
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: 1866 „Sicherheit im Internet“

Hauptklausur am 20.09.2003

Zutreffendes unbedingt ankreuzen !

Hörerstatus:

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

Klausurort:

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

Aufgabe	1	2	3	4	5	6	Summe
erreichbare Punktzahl	7	17	15	19	13	29	100
bearbeitet							
erreichte Punktzahl							

Note: _____

Hagen, den _____ Betreuer: _____

FernUniversität in Hagen

Fachbereich Informatik
Lehrgebiet Technische Informatik II
Prof. Dr. J. Keller
D - 58084 Hagen, den 20.09.2003

Bescheinigung zur Vorlage beim Finanzamt

Herr/Frau _____

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

hat am 20.09.2003 von 10:00 - 13:00 Uhr an der Hauptklausur zum

Kurs 1866 „Sicherheit im Internet“

in _____ teilgenommen.

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

FernUniversität in Hagen

Fachbereich Informatik
Lehrgebiet Technische Informatik II
Prof. Dr. J. Keller
D - 58084 Hagen, den 20.09.2003

Leistungsnachweis / Zertifikat

Herr/Frau _____

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

hat im SS 2003 m i t E r f o l g an der Klausur zum

Kurs 1866 „Sicherheit im Internet“

teilgenommen.

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

Hinweise zur Hauptklausur des Kurses 1866 am 20.09.2003

- 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 eigentliche Klausur, d.h. die Aufgaben, umfasst 12 Seiten.
- 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 Oktober 2003 erfolgt sein. Wir bitten, von vorzeitigen Nachfragen abzusehen.

Bei der Bearbeitung der Klausur wünschen wir Ihnen viel Erfolg!

Ihre Kursbetreuer

Name: Vorname: Matr.-Nr.:

Aufgabe 1 (7 Punkte)

Warum sollen Passwörter auch dann nicht für Benutzer zugänglich abgespeichert sein, wenn die Passwörter durch eine Einwegfunktion verschlüsselt sind?

Name: Vorname: Matr.-Nr.:

Aufgabe 2 (17 Punkte)

a) Zeichnen Sie das Prinzip der Berechnung eines Message Authentication Codes (MAC). (10 Punkte)

Name: Vorname: Matr.-Nr.:

b) Welches Verfahren erhält man, wenn man bei der Berechnung eines Message Authentication Code (MAC) den symmetrischen Verschlüsselungsalgorithmus gegen einen asymmetrischen Verschlüsselungsalgorithmus vertauscht? (7 Punkte)

Name: Vorname: Matr.-Nr.:

Aufgabe 3 (15 Punkte)

a) Nennen Sie 4 Maßnahmen zur Installation eines sicheren Webservers. (8 Punkte)

b) Warum sollte die Anzeige von Dateien in einem Verzeichnis des Webservers abgeschaltet sein? Warum kann man argumentieren, dass diese Vorgehensweise unter die Rubrik "Security by Obscurity" fällt? (7 Punkte)

Name: Vorname: Matr.-Nr.:

Aufgabe 4 (19 Punkte)

a) Nennen Sie die Aufgaben einer Firewall. (7 Punkte)

Name: Vorname: Matr.-Nr.:

b) Definieren Sie Paketfilter-Regeln für folgende Anforderungen: (12 Punkte)

- 3 interne Rechner A,B,C mit IP-Adressen 132.176.72.1,2,3
- jeder Rechner darf per WWW ins Internet
- Nur zu Rechner A darf eine WWW-Verbindung aus dem Internet aufgebaut werden.
- telnet ist verboten,
- Nur zu Rechner C darf eine telnet-Verbindung aus dem Internet aufgebaut werden
- Nur Rechner B darf emails senden und empfangen
- ftp ist verboten in beiden Richtungen

Name: Vorname: Matr.-Nr.:

Aufgabe 5 (13 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.

Name: Vorname: Matr.-Nr.:

Aufgabe 6 (29 Punkte)

a) Beschreiben Sie die Tätigkeiten zur Erstellung eines Paares aus öffentlichem und geheimem Schlüssel für den RSA Algorithmus. (6 Punkte)

Name: Vorname: Matr.-Nr.:

b) Beschreiben Sie die Berechnungen zur Ver- und Entschlüsselung mit dem RSA Algorithmus. (6 Punkte)

Name: Vorname: Matr.-Nr.:

c) Zeigen Sie, dass die Entschlüsselung eines Textes, der mit einem privaten Schlüssel verschlüsselt wurde, mit dem dazu gehörenden öffentlichen Schlüssel möglich ist. (6 Punkte)

Name: Vorname: Matr.-Nr.:

d) Person A hat als Primzahlen *p=23* und *q = 41* gewählt, sowie *e=7.* Person A teilt Person B ihren öffentlichen Schlüssel e, n mit. Person B verschlüsselt damit eine Nachricht M und erhält *C=545 .* Berechnen Sie für Person A den geheimen Schlüssel d und entschlüsseln Sie C. (11 Punkte)

Name: Vorname: Matr.-Nr.:

Hinweis:

1. Um d zu finden, suchen Sie kleine Vielfache von (p-1)(q-1), die, wenn sie um 1 erhöht werden, durch e teilbar sind.

2. Um 545^d zu rechnen, bestimmen Sie die Binärdarstellung $d_8d_7....d_0$ von d und benutzen

$$545^d \bmod n = 545^{\sum_{i=0}^{8} 2^i \cdot d_i} \bmod n = \prod_{i=0}^{8} 5^{2^i \cdot d_i} \bmod n$$

Hierbei gilt

i	$545^{2^i} \bmod n$
1	923
2	400
3	633
4	857
5	795
6	215
7	18