I. Verteilte Systeme

Aufgabe 1: 0-Adressmaschine

Der Ausdruck $R = a - \frac{b}{c^2}$ soll auf einer 0-Adressmaschine berechnet werden.

a) Schreiben sie den Ausdruck zunächst in Postfixnotation auf.

b) Schreiben sie die Befehlsfolge zum Berechnen des Ausdrucks auf, unter Verwendung der aus der Vorlesung bekannten Operatoren (`PUSH`, `POP`, `ADD`, `SUB`, `MUL`, `DIV`).

Operator	Operand	Stackinhalt
...	...	...

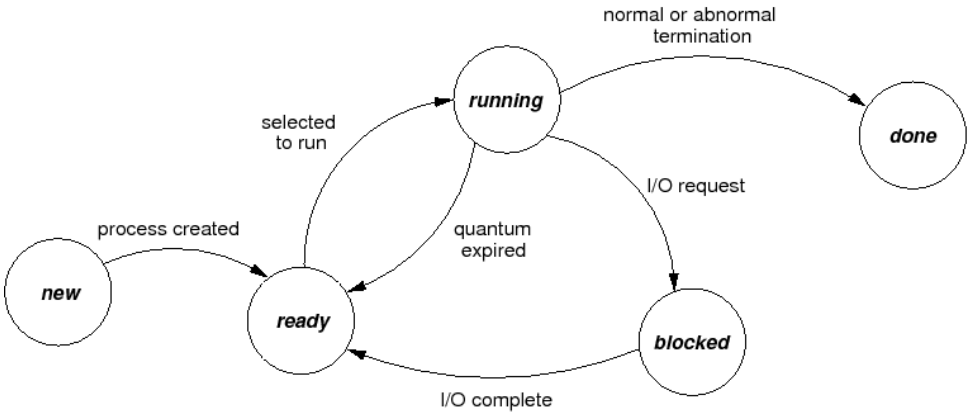
c) In Android wird keine 0-Adressmaschine für die JVM benutzt, sondern Dalvik, eine 2-Adressmaschine. Warum macht das auf einer mobilen Plattform Sinn?

d) Jede Anwendung wird in einer eigenen VM ausgeführt. Was bedeutet das für Sicherheit und Stabilität?

e) Früher wurde auf mobilen Geräten in der Regel eine Firmware eingesetzt anstatt eines richtigen Betriebssystems. Was könnte der Grund dafür sein?

Aufgabe 2: Prozessverwaltung

Folgender Graph ohne Kantenbeschriftung gegeben:



a) Beschriften sie die Kanten.

b) Nennen sie zwei Vorteile von Threads gegenüber Prozessen.

c) Wahr oder Falsch ankreuzen, falsche Kreuze geben keine Minuspunkte.

Wahr	Falsch	Frage
o	o	Ein Programm hat keinen Zustand
o	o	Jedes beliebige Programm kann durch multi-threading schneller gemacht werden
o	o	Ein multi-threading-fähiges Programm kann nur auf einer multi-core Maschine laufen
o	o	Noch 3 Fragen, irgendwas mit Prozessadressraum, Prozesszustand ...

d) Gegeben:

	P_1	P_1	P_1	P_1
Periode	21	7	10	8
Bedienzeit	2	1	2	2

Bestimmen sie, ob es mit einem optimalen Scheduler möglich ist, alle Prozesse innerhalb ihrer Periode abzuarbeiten. Prozesswechselzeit soll außer acht gelassen werden.

e) Das EDF Verfahren mit den gegebenen Prozessen illustrieren (bis $t = 25$).

f) Erklären sie das RMS Verfahren.

g) Erläutern sie einen Vor- sowie einen Nachteil großer Zeitscheiben Δt beim Round Robin Verfahren. Geben sie ein beispiel für ein Szenario, in dem große Zeitscheiben sinnvoll sind.

Aufgabe 3: Speicherverwaltung

a) Gegeben sei ein Hauptspeicher mit einem 15 Bit Adressen. Es wird Segmentierung mit Seiten benutzt, wobei eine Seite immer nur zu einem Segment gehört. Eine Seite ist 4 KiB groß.

Es soll jetzt ein Programm in drei Segmenten geladen werden: 16.384 B Programmcode, 5.120 B Daten und 11.264 B Stack.

Passt das gesamte Programm in den Hauptspeicher? Geben sie zur Begründung ihren Rechenweg an.

b) Wie ist es bei einer Seitengröße von 1024 B ?

c) In modernen multi-core Architekturen gibt es lokalen physischen Speicher, der von einer CPU schneller zugegriffen werden kann, aber generell von allen CPUs zugegriffen werden kann. Was muss das OS dann bei der Seitenverteilung beachten?

d) Folgende Seitentabelle sei gegeben:

Seitennr.	P/A-Bit	Ankunftszeit	letzter Zugriff	Anz. Zugriffe	referenziert	modifiziert
1	1					
2	0	hier				
3	1		irgendwelche			
4	1			Werte		
5	1					
6	0					
7	0					

Welche Seiten kommen für Verdrängung in Frage?

e) Welche Seite wird verdrängt mit

- LFU
- LRU
- RNU
- FIFO

Aufgabe 4: Synchronisation

```
public class Warenlager {
  private Semaphore sem;
  private Ware[] waren;

  ...

  public PreisBericht aktualisierePreise() {
    PreisBericht bericht = new PreisBericht();
    for (int i = 0; i < waren.length; i++) {
      Preis alterPreis = waren[i].getPreis();
      if (istVeraltet(alterPreis)) aktualisierePreis(waren[i]);
      Preis neuerPreis = waren[i].getPreis();
      if (alterPreis != neuerPreis) bericht.add(waren[i]);
    }
    return bericht;
  }
}
```

a) Mit welchem Wert sollte die Semaphore initialisiert werden?

b) Wo ist der kritische Bereich oder die kritischen Bereiche und zwischen welche Zeilen muss man die `sem.p()` und `sem.v()` Operationen einfügen?

c) Was könnte man noch grundsätzlich anders machen?

Aufgabe 5: Softwareagenten

Eine Fahrradverleihfirma möchte noch eine weitere Verleihstation eröffnen und möchte noch verschiedene potentielle Standorte evaluieren. Die hat auch Informationen über den öffentlichen Personennahverkehr und möchte eine Simulation mit Softwareagenten durchführen.

a) Nennen sie neben der Proaktivität noch drei weitere Eigenschaften von Softwareagenten und beschreiben sie, wieso sich Softwareagentn für die Simulation von Verkehrsteilnehmern eignen.

b) ...

c) Das Blackboardsystem für Multiagentensysteme erklären und wie es hier benutzt werden würde.

II. Sicherheit

Aufgabe 1:

a) Welche der drei Schutzziele können mit Kryptografie erreicht werden und welches nicht?

b) Nennen sie die vier Hauptpunkte eines Angreifermodells und erklären sie, was es beschreibt.

Aufgabe 2: RSA

[Analog zu Aufgabe 5: RSA aus GProt 2012]
Alice und Bob möchten ein Würfelspiel spielen und sich mit dem deterministischen RSA-Verfahren verschüsselt Würfelzahlen zusenden. Dazu haben sie vorher über einen sicheren Kanal ihre öffentlichen Schlüssel ausgetauscht.
Alice hat folgende Werte: $e_A = 3, p_A = 5, q_A = 11, d_A = 43$.
Bob hat folgende Werte: $e_B = ?, p_B = 17, q_B = 5, d_B = ?$.
Bob sendet Alice sein Würfelergebnis $c_B = 9$.

a) Zeigen sie, dass es Eve möglich ist, mit einem Chosen-Plaintext-Angriff und nur dem Wissen von c_B und den öffentlichen Schlüsseln von beiden das Ergebnis entschlüsseln kann.

b) Wie kann Bob sich dagegen schützen?

Aufgabe 3: Lückentext

Sinngemäß:
Ein (1)——— ist ein kleines Programm, dass sich in einem größeren Programm einnistet und (2)———- kann. Ein (3)——— ist ein Programm mit (4)——- und (5)——-. Ein (6)——— ist ähnlich zu (1), es kann auch (2), aber ist ein eigenständiges Programm.
Hier die vermuteten Lösungen:

1. Virus
2. Verbreiten / Vermehren
3. Trojanisches Pferd
4. offene Nutzenfunktion
5. verdeckte Schadfunktion
6. Wurm

Aufgabe 4: Timing-Attack

```
public boolean check(char[] x) {
  char[] pw = getStoredPassword();
  if (x.length != pw.length) return false;
  for (int i = 0; i < pw.length; i++) {
    if (x[i] != pw[i]) return false;
  }
  return true;
}
```

a) Nennen sie zwei Schwachstellen in der `check`-Methode, die einen Timing-Angriff möglich machen.

b) Mallory möchte einen Safe knacken. An dem Safe gibt man ein Passwort ein, dass dann auf einer zugehörigen Chipkarte mit der oben gezeigten Methode überprüft wird. Nach 100 Fehlversuchen zerstört sich die Chipkarte selbst.

Mallory hat hier schonmal 30 Passwörter ausprobiert und dabei die Zeit gestoppt:

Hier jetzt 30 Werte vorstellen. Unter anderem war dabei:

- 12345678 15316 ns; diverse andere mit 1531X
- scares 15364 ns
- schirm 15385 ns
- schutz 15384 ns

Was weiß Mallory jetzt über das Passwort und welche Passwörter sollte sie als nächstes testen? Kann sie das korrekte Passwort in den noch verbleibenden 70 Versuchen herausfinden?