Digital Rights Management (DRM)

Verfahren, die helfen Rechte an virtuellen Waren durchzusetzen

**Vorlesung im Sommersemester 2010 an der
Technischen Universität Ilmenau von
Privatdozent Dr.-Ing. habil. Jürgen Nützel,
Vorstand der 4FriendsOnly.com Internet Technologies AG (4FO AG)
JN (at) 4FO (dot) DE**

Technische Grundprinzipien

***Folien stellen ein zusätzliches Informationsangebot für die Teilnehmer der Vorlesung dar.
Die Vorlesung richtet sich an Studierende der Informatik,
der Ingenieurinformatik, Wirtschaftsinformatik, Medienwirtschaft,
Angewandten Medienwissenschaft und Medientechnik.***

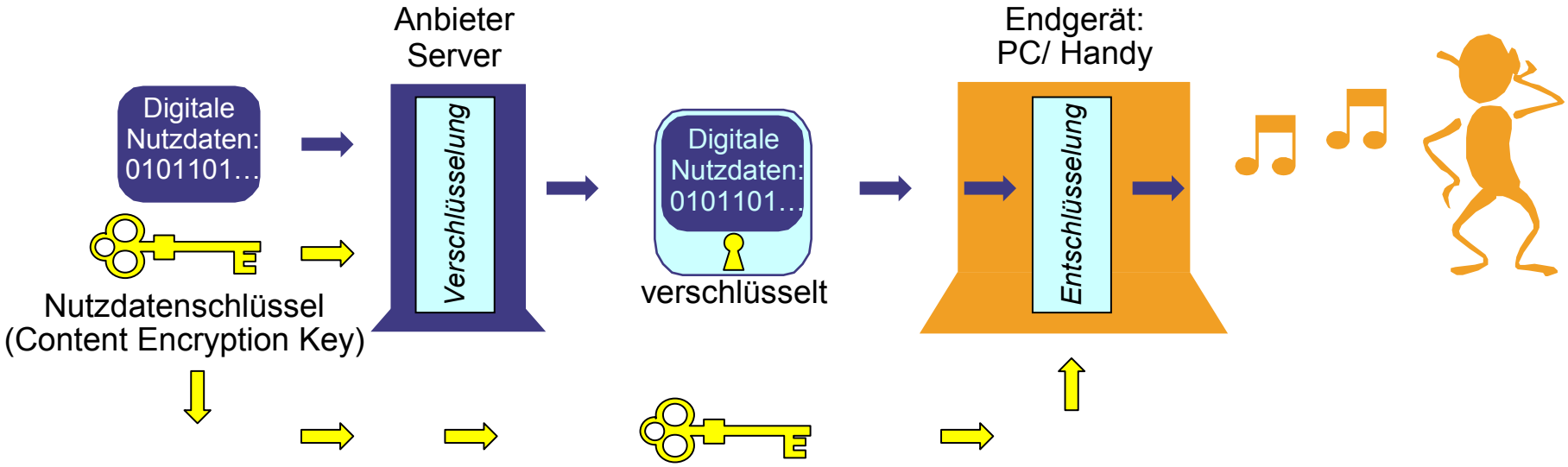
Diese Folien und weitere Informationen unter: www.juergen-nuetzel.de/drm_lecture.html

Überblick

- **Verschlüsselung der Nutzdaten**
- **Symmetrische Verschlüsselung**
- **Kontrolle des Schlüssels auf dem Endgerät**
- **Lizenzen mit Rechten und Schlüssel**

Verschlüsselung der Nutzdaten

Nutzdaten werden verschlüsselt verteilt



- ***Anbieter verteilt <u>nur</u> verschlüsselte Nutzdaten***
- ***Verschlüsselung und Entschlüsselung mit dem gleichen Schlüssel, z.B. mit AES (Advanced Encryption Standard)***
- ***Schlüssel wird getrennt und geheim übermittelt***

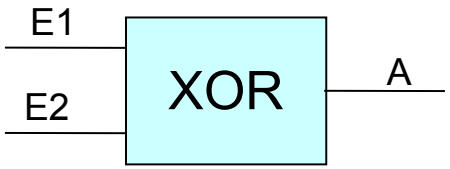
Symmetrische Verschlüsselung [1]

- **Einfacher Algorithmus: Bitweise Addition (XOR)**
  - ***Beispiel: Verschlüsselung***
  - ***Nutzdaten = 11 = 1011***
  - ***Schlüssel = 9 = 1001***

Nutzdaten E1: 1011
Schlüssel E2: 1001
Verschlüsselte ------
Nutzdaten A: 0010
= 2

  - ***Beispiel: Entschlüsselung***
  - ***Verschl. Nutzdaten = 2 = 0010***
  - ***Schlüssel = 9 = 1001***
  - ***Nutzdaten = ?***

E1	E2	A
0	0	0
0	1	1
1	0	1
1	1	0



Symmetrische Verschlüsselung [2]

XOR: One-Time-pad

Nutzdaten
Bild des Buchstaben X
Länge 25 Bit

1	0	0	0	1
0	1	0	1	0
0	0	1	0	0
0	1	0	1	0
1	0	0	0	1

XOR-Schlüssel
mit der gleichen
Länge: 25 Bit

0	1	1	0	1
1	1	0	1	0
0	0	0	1	0
0	0	1	0	1
0	1	0	1	0

Verschlüsselte
Nutzdaten

1	1	1	0	0
1	0	0	0	0
0	0	1	1	0
0	1	1	1	1
1	1	0	1	1

XOR: Block-Schlüssel

Mehrfache
Anwendung
eines XOR-Schlüssels
fester Länge: 5 Bit

0	1	1	0	1
0	1	1	0	1
0	1	1	0	1
0	1	1	0	1
0	1	1	0	1

1	1	1	0	0
0	0	1	1	1
0	1	0	0	1
0	0	1	1	1
1	1	1	0	0

Verschlüsselte
Nutzdaten

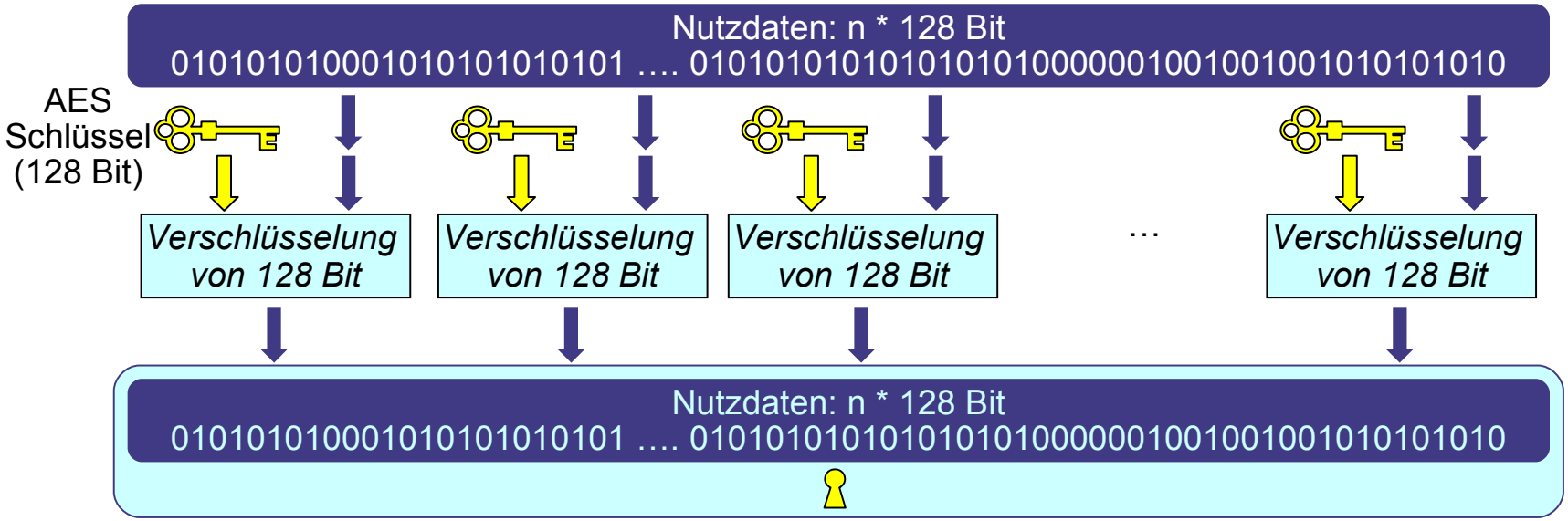
1	0	0	0	1
1	1	1	0	0
0	1	1	0	1

*Aber **Klartext-Angriff**:*
Sind nur 5 Bit der geheimen Nutzdaten bekannt, so kann der 5 Bit Schlüssel berechnet werden. Damit können die gesamten Nutzdaten entschlüsselt werden.

Symmetrische Verschlüsselung [3]

Blockweise Verschlüsselung

- *XOR kann in der Praxis nur einmalig (one-time pad) angewendet werden (Klartext-Angriff gelingt)*
- *Gute symmetrische Verfahren wie AES ermöglichen die wiederholte Anwendung des Schlüssels (Erklärung!)*
- *Blocklänge und Schlüssellänge z.B. 128 oder 256 Bit*



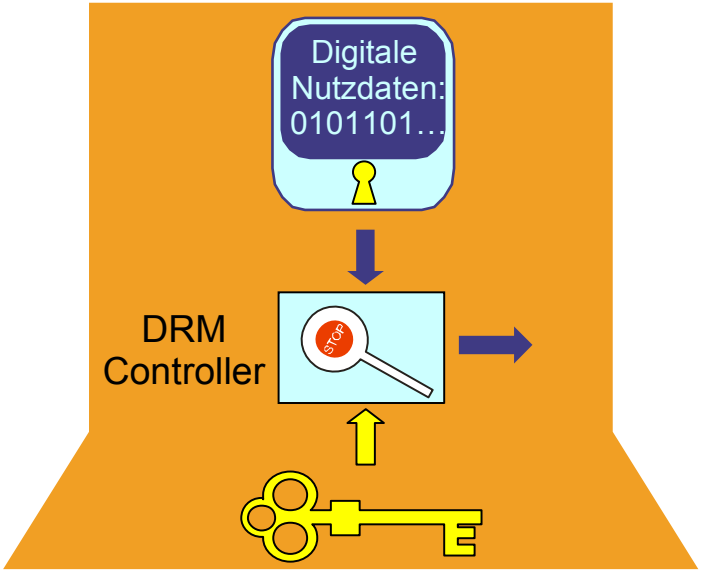
AES – Advanced Encryption Standard

- **Standard nach dem Verfahren von Rijndael**
  - *In 2000 Sieger eines Wettbewerbs der NIST*
  - *128 Bit Blocklänge mit 128, 192 oder 256 Bit Schlüssel*
  - *Realisierung in Hardware und Software sehr schnell*
  - *Je nach Schlüssellänge: 10, 12 oder 14 Runden*
  - *Frei von Patenten und unendgeldlich nutzbar*

  - *Tutorial hier: www.realtec.de/privat/arbeiten.shtml*

Kontrolle über den Schlüssel

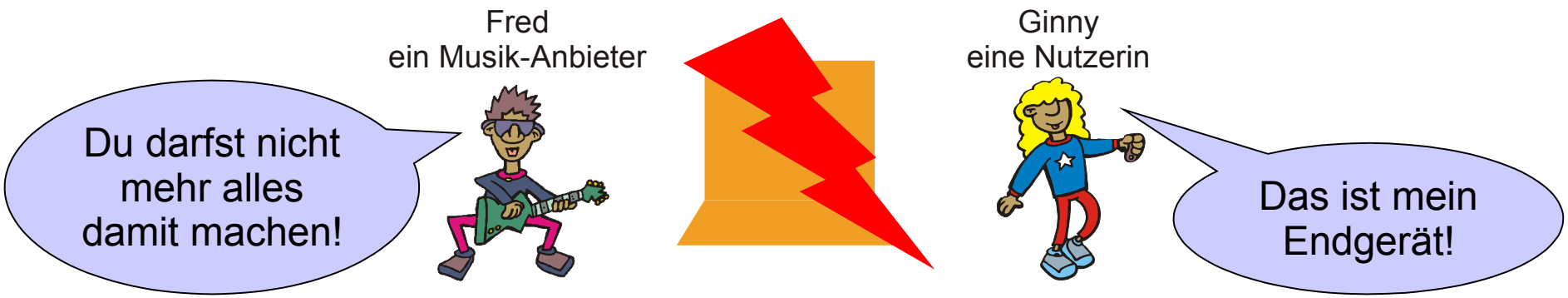
Schlüssel wird im Endgerät kontrolliert



- *Der DRM-Controller (bzw. DRM Agent) kontrolliert die Verwendung des Schlüssels*
- *Schlüssel muss vor Nutzer verborgen bleiben*
- *DRM-Controller darf nicht vom Nutzer umprogrammiert werden*

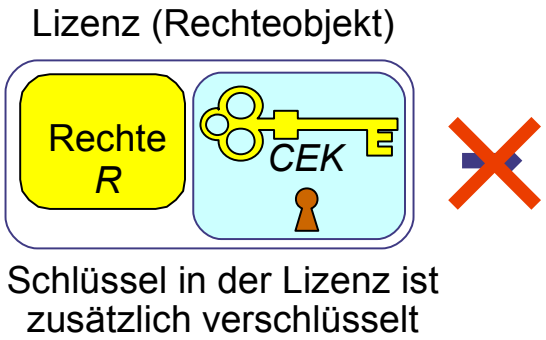
Mögliche Konflikte

- **DRM-Controller läuft auf Endgerät des Nutzers**
  - ***DRM-Controller schränkt die Funktionen (z.B. beliebiges Kopieren) des Endgerät des Nutzers (Ginny) ein.***
  - ***Der Nutzer könnte unbeobachtet die Funktion des DRM-Controllers untersuchen***
  - ***Anbieter (Fred) muss darauf vertrauen, dass die Nutzerin den DRM-Controller nicht verändert (manipuliert).***
  - ***Fred traut Ginny nicht und Ginny vertraut Fred nicht***



Lizenzen (oder Rechteobjekte)

- **Lizenzen enthalten den Schlüssel und eine Rechtebeschreibung**



  - ***Verschlüsselte Nutzdaten sind ohne Lizenz wertlos***
  - ***Rechtebeschreibung legt die zulässige Nutzungsart (abspielen) und Nutzungsdauer (3 mal) fest***
  - ***Verschlüsselte Nutzdaten können und sollen kopiert werden***
  - ***Lizenzen sind an das Endgerät gebunden (Weitergabe unmöglich oder wirkungslos)***

Mögliche Fragen

- Verschlüsselung mit XOR
- Warum ist XOR praktisch nicht geeignet?
- Was ist mit dem Schlüssel?
- …

Nächste Vorlesung

- **Rechte und ihre formale Notation**
  - ***Nutzungsrechte***
  - ***Mögliche Nutzungsrechte***
  - ***Spezieller Geschäftsmodelle***
  - ***Rechtebeschreibungssprachen***
  - ***Stammbau der Rechtebeschreibungssprachen***
  - ***ODRL***

Weitere Informationen

- *Jürgen Nützel: Die informatorischen Aspekte virtueller Güter und Waren, Oktober 2006 im Unversitätsverlag Ilmenau, www.juergen-nuetzel.de/habilitation.html*
- *Jürgen Nützel: Digital Rights Management (Seite 28 - 49), in Die Privatkopie, herausgegeben von Frank Fechner, 2007, Universitätsverlag Ilmenau, ISBN 978-3-939473-06-0, http://www.db-thueringen.de/servlets/DocumentServlet?id=7543*
- *http://de.wikipedia.org/wiki/One-Time-Pad*
- *http://de.wikipedia.org/wiki/Advanced_Encryption_Standard*
- *Tutorial zu AES: www.realtec.de/privat/arbeiten.shtml*