Fachhochschule Wiesbaden
Fachbereich Design Informatik Medien
Prof. Dr. Bernhard Geib

Security AI / Kryptographie und Datensicherheit

Probeklausur SS 2007
LV 3151 bzw. 7433

Name:
Vorname:
Matr.-Nr.:
Unterschrift:
Note:

Sie erhalten eine geheftete Klausur. Bitte lösen Sie die Heftung **nicht**. Bitte tragen Sie zu Beginn der Bearbeitungszeit Ihren Namen und Ihre Matrikelnummer an den dafür vorgesehenen Stellen ein und unterschreiben Sie die Klausur. Die Klausur ist nur mit Unterschrift gültig. Die Klausur muß mit dem Verlassen des Raumes abgegeben werden.

Dauer: 120 Minuten

Hilfsmittel: Taschenrechner

Punktevergabe:

Aufgabe	Soll-Punkte	Ist-Punkte
1	25	
2	10	
3	25	
4	15	
5	25	
Gesamt	100	

Aufgabe 1:

a) Was versteht man unter "Sicherheit eines IT-Systems"?

b) Nennen und erläutern Sie fünf grundsätzliche Aspekte der Informationssicherheit.

c) Benennen Sie die Bausteine eines Sicherheitskonzeptes und skizzieren Sie das zugehörige Prozeßmodell.

Aufgabe 2:

a) Welches sind die häufigsten Formen des Mißbrauchs informationstechnischer Systeme?

b) Wie schätzen Sie die prozentuale Verteilung der verschiedenen Mißbrauchsformen bzgl. statistisch erfaßter Schadensereignisse ein?

Aufgabe 3:

Für ein benutztes RSA-Verfahren möge der öffentliche Schlüssel Kp = 3 und n = 33 betragen. Versuchen Sie aus dieser Kenntnis heraus

a) den zugehörigen privaten Schlüssel Ks zu finden und

b) den verschlüsselten Nachrichtenblock C mit dem Wert 180630 bei einer internen Blocklänge von 2 Ziffern zu entschlüsseln.

Aufgabe 4:

Um einen Diffie-Hellman-Schlüsselaustausch durchzuführen einigen sich die beiden Kommunikationspartner A und B auf g = 31 und p = 7. A wählt als privaten Schlüssel x = 5; B legt für seinen privaten Schlüssel y = 7 fest.

a) Ermitteln Sie die öffentlichen Schlüssel von A und B, die jeweils mit der Gegenseite ausgetauscht werden.

b) Welche Berechnung hat A und B bei der Ermittlung des gewünschten gemeinsamen Schlüssels durchzuführen?

c) Wovon hängt die Sicherheit des DH-Verfahrens ab?

Aufgabe 5:

a) Welcher Zusammenhang besteht zwischen der Wahrung der Originalität von Dokumenten und der Wahrung ihrer Vertraulichkeit?

b) Warum lässt sich Verbindlichkeit nicht allein aus den drei klassischen Grundwerten der Informationssicherheit herleiten?

c) Warum benötigen informationstechnische Sicherheitspolitiken zu ihrer Durchsetzung Maßnahmen, die außerhalb der Kontrolle der IT-Sicherheit liegen?

Nennen Sie fünf Beispiele für solche Maßnahmen. Wobei können Sicherheitsmodelle eine Hilfestellung geben? Wann sind sie unabdingbar?

d) Warum wird bzgl. der in der Praxis verwendeten Verfahren zwischen der Authentisierung von Personen und der von informationstechnischen Instanzen unterschieden?

e) Welche positiven und negativen Eigenschaften haben passwortbasierte Authentisierungsverfahren?