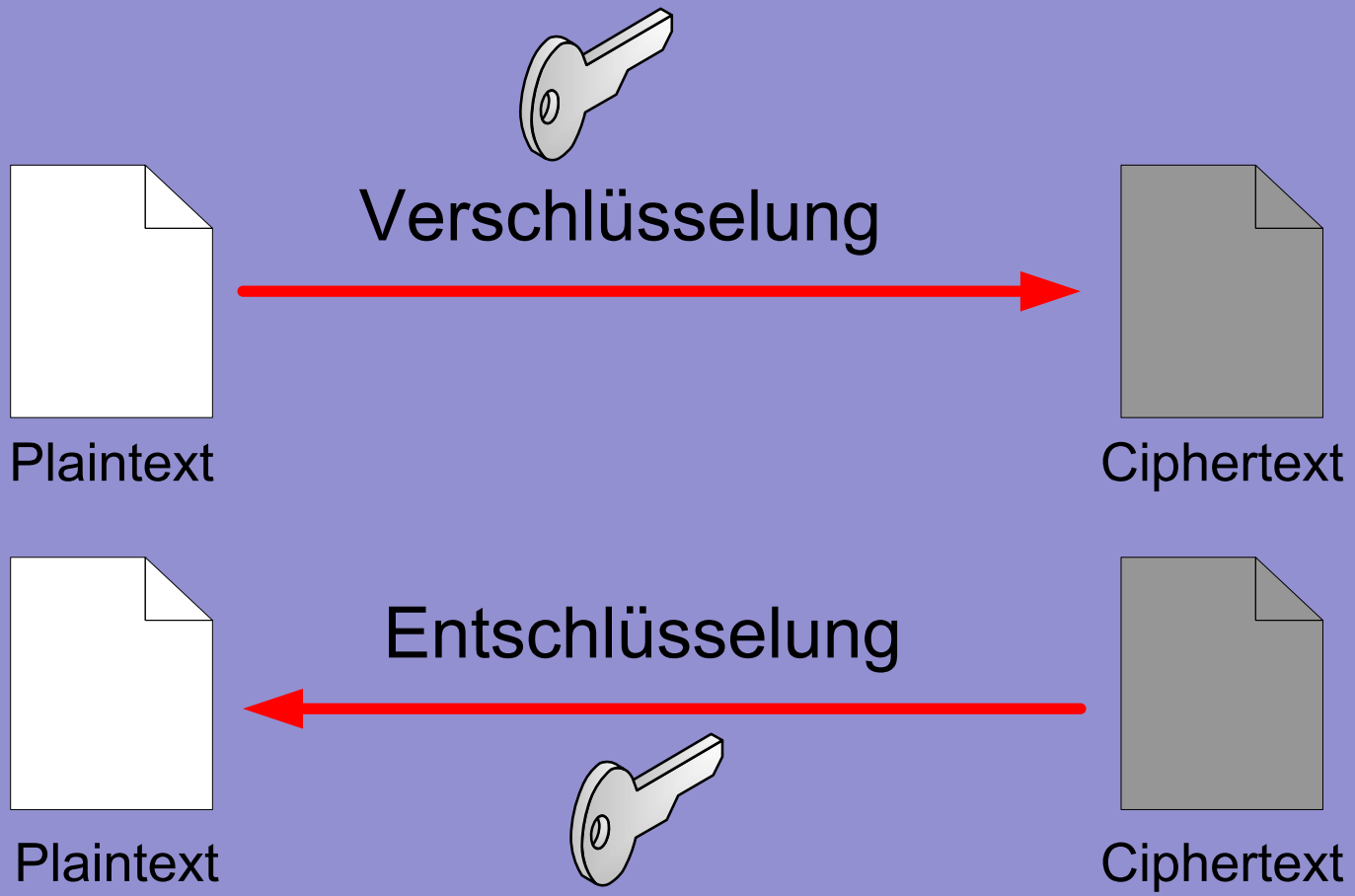
Eine Praxis-orientierte Einführung in die Kryptographie

Mag. Lukas Feiler, SSCP
lukas.feiler@lukasfeiler.com
http://www.lukasfeiler.com/lectures_brg9

Verschlüsselung & Entschlüsselung



Kryptographie & Informationssicherheit

-Vertraulichkeit

-Verfügbarkeit

-Integrität

Geschichte der Kryptographie

- Von den Ägyptern über Caesar zu totalitären Systemen des 20. Jhdt.
- Kryptographie zur Sicherung der Privatsphäre

Substitution (Ersetzung)

z.B alle a durch b, alle b durch c usw.

ersetzen (Caesar Cipher)

→ „secret“ wird „tfdsfu“

Transposition (Vertauschung)

Reihenfolge der Buchstaben ändern

z.B. Spalten-weise in Tabelle eintragen und dann Zeilen-weise lesen

→ „this-is-their-secret“ wird „t-trchih-riseses-iet“

t	-	t	r	c
h	i	h	-	r
i	s	e	s	e
s	-	i	e	t

```
# dies ist ein Kommentar
# das file lukas_plaintext.txt anlegen
echo „I am Batman'' > lukas_plaintext.txt

# lukas_plaintext.txt verschlüsseln mit AES 256 Bit und den
# verschlüsselten Inhalt des files in lukas_encrypted.aes256 speichern
openssl enc -e -in lukas_plaintext.txt -aes256 > lukas_encrypted.aes256

# lukas_plaintext.txt löschen
rm lukas_plaintext.txt

# die Nachricht wieder entschlüsseln und in lukas_decrypted.txt speichern
openssl enc -d -in lukas_encrypted.aes256 -aes256 > lukas_decrypted.txt
```

Demonstration der Verschlüsselung einer Datei

Drei Arten von Verschlüsselungs-Verfahren

- Symmetrische Verfahren
- Asymmetrische Verfahren
- Message Digest Functions (One-way encryption)

Symmetrische Verfahren

- selber Key für Ver- und Entschlüsselung
- z.B. DES, Triple-DES, Blowfish, AES

Key ist idR eine Passwort (beide Partner müssen dieses kennen)
40 - 1024 „Bit-Verschlüsselung“

Brute Force/Key Search Attack

alle mögl. Keys werden durchprobiert
je mehr Bits desto schwieriger

56 Bit	$ 10.000-Hardware (2007)	6,4 Tage
128 Bit	größeres Firmennetzwerk (10^9 Keys per Sekunde)	10^22 Jahre
256 Bit	Quantencomputer im Jahre 2040 (10^32 Keys per Sekunde)	10^37 Jahre

Kryptographische Analyse

den Algorithmus „knacken“

Nicht-Kryptographische Angriffe

Fehler in der Implementierung!

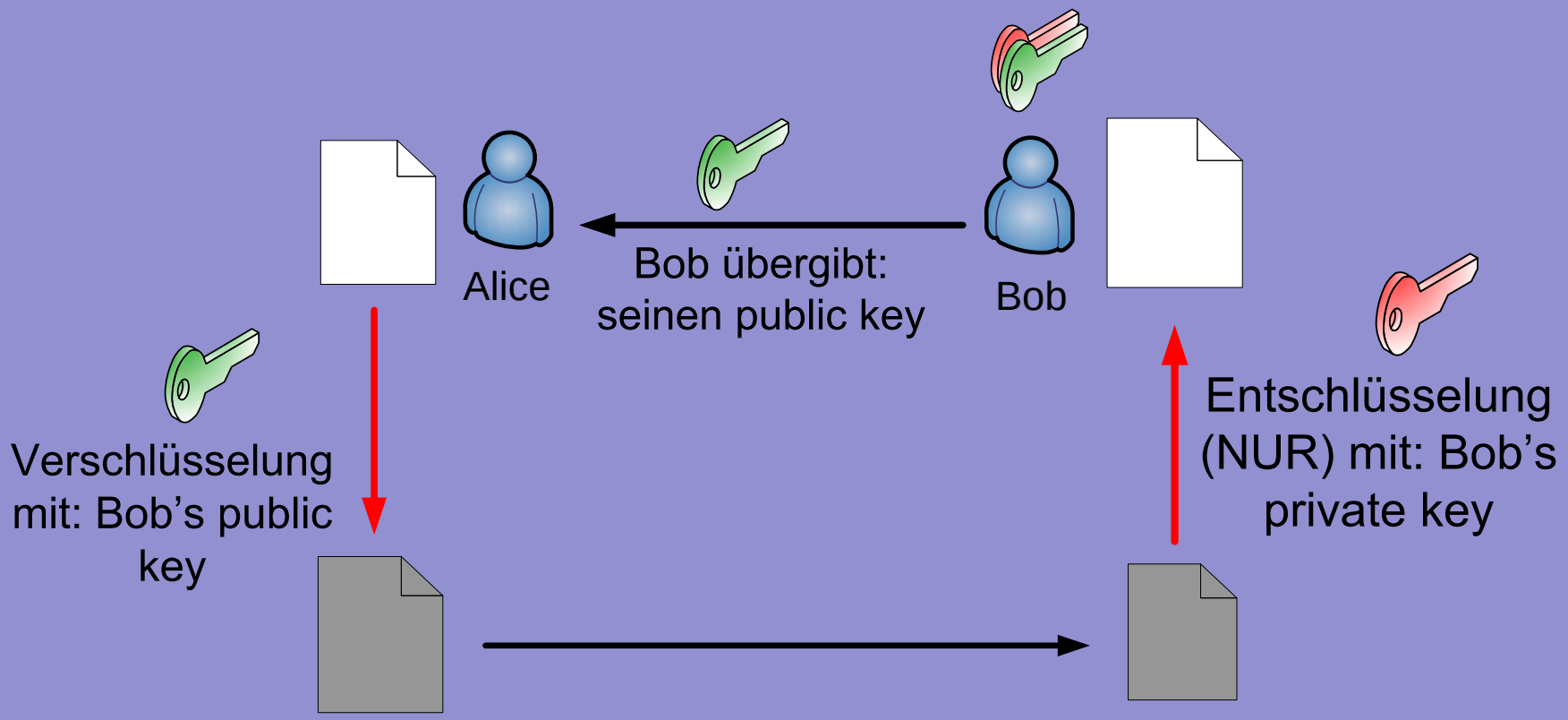
Angriffsmethoden gegen symmetrische Verfahren

Grenzen symmetrischer Verfahren

- Wie kann ich den „shared key“ sicher austauschen?
- Was wenn ich mit mir unbekannten verschlüsselt kommunizieren will?

Asymmetrische Verfahren (public key encryption)

- unterschiedliche komplementäre Keys für Ver- und Entschlüsselung (private and public key)
- z.B. DSA, RSA



Alice will Bob ein vertrauliches Dokument senden

Brute Force/Key Search Attack

- private key erraten
- „Probleme“
  1. idR > 1024 oder sogar 4096 Bit
  2. Asymmetrische Algorithmen idR sehr rechen-intensiv

Kryptographische Analyse

- den Algorithmus „knacken“
- z.B. Primfaktorzerlegung lösen

Nicht-Kryptographische Angriffe

- Fehler in der Implementierung!
- Ungesicherter private key

Angriffsmethoden gegen asymmetrische Verfahren

Message Digest Functions (One-Way-Encryption)

- Anhand des Plaintext wird eine eindeutige Zahl (idR 128 oder 256 Bit) errechnet
- Idee: digitaler „Fingerprint“ → jeder Plaintext hat anderen MD
- z.B. MD5, SHA-1

```
# dies ist ein Kommentar
# das file lukas1.txt anlegen
echo "This is a test" > lukas1.txt

# das file lukas2.txt anlegen
echo "This is a Test" > lukas2.txt

# komplett unterschiedliche MD5-Summen auf Grund eines Zeichens!
md5sum lukas1.txt lukas2.txt

# lukas2.txt dem file lukas1.txt gleichsetzen
echo "This is a test" > lukas2.txt

# selber Inhalt, selbe MD5-Summen!
md5sum test1.txt test2.txt
```

Demonstration von Message Digest Functions

Symmetrische Verfahren

- sehr schnell
- nicht geeignet bei unbekannten Kommunikationspartner

Asymmetrische Verfahren (public key encryption)

- langsam
- gut geeignet bei unbekannten Kommunikationsparntern

Message Digest Functions

- nur One-Way

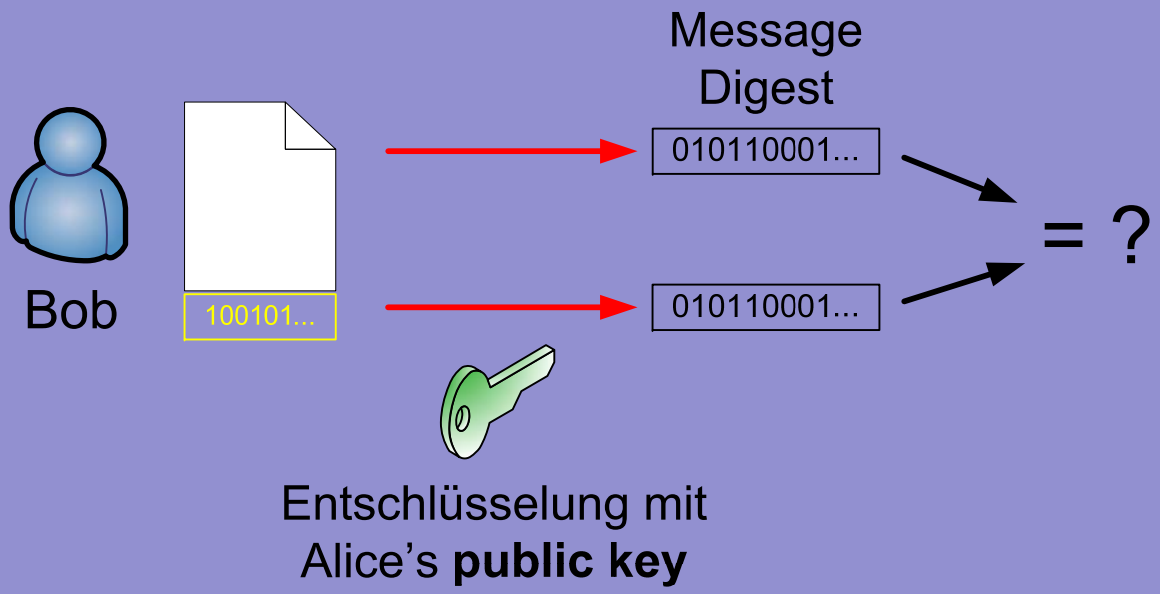
Vergleich der verschiedenen Verfahren

Einsatzzwecke der Kryptographie

- Vertraulichkeit (sym. & asym. Verfahren)
- Integrität (Message Digest Functions)
- Non-Repudiation (Nichtabstreitbarkeit)
- …

Elektronische Signaturen

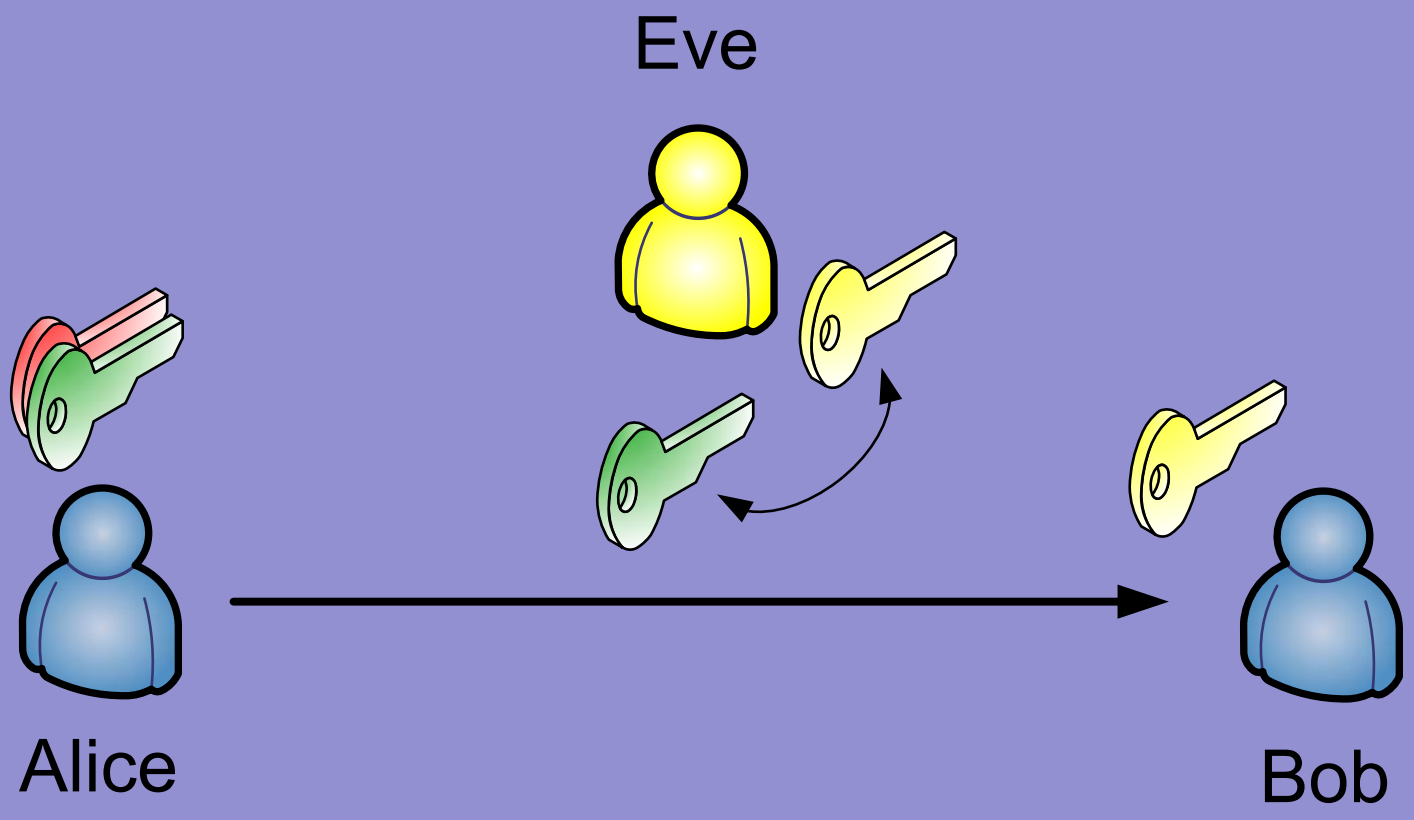
- Unterschreibender verschlüsselt mit?
  seinem private key
- Unterschreibender verschlüsselt was?
  Message Digest der Nachricht



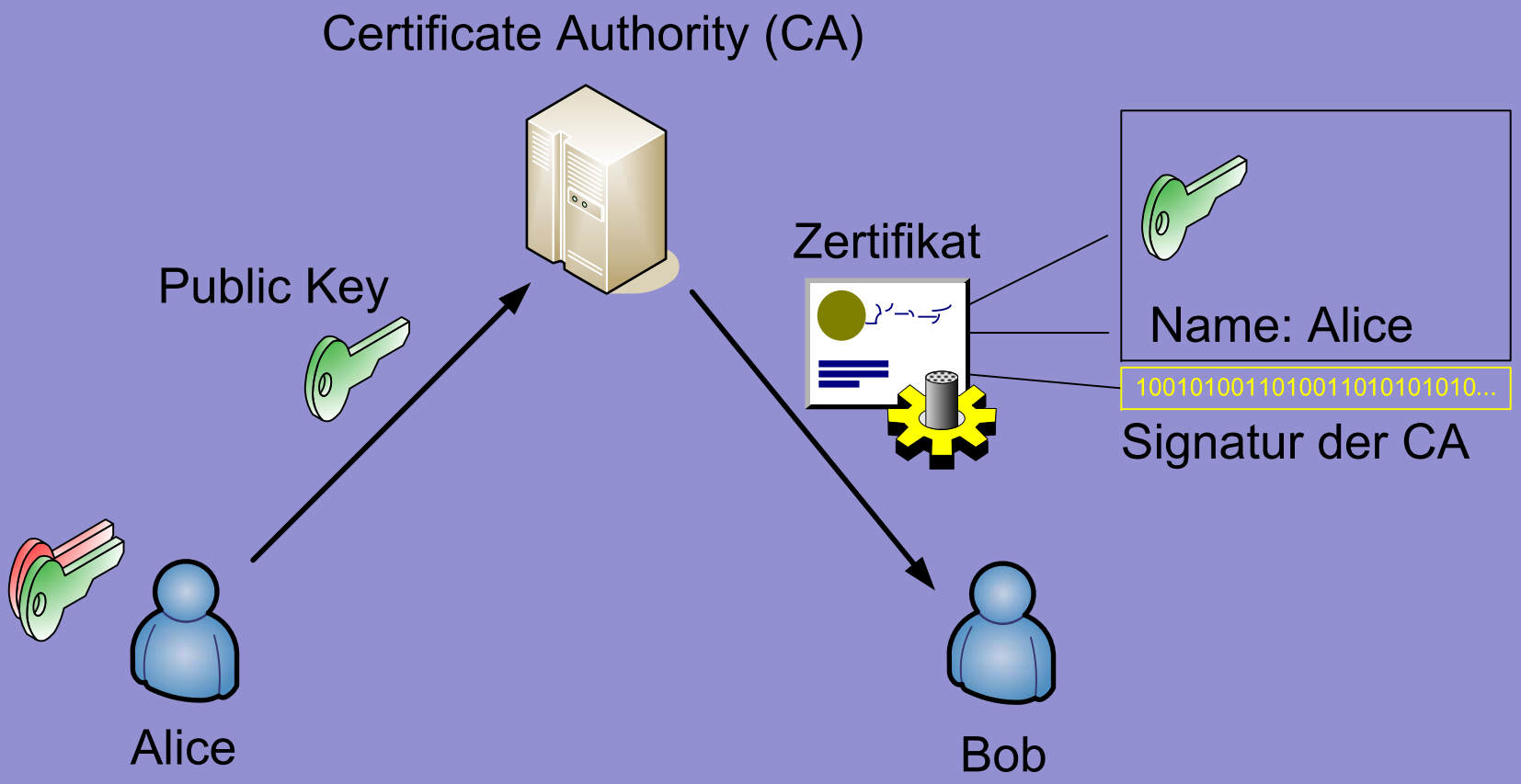
Erzeugen und überprüfen einer Signatur

```
# dies ist ein Kommentar
# das file lukas1.txt anlegen
echo "This is my message to the world" > lukas3.txt

# mit meinem default-key unterschreiben
gpg --sign -a lukas3.txt

# lukas3.txt.asc enthält jetzt die Signatur
cat lukas3.txt.asc

# Überprüfen der Signatur
gpg --verify lukas3.txt.asc
```

Wie bekommt Bob auf sichere Weise Alice‘s public key? – Public Key Infrastructures



Gefahr bei der Übermittlung des public key



Funktionsweise einer Public Key Infrastructure

Shon Harris, All-in-One CISSP Exam Guide, 4th Edition (2008), Seiten 659-768

Bruce Schneier, Applied Cryptography, 2nd Edition (1996)

Weiterführende Literatur

lukas.feiler@lukasfeiler.com

http://www.lukasfeiler.com/lectures_brg9

Danke für die Aufmerksamkeit