



Sicherheit: Fragen und Lösungsansätze

Übung 2

Übung 2 (Zweiter Termin)

- Hinweise
 - Gruppenübung
 - Besprechung der Abgaben
- Ziele:
 - Verschiedene Wissensblöcke in Prüfungen
 - Wissen für den Block 2
 - Aufgaben vom Typ: Anwenden

Hinweise zu Ihren Abgaben

- Stellen Sie die Lösung **präzise** und kurz dar
 - *Kurz* heißt nicht schludrig!
- Keine Email-Abgabe!
- Schreiben Sie nicht mehr Infos als nötig in die Lösungen
- Seien Sie eindeutig
- Fragen: Gerne
 - Bitte ins InPUD
- Jeder nur ein Kreuz.
- Wer seinen Zettel nicht zurückbekommen hat, sollte einen Termin mit mir machen :-)

Hinweise zu Ihren Abgaben

- ✓ Richtig (kleinere Probleme werden ignoriert)
- ~ Überwiegend Richtig
 - Ungenauigkeit
 - Unrichtigkeiten
 - Achten sie auf Unterstreichungen
- ¬ K „nicht knackig“
- NL nicht lesbar
- LB:
 - 10 ... 0 (lesbar bis unleserlich)
 - Schlechter als 5: Ich musste Raten! Gefahr von Punktverlust!

Wissensblöcke in Prüfungen

Übertragen auf andere Probleme

Über dem Strich

Anwenden und Durchführen

Unter dem Strich

Basis-Wissen: Grundbegriffe, Definitionen und Techniken

Anwenden

- Sie sollen Techniken, die Sie in der Vorlesung gelernt haben, auf Beispielen, die der Vorlesung gleichen anwenden können.
- Evtl. sind auch kleine Stolperfallen eingebaut.
 - Z.B. überflüssiger Arbeitsschritt
 - Ungewöhnlich erscheinendes Zwischenergebnis
 - Überflüssige Informationen

- Antworten Sie knackig.
- Nutzen Sie formale Schreibweisen.
- Machen Sie Ihre Zwischenschritte klar.
- Haupttyp der Aufgaben in der Klausur.
- Gliedern Sie die Aufgabe optisch.

Beispiel

- Aufgabe 2 aus HA2
 - Berechnungsmethoden wurden eingeführt (Vorlesung)
 - Ähnliches Verfahren war in der letzten Präsenzübung (Vergleich mit Randomzeichenfolge)

Aufgabe

- declaration of permissions and prohibitions
- control operations
- isolation, interception and mediation of messages
- proof of authenticity
- access decisions
- monitoring

HA1 A1

- Es gab zwei Typen von Antworten:
- Generische Antwort, die die Fragezeichen zusammen behandelt
- Spezielle Antwort, die auf jedes Fragezeichen eingeht.
 - Bzw. auf eine Teilmenge

- Achten Sie auf die Genauigkeit der Begriffe
- Stichpunkte sollten Subjekt und Verb haben
-

HA1 A2.0

- Wer die Aufgabe gelöst hat, hat sie ordentlich gelöst
- Einige haben die Aufgabeteile (0) „übersehen“

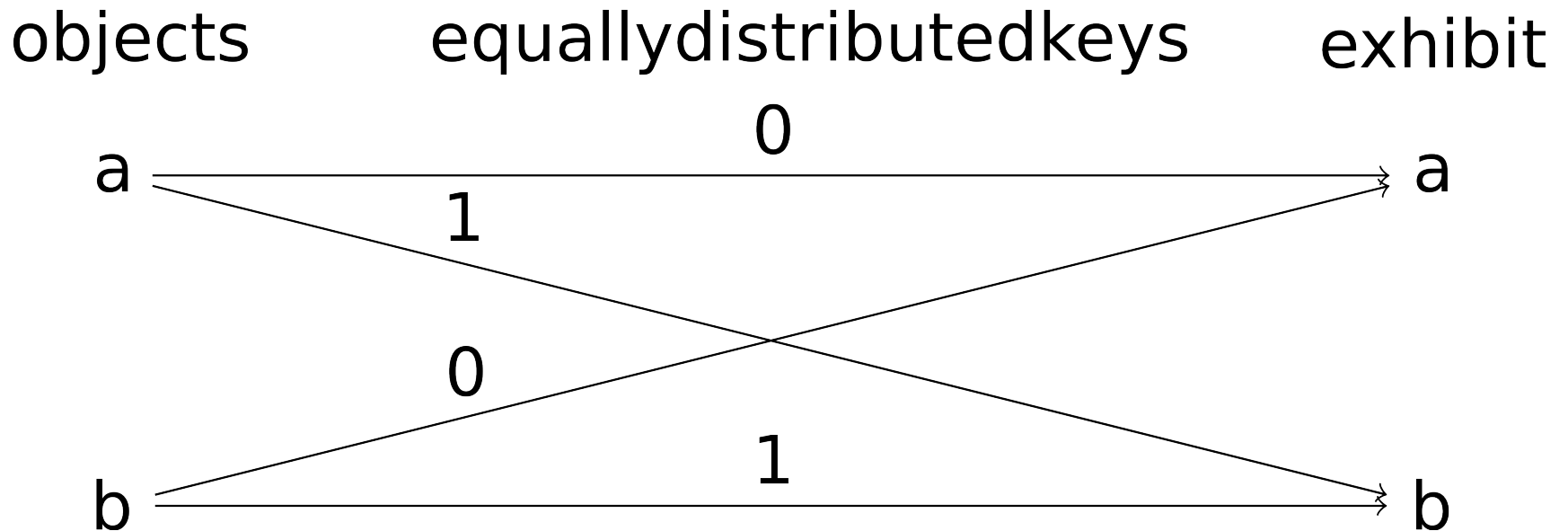
HA1 A2.1

- Wer die Aufgabe gelöst hat, hat sie ordentlich gelöst
- Einige haben die Aufgabeteile (0) „übersehen“

HA1 A2.2

- Berechnen der Wahrscheinlichkeiten!
 - $\text{Prob}[y=a] = .5 - .5 * q_2$
 - $\text{Prob}[y=b] = .5 * q_1 - .5 * q_2$
 - $\text{Prob}[y=c] = .5 - .5 * q_1$
- Reparatur: 3 Schlüssel

HA1 A2.3



HA1 A3

- Ja, viel Arbeit
- Siehe Korrektur

HA1 A4

- Häufigster Fehler: Teile wurden vergessen oder nicht bearbeitet:
 - Aufladen des Kontos
 - Fehlende Datenhaltung
- Aufgabe ist für eine strukturierte Antwort geeignet
 - Kein Fließtext!