Projektvereinbarung zur wissenschafts-propädeutischen Maturaarbeit

Die Projektvereinbarung ist bis spätestens Freitag, 03.06.2016, dem Sekretariat Gymnasium Oberstufe abzugeben. Sie kann in begründeten Fällen im gegenseitigen Einverständnis im Verlauf der Arbeit abgeändert werden. Wesentliche Änderungen sind dem Rektorat GOS zu melden.

## 1. Projektplan

|  |  |
| --- | --- |
| ***Lernende/r***  ***Klasse, email*** | Valdemar Thanner  5J, [valdemar.thanner@gmail.com](mailto:valdemar.thanner@gmail.com) |
|  |  |
| ***Betreuungsperson(en)***  (ggf. auch Englischlehrperson, externe Betreuungspersonen)  email | Bernhard Keller [beni.keller@ksz.ch](mailto:beni.keller@ksz.ch)  Margrit Oetiker-Odermatt [margrit.oetiker@ksz.ch](mailto:margrit.oetiker@ksz.ch) |
|  |  |
| ***Thema / Arbeitstitel***  ***Gegenstand***  der Untersuchung | The reasons for the historical transition from OTP to AES  Two different systems of Cryptography: AES (advanced encryption standard) and OTP (one-time pad) |
| ***Fragestellung***  Zielsetzung, Leitfrage(n)  Hypothese(n)  Zu erarbeitende Ergebnisse | The main goal is to illustrate the functionality and methodology of the two systems (AES and OTP), partly through a comparison between the two.   * Which problems are present in OTP, and how are these problems solved through using AES? * What is perfect secrecy, and why is it only attainable through the usage of OTP? * Why is AES considered “safe” despite not meeting the requirements for perfect secrecy? |
| ***Lösungsansatz***  Fachliche Verfahren, Methoden, Vorgehen, Experimente  ***Ressourcen***  Material, Quellen, Auskunftspersonen, Literatur. | Im Rahmen der Arbeit ist eine Umfrage vorgesehen: Ja …. Nein x  Theoretical research: a high level of understanding for the two systems will be necessary.  (Possibly) Some programming in order to better understand the two systems on a practical level.  MikTex (typesetting system)  Python / PyNacl  Main Sources:   * “Einführung in die Kryptographie” by Johannes Buchmann * "Introduction to Cryptography" by Professor Dan Boneh <https://class.coursera.org/crypto-preview/lecture> |
| ***Zeitplan und Termine***   * Zeitplan für die verschiedenen zu leistenden Arbeiten * Abgabe Probekapitel an Betreuungsperson (und Englisch-Lehrperson bei Immersionsarbeiten). * Zwischenevaluation * (obligatorische) Besprechungstermine (mindestens monatlich). * Abgabetermin | * Contents / Brainstorming: 1.7.2016 * OTP: 29.8.2016 * AES: 22.10.2016 * Comparison / code: 22.12.2016   Completion of first draft: 22.12.2016   * „Final Polish“ * Proofreading * Formatting   Handing in of the completed paper: 23.1.2017  The date for the next meeting will be decided after each completed meeting. The first meeting will take place on:  After each completed major section (listed above), a sample will be handed in to Mr. Keller as well as Ms. Oetiker-Odermatt. |
| ***Form*** Weicht die Arbeit allenfalls von einer üblichen wissenschaftspropädeutischen Arbeit ab?Sprache der schriftlichen Arbeit (Immersionsarbeiten).Voraussichtlicher Umfang der Arbeit. | The paper is largely theoretical. However, the actual comparison between the two systems is also of importance.  English  15-60 pages |
| ***Präsentation*** UmfangZielpublikumForm der Durchführung | 20-30 minutes, leaving 10-15 minutes for questions.  The presentation should be illustrate the concepts at hand in a manner which is understandable for students who have completed the fifth grade. This is to be achieved by using simple, “real life” examples, to illustrate the core concepts.  It should also serve as a complement to the actual paper, by commenting on and simplifying important parts of the paper. |
| ***Führung des Journals*** | ❒ Das Journal wird als Arbeitsprotokoll geführt, in dem Arbeitsschritte, Rohdaten und erste Ideen ohne spätere Überarbeitung festgehalten werden.  ❒ Im Journal wird der Arbeitsprozess beschrieben und analytisch und kritisch reflektiert. Skizzen, Ideen etc. werden also zu einem eigenen, umfassenden und redigierten Produkt aufgearbeitet.  Thematischer Fokus des Journals:      x Das Journal wird auf andere Weise geführt:  Wie?  The process will be documented through usage of GitHub. |
| ***Weitere Vereinbarungen***   * Wie wird mit der Betreuungsperson oder Aussenstehenden Kontakt aufgenommen * Wer ist wofür verantwortlich? * An welchen Leitfaden hat man sich bei der schriftlichen Arbeit zu richten? * … | Contact Should be made via E-Mail. |

# 2. Bewertungskriterien

***Allgemeine Bewertungskriterien:***

Product:

* Factual correctness
* Language (knowledge and utilisation of the English language)
* Formal aspect (readability, clarity, graphical / visual presentation)

Process:

* Ability to work independently
* Reliability (Punctuality in meetings, compliance with deadlines)

Presentation:

* Spoken language (knowledge and utilisation of the English language)
* Observation of the goals set in the field “Präsentation” (staying within the set time frame, illustrating concepts through usage of appropriate examples, complementing the actual paper)

***Auf das Projekt bezogene, spezifische Bewertungskriterien***

Product:

* Precise and clear explanations of the used algorithms
* Usage of practical examples to facilitate the comparison between the two systems
* Program Code:
  + Compliance with the general coding guidelines
  + Appropriate variable names
  + Good commenting

Process:

* Independently researching the topics at hand (AES and OTP)
* Independently learning to utilise LaTeX
* Independently learning GitHub, as well as appropriate usage of GitHub (useful commits, careful management of repositories, etc.)

Presentation:

* Reference to the paper, by commenting on and simplifying important sections
* Ability to answer posed questions within the frame of the actual project, thereby demonstrating a sufficient amount of background knowledge within the topics

# 3. Gewichtungen

|  |  |
| --- | --- |
| Produkt / schriftliche Arbeit (40-60%),  (davon 75-90% Inhalt,  10-25% Form) | * 40% * 70% product, 30% language * 80% content, 20% form |
| Arbeitsprozess  (20-40%) | * 30% |
| Präsentation  (15-30%) | * 30% * 70% presentation, 30% language |

|  |  |  |
| --- | --- | --- |
| Datum und Unterschrift | Betreuungsperson |  |
|  |  |
| Lernende/r |  |
|  |  |