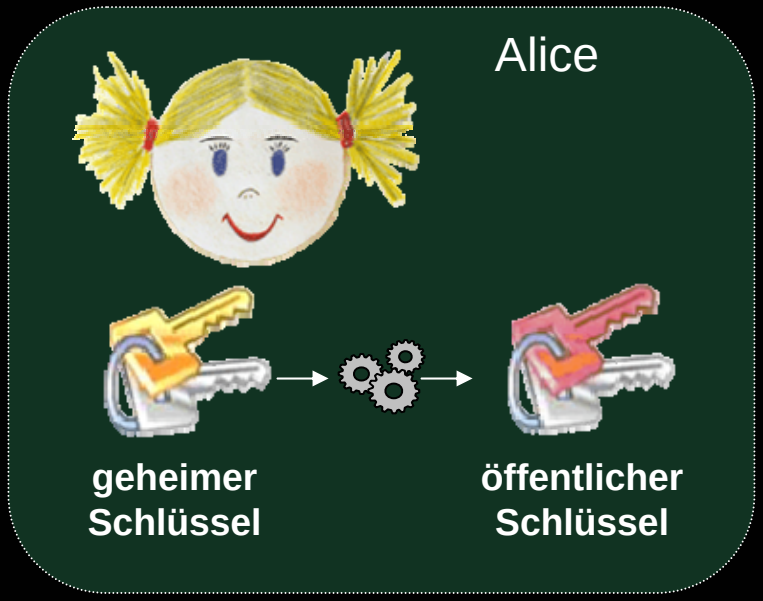


öffentlicher und geheimer Schlüssel dienen zum gegenseitigen Ver- und Entschlüsseln

Informatik der digitalen Medien
Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

- Grundlagen der Kryptografie
  - **Verfahren mit öffentlichem Schlüssel**
    - Sender **behält den geheimen Schlüssel** für sich
    - nur der **öffentliche Schlüssel wird an alle weitergegeben**, die mit dem Sender kommunizieren wollen

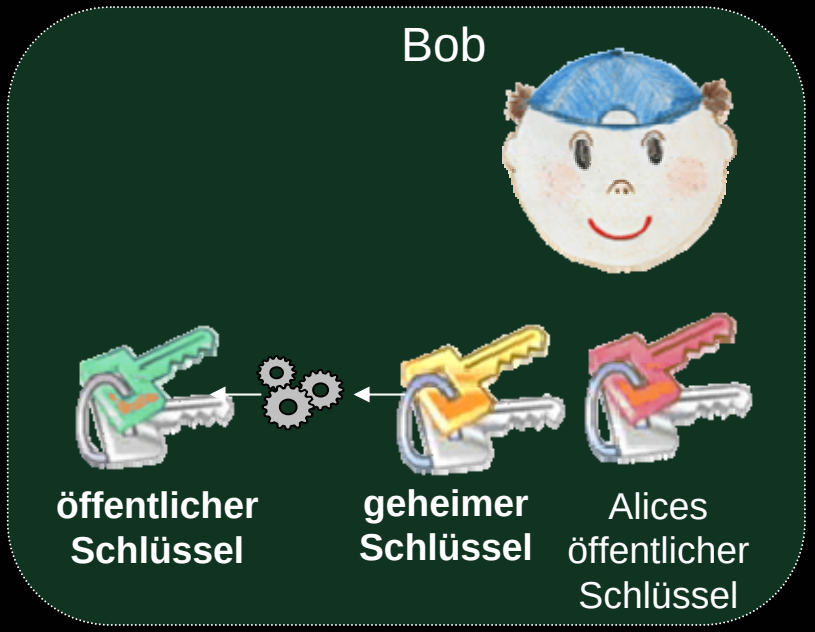


Informatik der digitalen Medien
Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

- Grundlagen der Kryptografie
  - **Verfahren mit öffentlichem Schlüssel**
    - Sender **behält den geheimen Schlüssel** für sich
    - nur der **öffentliche Schlüssel wird an alle weitergegeben**, die mit dem Sender kommunizieren wollen

Alice



Informatik der digitalen Medien
Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

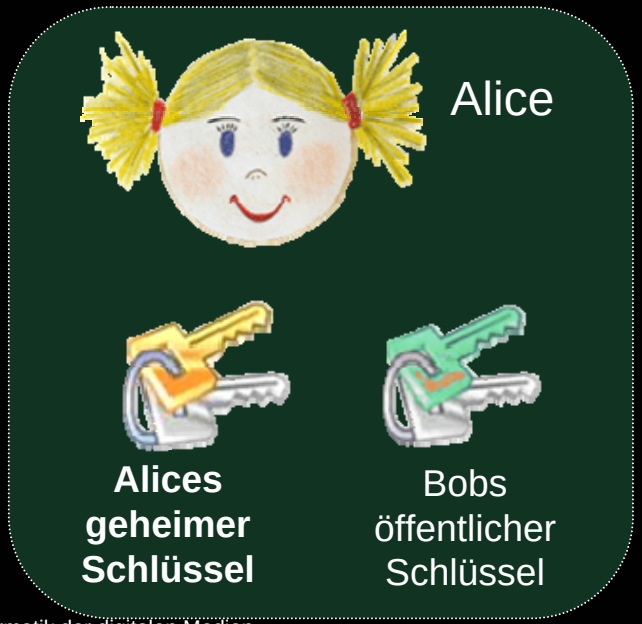
Internet und WWW (6)

- Grundlagen der Kryptografie
  - **Verfahren mit öffentlichem Schlüssel**
    - Sender **behält den geheimen Schlüssel** für sich
    - nur der **öffentliche Schlüssel wird an alle weitergegeben**, die mit dem Sender kommunizieren wollen

Informatik der digitalen Medien
Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

- Grundlagen der Kryptografie
  - **Verfahren mit öffentlichem Schlüssel**

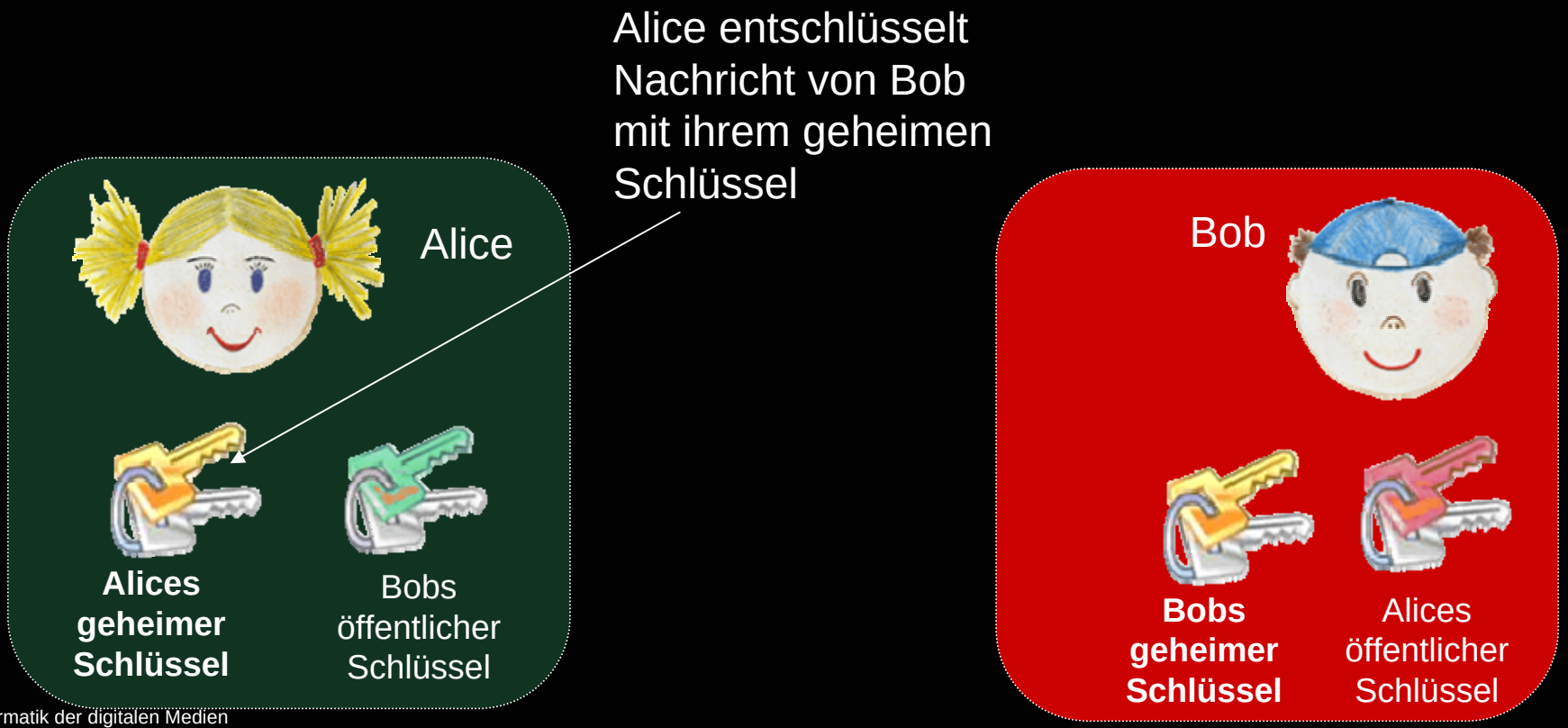


Bob verschlüsselt Nachricht an Alice mit Alices öffentlichem Schlüssel

Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

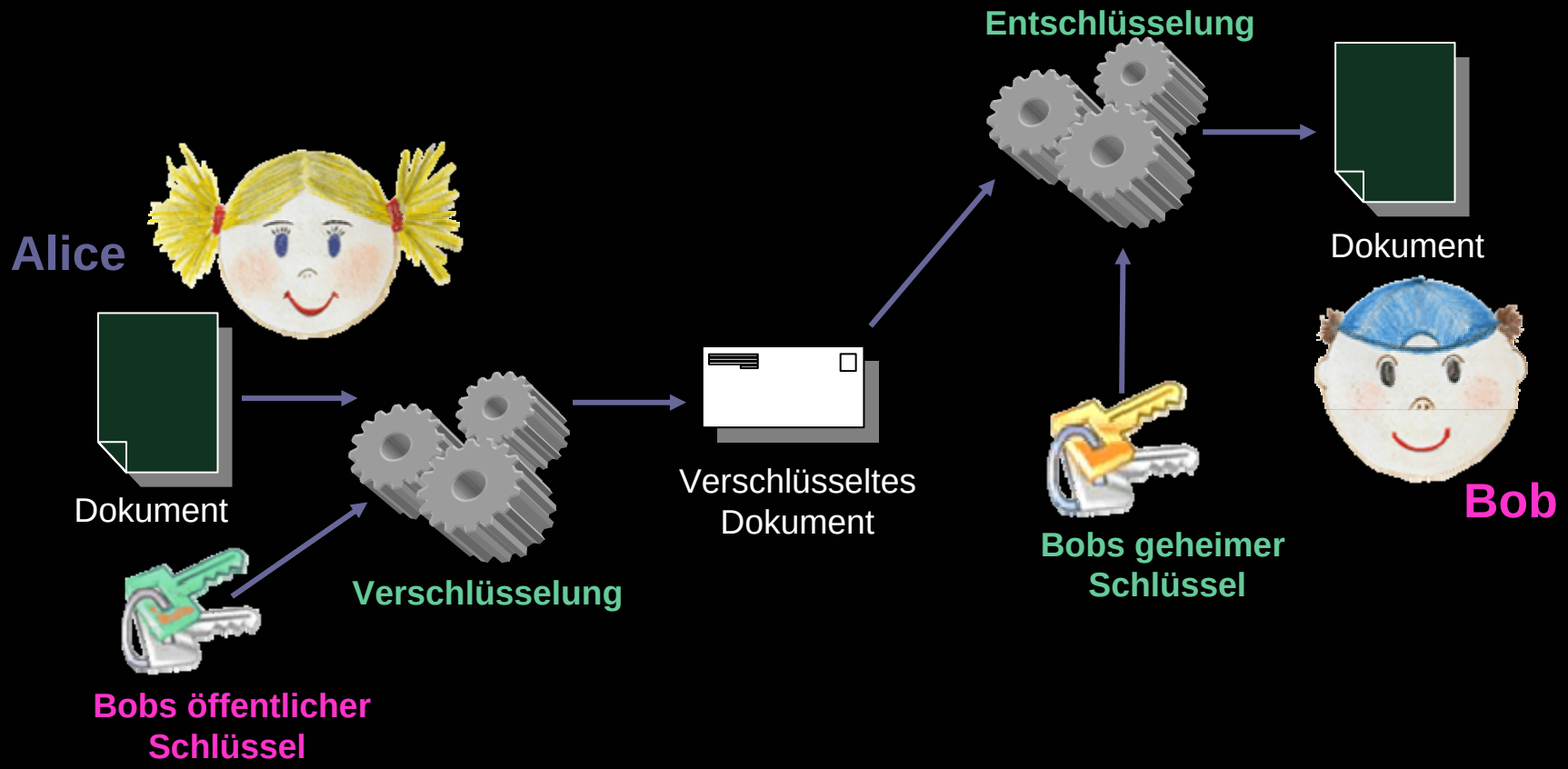
- Grundlagen der Kryptografie
  - **Verfahren mit öffentlichem Schlüssel**



Informatik der digitalen Medien
Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

- Grundlagen der Kryptografie
  - **Verfahren mit öffentlichem Schlüssel**



Informatik der digitalen Medien
Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

- Grundlagen der Kryptografie
  - **Verfahren mit öffentlichem Schlüssel**
    - Niemand außer Alice kann eine Nachricht entschlüsseln, die mit ihrem öffentlichen Schlüssel verschlüsselt wurde
    - Bob kann also sicher sein, dass seine Nachricht von niemandem sonst als Alice gelesen werden kann

    - Verfahren garantiert
      - **Vertraulichkeit der Nachricht**
      - **Authentizität des Empfängers**
    - Aber wer garantiert, dass die empfangene Nachricht nicht doch verfälscht wurde… (**Integrität**)...??

Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Informatik der digitalen Medien

3. Internet und WWW (6)

- Grundlagen der Kryptografie
  - Sicherheitsziele
  - Kurze Geschichte der Kryptografie
  - Symmetrische Schlüsselverfahren
  - Verfahren mit öffentlichem Schlüssel
  - **Digitale Signaturen**
  - Zertifikate und Sicherheitsinfrastrukturen

Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

- Grundlagen der Kryptografie
  - **Digitale Signaturen**
    - Eine **Unterschrift** garantiert
      - Echtheit eines Dokuments
      - Unterzeichner erklärt sich mit dem Dokumenteninhalt einverstanden

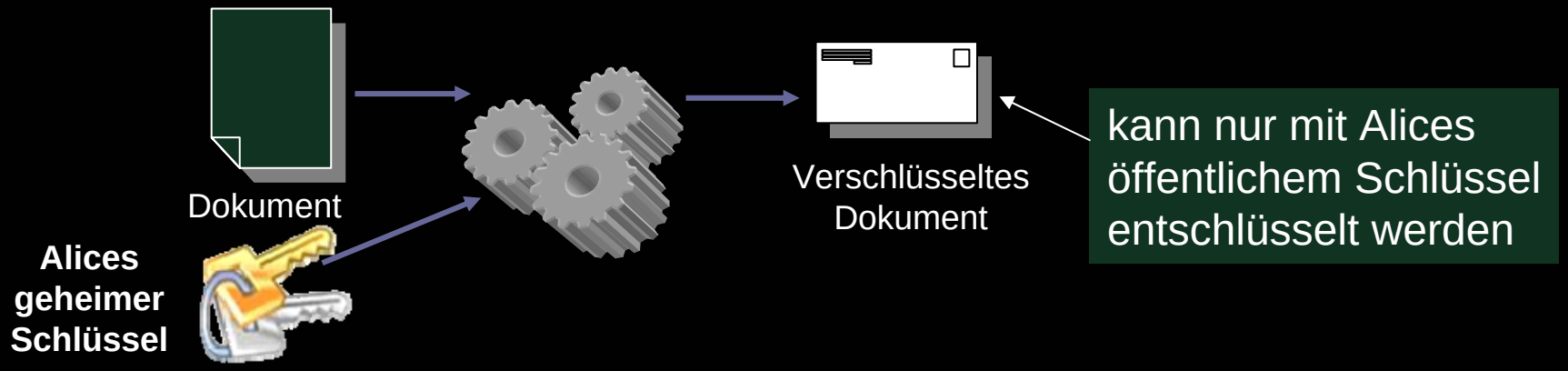
    - Einführen einer **digitalen Unterschrift** für elektronische Nachrichten
    - Digitale Unterschrift muss
      - **fälschungssicher**
      - **überprüfbar** und
      - **verbindlich** sein

Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

- Grundlagen der Kryptografie
  - **Digitale Signaturen**
    - Idee: drehe das Verschlüsselungsverfahren mit öffentlichem Schlüssel einfach um:

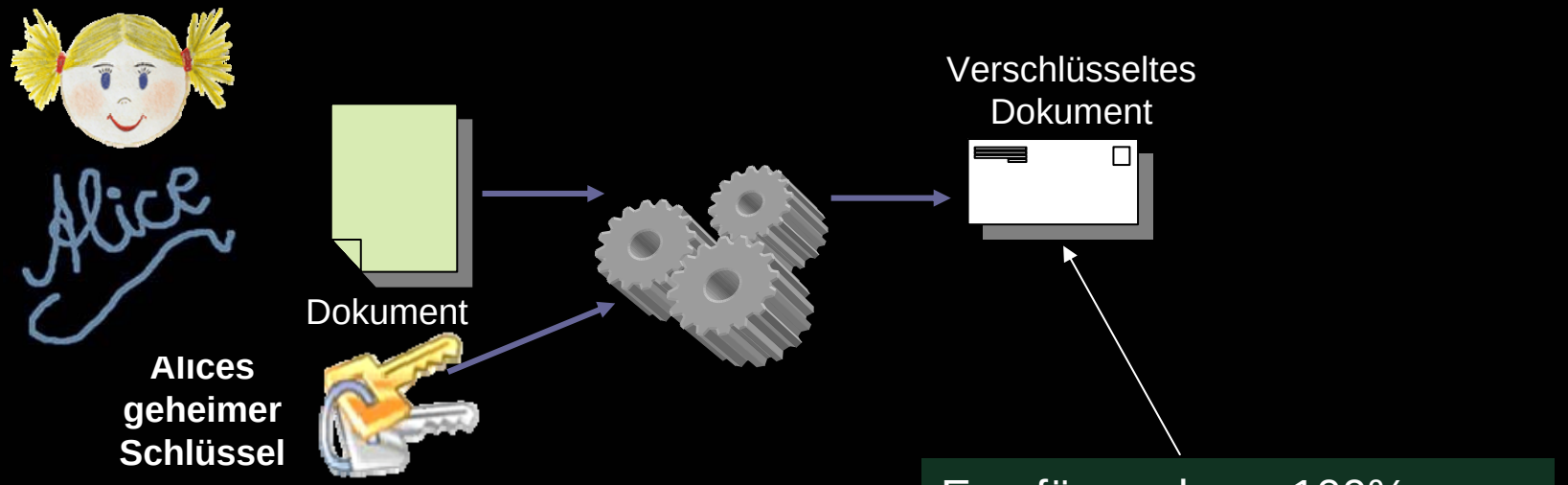
- Alice verschlüsselt eine Nachricht für Bob mit ihrem geheimen Schlüssel
- Bob kann diese Nachricht mit dem öffentlichen Schlüssel von Alice entschlüsseln



Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

- Grundlagen der Kryptografie
  - **Digitale Signaturen**



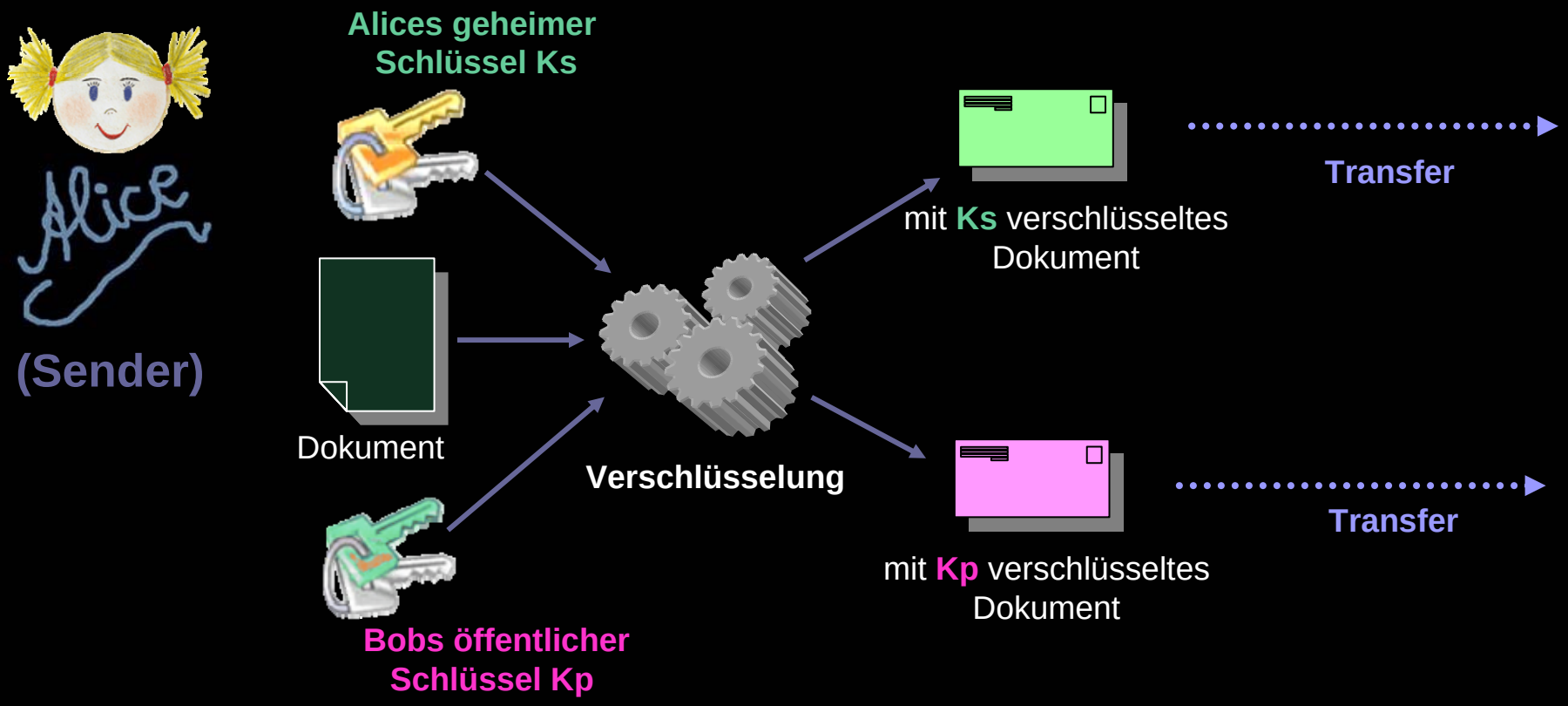
Internet und WWW (6)

- Grundlagen der Kryptografie
  - **Digitale Signaturen**
    - Nutze daher **beide Varianten zusammen**
      - Verschlüsselung mit eigenem geheimen Schlüssel UND
      - Verschlüsselung mit dem öffentlichen Schlüssel des Empfängers
    - zur gesicherten Übertragung vertraulicher Nachrichten

Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

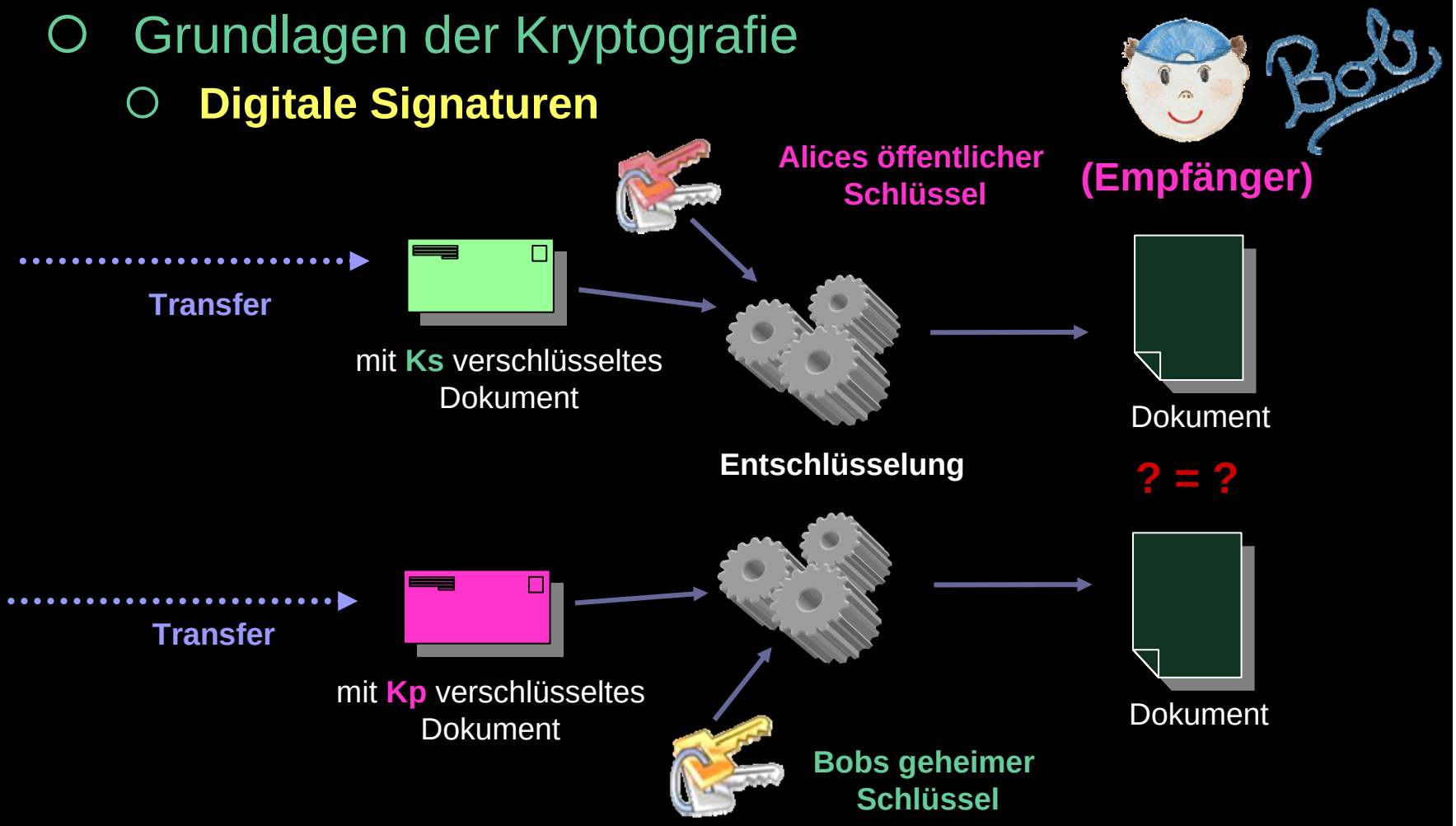
- Grundlagen der Kryptografie
  - **Digitale Signaturen**



Informatik der digitalen Medien
Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

- Grundlagen der Kryptografie
  - **Digitale Signaturen**



Informatik der digitalen Medien
Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

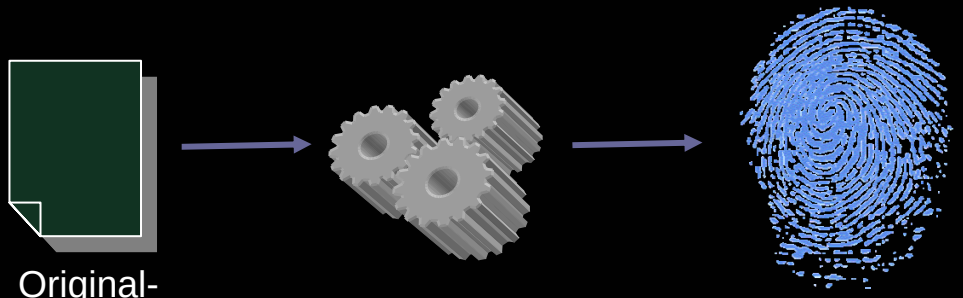
Internet und WWW (6)

- Grundlagen der Kryptografie
  - **Digitale Signaturen**
    - **Integrität** des versendeten Dokuments bleibt mit Versenden einer digitalen Signatur stets gewahrt
    - **Problem**:
      - **Jeder kann das Originaldokument lesen**, indem er Alices öffentlichen (und daher frei verfügbaren) Schlüssel anwendetSignatur besitzt Größe des Originaldokuments
      - Was tun bei Grafik- / Audio- / Videodateien ???
      - Verbraucht doppelte Bandbreite und immense Rechenzeit
    - **Idee:**
      - Versende nicht das Originaldokument als Signatur sondern lieber eine Art „**Fingerabdruck**“ des Originaldokuments

Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

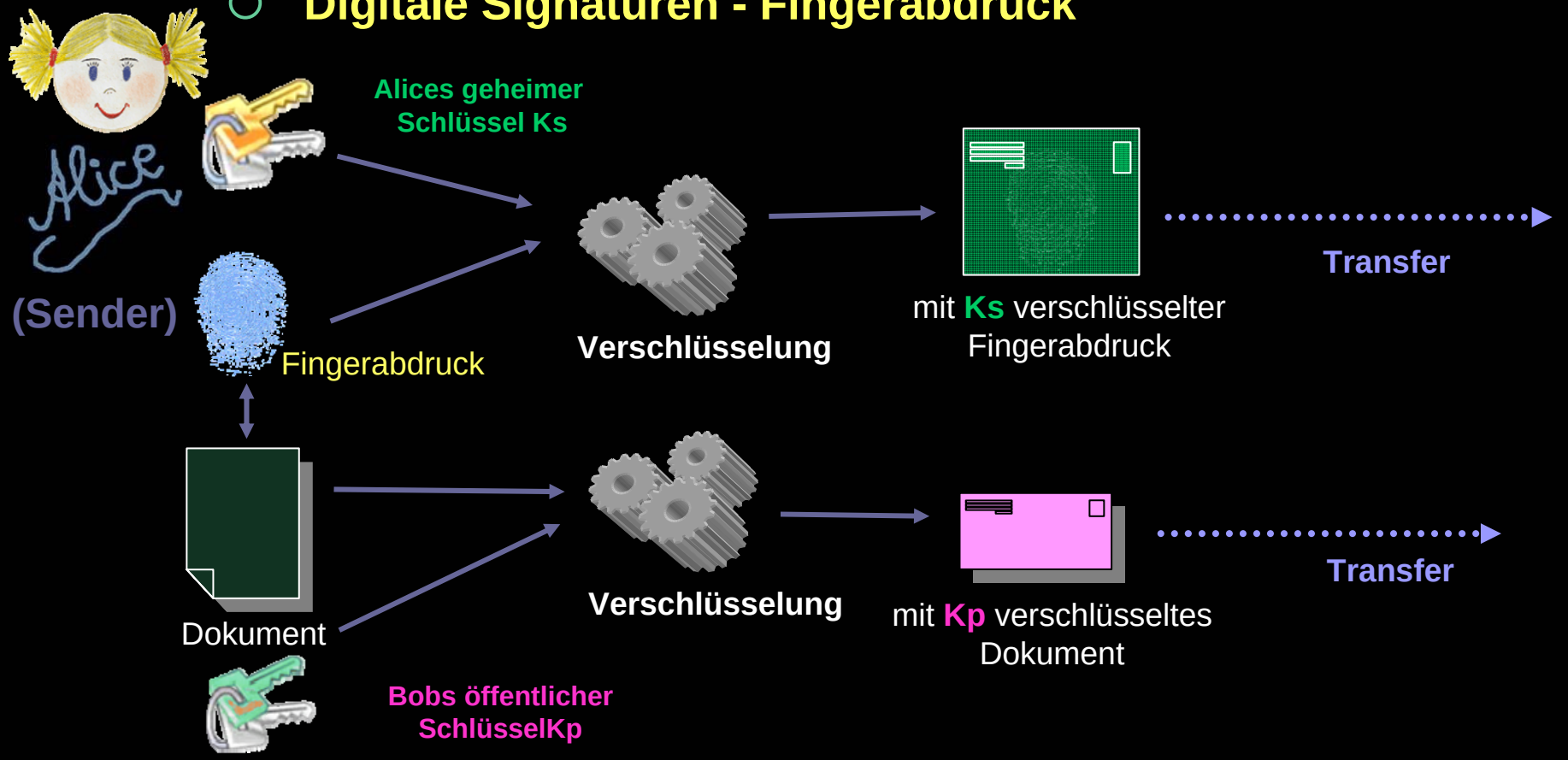
- Grundlagen der Kryptografie
  - **Digitale Signaturen - Fingerabdruck**
    - Ein Fingerabdruck muss folgende **Eigenschaften** besitzen:
      - Er ist wesentlich **kleiner** als das Original
      - Er **identifiziert das Original** mit sehr hoher Wahrscheinlichkeit (Sicherheit), d.h.
      - die Wahrscheinlichkeit, dass zwei Originale denselben Fingerabdruck besitzen ist sehr, sehr gering.



Informatik der digitalen Medien
Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

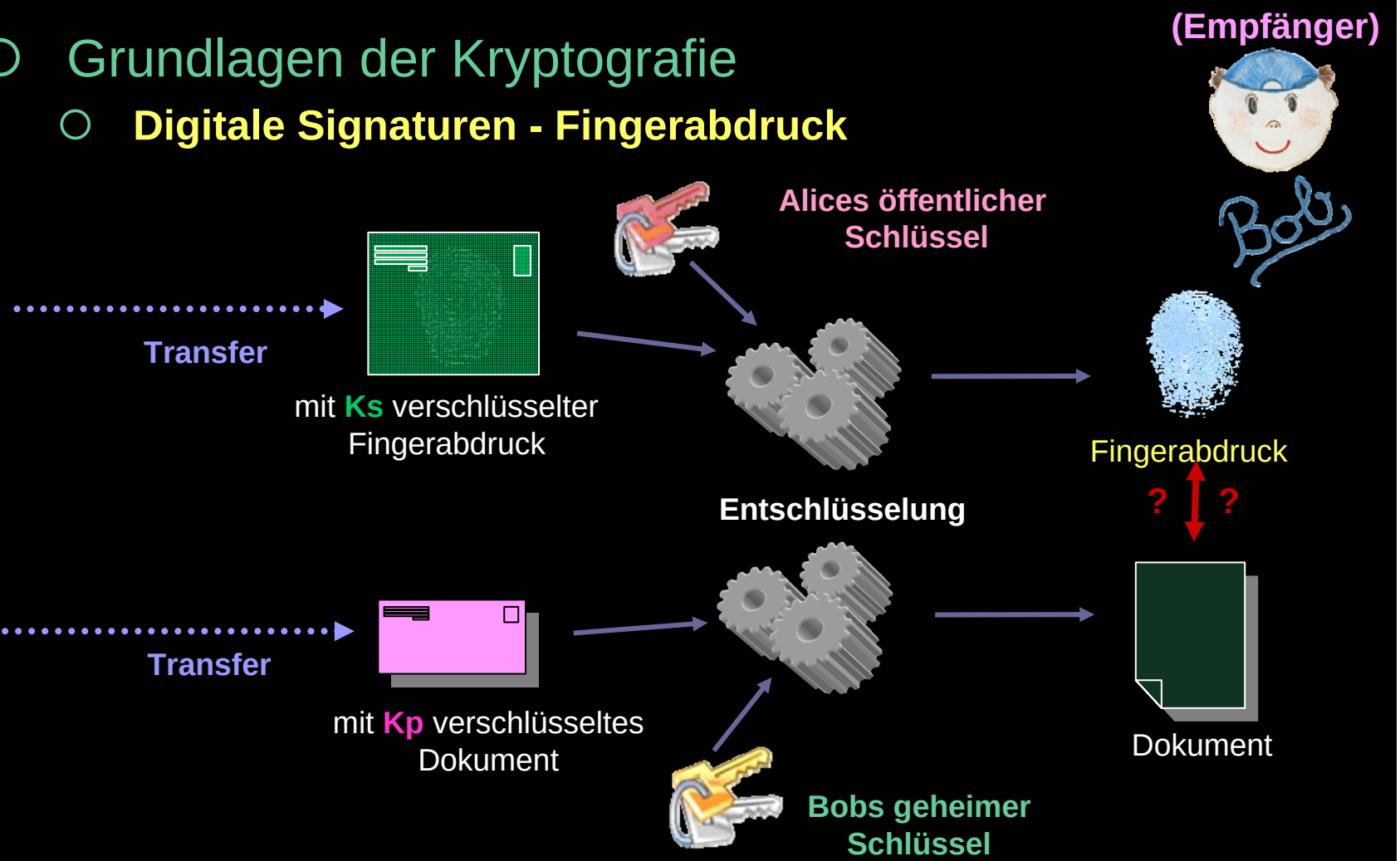
- Grundlagen der Kryptografie
  - **Digitale Signaturen - Fingerabdruck**



Informatik der digitalen Medien
Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

- Grundlagen der Kryptografie
  - **Digitale Signaturen - Fingerabdruck**



Informatik der digitalen Medien
Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Informatik der digitalen Medien

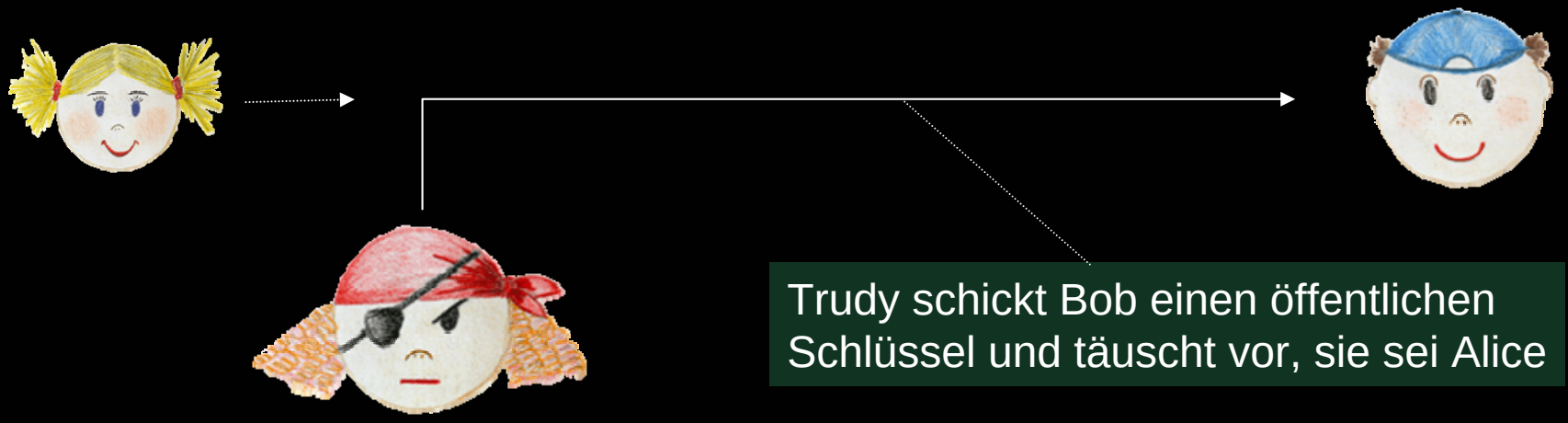
3. Internet und WWW (6)

- Grundlagen der Kryptografie
  - Sicherheitsziele
  - Kurze Geschichte der Kryptografie
  - Symmetrische Schlüsselverfahren
  - Verfahren mit öffentlichem Schlüssel
  - Digitale Signaturen
  - **Zertifikate und Sicherheitsinfrastrukturen**

Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

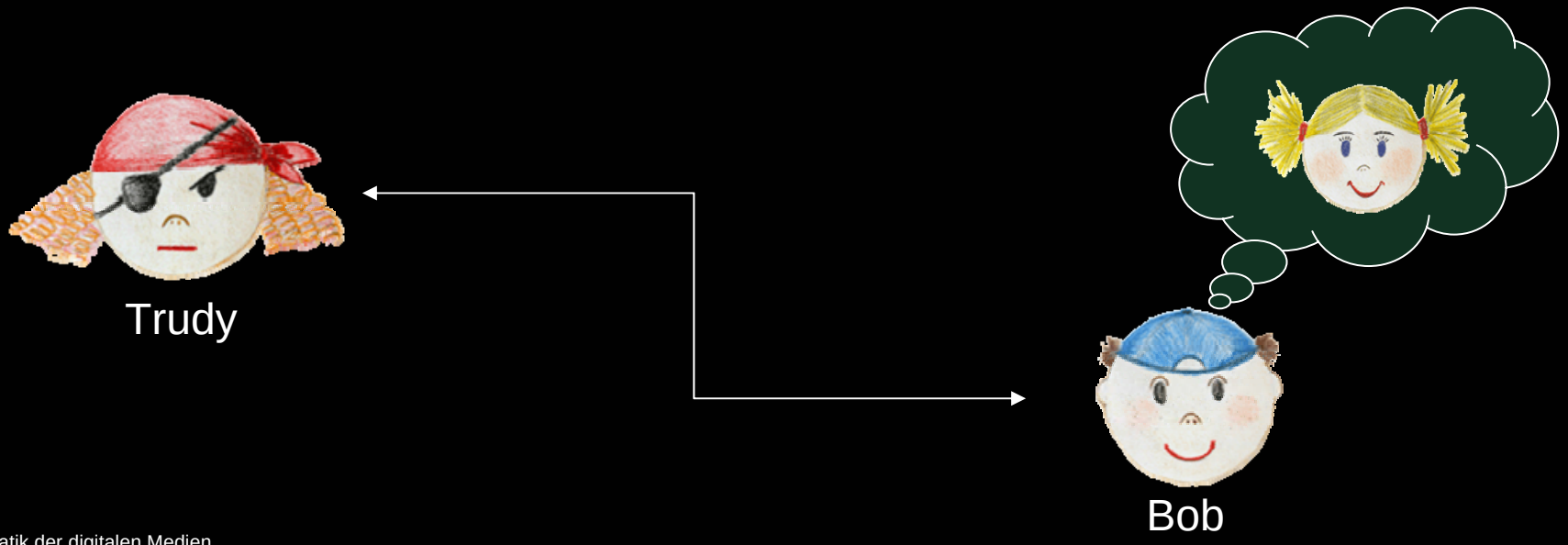
- Grundlagen der Kryptografie
  - **Zertifikate und Sicherheitsinfrastrukturen**
    - Wie kann Bob eigentlich sicher sein, dass der öffentliche Schlüssel von Alice eigentlich tatsächlich Alice gehört??
    - Trudy könnte versuchen, Bob vorzutäuschen, sie sei Alice



Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

- Grundlagen der Kryptografie
  - **Zertifikate und Sicherheitsinfrastrukturen**
    - Bob kommuniziert mit Trudy im guten Glauben, sie sei Alice
    - Er ist sich dabei auch ganz sicher, da er glaubt Alices öffentlichen Schlüssel zu benutzen



Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

- Grundlagen der Kryptografie
  - **Zentrale Behörde (Zertifizierungsstelle / CA / Trust Center)**

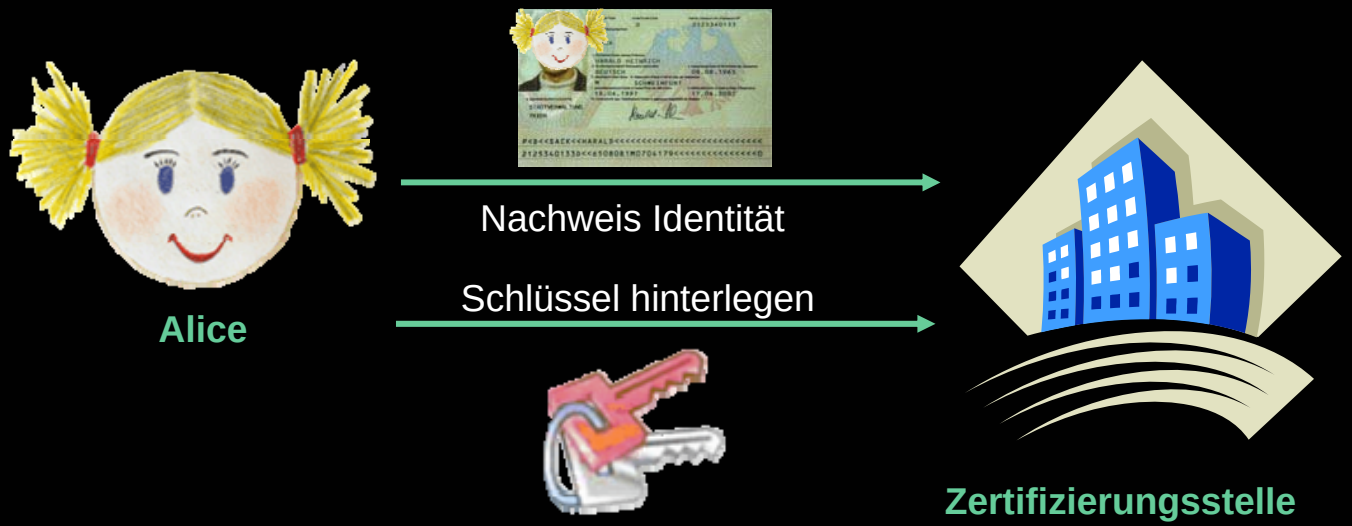
    - **prüft Identität** der Kommunikationspartner und
    - **hinterlegt** deren **öffentliche Schlüssel**

    - **vergibt** auf Anfrage hin einen angeforderten **öffentlichen Schlüssel**
    - **überprüft** auf Anfrage hin einen angefragten **öffentlichen Schlüssel**

Informatik der digitalen Medien
Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

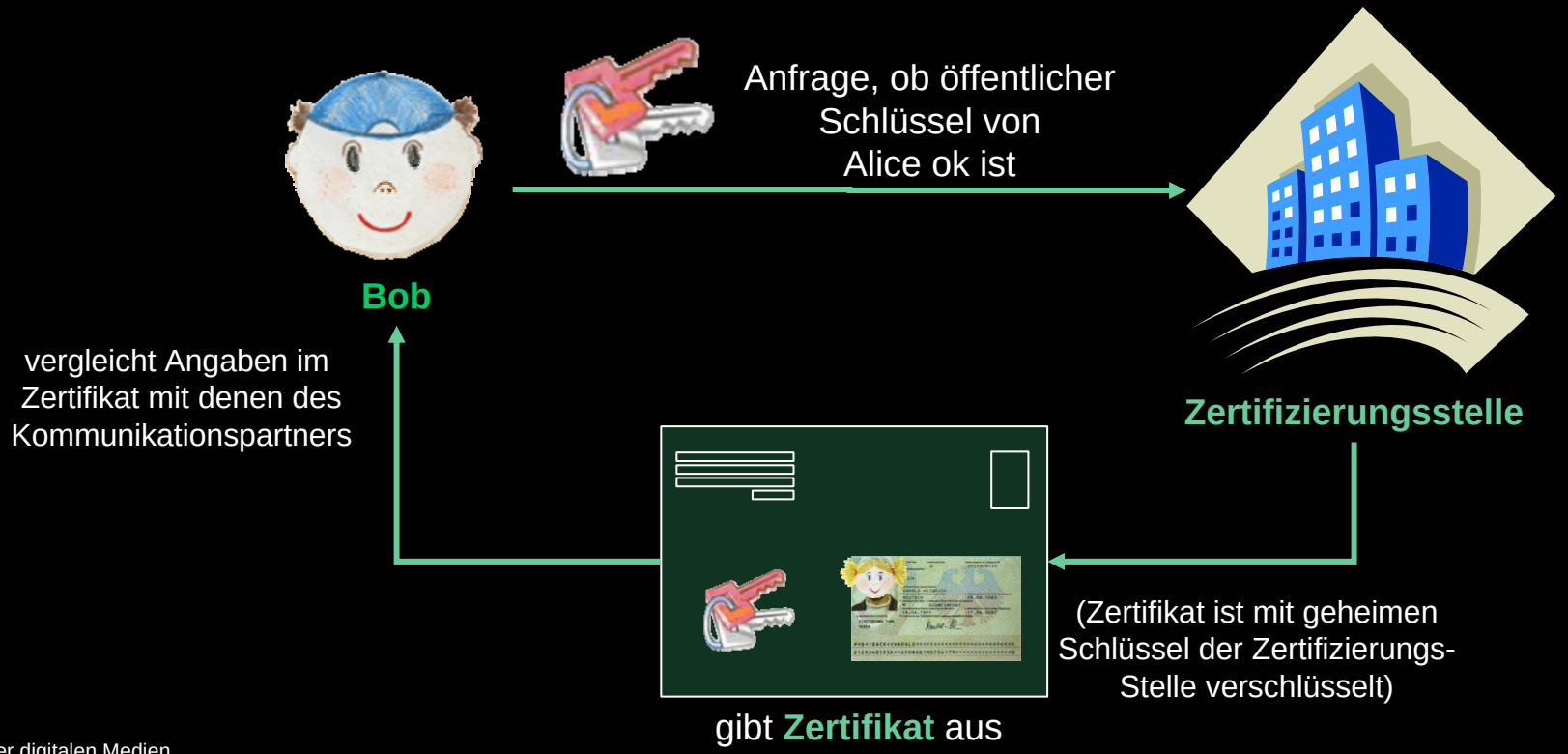
- Grundlagen der Kryptografie
  - **Zertifikate und Sicherheitsinfrastrukturen**
    - Anmelden eines öffentlichen Schlüssels und Überprüfung der Identität des Besitzers



Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

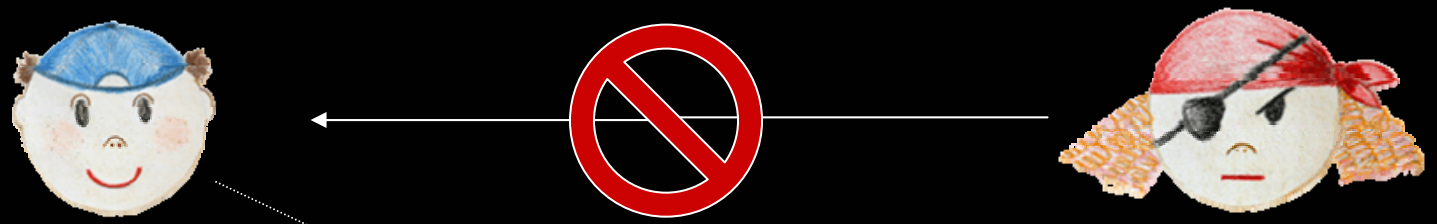
- Grundlagen der Kryptografie
  - **Zertifikate und Sicherheitsinfrastrukturen**
    - Überprüfung eines öffentlichen Schlüssels



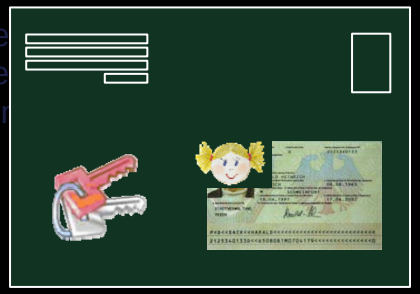
Informatik der digitalen Medien
Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Internet und WWW (6)

- Grundlagen der Kryptografie
  - **Zertifikate und Sicherheitsinfrastrukturen**
    - Bob überprüft anhand des Zertifikats, ob der von Trudi gesendete öffentliche Schlüssel mit dem im Zertifikat angegebenen übereinstimmt



Bob



Zertifikat

Bob erkennt, dass der von Trudi gesendete Öffentliche Schlüssel gefälscht ist

Informatik der digitalen Medien
Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Informatik der digitalen Medien

3. Internet und WWW (6)

- Grundlagen der Kryptografie
  - Sicherheitsziele
  - Kurze Geschichte der Kryptografie
  - Symmetrische Schlüsselverfahren
  - Verfahren mit öffentlichem Schlüssel
  - Digitale Signaturen
  - Zertifikate und Sicherheitsinfrastrukturen

Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de

Informatik der digitalen Medien

3. Internet und WWW (6)

Literatur

- Ch. Meinel, H. Sack:
  WWW– Kommunikation, Internetworking, Web-Technologien,
  Springer, 2004.
- J. Schwenk:
  Sicherheit und Kryptografie im Internet,
  Vieweg Verlag, 2002.
- S. Singh:
  Geheime Botschaften,
  Deutscher Taschenbuchverlag, 2002.

Dr.rer.nat. Harald Sack, Institut für Informatik, FSU Jena, Ernst-Abbe-Platz 2-4, D-07743 Jena, E-Mail: sack@minet.uni-jena.de