Prüfung »Verlässlichkeit offener Computernetze« oder »DuD« (22.06.2006)

Bitte zutreffenden Namen der Vorlesung einringeln, damit Sie das richtige Zeugnis ausgestellt erhalten!!

Name	Vorname	Matrikelnummer	Kennzahl

Haben Sie in der Vorlesung einen Vortrag gehalten? (bei „ja“ plus 10 Punkte) ja nein

1. Die Projektleitung eines EU-Projekts mit vier Partnern möchte sicherstellen, dass nur mindestens drei von den vier Partnern **gemeinsam** an die Projektkassa herankommen. Sie verteilt folgende Teilschlüssel: Frau 1 erhält den Teilschlüssel 12, Herr 2 den Teilschlüssel 17, Herr 3 den Teilschlüssel 24 und Frau 4 den Teilschlüssel 33. Wenn 2, 3, und 4 ihre Teilschlüssel zusammentun, erhalten sie den gleichen Gesamtschlüssel wie 1, 2 und 3? Wenn ja, wie lautet er, wenn nein, warum nicht? (bitte Nebenrechnungen hinschreiben!). (15 Punkte)

2. Inwieweit ist der commons keine/eine Metapher für das Mobilkommunikationsnetz? (bitte begründen!) (5 Punkte)

- 3a. Bitte geben Sie je ein konkretes Beispiel für die vier Schichten des Internet-Outputs an. (8 Punkte)

- 3b. Bitte geben Sie vier Beispiele für nicht-kommerzielle Aktivitäten, die Sie auf Grund des Internet durchführen können (8 Punkte)

4. Welche Vorteile und Schwächen besitzen unsymmetrische Verschlüsselungssysteme im Vergleich zu symmetrischen? (4 Punkte)

5. Bitte berechnen Sie aus dem Bitstring $\{x_5, x_4, x_3, x_2, x_1, x_0\} = \{100101\}$ das Ergebnis für x_6 und x_7 in einem linearen Schieberegister, dessen Koeffizienten c_i alle gleich 1 sind. (10 Punkte)

6. Welche der folgenden Aussagen sind richtig und welche nicht? (max 50 Punkte bei 25 Fragen)
 (Jede korrekte Antwort = + 2, falsche Antwort = - 1, keine Antwort = 0 Punkte.)

Statement	Falsch	Richtig
Die Gleichstellung von Mann und Frau ist eine Form der Effektivierung	☐	☐
Ein türkischer Bürger hat in Österreich kein Recht auf Löschung seiner hier unzulässig verarbeiteter Daten	☐	☐
Das TCP/IP Protokoll besitzt einen Modus zur Kostenverrechnung der übertragenen Daten	☐	☐
Bei einer Datenschutzverletzung durch meinen Hausarzt ist das Bezirksgericht zuständig	☐	☐
Ein EDV-Dienstleister in Österreich verarbeitet personenbezogene Daten für eine deutsche Firma. Bei Problemen ist das österreichische DSGVO anzuwenden.	☐	☐
Ein Patent ist bis 90 Jahre nach dem Tod des Inhabers in Kraft	☐	☐
Das GATS-Abkommen schreibt derzeit in Österreich vor, dass Bildung auch von Privaten angeboten werden kann.	☐	☐
Ein Unternehmen kann keine Urheberrechte an einem selbst erzeugten Werk haben	☐	☐
UNIX vergibt Zugriffsrechte nach „Owner“, „Group“ und „Others“	☐	☐
Eine GNU-Lizenz ermöglicht die freie Verfügbarkeit über den Quellcode	☐	☐
Ein Trojanisches Pferd ist kein eigenständiges Programm	☐	☐
Ich kann eine Bürgschaft rechtsgültig elektronisch unterschreiben	☐	☐
Mein Partner in einer verschlüsselten Kommunikation unterschreibt seine e-mail an mich korrekterweise mit seinem privaten Schlüssel	☐	☐
Ein ZDA muss im Zweifelsfall über seine Rechtmäßigkeit ein Zertifikat sofort sperren.	☐	☐
Die EU verbietet in der Datenschutzrichtlinie die Umgehung technischer Schutzmaßnahmen zwecks Aneignung fremden geistigen Eigentums	☐	☐
Das Geburtstagsphänomen tritt bei kurzen symmetr. Schlüsseln auf	☐	☐
Laut Datenschutzgesetz dürfen urheberrechtlich geschützte Werke für Studierende vervielfältigt werden (fair use)	☐	☐
Ein Patent dient zur Geheimhaltung einer Erfindung	☐	☐
Der Netzwerkeffekt besagt, dass der Nutzen eines Konsumenten durch weitere Netzteilnehmer kleiner wird	☐	☐
Rotor-Chiffriersysteme wurden nur in Hubschraubern eingesetzt	☐	☐
Ein vom Erblasser stark blind unterschriebenes Testament ist rechtsgültig	☐	☐
Asymmetrische Verschlüsselung ist einfacher zu handhaben als symmetrische	☐	☐
In Deutschland müssen die Kosten einer Warenrücksendung im Wert unter 10 Euro vom on-line Händler bezahlt werden.	☐	☐
Der Datenschutzkommission gehört von Amts wegen immer der Bundespräsident an	☐	☐
Die Vigenère-Verschlüsselung ist das erste unsymmetrische Verschlüsselungsverfahren der Geschichte	☐	☐