Bearbeiter:
Felix Kallenbach
Matthias Schober

Thema:
RSA Verschlüsselung

Kurzbeschreibung:
Dieser Kurs soll Wissen zur RSA Verschlüsselung vermitteln. Dazu sollen verschiedene eLearning Techniken verwendet werden. RSA ist das am häufigsten verwendete Verfahren zur Sicherung sensibler und privater Daten und Nachrichten.

verwendetes LMS (mit kurzer Begründung der Auswahl):
Opal – da sich dieses LMS als Standard an der TU Dresden etabliert, wollen wir diese Entwicklung mittragen. Der Nutzer ist in den meisten Fällen mit dem LMS vertraut und eine mögliche Frustration aufgrund von hoher Einarbeitungszeit entfällt. Die Oberfläche ist gut verständlich und alle Funktionen, die für den Kurs relevant zu sein scheinen, sind vorhanden.

Gliederung und gedachte Quellen:

- Verschlüsselung
  - Motivation
  - Verfahren
  - Ablauf
- Mathematische Grundlagen
  - Modulo
  - Satz von Euler
  - euklidischer Algorithmus
- RSA
  - Berechnung der Schlüssel
  - Verschlüsseln/Entschlüsseln

Quellen:
Wikipedia
inf-schule.de/kommunikation/kryptologie/rsa
swisseduc.ch/informatik/
cryptool.org
curi0sity.de
mathe-online.at/materialien/Franz.Embacher/files/RSA/

kognitive Ziele:

I

- Der Schüler kennen verschiedene Verschlüsselungsarten und können diese in symmetrische und asymmetrische Verschlüsselung unterteilen
- Der Schüler kennen den Ablauf des Verschlüsselungsverfahren RSA

II

- Der Schüler beherrschen mathematische Grundfähigkeiten zur RSA
- Der Schüler können einen Text mit RSA verschlüsseln und entschlüsseln

III

- Der Schüler ist in der Lage, passende Situationen, in denen RSA verwendet werde sollte, herauszufinden und in diesen RSA anzuwenden

Darstellung der erwarteten Vorkenntnisse (mit Angaben aus Lehrplan Klassenstufe/Lernbereich):

- Sicherheit von Funktionen (Informatik Grundkurs 11/12 Lernbereich 3)
- Programmierung (Informatik Grundkurs 11/12 Lernbereich 8c)
- Teilbarkeitsregeln (Mathematik 6 Wahlpflicht 3)
- Potenzen (Mathematik Grundkurs 9 LB 1)
- Funktionsbegriff (Mathematik Grundkurs 8 LB 3)

Geeignet für folgende Studiengänge:
Informatik, Informationssystemtechnik, Mathematik, Medieninformatik, Lehramt Informatik, Wirtschaftsinformatik

Kurze Darstellung des weiteren Vorgehens (Zeitplan):

- Recherche bis 16.05
- Erstellung und erste Schritte/Test Opal Kurs bis 23.05
- Informationen aufbereiten und einfügen 06.06
- Tests konstruieren 20.06
- Überarbeitung 04.07
- Entwurf Abschlusspräsentation 11.07

erstellt am:09.05.19