
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

INF

FERNUNIVERSITÄT
in Hagen
D-58084 Hagen

Fachbereich Informatik

Kurs: 01866 „Sicherheit im Internet“

Hauptklausur am 18.09.2004

Zutreffendes unbedingt ankreuzen!

Hörerstatus:

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

Klausurort:

- ☐ Berlin
- ☐ Bochum
- ☐ Frankfurt
- ☐ Hamburg
- ☐ Karlsruhe
- ☐ Kassel
- ☐ Bonn
- ☐ München
- ☐ Bregenz
- ☐ Wien
- ☐ . . . . . .

Aufgabe	1	2	3	4	5	6	Summe
erreichbare Punktzahl	10	20	15	18	20	17	100
bearbeitet							
erreichte Punktzahl							

Note: _____

Hagen, den _____ Betreuer: _____

FernUniversität in Hagen

Fachbereich Informatik
Lehrgebiet Parallelität und VLSI
Prof. Dr. J. Keller
58084 Hagen, den 18.09.04

Bescheinigung zur Vorlage beim Finanzamt

Herr/Frau _____

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

hat am 18.09.2004 von 10:00 - 13:00 Uhr an der Hauptklausur zum Kurs

01866 „Sicherheit im Internet“

in _____ teilgenommen.

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

FernUniversität in Hagen

Fachbereich Informatik
Lehrgebiet Parallelität und VLSI
Prof. Dr. J. Keller
58084 Hagen, den 18.09.04

Leistungsnachweis / Zertifikat

Herr/Frau _____

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

hat im SS2004 m i t E r f o l g an der Hauptklausur zum Kurs

01866 „Sicherheit im Internet

teilgenommen.

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

Hinweise zur Hauptklausur des Kurses 01866 am 18.09.2004

- Die Klausurdauer beträgt: drei Stunden (10.00 bis 13.00 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 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 Kopfseiten, 9 Seiten mit 6 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 zum Bestehen der Klausur erforderliche Punktzahl liegt noch nicht fest. Sie wird erst aus der tatsächlich erreichten Punkteverteilung ermittelt, liegt aber sicher nicht über 50% bzw. unter 30% der erreichbaren Punkte.
- Die Korrektur der Klausur wird voraussichtlich bis Anfang Oktober 2004 erfolgt sein. Wir bitten, von vorzeitigen Nachfragen abzusehen.

Bei der Bearbeitung der Klausur wünschen wir Ihnen viel Erfolg!

Ihre Kursbetreuer

Aufgabe 1 (10 Punkte):

a) Warum sollen Passwörter nicht für Benutzer zugänglich in einer Datei abgespeichert werden, auch wenn nur der Administrator diese Datei lesen kann? (5 Punkte)

b) Warum sollen Passwörter auch dann nicht für Benutzer zugänglich in einer Datei abgespeichert werden, wenn die Passwörter durch eine Einwegfunktion verschlüsselt sind? (5 Punkte)

Aufgabe 2 (20 Punkte):

a) Ist bei der Nutzung eines Message Authentication Code (MAC) die Vertraulichkeit der Nachricht gegeben? (5 Punkte)

b) Warum kann bei Übertragung einer Nachricht zusammen mit einem Message Authentication Code (MAC) der Sender bestreiten, die Nachricht abgeschickt zu haben? (8 Punkte)

c) Was erhält man, wenn man beim Message Authentication Code die symmetrische Verschlüsselung durch eine asymmetrische Verschlüsselung ersetzt? Wer muss in diesem Fall den privaten Schlüssel benutzen? (7 Punkte)

Aufgabe 3 (15 Punkte):

a) Unter dem Begriff „Security by Obscurity" versteht man, dass Geheimhaltung alleine auf der Unkenntnis des Angreifers über bestimmte Vorgehensweisen beruht. Inwiefern zählt hierzu die Vertraulichkeit von Dateien in einem Verzeichnis eines Webservers, wenn die Dateien selbst unverschlüsselt sind und lediglich die Anzeige der Dateinamen in diesem Verzeichnis abgeschaltet ist? (5 Punkte)

b) Warum sollte auf einem Webserver das Verfolgen symbolischer Links ausgeschaltet sein? (5 Punkte)

c) Warum sollten bei der Nutzung eines Integritätstest-Programms in einem Webserver die Prüfsummen nicht auf der Festplatte des Webservers gespeichert werden? (5 Punkte)

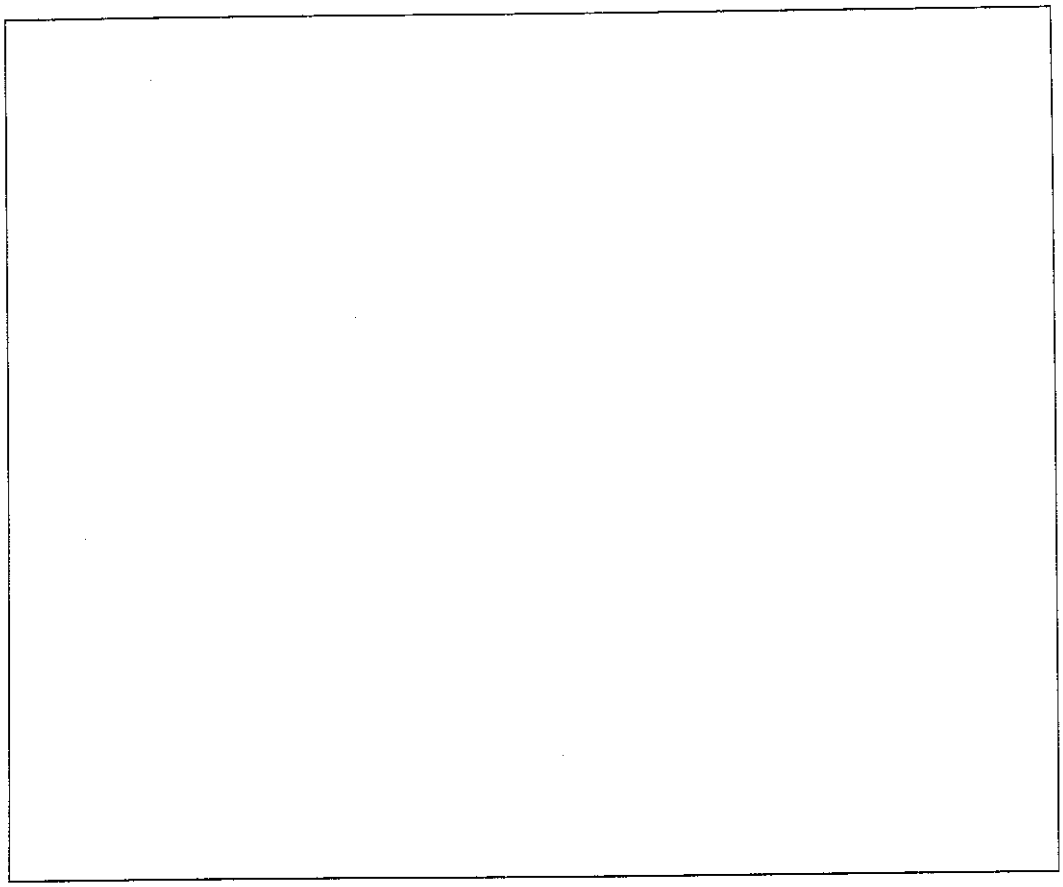
Aufgabe 4 (18 Punkte):

a) Warum werden die Aufgaben einer Firewall untergraben, wenn es neben dem Internet-Zugang über die Firewall noch eine Modemverbindung vom internen Netz zum Internet gibt? (5 Punkte)

b) Warum sollte es nicht für jeden Fall in einem Paketfilter eine Regel geben? Welche beiden Strategien können bei den Paketen verfolgt werden, bei denen keine Regel des Paketfilters zutrifft? Vergleichen Sie die Vor– und Nachteile der beiden Strategien. (13 Punkte)

Aufgabe 5 (20 Punkte):

Beschreiben Sie die Authentisierung eines Clients, der mit einem Server kommunizieren will, mittels eines Kerberos Authentication-Servers. Unterscheiden Sie dabei die Varianten mit bzw. ohne Ticket-Granting-Server.



Aufgabe 6 (17 Punkte):

Es sei E_k die DES-Verschlüsselung mit Schlüssel k, und D_k die dazugehörige DES-Entschlüsselung. Für einen festen Schlüssel k stellen E_k und D_k Permutationen auf der Menge der 64-Bit-Worte dar. Die Menge aller Permutationen auf 64-Bit-Worten bildet mit der Operation „Hintereinanderausführung“ ($A \circ B$ bedeutet hier, dass A nach B ausgeführt wird) eine Gruppe P. In dieser Gruppe sind E_k und D_k zueinander invers. Bei Anwendung des Triple-DES wird die Berechnung $E_{k3} \circ D_{k2} \circ E_{k1}$ ausgeführt.

a) Begründen Sie, warum erst aus der Tatsache, dass die Menge der DES-Permutationen $\{E_k$: k ist 56-Bit Schlüssel$\}$ keine Untergruppe U von P bildet, gefolgert werden kann, dass Triple-DES eine höhere Sicherheit als DES bietet. (12 Punkte)

b) Meist wählt man beim Triple-DES $k1 = k3$. Dies hat keinen Einfluß auf die Sicherheit. Worin liegen die Vorteile dieser Wahl? (5 Punkte)