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: 01868 „Sicherheit im Internet I - Ergänzungen"

Klausur am 05.02.2011

Hörerstatus:

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

Klausurort:

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

Zutreffendes unbedingt ankreuzen!

_

Aufgabe	1	2	3	4	5	6	7	Summe
erreichbare Punktzahl	8	9	6	9	6	8	4	50
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

01868 „Sicherheit im Internet I - Ergänzungen"

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

01868 „Sicherheit im Internet I - Ergänzungen"

teilgenommen.

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

Hinweise zur Klausur des Kurses 01868 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 8 Seiten mit 7 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 Klausurexemplares (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 2010** erfolgt sein. Wir bitten, von vorzeitigen Nachfragen abzusehen.

Bei der Bearbeitung der Klausur wünschen wir Ihnen viel Erfolg!

Ihre Kursbetreuer

Aufgabe 1: **(8 Punkte)**

Geben Sie vier Systeminformationen an, die zum Systemzustand im Sinne der Computerforensik gehören. Ein Beispiel einer solchen Systeminformation ist der Inhalt des Hauptspeichers.

Aufgabe 2: **(9 Punkte)**

Welche der folgenden Aussagen treffen zu?

☐ Ein Angreifer muss alle Mixe einer Mix-Kaskade übernehmen, um eine Verbindung nachverfolgen zu können.

☐ Von einem digital signierten ActiveX-Control ist bekannt, dass es keine Schadfunktionen enthalten kann.

☐ Ein Rollenpseudonym wird von einer Person immer dann benutzt, wenn die Person sich in der zugehörigen Rolle befindet. Dabei ist es egal, wer die Kommunikationspartner sind.

☐ Java-Applets dürfen keine Dateien des lokalen Dateisystems lesen.

☐ Beim Konzept des Dummy Traffic verschickt der Benutzer seine Nachrichten verschlüsselt, jedoch keine überflüssigen Nachrichten.

☐ Ein Rewebber leitet einen http-Request eines Client unverändert an den Web-Server weiter.

Aufgabe 3: **(6 Punkte)**

Wie viele Ringe bieten typische Intel-CPUs. Welche Ringe entsprechen dabei dem Benutzer-Modus (Anwendungsprogramme) und dem System-Modus (Betriebssytem)?

Aufgabe 4: **(9 Punkte)**

Welche der folgenden Aussagen treffen zu?

☐ Beim Konzept der Access-Control-Listen wird die Zugriffskontrollmatrix (pro Benutzer eine Zeile, pro Ressource eine Spalte) zeilenweise bei den Benutzern gespeichert.

☐ Beim Konzept der Access-Control-Listen wird die Zugriffskontrollmatrix (pro Benutzer eine Zeile, pro Ressource eine Spalte) spaltenweise bei den Ressourcen gespeichert.

☐ Die False Acceptance Rate sagt aus, wie oft ein legitimer Benutzer fälschlicherweise nicht vom System akzeptiert wird.

☐ Im Bell-LaPadula-Modell der Informationsflusskontrolle benötigt man besonders vertrauenswürdige Personen, die die Sicherheitsklasse von Objekten auch wieder herunterstufen dürfen. (Denn sonst hätten irgendwann alle Objekte die höchste Sicherheitsstufe, was nicht sinnvoll ist.)

☐ Das Modell der Informationsflusskontrolle von Kenneth Biba versucht, die Vertraulichkeit von Daten sicherzustellen.

☐ Beim Konzept der Paravirtualisierung weiß das Gast-Betriebssystem, dass es nicht direkt auf der Hardware läuft, sondern in einer virtuellen Maschine.

Aufgabe 5: **(6 Punkte)**

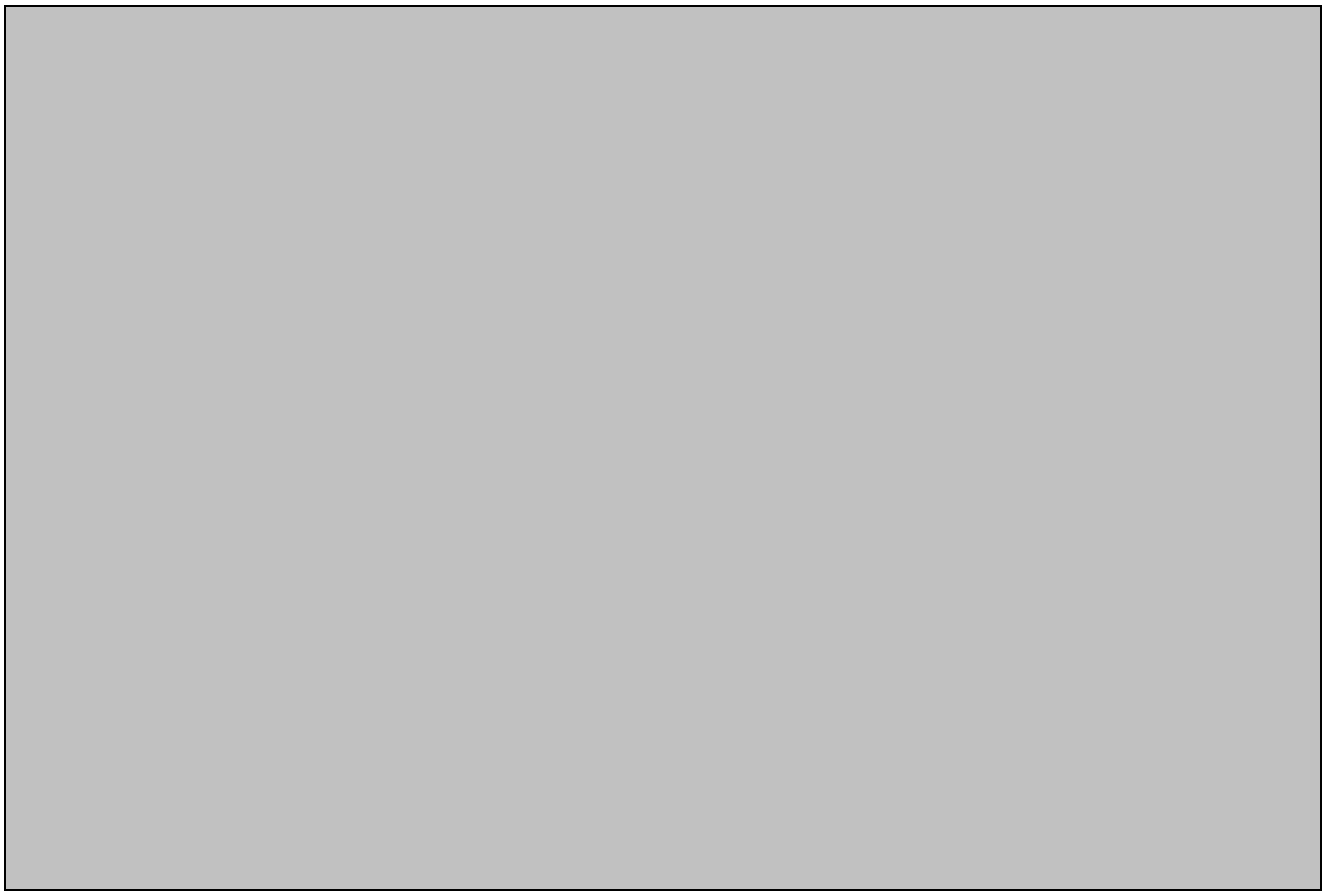
Auf welche Weise ist ein Betrug (gefälschtes Dokument) möglich, wenn ein Client bei einer Challenge-Response-Authentisierung die Challenge unverändert signiert?

Aufgabe 6: **(8 Punkte)**

Das WEP-Verfahren in WLANs benutzt RC4 als Stromchiffre mit einem 24-Bit Initialisierungsvektor und einem 40-Bit Schlüssel.

Wir machen folgende Annahmen: der Initialisierungsvektor wird im Klartext übertragen und abgehört. Der Klartext eines übertragenen und abgehörten Pakets ist bekannt. Ein Angreifer kann pro Sekunde den Klartext 2^{17} mal verschlüsseln und mit dem verschlüsselten abgehörten Paket vergleichen. Im Mittel muss der Angreifer die Hälfte aller Schlüssel ausprobieren, bis er den richtigen findet.

Wie viele Tage (Zweierpotenz) braucht der Angreifer im Mittel, um den richtigen Schlüssel zu finden?
Gehen Sie davon aus, dass ein Tag 2^{16} Sekunden hat.



Aufgabe 7: **(4 Punkte)**

Welche der folgenden Aussagen treffen zu?

☐ WEP Verschlüsselung ist sicher, wenn der Access Point die SSID im Beacon Frame leer lässt (sog. Hide SSID) und zusätzlich eine Filterung anhand der MAC-Adresse vornimmt.

☐ Das Verschlüsselungsverfahren WPA/TKIP ist ein Blockverschlüsselungsverfahren.

☐ Bei der WPA Enterprise Mode Authentisierung mit EAP-TLS müssen der Access Point und alle Clients, die sich mit ihm verbinden wollen, ein X.509-Zertifikat besitzen.

☐ Über einen RADIUS-Server kann eine Authentisierung mit Hilfe von individuellen Benutzer-Passwörtern realisiert werden.