Digital Rights Management (DRM) -
Verfahren, die helfen Rechte an virtuellen Waren durchzusetzen

Übungsaufgaben (download von www.juergen-nuetzel.de/drm.html)
zur Probevorlesung im Rahmen des Habilitationsverfahren von Dr.-Ing. Jürgen Nützel an der Fakultät für Informatik und Automatisierung der Technischen Universität Ilmenau
(**zurück per Fax an 03677 / 69-4724 oder E-Mail an Juergen.Nuetzel@tu-ilmenau.de**)

Name : _____ *freiwillig*

E-Mail: _____ *freiwillig, für die Zusendung der Korrektur*

Student(in): ☐ Mitarbeiter(in):☐ Hochschullehrer(in): ☐ Andere(r): ☐

■ Fragenkomplex 1: Ausgangslage und Definitionen

- Nennen Sie drei charakteristische Eigenschaften digitalisierter virtueller Waren!

  _____ _____ _____

- Welches Problem hat ein Anbieter digitalisierter virtueller Waren, das ein Anbieter körperlicher realer Waren nicht hat?

  _____

■ Fragenkomplex 2: Technische Grundprinzipien

- Nennen Sie die beiden technischen Grundprinzipien moderner DRM-Systeme!

  _____ _____

- Verschlüsseln (XOR-Funktion) Sie die Nutzdaten: 10101110 mit dem Schlüssel:11110000 !

  Ergebnis: _____ Ergebnis nach nochmaliger Verschlüsselung: _____

- Was steht in einer Lizenz?

  _____ _____

■ Fragenkomplex 3: Rechte und Rechtebeschreibung

- Vervollständigen Sie folgende Aussage zum Begriff Rechtebeschreibung:

  Einem _____ wird das _____ gewährt unter einer definierten _____ eine bestimmte (virtuelle) Ware in einer definierten _____ zu nutzen.

- Nennen Sie drei mögliche Nutzungsrechte für Musik!

  _____ _____ _____

Fragenkomplex 4: Public-Key-Kryptographie

- Nennen Sie zwei Anwendungen der Public-Key-Kryptographie bei DRM!

- Welche Eigenschaften muss eine kryptographische Hash-Funktion besitzen?

- Welche mathematische Operation müsste ein Angreifer auf das RSA-Verfahren durchführen?

- Wie erhöht man die Sicherheit beim RSA-Verfahren?

Fragenkomplex 5: Referenz-Modell und neue Geschäftsmodelle

- Welche Komponente in einem Endgerät mit DRM interpretiert und exekutiert die Rechte?

- Wodurch wird das Geschäftsmodell „Musik im Abo“ technisch möglich?

Fragenkomplex 6: Open Mobile Alliance (OMA)

- Was ist das Ziel des Domain-Konzeptes?

- Was verschlüsselt ein Domain-Key?

Fragenkomplex 7: Sicherheitsprobleme

- Was ist aus Sicht der Anbieter der schlimmste Angriff auf ein DRM-System?

- Kann der Betreiber eines Lizenz-Server einen solchen Angriff erkennen?