

# Kodierungstheorie und Kryptographie

Dauer: 25 Minuten

## Vorbereitungsphase

Wie lange sollte man sich auf die Klausur vorbereiten?

einige Tage

Welche Literatur/Skripte waren hilfreich?

Skript zur Vorlesung

Wo lagen Deiner Meinung nach besondere Schwierigkeiten der Klausur?

Es ist relativ viel zu lernen gewesen.

## Verlauf der Prüfung

Welche Fragen wurden konkret gestellt?

Zur Kodierungstheorie:

- Definition von Code
- die nächsten beiden Sätze, wo ein anderes Kriterium für Code gezeigt wird
- dann was zur Entscheidbarkeit der Eigenschaft Code zu sein (also das mit dem  $K_0(C) = C$ ,  $K_i(C) = \dots$ ), wie man algorithmisch bestimmen kann ob eine Menge C Code ist
- Kosten eines Codes
- optimaler Code
- wie man einen solchen optimalen Code erzeugt (Huffman)

Zur Kryptographie:

- Nenne klassische Verschlüsselungen (Monoalph., Polyalpha. Subst.chif.)
- davon Verschiebungschiffre, Fairplay-Chiffre und Vigenère-Chiffre erklären
- Was ist ein öffentliches Schlüsselsystem? (die 4 Punkte erklären)
- ein öffentliches Schlüsselsystem auswählen und genauer beschreiben