Die Zahlentheorie als Grundlage der Kryptologie am Berufskolleg in NRW

Martin Epkenhans, Münster

28. September 2013

Westfälische Wilhelms-Universität Münster

Inhalt I

1. Struktur der Bildungsgänge am Berufskolleg in NRW
2. Entwicklung zum Zentralabitur
3. Bildungsplan Informatik D21
4. Bildungsplan Mathematik D21
5. Kryptologie und Zahlentheorie im Zentralabitur

Struktur des beruflichen Gymnasiums in NRW

- Einteilung in Bildungsgänge mit je einem profilbildenden LK und einem weiteren LK
- nur bestimmte Grundkurse
- Klassenverband

Struktur des beruflichen Gymnasiums in NRW

Einteilung in Fachbereiche

- Erziehung und Soziales
- Informatik
- Kunst und Gestaltung
- Technik
- Wirtschaft und Verwaltung

Bildungsgang D21-Informatikabitur

- 1. LK=weiterer LK: Mathematik
- 2. LK= profilbildender LK: Informatik
- beide LK's 5-stündig über 3 Jahre

Zentralabitur am BK

- 2007 Einführung an Gymnasien und Gesamtschule
- ab 2008 gestufte Einführung am Berufskolleg
  - 2008 nur profilbildender LK zentral
  - 2009 beide Leistungskurse zentral
  - ab 2010 2 LK's und 1 GK zentral

Bildungsplan Informatik

Kryptologie 13.1

- Schutzziele und Bedrohungen
- Symmetrische Verschlüsselung
- Asymmetrische Verschlüsselung mit dem RSA-Verfahren
- Digitale Signatur

Schutzziele und Bedrohungen

- Vertraulichkeit, Integrität, Verbindlichkeit
- Abhören, Verfälschen, Leugnen der Urheberschaft

Symmetrische Verschlüsselung

- Verfahrensbeispiele
- Chiffrieren und Dechiffrieren
- Kryptoanalyse

Asymmetrische Verschlüsselung mit dem RSA-Verfahren

- Modulare Arithmetik
- Satz von Euler
- erweiterter Euklidischer Algorithmus
- Vielfachsummendarstellung
- Potenzieren in der Modulo-Rechnung durch wiederholtes Quadrieren und Multiplizieren
- Sicherheit des RSA-Verfahrens

Digitale Signatur

- Anforderungen an eine digitale Signatur
- Notwendigkeit von Hashfunktionen und von Zertifizierungsinstanzen

Bildungsplan Mathematik

- Analysis
- lineare Algebra/ Geometrie
- Stochastik
- Zahlentheorie als Basis der Kryptologie

Zahlentheorie als Basis der Kryptologie 13.1

- Modulare Arithmetik
- Euklidischer Algorithmus
- Satz von Euler-Fermat

Modulare Arithmetik

- Modul-Begriff, Kongruenzen und Restklassen $\mod m$
  $\bar{a} = \{x \in \mathbb{Z} \text{ und } \mid x \equiv a \mod m\}$
- Eigenschaften von Restklassen, Restklassenaddition und -multiplikation
- Menge der Restklassen als Gruppe $\mathbb{Z}_m = \{\bar{1}, \bar{2}, \bar{3}, \ldots, \bar{m}\}$ mit additiven und multiplikativen Inversen
- $(\mathbb{Z}_m, +, *)$ als Ring bzw. Körper falls m Primzahl
- Eulersche φ-Funktion

Euklidischer Algorithmus

- Euklidischer Algorithmus
- Erweiterter Euklidischer Algorithmus in der Form $ax + by = ggT(a, b)$

Satz von Euler-Fermat

- $a^{\varphi(n)} \equiv 1 \mod n$
- Reduktion großer Exponenten modulo n

Durchführung des Zentralabiturs

- Kommission aus 3-5 Lehrkräften erstellt konkrete Vorgaben für jeden Abiturjahrgang.
- Ausgewählte Schulen erstellen Abiturvorschlag
- Kommission sichtet Vorschläge und erstellt daraus drei schriftliche Abiturvorschläge
- Pretester aus Lehrkräften testen Aufgaben

Kryptologie und Zahlentheorie im Zentralabitur

Jahr	Kryptologie	Zahlentheorie
2008	nein	dezentral
2009	nein	nein
2010	Ja	Ja
2011	Ja	Ja
2012	Ja	Nein (CAS) Ja (ohne CAS)
2013	nein	nein
2014	nein	(ja)
2015	nein	(ja)
2016	nein	(ja)

Abituraufgaben Informatik

Abituraufgaben Mathematik