Vorbemerkungen und Abgabe

Das SVS-Übungsblatt besteht aus Pflicht-Aufgaben und optionalen Aufgaben. Nur die Pflicht-Aufgaben müssen von Ihnen abgegeben werden. Wir erwarten, dass Sie diese eigenständig lösen. In den optionalen Aufgaben behandeln wir ausgewählte Detailaspekte, die Inhalte aus der Vorlesung erweitern bzw. vertiefen. Die optionalen Aufgaben müssen nicht abgegeben werden. Die Auseinandersetzung mit diesen Aufgaben ist jedoch u. U. zur Beantwortung der Pflicht-Aufgaben erforderlich, in jedem Fall aber eine gute Vorbereitung auf die Klausur. Nur die Pflicht-Aufgaben werden korrigiert und für den Erhalt des Übungsscheins herangezogen (50%-Regel). Der Inhalt aller Aufgaben ist klausurrelevant.

Der Besuch der Vorlesung ist für das Verständnis der Inhalte und die erfolgreiche Teilnahme an der Klausur essenziell. Die Termine finden Sie unter **https://www.inf.uni-hamburg.de/de/inst/ab/svs/courses/master/vis.html**

Die Abgabe erfolgt online unter **https://svs.informatik.uni-hamburg.de/submission/for/vis17-4**; bitte nicht per E-Mail abgeben! Abgaben müssen exakt eine PDF-Datei umfassen und können bis zum Ablauf der Frist mittels eines Zugriffscodes (VISxx-xxxx-xxxx-xxxx-xxxx), der beim 1. Hochladen angezeigt wird, beliebig oft aktualisiert werden. Eine spätere Abgabe ist nicht möglich. Wird kein Zugriffscode angezeigt wird, war das Hochladen wahrscheinlich nicht erfolgreich. Versuchen Sie es in diesem Fall erneut. Falls das System nicht erreichbar ist, können Sie zur Wahrung der Frist ihre Lösung notfalls per E-Mail an ezimmer@informatik. . . schicken. Die Bewertungen sind rechtzeitig vor den Übungen (spätestens am Tag der Übung morgens) ebenfalls online einsehbar. Bitte bringen Sie ggf. selbst einen Ausdruck Ihrer Lösung zum Übungstermin mit.

Fehlertoleranz

Aufgabe 1 (Optional): Einzelnes System (Ausfallwahrscheinlichkeit)

Ein System ist insgesamt 8 Stunden 45 Minuten pro Jahr unverfügbar. Wie hoch ist seine Ausfallwahrscheinlichkeit bezogen auf ein Jahr?

Aufgabe 2 (Optional): Gekoppelte Systeme

Ein System besteht aus einer Hardwarekomponente mit einer Verfügbarkeit von $P_{HW} = 99,99$ Prozent und einer Softwarekomponente mit $P_{SW} = 99,9$ Prozent. Wie hoch ist die Gesamtverfügbarkeit? Wie hoch ist die jährliche Ausfallzeit?

Aufgabe 3 (Pflicht, 2 P.): Serverfarm eines Webmail-Anbieters

Ein großer Webmail-Anbieter möchte damit werben, 365 Tage im Jahr verfügbar zu sein, d.h. die Ausfallzeit seines Dienstes muss pro Jahr einen Tag (24 Stunden) unterschreiten. Er verwendet zur Steigerung der Performance und Verfügbarkeit eine Serverfarm aus 150 gleichartigen Webservern,

jeweils mit einer Verfügbarkeit von 95 Prozent. Im Hintergrund arbeitet eine gedoppelte Datenbank, die zudem diversitär ausgelegt ist. Der eine Datenbankserver hat 95 Prozent Verfügbarkeit, der andere erreicht 90 Prozent. Die restliche Systemumgebung hat eine ideale Verfügbarkeit (100 Prozent). Bitte beurteilen Sie, ob das Werbeversprechen (höchstens 1 Tag Ausfall pro Jahr) erfüllt werden kann.

Aufgabe 4 (Optional): Zuverlässigkeit

Angenommen, eine Chipkarte verkraftet im Mittel etwa 100.000 Kontaktzüge, bevor sie unbrauchbar ist. Sie wird durchschnittlich zehnmal am Tag in ein Lesegerät gesteckt. Wie zuverlässig ist die Kontaktgabe nach 1, 5 und 10 Jahren? Gehen Sie von einer gleichverteilten Ausfallwahrscheinlichkeit aus.

Aufgabe 5 (Pflicht, 4 P.): Reparaturdauer bei RAID

Ein Dateiserver ist fünf Jahre in Betrieb gewesen und während dieser Zeit insgesamt nur 4 Stunden und 20 Minuten unverfügbar gewesen.

a) Wie hoch war seine Gesamtverfügbarkeit in Prozent? (Erforderliche Genauigkeit: 3 Nachkommastellen)

b) Der Dateiserver soll nun durch einen neuen mit vergleichbarer Verfügbarkeit und Betriebsdauer ersetzt werden. Zur Verbesserung der Performance erwägen Sie den Einsatz eines RAID-0-Systems (Striping, keine Redundanz) mit 4 Festplatten. Die MTBF der eingesetzten Festplatten betrage ca. 50.000 Stunden je Platte, die MTTR betrage 1 Stunde je Platte (inkl. Recovery). Die Verfügbarkeit der restlichen Komponenten sei ideal 100 Prozent. Ist die geforderte Verfügbarkeit mit RAID-0 noch erreichbar? Begründen Sie Ihre Antwort kurz.
Hinweis: Es existieren unterschiedliche Definitionen von MTBF. Für die Bearbeitung der Aufgabe wird die Definition aus der Vorlesung verlangt.

Aufgabe 6 (Optional): Storage Area Network (SAN) aus RAID-5-Systemen

Eine sehr moderne Behörde möchte ihr Archiv auf elektronische Datenhaltung umstellen. Es sollen zur Archivierung die bei einer Inventur „aufgetauchten“ 120 Gigabyte-Festplatten eingesetzt werden. Zusammen sollen diese ein Storage Area Network (SAN) bilden. Es sollen jeweils x Festplatten über RAID-5 zusammengeschaltet werden. Insgesamt y solcher RAID-5 bilden zusammen das (SAN). Das SAN soll insgesamt 30 Terabyte Speicher netto bereitstellen, d.h. zzgl. der Redundanz von 1 Festplatte pro RAID-5. Die Verfügbarkeit pro RAID-5 darf 99,9 Prozent nicht unterschreiten. Die MTTF einer Festplatte sei 40.000 Stunden. Die MTTR sei 2 Stunden pro Ausfall. Es werden nur gleichartige 120 Gigabyte-Platten verbaut.

a) Wieviele Platten dürfen maximal pro RAID eingesetzt werden?

b) Wieviele Platten müssen insgesamt im SAN verbaut werden?

c) Berechnen Sie die Gesamtverfügbarkeit des SAN in Prozent. Hinweis: Das Gesamtsystem gilt als „verfügbar“, wenn alle RAID verfügbar sind. Nehmen Sie dazu an, dass ein RAID bereits bei einer ausgefallenen Festplatte zur Reparatur außer Betrieb genommen wird.

Kryptographie

Aufgabe 7 (Pflicht 6 P.): Informationstheoretisch sichere Verschlüsselung

Das One-Time-Pad (Vernam-Chiffre) ist ein sehr einfaches, aber informationstheoretisch sicheres symmetrisches Verschlüsselungsverfahren: Die Klartextzeichen x_i werden einzeln XOR-verknüpft mit einer zufälligen Schlüsselfolge k_i gleicher Länge, die nur ein einziges Mal verwendet wird (Schlüsseltext $s_i = x_i \oplus k_i$ mit $i = 1, 2, ...$).

a) Was erfährt der Angreifer, der den Schlüsseltext abfängt, über den Klartext?

b) Warum darf die Schlüsselfolge nicht mehrmals verwendet werden? Überlegen Sie sich, was passieren würde, wenn der Angreifer zwei Schlüsseltexte s_1 und s_2 (oder gar noch weitere) abfangen würde, die unter dem gleichen Schlüssel $k = k_1 = k_2$ verschlüsselt wurden. Annahme: Es handelt sich um sinnvolle Klartexte.

c) Ihnen sind eine Reihe verschlüsselter deutscher Substantive in die Hände gefallen. Sie gehen davon aus, dass der Urheber fahrlässigerweise alle Wörter mit dem selben One-Time-Pad byteweise verschlüsselt hat. Versuchen Sie den Schlüssel zu ermitteln, indem Sie einen geeigneten Angriff implementieren. Wie lautet der Schlüssel? Hinweis: Passwort und Substantive sind ASCII-Codiert (Alphabet = A,B,C, ... ,Z). Die Schlüsseltexte (der Substantive) in Dezimalschreibweise lauten:

```
09 00 04 10
10 20 28 09
10 16 02 02
10 20 05 08
26 26 03 00
28 16 03 17
```

Jede Zeile entspricht einem Substantiv.