

Anonym prüfen, besser bewerten

KI und Datenschutz im Praxiseinsatz

Prof. Dr. Dominik Herrmann – Universität Bamberg

Folien (ab heute Abend): dhgo.to/ki-ds-exam

E-Prüfungen: Hoffnung vs. Realität

- Effizienz: schnellere, skalierbare Korrektur durch digitale Werkzeuge
- Gleichbehandlung: Potenzial für standardisierte Bewertungen und Pseudonymisierung
- Aber: Umsetzung rechtlich und organisatorisch komplex

KI-Chancen: Assistenz, automatisches Feedback und neue Prüfungsformate

echte Tools
statt Ankreuztests

lesbare Antworten

keine PC-Pools nötig

sicher

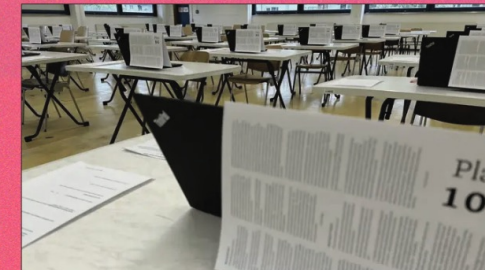
psi-exam
Digitale Klausuren an der Universität Bamberg



funktioniert komplett offline
Linux-System · Lenovo-Laptops
max. 320 Plätze · Kapellenstr. 13

verschlüsselt und signiert
Backup und Archiv

**Pilotierung in 10 Veranstaltungen
mit über 1000 Klausuren seit 2023**

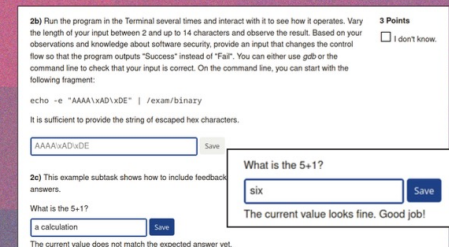


Kompetenzen prüfen mit Fachanwendungen
und Hilfsmitteln: z.B. Webseiten · PDFs
LaTeX · Datenbanken · RStudio · VS Code

Übersichtliche und flexible Korrektur:
Volltextsuche, Gruppieren und Sortieren

Digitale Einsicht und Remonstration

Geplant: Online-Korrektur und
Aufgabenerstellungstool



2b) Run the program in the Terminal several times and interact with it to see how it operates. Vary the length of your input between 2 and up to 14 characters and observe the result. Based on your observations and knowledge about software security, provide an input that changes the control flow so that the program outputs "Success" instead of "Fail". You can either use git or the command line to check that your input is correct. On the command line, you can start with the following fragment:

```
echo -e "AAAA\xAD\xDE" | ./exam/binary
```

It is sufficient to provide the string of escaped hex characters.

AAAA\xAD\xDE

Save

2c) This example subtask shows how to include feedback answers.

What is the 5+1?

a calculation

Save

The current value does not match the expected answer yet.

What is the 5+1?

six

Save

The current value looks fine. Good job!

Auf Wunsch Live-Feedback zu Antworten
während der Klausur (reduziert Stress)

HERAUSFORDERUNGEN:
varierende Technik-Kenntnisse
langsamere Bearbeitung · Tastaturlayout
Aufgabenerstellung aktuell nur in HTML

IDEE: INTERAKTIVE KLAUSUREN
Prüfende könnten Aufgaben während
der Prüfung aufgrund von Fragen oder
Antworten der Prüflinge *überarbeiten*

1 Datenschutz vs. KI-Mehrwert

Prüfer wollen z.B.:

KI zur Zeitersparnis (autom. Bewertung)
und Qualitätsverbesserung (Konsistenz)

Studenten wollen:

Ihre Daten nicht bei OpenAI

2 Anonymität vs. Kontrolle

Fairness: Pseudonyme/anonyme Korrektur

Rechtssicherheit: Täuschungsverhinderung
und Nachvollziehbarkeit

Vertrauen: Transparenz/Mächtigegleichgewicht

echte Tools
statt Ankreuztests

lesbare Antworten

keine PC-Pools nötig

sicher

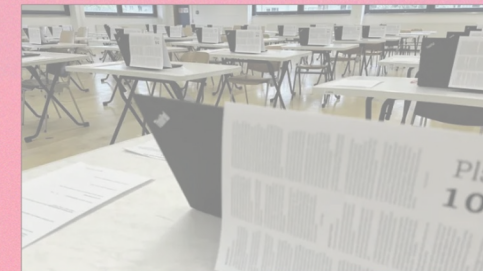
psi-exam
Digitale Klausuren an der Universität Bamberg



funktioniert komplett offline
Linux-System · Lenovo-Laptops
max. 320 Plätze · Kapellenstr. 13

verschlüsselt und signiert
Backup und Archiv

**Pilotierung in 10 Veranstaltungen
mit über 1000 Klausuren seit 2023**



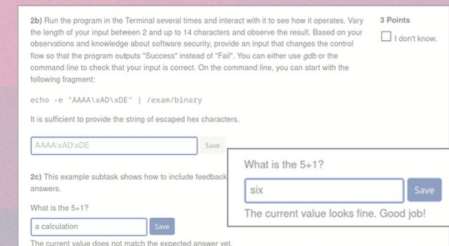
Kompetenzen prüfen mit Fachanwendungen
und Hilfsmitteln: z.B. Webseiten · PDFs
LaTeX · Datenbanken · RStudio · VS Code

Übersichtliche und flexible Korrektur:
Volltextsuche, Gruppieren und Sortieren

Digitale Einsicht und Remonstration

Geplant: Online-Korrektur und
Aufgabenerstellungstool

HERAUSFORDERUNGEN:
varierende Technik-Kenntnisse
langsamere Bearbeitung · Tastaturlayout
Aufgabenerstellung aktuell nur in HTML



2b) Run the program in the Terminal several times and interact with it to see how it operates. Vary the length of your input between 2 and up to 14 characters and observe the result. Based on your observations and knowledge about software security, provide an input that changes the control flow so that the program outputs "Success" instead of "Fail". You can either use `gdb` or the command line to check that your input is correct. On the command line, you can start with the following fragment:

```
echo -e "AAAA\xAD\xDE" | ./exam/binary
```

It is sufficient to provide the string of escaped hex characters.

AAAA\xAD\xDE

Save

2c) This example subtask shows how to include feedback answers.

What is the 5+1?

a calculation

Save

The current value does not match the expected answer yet.

What is the 5+1?

six

Save

The current value looks fine. Good job!

Auf Wunsch Live-Feedback zu Antworten
während der Klausur (reduziert Stress)

IDEE: INTERAKTIVE KLAUSUREN
Prüfende könnten Aufgaben während
der Prüfung aufgrund von Fragen oder
Antworten der Prüflinge *überarbeiten*

psi-exam im Überblick

- **Bearbeitung** im Browser an von der Uni präparierten Offline-Laptops; Personenbezug (noch) vorhanden: feste Sitzplätze / Ausweiskontrolle.
- **Korrektur** ebenfalls im Browser.
- Organisator (Technikteam) lädt Rohdaten auf Webserver; dort nur verschlüsselte Daten.
- Prüfer-Links können so erzeugt werden, dass nur Pseudonyme (Tiernamen) sichtbar sind — technisch erzwungen, nicht nur organisatorisch.

Overview

List of examinees

29 registered examinee(s)

Anonymized name ▾	Achieved Points ⬆	Possible Points ⬆	Grading Status ⬆
Brave Elk	👤 No-show (5.0)	–	✅ Done
Brave Giraffe	👤 No-show (5.0)	–	✅ Done
Clever Jaguar	✗ 8 (5.0)	–	✅ Done
Clever Nightingale	✓ 33 (3.7)	–	✅ Done
Curious Gazelle	👤 No-show (5.0)	–	✅ Done
Dazzling Okapi	👤 No-show (5.0)	–	✅ Done
Dazzling Oryx	✓ 43 (2.7)	–	✅ Done
Elegant Jaguar	👤 No-show (5.0)	–	✅ Done
Elegant Quetzal	✗ 11 (5.0)	–	✅ Done
Elegant Squirrel	✗ 9 (5.0)	–	✅ Done
Friendly Ibis	👤 No-show (5.0)	–	✅ Done
Gentle Seahorse	✓ 31 (4.0)	–	✅ Done

Korrekturablauf und Qualitätssicherung

- Aufgabenweise Korrektur.
- Studierende erhalten **vorab Einsicht**, wodurch Fehler früher entdeckt werden.
- Korrekturfehler dadurch unkompliziert auch in allen anderen Prüfungen behebbar.
- Entpseudonymisierung erst am Ende; Klarnamen nur zur Übermittlung ans Prüfungsamt.

Group grading

Grouping and filtering options

Frequency: most frequent first

Enter an expression to filter the displayed submissions.

Submission groups (11 groups of 13 submissions)

Partial private keys

► 1 P: correct

► Found
3x (23.1%)

key

► 0 P: incorrect

► Found
1x (7.7%)

partial private keys

► 1 P: correct

► Found
1x (7.7%)

private key

► 0 P: incorrect

► Found
1x (7.7%)

❖ Empty submission (none)

► 0 P: ✓

► Found
1x (7.7%)

1 Datenschutz vs. KI-Mehrwert

Prüfer wollen z.B.:

KI zur Zeitersparnis (autom. Bewertung)
und Qualitätsverbesserung (Konsistenz)

Studenten wollen:

Ihre Daten nicht bei OpenAI

2 Anonymität vs. Kontrolle

Fairness: Pseudonyme/anonyme Korrektur

Rechtssicherheit: Täuschungsverhinderung
und Nachvollziehbarkeit

Vertrauen: Transparenz/Mächtigegleichgewicht

KI als Korrekturdialogpartner

- In schwierigen, mehrdeutigen Fällen: Dialog mit einem Sprachmodell (Vorlesungsfolien, Transkripte, Aufgabenkontext als Input).
- Studentische Antworten vor Übermittlung an Cloud-Anbieter paraphrasiert.
- Sehr zeitaufwändig, aber lohnenswert.

KI zur Aufgabenerstellung

- Größerer Hebel: Aufgaben vor der Prüfung auf Missverständnisse und implizite Annahmen prüfen lassen.
- LLMs finden oft blinde Flecken;
- Gefahr: endlose Optimierungsschleifen mit vielen Varianten
- Effizienzerwartungen nicht eingelöst: vollautomatische Generierung liefert oberflächliche Fragestellungen — nützlich als Inspirationsquelle, nicht als Ersatz.

Verlockend: Automatische Bewertung

- Cloud-Modelle: gute Bewertungen, aber rechtlich problematisch (DSGVO, EU-AI-Act).
- Lokale Modelle entweder (noch) zu untermverlässig oder (noch) zu teuer.
- Unabhängig davon aus psychologischen Gründen didaktisch problematisch: plausible, Vorschläge verleiten zur unkritischen Übernahme.

Weitere Überlegungen

Predictive Learning Analytics: Forschung deutet darauf hin, dass Feedback-Interventionen Motivation erhöhen können – aber rechtliche Fragen offen.

Zwischenfazit: KI ist ein nützliches Werkzeug für eine weitere Qualitätsverbesserung, weniger zur Beschleunigung der Korrektur.

1 Datenschutz vs. KI-Mehrwert

Prüfer wollen z.B.:

KI zur Zeitersparnis (autom. Bewertung)
und Qualitätsverbesserung (Konsistenz)

Studenten wollen:

Ihre Daten nicht bei OpenAI

2 Anonymität vs. Kontrolle

Fairness: Pseudonyme/anonyme Korrektur

Rechtssicherheit: Täuschungsverhinderung
und Nachvollziehbarkeit

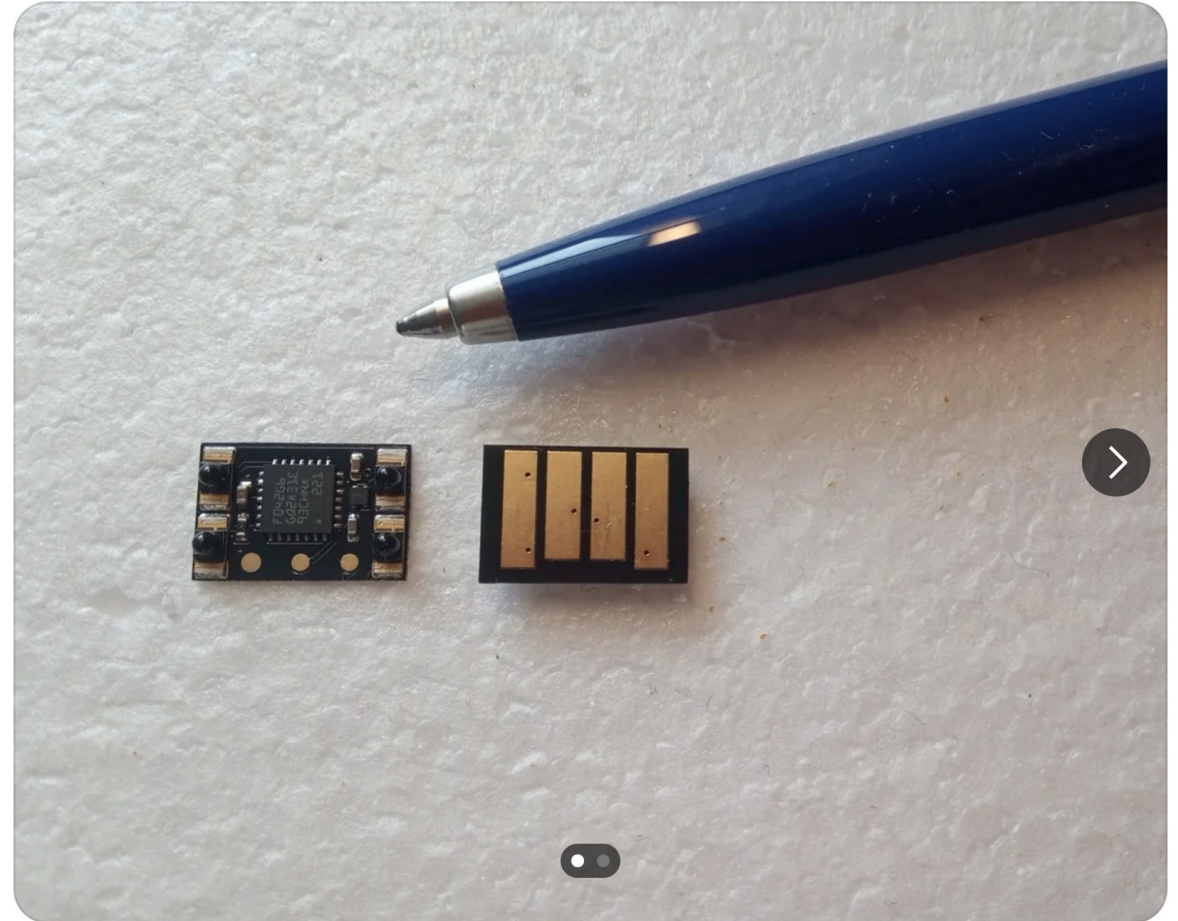
Vertrauen: Transparenz/Mächtigegleichgewicht

Anforderungen & Angriffsvektoren

- E-Prüfungen müssen vor Gericht standhalten: Täuschungen verhindern und im Streitfall beweisbar dokumentieren.
- Kreative Angriffsformen: USB-Rubber-Ducky (Tastatur-Emulation), nachträgliche Reklamationen zu technischen Problemen, Behauptungen über andere auf dem Bildschirm gezeigte Aufgaben.

←  r/hacking • 8 mo. ago
SisterSeagull

I made the world's smallest USB rubber ducky



The guys at [r/embedded](#) seemed to enjoy this so I thought I'd post it here as well ;)

Basically it's a tiny single-PCB USB rubber ducky that slots into a USB port and injects keystrokes. Once inserted, it disappears completely inside the port and is almost invisible to the untrained eye. It comprises a USB enabled STM32 microcontroller and four phototransistors, which both hold the PCB in place and allow remote (IR) activation and deactivation.

Beweissicherung – verhältnismäßig?

- Nur Bildschirmaufzeichnungen (Screenshots alle paar Sekunden), kein klassisches Proctoring.
- Transparenz und Zweckbindung: Studierende werden gem. Art. 13 DSGVO informiert; Zugriff nur bei konkreten Streitfällen.
- Prüfer sieht keine Screenshots; nach Widerspruchsfrist gelöscht
- Erwartung: Die bloße Existenz der Aufzeichnung wirkt präventiv.

Didaktischer Mehrwert (2. Zweck?)

- Sekundärer Nutzen: Auswertung von Navigations- und Zeitmustern: *Welche Aufgaben werden übersprungen? Wo bleibt man hängen? (wertvoll für Aufgabenoptimierung)*
- Rechtsgrundlage unklar: Öffentliches Interesse an besserer Lehre versus Erforderlichkeit.
- Einwilligung als Basis?

1 Datenschutz vs. KI-Mehrwert

Prüfer wollen z.B.:

KI zur Zeitersparnis (autom. Bewertung)
und Qualitätsverbesserung (Konsistenz)

Studenten wollen:

Ihre Daten nicht bei OpenAI

2 Anonymität vs. Kontrolle

Fairness: Pseudonyme/anonyme Korrektur

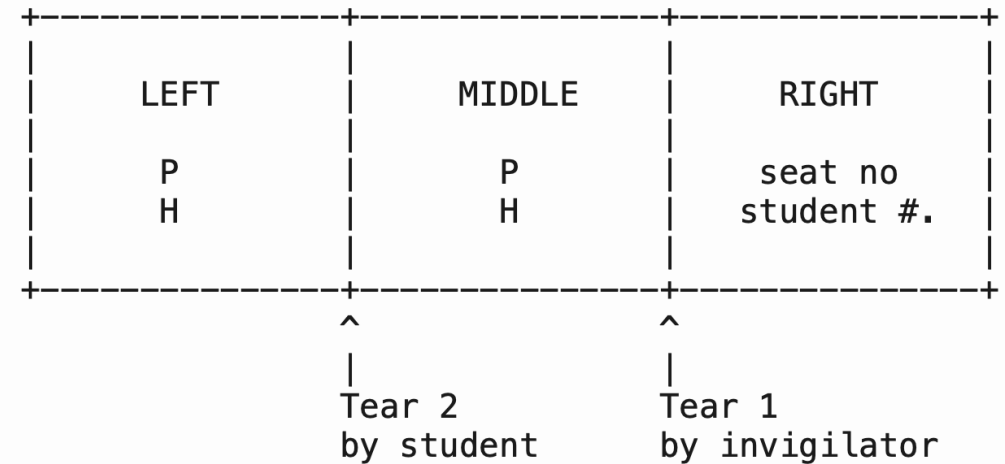
Rechtssicherheit: Täuschungsverhinderung
und Nachvollziehbarkeit

Vertrauen: Transparenz/Mächtigegleichgewicht

TEARS: Idee und Ablauf

- Papierticket mit zwei Sollbruchstellen; Risskanten: unfälschbares Zuordnungsmerkmal.
- Rechte Teile (Platznummer) werden vor der Prüfung eingesammelt
- Prüfling notiert Zufalls-Pseudonym und Prüfsumme auf mittlerem und linkem Teil
- linker Teil nach Prüfung in Urne, mittlerer Teil behält Student.

- stores all exam data.
- There is no network connection for the laptops during the exam. The subsequently send the “pseudonym + answers” (“**pseudonymized script**”) to the central invigilator’s laptop via a dedicated offline WiFi after exam completion.
- **Paper artifact:** Every student receives a three-segment **ticket** pre-perforated into Left | Middle | Right parts.
- The two pre-perforated edges are 1 cm straight cuts into the ticket’s paper to help in tearing the ticket later. Later, an irregular “zig-zag” tear **edge** is made so that the ticket parts are hand-torn during the exam.



1 • Goals

- **G-1: Anonymity while marking** – a **marker** (= examiner) who sees the pseudonymized script must still be unable to link it to a person even if they share all their notes.
- **G-2: Post-exam verifiable return** – when a student comes to claim their work, the examiner must be sure it is that student’s work, and the student can retrieve their graded answers.
- **G-3: No special hardware / no trusted third party** – everything runs on standard paper with offline laptops. Laptops don’t do any calculations that can

Analyse von TEARS

- Trennung: Aufsicht kennt Namen, Prüfer kennt nur Pseudonyme, Verbindung kann ausschließlich vom Prüfling hergestellt werden.
- Kollusionsresistenz: Selbst kooperierende Beteiligte können die Zuordnung nicht rekonstruieren ohne den mittleren Teil.
- Integrität: Unregelmäßige Risskanten sind praktisch kaum zu fälschen.

Die Kosten der Anonymität

- Verlust des mittleren Teils → irreversibler Identitätsverlust; kluge Backup-Verfahren nötig.
- Logistik und Supportaufwand (Verteilung, Urnen, Verlustfälle, Beweisführung bei Schadensfällen).
- Anreizeffekte: Studierende könnten Verluste strategisch nutzen; Verfahren benötigt klare Regelungen.

Schlussfolgerungen und Ausblick

Datenschutz ist gestaltbar.

Pseudonymität, Datensparsamkeit und strikte Schlüsseltrennung sind praktikable Bausteine, aber sie brauchen klare Prozesse.

KI ist Hilfswerkzeug, kein Ersatz.

Stärken: Qualitätssicherung, Aufgabenprüfung, Reflexion.

Schwächen: Datenschutz- und Reliabilitätsrisiken bei automatischer Bewertung

Anonymität versus Nachvollziehbarkeit

bleibt ein Trade-off. Technische Konzepte (Screenshots, TEARS) verschieben die Balance, lösen den Zielkonflikt aber nicht vollständig

Operative und rechtliche Rahmenbedingungen entscheiden.

Akzeptanz durch Prüfungsämter, gerichtsfeste Dokumentation und transparente Informationspflichten sind Voraussetzung für breiten Einsatz

Anonym prüfen, besser bewerten

KI und Datenschutz im Praxiseinsatz

Prof. Dr. Dominik Herrmann – Universität Bamberg – <https://herdom.net/>

LinkedIn – BlueSky, Mastodon: @herdom

Folien (ab heute Abend): dhgo.to/ki-ds-exam