
Bitte hier unbedingt Matrikelnummer und Adresse eintragen, sonst keine Bearbeitung möglich.

Postanschrift: FernUniversität, D-58084 Hagen

Name, Vorname

Straße, Nr.

PLZ, Wohnort

FERNUNIVERSITÄT
in Hagen
EINGANG

MI

FERNUNIVERSITÄT
in Hagen
58084 Hagen

Fakultät für

Mathematik und Informatik

Kurs: 01867 „Sicherheit im Internet II“

Klausur am 05.02.2011

Zutreffendes unbedingt

Hörerstatus:

- ☐ Vollzeitstudent
- ☐ Teilzeitstudent
- ☐ Zweithörer
- ☐ Gasthörer
- ☐ Bachelor
- ☐ Lehramt
- ☐ . . . . . .

Klausurort:

- ☐ Berlin
- ☐ Bochum
- ☐ Frankfurt
- ☐ Hamburg
- ☐ Karlsruhe
- ☐ Köln
- ☐ München
- ☐ Bregenz
- ☐ Wien
- ☐ Bern
- ☐ . . . . . .

_

Aufgabe	1	2	3	4	5	6	7	8	9	10	Summe
erreichbare Punktzahl	14	9	10	8	8	10	12	11	10	8	100
bearbeitet											
erreichte Punktzahl											

Note: _____

Hagen, den _____ Betreuer: _____

FernUniversität in Hagen

Fakultät für
Mathematik und Informatik
Lehrgebiet Parallelität und VLSI
Prof. Dr. J. Keller
58084 Hagen, 05.02.2011

Bescheinigung zur Vorlage beim Finanzamt

Herr/Frau _____

geb. am _____ , Matr.-Nr.: _____ ,

hat am 05.02.2011 von 10:00 - 12:00 Uhr an der Klausur zum Kurs

01867 „Sicherheit im Internet II“

in _____ teilgenommen.

_____ (Stempel) (Prof. Dr. J. Keller)

FernUniversität in Hagen

Fakultät für
Mathematik und Informatik
Lehrgebiet Parallelität und VLSI
Prof. Dr. J. Keller
58084 Hagen, 05.02.2011

Leistungsnachweis / Zertifikat

Herr/Frau _____

geb. am _____ , Matr.-Nr.: _____ ,

hat im WS 2010/2011 m i t E r f o l g an der Klausur zum Kurs

01867 „Sicherheit im Internet II“

teilgenommen.

Note: _____ (Siegel) (Prof. Dr. J. Keller)

Hinweise zur Klausur des Kurses 01867 am 05.02.2011

- Die Klausurdauer beträgt: zwei Stunden (10:00 bis 12:00 Uhr)
- **Es sind keine Hilfsmittel erlaubt.**
- Legen Sie Ihren Studenten- und Personalausweis zur Überprüfung durch die Aufsicht bereit.
- Füllen Sie vor Beginn der Klausur unbedingt das Deckblatt aus - und zwar in leserlicher Druckschrift.
- Füllen Sie bitte vor Inangriffnahme der Klausuraufgaben die Bescheinigung und den/das Leistungsnachweis/Zertifikat leserlich aus (natürlich bis auf die Note und Unterschrift). **Andernfalls wird kein Leistungsnachweis erstellt.**
- Die Bescheinigung für das Finanzamt ist nur mit Unterschrift und Stempel gültig.
  Nur vollständig ausgefüllte Bescheinigungen werden von uns abgestempelt, unterschrieben und Ihnen zugestellt.
- Überprüfen Sie die Vollständigkeit der Aufgabenstellungen!
  Die Klausur umfasst einschließlich der drei Deckblätter insgesamt 10 Seiten mit 10 Aufgaben.
- Schreiben Sie auf alle Lösungsbögen Ihren Namen und Ihre Matrikelnummer !
- Tragen Sie Ihre Lösungen in die dafür vorgegebenen Felder ein. Falls Sie damit nicht auskommen, benutzen Sie bitte die Rückseite der vorhergehenden Aufgabe. Verweisen Sie in diesem Fall darauf, dass diese Rückseite beschrieben ist.
- Bei Abgabe Ihrer Arbeit heften Sie bitte die ersten Seiten des übergebenen Klausur-exemplares (Deckblatt, Bescheinigungen und Hinweise zur Klausur) vor Ihre Lösungsblätter. Kontrollieren Sie zum Schluss, dass Sie Ihre gesamte Arbeit geheftet abgeben. Nachträglich eingereichte Lösungen werden von uns nicht akzeptiert.
- Die Korrektur der Klausur wird voraussichtlich bis Mitte März 2011 erfolgt sein. Wir bitten, von vorzeitigen Nachfragen abzusehen.

Bei der Bearbeitung der Klausur wünschen wir Ihnen viel Erfolg!

Ihre Kursbetreuer

Aufgabe 1: **(14 Punkte)**

a) Ein Wörterbuch enthält 10^6 Wörter. Ein Benutzer generiert nun sein Passwort wie folgt: er nimmt eine Ziffer von 0 bis 9, daran hängt er ein Wort w_1 aus dem Wörterbuch, und daran hängt er ein Wort w_2 aus dem Wörterbuch. Sind allerdings die Wörter w_1 und w_2 identisch, so ersetzt er w_2 im Passwort durch ein Semikolon. Wie viele Passwörter muss ein Angreifer, der diese Erzeugungsroutine kennt, bei einem Wörterbuchangriff maximal probieren, bis er das Passwort des Benutzers ermittelt hat. Geben Sie die Zahl als Zehnerpotenz an. **(6 Punkte)**

b) Klassifizieren Sie Angriffe auf Verschlüsselung nach der Menge an verschlüsselter bzw. unverschlüsselter Information, die dem Angreifer zur Verfügung steht. Geben Sie jeweils an, wie die Angriffsklasse heißt, und welche Information zur Verfügung steht. Nennen Sie auch die drei weiteren Angriffstypen nach Schneier. Die erste Klasse (ciphertext only Angriffe) brauchen Sie nicht zu beschreiben. **(8 Punkte)**

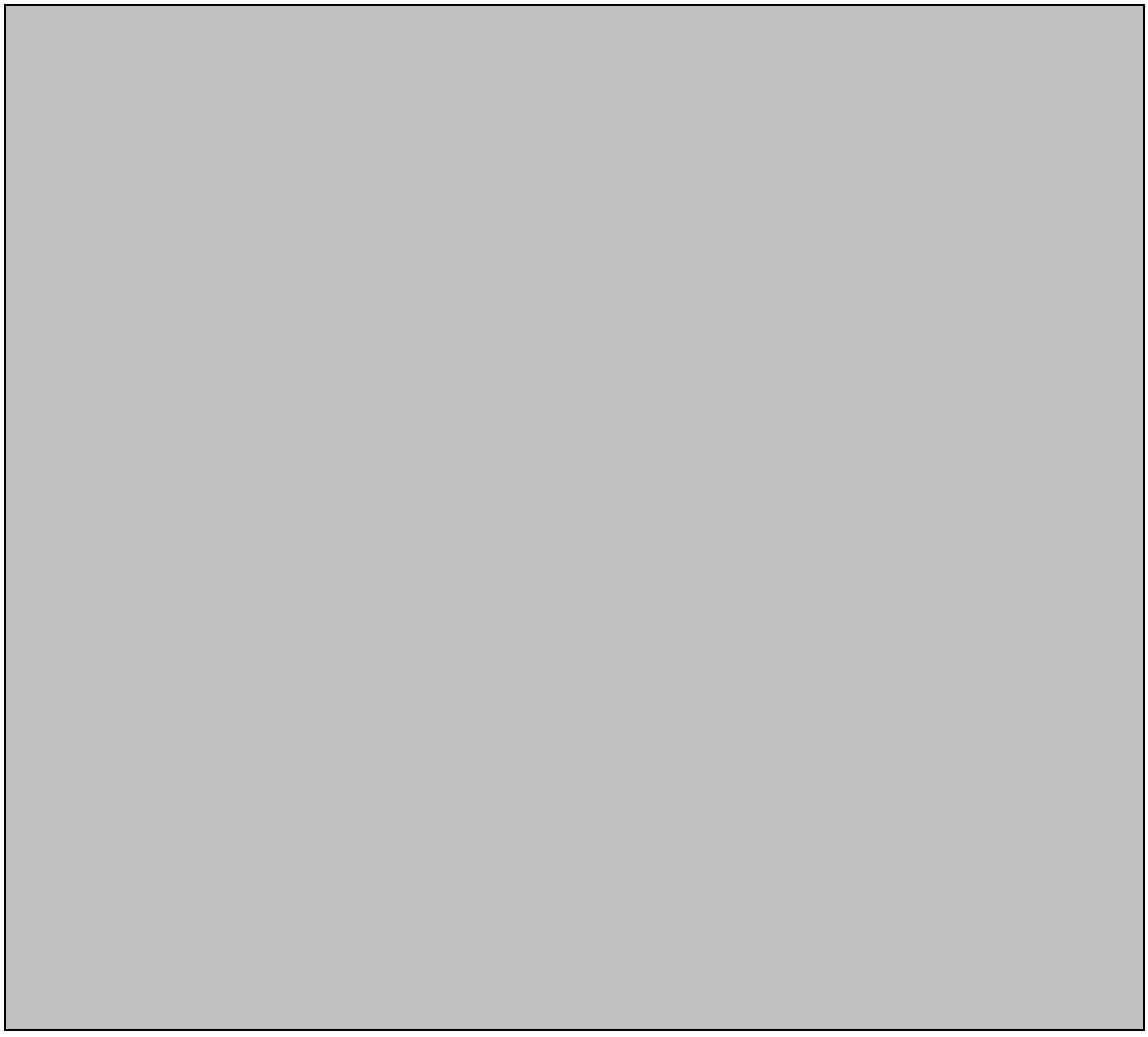
Aufgabe 2: **(9 Punkte)**

Gegeben sei eine SQL-Datenbank mit einer Tabelle user, die eine Spalte kennung enthält. In einem Java-Programm kann ein Benutzer eine Tastatureingabe vornehmen, die in einer Variablen Eingabe vom Typ String abgelegt wird. Mittels des Kommandos

String anw = new String("select * from user where kennung = '" + eingabe + "';");

erzeugt das Programm eine SQL-Anweisung in der Variablen anw und führt diese Anweisung auf obiger Datenbank-Tabelle aus.

Schildern Sie den in Kurseinheit 1 beschriebenen Angriff, der zur Löschung der Tabelle user führt, und beschreiben Sie Gegenmaßnahmen, um diesen Angriff zu verhindern.



Aufgabe 3: **(10 Punkte)**

a) Wie erkennt beim Konzept der blinden Signatur die Bank den Wert einer von einem Benutzer erstellten Münze, wenn die Bank die Münze selbst nicht lesen kann, da sie vom Benutzer verändert wurde? **(5 Punkte)**

b) Wie erzeugt der Benutzer beim Konzept der blinden Signatur die Seriennummern seiner Münzen? **(5 Punkte)**

Aufgabe 4: **(8 Punkte)**

Beschreiben Sie den Miller-Rabin-Primzahlest. Ist dieser Test ein Monte-Carlo- oder ein Las-Vegas-Verfahren?

Aufgabe 5: **(8 Punkte)**

a) Welche Kreislänge (=Periodenlänge) können Sie erwarten, wenn Sie einen Pseudozufallszahlengenerator mit k-Bit Zuständen benutzen und die Zustandsübergangsfunktion zufällig aus der Menge aller möglichen Zustandsübergangsfunktionen gewählt ist? Geben Sie die Periodenlänge mithilfe von k und der O-Notation an. **(4 Punkte)**

b) Welche Kreislänge kann maximal bei einem solchen Pseudozufallszahlen-generator auftreten? Geben Sie die Kreislänge mithilfe von k an. **(4 Punkte)**

Aufgabe 6: **(10 Punkte)**

a) Beschreiben Sie kurz das 3-Wege Challenge/Response Verfahren beim Challenge Handshake Authentication Protocol (CHAP). **(5 Punkte)**

b) Beschreiben Sie kurz die benötigte Infrastruktur, wenn man bei einem OpenVPN eine Authentisierung des VPN-Servers mittels Zertifikat vornehmen will. **(5 Punkte)**

Aufgabe 7: **(12 Punkte)**

Ein Sensor eines network-based Intrusion Detection Systems (IDS) soll die Paketköpfe (Header) aller IP-Pakete speichern, die innerhalb von 1 Minute und 40 Sekunden durch die Leitung transportiert werden, an die der Sensor angeschlossen ist.

Welche der folgenden Aussagen treffen zu? (Hinweis: 8 MBit = 1 MByte)

☐ Bei einer Fast Ethernet Leitung (100 MBit/s), bei der 80% der Kapazität durch IP-Pakete belegt sind, fällt im genannten Zeitraum, wenn die Header 10% der Paketgröße ausmachen und keine weiteren Overheads betrachtet werden, eine zu speichernde Datenmenge von 100 MByte an.

☐ Bei einer Fast Ethernet Leitung (100 MBit/s), bei der 80% der Kapazität durch IP-Pakete belegt sind, fällt im genannten Zeitraum, wenn die Header 10% der Paketgröße ausmachen und keine weiteren Overheads betrachtet werden, eine zu speichernde Datenmenge von 10 MByte an.

☐ Bei einer Ethernet-Leitung (10 MBit/s), bei der 80% der Kapazität durch IP-Pakete belegt sind, fällt im genannten Zeitraum, wenn die Header 5% der Paketgröße ausmachen und keine weiteren Overheads betrachtet werden, eine zu speichernde Datenmenge von 5 MByte an.

☐ Bei einer Ethernet-Leitung (10 MBit/s), bei der 80% der Kapazität durch IP-Pakete belegt sind, fällt im genannten Zeitraum, wenn die Header 5% der Paketgröße ausmachen und keine weiteren Overheads betrachtet werden, eine zu speichernde
Datenmenge von 1 MByte an.

☐ Bei einer Ethernet-Leitung (10 MBit/s), bei der keine IP-Pakete übertragen werden, fällt eine zu speichernde Datenmenge von 0 Bytes an.

Aufgabe 8: **(11 Punkte)**

Welche der folgenden Aussagen treffen zu?

☐ In der Telekommunikations-Überwachungsverordnung (TKÜV) ist festgelegt, welche Möglichkeiten den Überwachungsbehörden wie Polizei und Nachrichtendiensten durch die Provider eingeräumt werden müssen.

☐ Die Vergabe von Domänen-Namen wird von der Internet Corporation for Assigned Names and Numbers (ICANN) gesteuert, die Vergabe von Domänen innerhalb der Domäne .de ist aber an das Deutsche Network Information Center (DENIC) delegiert.

☐ Ein Zugangsanbieter muss immer auch Inhalteanbieter sein.

☐ Das Einbinden einer Grafik in eine HTML-Seite mittels <img src="http://www.xyz.de/bilder/grafik1.gif"> kann in keinem Fall eine Urheberrechtsverletzung darstellen.

☐ Bei der Domänen-Registrierung prüfen die Verwaltungsorganisationen der DNS-Namen, ob die zu registrierende Domäne als Marke geschützt ist.

☐ Ein Diensteanbieter braucht ein Impressum (von wem werden Daten gespeichert/verarbeitet) und eine Unterrichtung (welche Daten werden zu welchem Zweck gespeichert/verarbeitet) für seine Nutzer.

Aufgabe 9: **(10 Punkte)**

a) Nennen Sie die drei Phasen, in denen sich verschiedene Versionen einer komplexen, 3-Schichten Web-Anwendung befinden können, so dass die Anforderungen an die verschiedenen Umgebungen maximal werden. **(3 Punkte)**

b) Nennen Sie die Software-Komponenten, die auf den Rechnern für die verschiedenen Phasen installiert sein sollten. **(7 Punkte)**

Aufgabe 10: **(8 Punkte)**

Erklären Sie die Techniken Interposition und Compartmentalization.