# Klausur Datensicherheit

| | | | |
|---|---|---|---|
| Semester: | AI5, Bachelor | **SS 09**, | 5.7.2009 |
| Bearbeitungszeit: | 60 Minuten | Hilfsmittel: | nicht prog. C |

**Auf jedem Blatt Name eintragen! — Punkteangaben ohne Gewähr!**

## Aufgabe 1 (5 Punkte)

**a)** Was ist das Kerkhoffs-Prinzip?

Die Sicherheit der Verschlüsselung darf nicht von der Geheimhaltung des Algorithmus/Implementierung abhängen.

**b)** Warum ist dieses so wichtig? Nennen Sie mindestens 3 Gründe.

- Ist der Algorithmus wirklich sicher?
- Sind Hintertüren eingebaut?
- Gibt es Implementierungsfehler?
- Tauschen eines Schlüssels leichter als Tausch der Verschlüsselung

## Aufgabe 2 (5 Punkte)

**a)** Wie funktioniert der CBC-Modus bei Blockchiffren?

```
C[0] = E[k](M[0])
C[n] = E[k](M[n] XOR M[n-1])

[] = Index

Also jeder Block wird mit dem Vorgängerblock verrechnet (XOR) und erst
dann verschlüsselt. Optional wird der erste Block mit einem
Initialisierungsverktor verknüpft.
```

**b)** Welchen Vorteil bietet er gegenüber dem ECB-Modus?

Manipulation an den Blöcken erschwert. Das Weglassen oder Hinzufügen von Blöcken bzw. die Änderung der Reihenfolge ist nicht ohne Weiteres möglich.

### Aufgabe 3 (3 Punkte)

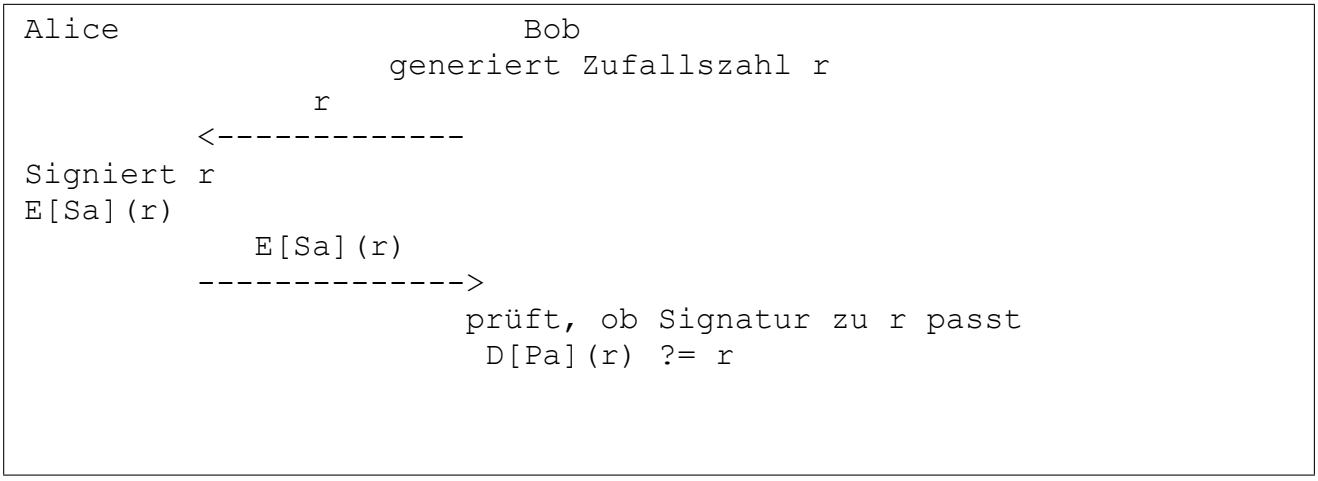
Wozu werden Einweg-Hashfunktionen in der modernen Kryptographie verwendet? Nennen Sie 3 Anwendungen.

- Server-seitige Passwortspeicherung (und Passwortvergleich)
- Digitale Signaturen (es werden nur Hash-Werte signiert)
- Pseudo-Zufallszahlengenerator
- Finger-Prints (von Schlüsseln)

### Aufgabe 4 (5 Punkte)

Alice will sich auf dem Server Bob mittels Digitaler Signatur authentifizieren.

**a)** Beschreiben oder skizzieren Sie den Ablauf.




**b)** Warum ist diese Art der Authentifikation besser als das klassische Passwortverfahren mit Einweg-Hash-Funktion?

Der Server muss das gehashte Passwort nicht auf dem Server speichern (Wörterbuchangriff). Es ist kein Replay-Angriff möglich durch Mitschnitt der Authentifizierung.

### Aufgabe 5 (4 Punkte)

Was ist die zentrale Aufgabe einer Public Key Infrastruktur? (mit Begründung)

Wichtigste Aufgabe ist die Zertifizierung von Public-Keys. Das Public-Key-Verfahren hängt von der Vertrauenswürdigkeit der öffentlichen Schlüssel ab. Durch Signieren der Schlüssel kann die Zugehörigkeit sichergestellt werden.

### Aufgabe 6 (7 Punkte)

Gegeben seien der öffentliche Schlüssel $e = 7$ und der Modul $n = 85$ für den RSA-Algorithmus. Knacken Sie diese Chiffre, indem Sie den zugehörigen geheimen Schlüssel bestimmen.

```
p * q = 85 => p = 5; q = 17
phi(n) = (5-1)*(16-1) = 64

ggT(64, 7):
64 = 9*7 + 1

Erweiterer Euklid:
 1 = 64 - 9*7
   = -9*7 mod 64
   = (-9 + 64)*7 mod 64
   = 55*7 mod 64
=> d = 55

Prüfung:
1. Mgl: 55*7 / 64 = 385 / 64 = 6,015625; 0,015625 * 64 = 1 => passt
2. Mgl:
  Das erwartete Ergebnis 1 auf die andere Seite bringen und erst dann
  durch 64 teilen, wenn kein Rest bleibt passt es:
  (55*7 - 1) / 64 = 384 / 64 = 1 = Ganzzahl, kein Rest
```