Hochschule
Ravensburg-Weingarten
Technik | Wirtschaft | Sozialwesen

Name, Vorname:

Matrikelnummer:

Prüfer: Prof. Dr. Tobias Eggendorfer

Übertrag:
Punkte:
Gesamt:

Hinweise:

1. Schreiben Sie auf ***jedes*** Blatt Ihren Namen und Matrikelnummer.
2. Diese Prüfung hat einen Umfang von 12 Seiten. Bitte prüfen Sie Ihre Angabe auf Vollständigkeit.
3. Lassen Sie den Prüfungsbogen bitte zusammengeheftet.
4. Schreiben Sie bitte Ihre Antworten in die vorgesehenen Felder. Bitte lassen Sie den vorgesehenen Korrekturrand rechts frei. Sollte Ihnen der Platz nicht reichen, schreiben Sie bitte auf der Rückseite der Bögen. Geben Sie dabei klar an, auf welche Aufgabe sich Ihre Lösung bezieht.
   Für umfangreichere Antworten kann es auch leere Seiten zwischen den Aufgaben geben. Bitte arbeiten Sie die ganze Prüfung durch.
5. Schreiben Sie bitte lesbar. Unlesbare Antworten werden nicht bewertet.
6. Bitte schreiben Sie nicht mit roter (Korrektur) oder grüner (Zweitkorrektur) Farbe.
7. Geben Sie eindeutige Antworten. Wenn Sie mehr als eine mögliche Lösung angeben, wird die schlechteste bewertet.
8. Geben Sie bei Berechnungen etc. stets Ihren Rechenweg an.
9. „Schmierpapier“ ist mit abzugeben. Sie finden am Schluß dieses Prüfungsbogens Seiten für Ihre Notizen / Nebenrechnungen. Der Inhalt dieser Seiten wird nicht bewertet.
10. Diese Prüfung hat einen Umfang von 110 Punkten.
11. Die Prüfung wurde für eine Bearbeitungszeit von 60 Minuten konzipiert.
12. Die Verwendung von anderen als den unten angegebenen zulässigen Hilfsmitteln führt zum sofortigen Ausschluß von der Prüfung.

Zulässige Hilfsmittel:

- keine -

Erreichte Punktzahl: ______ / 110 → Note: ______

Punkte	Note
99	1,0
98	1,1
97	1,2
95	1,3
93	1,4
92	1,5
90	1,6
88	1,7
87	1,8
85	1,9
83	2,0
82	2,1
80	2,2
78	2,3
77	2,4
75	2,5
73	2,6
72	2,7
70	2,8
68	2,9
67	3,0
65	3,1
63	3,2
62	3,3
60	3,4
58	3,5
57	3,6
55	3,7
53	3,8
52	3,9
50	4,0
49	5,0

Name, Vorname:

Matrikelnummer:

Prüfer: Prof. Dr. Tobias Eggendorfer

Übertrag:
Punkte:
Gesamt:

Teil 1 - Mutltiple Choice Fragen

Hinweis:

Markieren Sie die korrekten Antworten eindeutig durch ein Kreuz. Sollten Sie Ihre Markierung ändern müssen, schwärzen Sie bitte das entsprechende Feld. Soweit nichts anderes angegeben ist, ist eine Antwort pro Frage richtig.

Eine richtige Antwort bedeutet einen Punkt. Unabhängig von der Zahl der richtigen Antworten führt eine Falschantwort in einer Frage mit nur einer richtigen Antwort für diese Frage zur Bewertung mit null Punkten.

Bei Fragen, bei denen mehrere Antwortmöglichkeiten bestehen, erhalten Sie für jede richtige Antwort einen Punkt, für jedes falsch gesetzte Kreuz zwei Punkte Abzug. In keinem Fall können Sie weniger als 0 Punkte erhalten.

Gesamtpunktzahl: 10 Punkte

1. Um Sicherheitslücken zu melden, kann man ...
   - ✓ **Möglichkeit1**
   - ○ Möglichkeit2
   - ✓ **Möglichkeit3**
   - ○ Möglichkeit4
   - ✓ **Möglichkeit5**
   - ✓ **Möglichkeit6**
   - ✓ **Möglichkeit7**

2. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.
   - ○ 16
   - ✓ **20**
   - ○ 24
   - ✓ **abhängig**
   - ○ je nachdem
   - ✓ **kommt drauf ankommt drauf ankommt drauf ankommt drauf ankommt drauf an**

3. Wie lautet der Befehl zum Anzeigen von Dateien, die als Endung '.tex' besitzen?
    - ○ Befehl1
    - ✓ **Befehl2**
    - ○ Befehl3
    - ○ Befehl4
    - ○ Befehl5
    - ✓ **Befehl6**
    - ○ Befehl7

Teil 2 - Wissensfragen

Gesamtpunktzahl: 70 Punkte

4. Was ist ein Brute-Force-Angriff?
   (12 Punkte)

Name, Vorname:

Matrikelnummer:

Prüfer: Prof. Dr. Tobias Eggendorfer

Übertrag:
Punkte:
Gesamt:

Lösung: Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua.

Name, Vorname:

Matrikelnummer:

Prüfer: Prof. Dr. Tobias Eggendorfer

Übertrag:
Punkte:
Gesamt:

5. Um nicht angreifbar zu sein, werden häufig. Erklären Sie, ob diese Methode Sinn ergibt, und in welchen Bereichen Sie Anwendung finden kann. (10 Punkte)

Lösung: Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

6. Der selbe Kartenhersteller gibt Ihnen nun eine weitere Karte zur Untersuchung. Die offentlichen Parameter dieser Chipkarte lauten: n = 221 und e = 5. Sie manipulieren die Karte so, dass bei der Signaturerstellung ein Fehler in mp auftritt. Daraufhin gibt Ihnen die Karte für die Nachricht m = 18 die (fehlerhafte) Signatur s 0 = 52 aus. Faktorisieren Sie mit diesen Informationen n in p und q! (6 Punkte)

Lösung: Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

7. Nennen Sie mindestens 3 Methoden, mit denen Angreifer ...
(10 Punkte)

Lösung: Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

8. Wenn man zur Aktivierung einer Pay-TV-Chipkarte durch positive Adressierung eine Schlüsselhierarchie verwendet, der für 1.000.000 Kunden ein ternärer Baum (d.h. ein Baum, bei dem jeder Knoten drei Nachfolger hat) verwendet, wie viele Kryptogramme benötigt man dann zur Deaktivierung einer Chipkarte?
(15 Punkte)

Lösung: Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

9. Erläutern Sie das Prinzip des ’Social Hackings’!
   (7 Punkte)

Lösung: Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

10. Erläutern Sie das "Hand-Shake-Verfahren"!
    (10 Punkte)

Lösung: Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Name, Vorname:

Matrikelnummer:

Prüfer: Prof. Dr. Tobias Eggendorfer

Übertrag:
Punkte:
Gesamt:

Teil 3 - Transferaufgaben

Gesamtpunktzahl: 30 Punkte

11. Wenn A gleich B ist, und C gleich 200, wie schwer ist der Sinn des Leben? Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. (10 Punkte)

    Lösung: Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

12. Transfer Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. (10 Punkte)

    Lösung: Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

13. Abgesehen von ... gibt es eine Vielzahl von ... . Wieso kann man nicht davon ausgehen, dass aufgrund ... (10 Punkte)

    Lösung:

Anhang - Platz für Ihre Notizen

Die folgenden Seiten können Sie für Ihre Notizen, Nebenrechnungen etc. nutzen. Der Inhalt dieserSeiten wird, sofern Sie es nicht explizit markieren, nicht bewertet.

Anhang - Platz für Ihre Notizen

Die folgenden Seiten können Sie für Ihre Notizen, Nebenrechnungen etc. nutzen. Der Inhalt dieserSeiten wird, sofern Sie es nicht explizit markieren, nicht bewertet.