405 270 VO Kryptographie
Universität Salzburg
SS 2011
Peter Hellekalek

---

1 Prüfungsbedingungen

1. Die Prüfung ist mündlich und dauert 30 bis 45 Minuten. Sie findet am Fachbereich Mathematik nach vorheriger Vereinbarung per Email statt.
2. Die Prüfung muss **vor dem 1.10.2012** stattfinden. Ausnahmen von dieser Regelung gibt es nur in begründeten Härtefällen.
3. Jeder Beweis, der in Ihrer Handschrift länger als eine halbe A4-Seite ist, darf von Ihnen an Hand eines (eigenen oder fremden) Skriptums vorgeführt werden.
4. Besonderen Wert lege ich auf das Verstehen der Konzepte, der Zusammenhänge und der Beispiele und auf die genauen Übergänge zwischen einzelnen Schritten in den Beweisen.
5. Im Fall einer Unklarheit: senden Sie eine Email an `peter.hellekalek@sbg.ac.at`

2 Prüfungsstoff

- Kapitel 1: Historische Chiffren
  1. Teilkapitel 1.1 bis 1.4 sowie 1.6 bis 1.8:
     Der gesamte Stoff ist vorzubereiten, mit einer Ausnahme: bei den Stromchiffren reicht der Prüfungsstoff nur bis einschließlich dem one-time pad.
  2. Teilkapitel 1.5 (Hillchiffre):
     wird *nicht* geprüft.
  3. Hinweis:
     Beachten Sie bitte, dass die Numerierung des Skriptums von der Numerierung der Vorlesung abweicht. In der Vorlesung wurde Teilkapitel 1.5 ausgelassen und daher die Numerierung mit 1.5 Transpositionschiffren, 1.6 Perfekte Sicherheit und 1.7 Stromchiffren fortgesetzt.
- Anhang I: Elementare Zahlentheorie
  Dieser Anhang dient Ihrer Information. Die Methoden und Begriffe dieses Kapitels treten in diversen Chiffren auf und werden daher in Zusammenhang mit der entsprechenden Anwendung geprüft: die Lösungsmethode für lineare Kongruenzen wird zum Beispiel bei RSA benötigt, usw.
- Anhang II: Entropie
  Wird nicht geprüft.
- Anhang III: Blockchiffren
  1. Teilkapitel 1.1 (Grundlegendes) wird nicht geprüft.

2. Teilkapitel 1.2 (Algebraische Grundlagen) wird geprüft, allerdings *ohne Beweise*. Besonderen Wert lege ich darauf, dass Sie die Definition der Multiplikation von Bitvektoren erläutern können. Dazu ist es erforderlich, dass Sie sich eingehend mit den Polynomringen $R[X]$ und $K[X]$ auseinandersetzen.
3. Teilkapitel 1.3.1 "Betriebsarten" des Kapitels über DES wird nicht geprüft.
4. Der restliche Stoff von Anhang II ist vorzubereiten, insbesondere die Funktionsweise von AES.
5. Es ist nicht erforderlich, daß Sie die Schemata zu DES und AES auswändig lernen. Es reicht aus, diese Schemata anhand eines Skriptums erläutern zu können.

- Anhang IV: Public-Key Kryptographie
  Alle Teilkapitel werden geprüft.
- Anhang V: Hashfunktionen
  Alle Teilkapitel werden geprüft.

29. Juni 2011 Peter Hellekalek