Foundations of Cryptography (in English) (Masterstudiengang Informatik)

Der Kurs *Foundations of Cryptography* von Prof. Dr. Johannes Blömer setzt auf asynchrone Lehre, bietet aber mittels eines gesonderten Forums eine kursübergreifende Kommunikationsplattform. Das Kursmaterial besteht aus wöchentlichen Tutorials über YouTube, einem Skript und dem eben genannten Forum auf einer gesonderten Website, in dem die Studierenden sich austauschen und Fragen stellen können, die von anderen Studierenden oder den Lehrenden beantwortet werden. Das gesamte Material wird zeitig veröffentlicht. Maßgeblich unterstützt wird dieses Projekt durch Jan Bobolz und Fabian Eidens, die in ihrer Funktion als Mitarbeiter von Herrn Blömer u.a. die Videotutorials und Aufgaben erstellen und betreuen. Folgende Aspekte wurden von Studierenden hervorgehoben:

- Videotutorials mit Tutoren (über Youtube oder VimP abrufbar)
- Externes Forum und gute interne Kommunikation
- Die Mischung aus kurzen und längeren Aufgaben
- Übersichtliche Struktur der Kursseite
- Abschlussverfolgung zur Orientierung, was bereits erledigt wurde
- Einleitende Texte zu jedem Block
- Englische Sprache

Insgesamt haben die Studierenden hervorgehoben, dass dieser Kurs ihnen das Lernen des Stoffes wesentlich erleichtert. Darüber hinaus ist es Herrn Blömer gelungen trotz asynchroner Arbeitsweise ein gewisses Maß an „Präsenz-Feeling“ zu erzeugen. Daher ist dieser Kurs ein besonderes Beispiel dafür, wie sich asynchrone Lehre gut umsetzen lässt.

VIDEOPORTAL DER UNI PADERBORN

Suche etwas ... | Hochladen | Sprache | Login

Home | Medien | Channels | Alben | Gruppen | Livestreams

Channels

- Hochschulsport
- Chemische Grundlagen – Sachunterricht
- Cooperative Mobile Systems
- Technische Mechanik 2 - SS20
- Stochastik für Ingenieure SS20

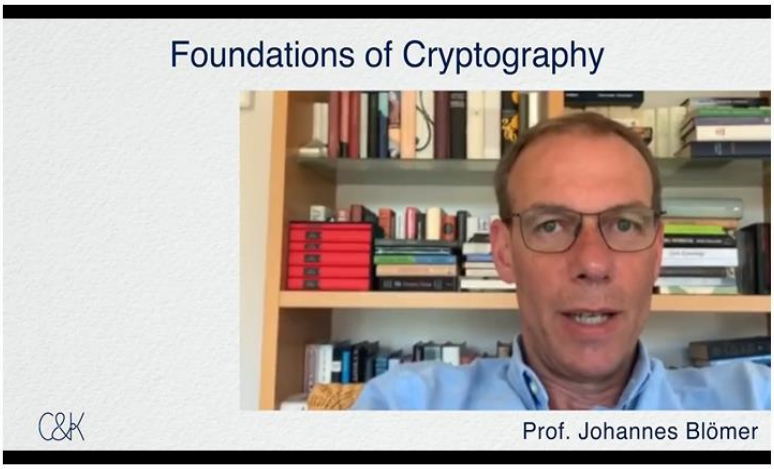
Alle Channels anzeigen

Livestreams

- UPB

Medien > FoC - Welcome and Introduction

FoC - Welcome and Introduction



☆☆☆☆☆ 2 0 0 0 | Teilen

Empfohlen


PANDA Tutorial Aufgabenabg...


PANDA Tutorial Datei Wieder...


Arbeitsrecht II Ausschnitt aus ...

L.079.05801 Foundations of Cryptography (in English)

Dashboard / My courses / SS20 / L.079.05801 Foundations of Cryptography (in English)

Turn editing on

General

Your progress

- Announcements
- Discussion forum
- Literature
- Lecture notes

Modified 13/07/20, 16:20

The canonical content of this course. Continually updated.

Lecture slides last updated 12/07/2020

- Lecture Slides
  - 00_Introduction.pdf
  - 01_Perfect_Secrecy.pdf
  - 02_IE_PRG.pdf
  - 03_CPA_PRF.pdf

Upcoming events

There are no upcoming events
Go to calendar...

FoC Forum - Latest topics

ECB/CTR mode for eavesdropping secure schemes?

9.3 for non-one time signatures?

Tree-based signature scheme

Proof of Theorem 10.14?

Week 13: That's it.

July 13 - July 20

Thank you for participating in the course. If you have any questions, the forums are open.

To help you prepare for the exam, Prof. Blömer has added a list of examples for typical exam questions to the lecture notes.

13 Reading material

Week 1: Perfect secrecy

April 20-27

We're starting this course with the question *how can we ensure confidentiality of data?* For example, you may want to transmit data over an insecure channel like the internet such that nobody but the intended recipient is able to read it. We'll start with the easiest security notion of confidentiality, which, in a way, also happens to be the strongest: Perfect secrecy.

This week, our goal is to learn and understand:

- What an encryption scheme is (in the sense of a set of algorithms as in Definition 1.1) and how to use it.
- The definition of perfect secrecy (Definition 1.2).
- How the *one time pad* works and why it is perfectly secret.
- The inherent drawback of perfect secrecy: Shannon's Theorem (Theorem 1.6).
- The alternative characterization of perfect secrecy through a game-based definition (Theorem 1.7).

01 Reading material

01 Tutorial

01 Exercises (Type 1, mandatory)

01 Exercises (attempt for latecomers)

Restricted Not available unless:

- You belong to **Latecomers**
- The activity **01 Exercises (Type 1, mandatory)** is incomplete

Sprache in den sozialen Medien (Germanistik und vergleichende Literaturwissenschaften)

Der Kurs *Sprache in den sozialen Medien* von Dr. Anna-Katharina Kurpiers ist ein gutes Beispiel dafür, wie man auf einfache Art und Weise viel aus PANDA als Lernplattform herausholen kann. Der oberflächlich schlichte Kurs, der fast schon leer wirkt, zeigt bei genauer Betrachtung, dass ein gut durchdachtes Konzept dahinter steckt: Neben Texten und Links zu Videos stellt Frau Kurpiers jede Woche ein „Skript“ ein, in dem die Arbeits- und Lernaufträge für ihre Studierenden genau beschrieben sind. Dieses Vorgehen führt zu einem weitestgehend asynchronen Arbeitsverhalten, was bis einschließlich eines Abschlusstests für die Qualifizierte Teilnahme (dieser hat ein Zeitfenster von einer Woche) fortgeführt wird. Besonders hervorgehoben wurden:

- Das persönliche Vorstellungsvideo
- Die Themenstruktur des Kurses
- Simple Gesamtstruktur des Kurse ohne viel „Schnickschnack“
- Die klar formulierten Aufgaben und Erwartungen
- Die offene Kommunikation im Kurs
- Der gute Einsatz von Frau Kurpiers Hilfskraft

Insgesamt zeigt dieser Kurs, wie ein gut durchdachtes Konzept simpel und für die Teilnehmer*innen leicht nachvollziehbar umgesetzt werden kann. Auch die durchgängig asynchrone Arbeitsweise ist besonders gut ausgeprägt und zeugt von viel gegenseitigem Vertrauen zwischen Frau Kurpiers und ihren Studierenden.

Vorstellungsvideo Dr. Anna Kurpiers

L.067.31222 Sprache in den sozialen Medien A

Bearbeiten einschalten

Forum: Fragen und Diskussionen zu "Sprache in den sozialen Medien"
1 ungelesener Beitrag

Hier können Sie Fragen zum Seminar stellen, mit weiteren Seminarteilnehmern diskutieren, etc.

Das Forum wird moderiert von meiner Hilfskraft Hannah Nolte. Sie wird Ihre Fragen soweit wie möglich beantworten.

Chat für Fragen

Einführung und Organisatorisches

Sie finden unter den zu bearbeitenden Themenblöcken jeweils ein Skript mit Anweisungen, die Literatur sowie ggf. weiteres Material.

Vorstellungsvideo Dr. Anna Kurpiers

Infomail PAUL/Anforderungen aqT und PL

(Soziale) Medien

- Marx & Weidacher (2014) Kap. 2
- Skript
- ergänzende Folien zu Gemeinschaften

Plattformen, Kommunikationsformen, Textsorten

- Klemm (2017)
- Skript
- Dürscheid (2005)
- Günthner (1995)
- Seiler (2016)

Texte und Gespräche

- Dürscheid (2016)
- Skript
- Video: Texte und Gespräche

Konquista und Mission - Katholische Kultur(en) im frühneuzeitlichen Lateinamerika (katholische Theologie)

Der Kurs *Konquista und Mission - Katholische Kultur(en) im frühneuzeitlichen Lateinamerika* von Dr. Tilman Moritz (katholische Theologie, Kirchen- und Religionsgeschichte) verfolgt einen vollkommen anderen Ansatz, als es für gewöhnlich der Fall ist: PANDA wird hier nicht als Sammelseite verschiedener Tools genutzt, sondern mehr wie ein Buch gedacht. Herr Moritz schreibt fortwährend die Arbeitsaufträge direkt auf der Kursseite. Lediglich längere oder detailliertere Aufgaben schreibt er in ein PANDA Buch oder auf eine Textseite. Diese besondere Art der Kurserstellung ist auf Studierende aus den ersten Semestern zugeschnitten. Die Studierenden hatten ihrerseits ebenfalls Einfluss darauf, wie sich der Kurs schrittweise aufbaut: In jeder Aufgabe und über Zwischenfeedbacks konnten die Studierenden Verbesserungsvorschlänge anbringen. Einige dieser Vorschläge kamen auch im persönlich Austausch zwischen Dozent und Studierenden. Allerdings wurde darauf geachtet, dass der Kurs insgesamt einem wiedererkennbaren Schema entspricht.

Durch Hervorheben bzw. Ausgrauen bestimmter Bereiche fällt die Orientierung auf der Seite nicht schwer. Diese einmalige Kursorganisation mag nicht für jedes Lehrszenario geeignet sein, jedoch funktioniert es in Herrn Moritz‘ Seminarkontext gut und kann vielleicht als Gedankenanstoß für andere Kurse gesehen werden.

Begleitaufgabe 20. April bis 11. Mai

Lesen Sie bitte aus Huber, *Die Konquistadoren* (2019) die *Einleitung* (S. 7–11) sowie Abschnitt 5 *Das Konquistadorenbild in der Historiografie* (S. 99–118).

Tragen Sie ins **Glossar** ein,

- welche Begriffe, Namen usw. Ihnen *unbekannt* sind (Überschrift eingeben, ins Feld "Definition" dann "???" eintragen),
- welche Ihnen bisher unbekannten Begriffe, Namen usw. der Text Ihnen *erklärt* hat (Seitenzahlen als Nachweis nicht vergessen!).

Woche 1, 20.–26. April

Zuerst, etwas ansehen:

"A Vision of Students Today", Kansas State University 2007 (LINK zum Video).

Dann, etwas tun:

1) Notieren Sie möglichst spontan (!) *jeweils einen Satz oder ein Stichwort* zu folgenden Fragen:

- Wie lernen Sie?
- Was glauben Sie, noch lernen zu müssen?
- Welche beruflichen Ziele haben Sie?
- Worauf hoffen, wovon träumen Sie?
- Wie wird Ihr Leben im Jahr 2040 aussehen?
- Welche Veränderung wäre bis dahin die wichtigste für Sie?

2) *Stellen Sie sich uns im Teamforum kurz vor*. Die Form ist ganz Ihnen überlassen: Ganz klassisch ein Biogramm in ein bis drei Sätzen. Eine Stichwortsammlung zu Themen, die Ihnen wichtig sind. Eine Sechs-Wort-Geschichte (hier ein paar englischsprachige Beispiele). Ein Bild von etwas, das Sie repräsentiert.
Lassen Sie sich gerne von den oben abgefragten Aspekten inspirieren.

3) Falls noch nicht geschehen, *vervollständigen Sie Ihr PANDA-Profil mit einem Profilbild* – es muss nicht notwendigerweise Sie selbst zeigen.

Woche 13, 13.–17. Juli

Zuletzt, etwas tun:

Definieren Sie gemeinsam den Begriff "Lateinamerika". Also, was meint das geografisch, politisch, kulturell, religiös, historisch wie heute? und warum heißt das eigentlich so?
Versuchen Sie, so viele Verweise innerhalb des Glossars wie Bezüge auf Seminarinhalte wie möglich einzufügen.

Wir sammeln Ihre Definitionen **bis Freitag, 17. Juli,** im zugehörigen Forumsthread. Wichtiger als lauter komplett eigenständige Definitionen ist mir, dass Sie noch einmal miteinander interagieren. Also, lesen Sie die Thesen und Kommentare der anderen, antworten Sie darauf und reagieren Sie selbst auf Ergänzungen, Nachfragen usw.

Und ganz zum Schluss (ehrlich!):

Nehmen Sie an der Gesamtevaluation des Seminars teil: LINK.
Über Feedback, Kritik und, ja, vielleicht auch Lob freue ich mich sehr und hoffe auf rege Beteiligung!

Etherpad "Kulturtransfer"

Eingeschränkt Nicht verfügbar, es sei denn: Sie gehören zu **Kulturtransfer** (ansonsten verborgen)

Hier erarbeiten Sie gemeinsam den Glossareintrag.

Zuerst, etwas lesen:

Ulrike Lindner: Neuere Kolonialgeschichte und Postcolonial Studies. In: Docupedia-Zeitgeschichte, 15.4.2011, URL: http://docupedia.de/zg/lindner_neuere_kolonialgeschichte_v1_de_2011 [letzter Zugriff: 21.04.20].

Dann, etwas tun:

In dieser Woche werden Sie in einer von zwei Gruppen einen *Glossareintrag* verfassen. Für Ihre Gruppe lautet die Überschrift: "Postcolonial Studies". Der besseren Übersicht halber hier die Kurzfassung der Aufgabenstellung mit grobem Zeitplan (die ausführliche Variante finden Sie weiter unten):

1. Sammeln Sie Leseeindrücke (spätestens bis Mittwoch, 13. Mai).
2. Tragen Sie im *Etherpad* Aspekte zusammen (spätestens bis Mittwoch, 13. Mai).
3. Verständigen Sie sich mit den anderen Gruppenmitgliedern, was in den Glossareintrag aufgenommen werden soll (ab Donnerstag, 14. Mai).
4. Erarbeiten Sie zusammen den Glossareintrag (ab Donnerstag, 14. Mai; "Intensivsitzung" am Montag, 18. Mai, Fertigstellung bis 18 Uhr).

Wichtig! Den genauen Ablauf bestimmen Sie selbst, indem Sie sich innerhalb Ihrer Gruppe absprechen. Sie können dafür das Etherpad oder auch andere Möglichkeiten nutzen. Verbindlich ist allein der Abgabetermin.

Zu Ihrer Gruppe gehören: Julie Adamik, Lara Leila Afsar, Silke Böddeker, Ruth Regina Lahme, Claire Tilson und Lars Wessels.

Eingeschränkt Nicht verfügbar, es sei denn: Sie gehören zu **Postcolonial Studies** (ansonsten verborgen)

Detaillierte Aufgabenstellung (Gruppe "Postcolonial Studies")

Eingeschränkt Nicht verfügbar, es sei denn: Sie gehören zu **Postcolonial Studies** (ansonsten verborgen)

Hier finden Sie die (noch) ausführlichere Version.

Etherpad "Postcolonial Studies"

Eingeschränkt Nicht verfügbar, es sei denn: Sie gehören zu **Postcolonial Studies** (ansonsten verborgen)

Hier erarbeiten Sie gemeinsam den Glossareintrag.

Einführung in die Kunstpädagogik (Kunstdidaktik)

Der Kurs *Einführung in die Kunstpädagogik* von Frau Prof. Dr. Rebekka Schmidt ist ein exzellentes Beispiel dafür, wie Studierende auf unterschiedlichen Wegen über PANDA betreut werden können. Frau Schmidt bietet ihren Studierenden an, entweder an synchronen Online-Seminaren teilzunehmen oder komplett asynchron im Kurs zu arbeiten. Der damit verbundene Aufwand, mehrere Seminarpläne zu erstellen, wird von ihr sehr gut gelöst. Dies merkten auch ihre Studierenden bei uns an. Weitere Punkte, die hervorgehoben wurden, sind:

- Ansprechende Webinare (synchrone Variante)
- Die Möglichkeit zu persönlichen Einzelgesprächen oder der Nutzung eines Frageforums
- Gruppenarbeiten in Webinaren und/oder auf PANDA
- Vielfältige, aber nicht zu überladene Methodenwahl bei den Aufgaben
- Nutzung weiterer Tools zur Ergänzung wie *Etherpads* oder *Mural*
- Besonderheiten des PANDA-Kurses
    - Ansprechende Bilder
    - Erkennbares, persönliches Design der Kunstdidaktik
    - Abschlussverfolgung
    - Gute Aufteilung des Kurses zur besseren Orientierung

Die Grundlage der Sitzungen bildeten wöchentlich abzugebende Vorbereitungen, deren Inhalt dann vertieft wurde. Trotz der Ausnahmesituation, die viele Störfaktoren mit sich bringt, haben die Studierenden die Motivation bei ihr im Seminar nicht verloren.

L.091.40100 Einführung in die Kunstpädagogik

Bearbeiten einschalten

Fortschritte

Um Zugriff auf alle Inhalte des PANDA-Kurses zu haben, müssen Sie den ASB (Allgemeine Seminarbedingungen) zustimmen.

Bestätigung ASB

Teilnahme am Seminar - Synchron oder Asynchron?

Erste Schritte in PANDA

Ankündigungen

Frageforum - Technische Fragen

Kursleitung

Rebekka Schmidt

rebekka.schmidt@u
paderborn.de

Bitte verwenden Sie
im Betreff das Kürze
EKP

Sprechstunde

Allgemeine Informationen

Eingeschränkt Nicht verfügbar, es sei denn:

- Sie haben die erforderliche Punktzahl in **Bestätigung ASB** erhalten
- Die Aktivität **Teilnahme am Seminar - Synchron oder Asynchron?** ist als abgeschlossen markiert

Hier finden Sie allgemeine Informationen sowie den Zugang zu weiteren wichtigen PANDA-Kursen für dieses Seminar.

Aktiv!

Bitte nutzen Sie für Fragen die bereitgestellten Foren oder wenden sich direkt an mich.
Verwenden Sie bei Mails im Betreff das Kürzel **EKP**

Seminarplan und -informationen

Zu den virtuellen Seminarräumen

Eingeschränkt Nicht verfügbar, es sei denn: Sie gehören zu **01 Videokonferenz (synchron)**

Glossar der Kunstpädagogik

Kennwort zur Einschreibung: Wissen_4.0

Texto-Werkstatt

Unnamed area

Geschichte der Kunstpädagogik