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

Security AI
(Kryptographie und Datensicherheit)

Klausur SS 2007
LV 3151

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

Bitte ankreuzen: **o Diplom** **o Bachelor**

Sie erhalten eine geheftete Klausur. Bitte lösen Sie die Heftung **nicht**. Bitte tragen Sie zu Beginn der Bearbeitungszeit Ihren Namen, Ihren Vornamen 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.

Bearbeitungsdauer: 100 Minuten Erlaubte Hilfsmittel: Taschenrechner

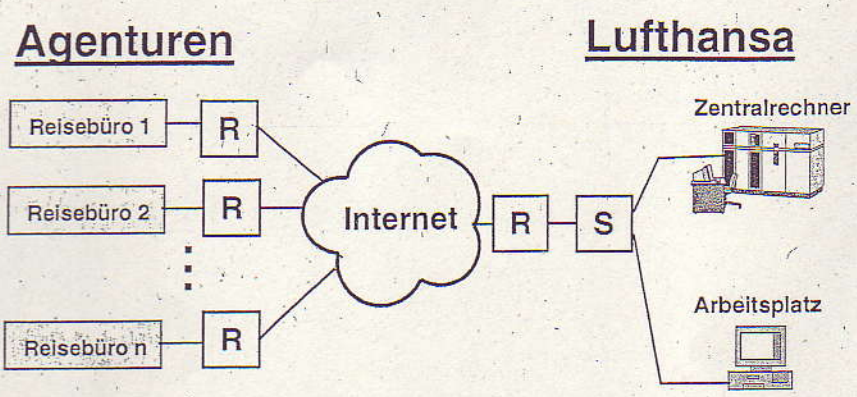
Punktevergabe:

Aufgabe	Soll-Punkte	Ist-Punkte
1	20	
2	10	
3	20	
4	20	
5	15	
6	15	
Gesamt	100	

Zum Bestehen der Klausur müssen mindestens **50 Punkte** erreicht werden!

Aufgabe 1 (Sicherheitsbewertung eines Buchungssystems – 20 P.)

Als eine typische Aufgabenstellung aus Bereich des Electronic Commerce wird das Flugreservierungssystem der Lufthansa betrachtet. Bei diesem Szenarium nehmen verschiedene Agenturen (Reisebüros, Lufthansaagenturen) im Auftrag von Kunden Flugreservierungen vor und wickeln den anfallenden Zahlungsverkehr ab. Die informationstechnische Infrastruktur besteht (vereinfacht gesehen) aus dem Zentralrechner der Lufthansa und den lokalen Systemen der Agenturen, die über ein öffentliches Netz mit dem Lufthansa-Rechner verbunden sind. Die nachstehende Abbildung zeigt für das Szenarium eine geeignete Kommunikationsinfrastruktur mit den daran angeschlossenen Endsystemen.



a) Identifizieren Sie mindestens drei schutzwürdige Objekte, die innerhalb des Flugreservierungssystems erzeugt, gespeichert, übertragen oder verarbeitet werden.

Reservierung, Kundeninformation, Flugbelegdaten

b) Bewerten Sie die aus ihrer Sicht aus den Grundbedrohungen ableitbaren Sicherheitsrisiken.

passiver Angriff abhören der Verbindung bei austausch mit dem Zentralrechner nicht möglich

c) Überlegen Sie sich für das Flugreservierungssystem mindestens fünf sinnvolle und charakteristische technische Sicherheitsanforderungen.

Verschlüsselung der Verbindung zwischen Büros + Zentralrechner

Aufgabe 2 (Zahlentheoretische Aussagen – 10 P.)

Ergänzen Sie die folgenden Sätze mit jeweils 1 bis 2 Wörter derart, dass hierdurch richtige Aussagen getroffen werden!

a) Sei p eine Primzahl. Dann ist die prime Restklassengruppe mod p ..... bezüglich der Ordnung p – 1.

b) Sei $A = g^a \bmod p$. Der Exponent a heißt ..... Logarithmus von A zur Basis g.

c) Die RSA-Entschlüsselung kann beschleunigt werden, wenn man den ..... Restsatz benutzt.

d) Um die Faktorisierung eines RSA-Moduls möglichst schwierig zu machen, werden seine Primfaktoren p und q ..... gleich groß gewählt.

e) Die Exponentiation in der primen Restklassengruppe $B = a^b \bmod n$ ist in ..... Zeit möglich.

Aufgabe 3 (DH-Schlüsselaustausch – 20 P.)

Um einen Diffie-Hellman-Schlüsselaustausch durchzuführen einigen sich die beiden Kommunikationspartner A und B auf g = 3 und p = 17. A wählt als privaten Schlüssel x = 7; B legt für seinen privaten Schlüssel y = 4 fest.

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

Lösung:

$\alpha = 3^7 \bmod 17$ $\quad\quad$ $\beta = 3^4 \bmod 17$

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

Lösung:

$K_A = K_B := K$

$K_A = \beta^a \bmod p$

$\alpha = g^a \bmod p \rightarrow$ **K = ...** $\quad\quad$ $K_B = \alpha^b \bmod p$

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

Antwort: weil verfahren asymmetrisch

verfügen beide partner nicht über ein schlüssel

d) Welcher bekannte Angriff besteht beim DH-Schlüsselaustauschprotokoll?

Antwort:

Man-in-the-middle

key stream reuse

Aufgabe 4 (RSA-Schlüsselerzeugung – 20 P.)

Als Public-Key-Verfahren stützt sich der RSA-Algorithmus auf einen öffentlichen Schlüssel (P_K, n) und einen privaten Schlüssel (S_K, n), wobei mit n der Modulus (öffentlich) bezeichnet wird. Dieser sei durch das Produkt zweier Primzahlen $n = p \cdot q$ mit $p = 23$ und $q = 59$ vorgegeben. Für die Erzeugung des öffentlichen Schlüssels stehen die folgenden ganzen Zahlen zur Auswahl:

$$(P_K, n) = (11, 1357) \text{ oder } (14, 1357) \text{ oder } (15, 1357)$$

a) Welcher der drei Schlüsselwerte kommt als öffentlicher RSA-Schlüssel in Betracht?

Antwort:

$$(P_K, n) =$$

$\phi(n) = (23-1)(59-1) =$

b) Begründen Sie Ihre Auswahl!

Lösung:

c) Berechnen Sie den zugehörigen privaten RSA-Schlüssel.

Lösung:

$S_k \cdot p_k \bmod \phi(n) = 1$

$S_k \cdot p_k = z \cdot \phi(n) + 1$

$S_k = \underbrace{z \cdot \phi(n) + 1}_{\text{ist}}$

Aufgabe 5 (Divisionsrest – 15 P.)

a) Zeigen Sie, dass für a, b ∈ **Z** (Menge der ganzen Zahlen) gilt:

$$(a \cdot b) \bmod n = ((a \bmod n) \cdot (b \bmod n)) \bmod n.$$

Lösung:

b) Berechnen Sie mit Hilfe des erweiterten Euklidischen Algorithmus die Lösung (x, y) der Gleichung $63 \cdot x + 36 \cdot y = 27$, sofern diese existiert. Bei der Lösung bitte vollständigen Rechengang angeben!

Lösung:

Aufgabe 6 (Kongruenzen – 15 P.)

a) Es sei $n = p \cdot q$ mit $p, q \in \mathbf{P}$ (Menge der Primzahlen). Zeigen Sie, dass aus $x \equiv a \pmod{p}$ und $x \equiv a \pmod{q}$ folgt: $x \equiv a \pmod{n}$.

Lösung:

b) Berechnen Sie mit Hilfe eines Taschenrechners die Zahl $z = 257^{887} \bmod 31$.

Lösung: