

Skript zur Vorlesung**Diskrete Mathematik****Prof. Dr. Wolfgang Konen****WS08/09**

1.	Modulare Arithmetik	3
1.1.	Primzahlen	4
1.2.	Modulare Arithmetik	6
1.2.1.	Teilbarkeitsregeln	8
1.2.2.	Der Chinesische Restsatz (CRT)	10
1.2.3.	Der Algorithmus Erweiterter Euklid	13
2.	Diophantische Gleichungen	16
2.1.	Was ist eine diophantische Gleichung und wozu braucht man sie?	16
2.2.	Wie löst man diophantische Gleichungen?	17
3.	Kryptographie	22
3.1.	Rechnen mit großen Zahlen	22
3.2.	Kryptographische Protokolle: RSA	24
3.3.	Hashfunktionen und Digitale Signatur	26

Literatur / Links

(s. auch [Lit_DisMa.htm](#))

- www.cryptool.de: CrypTool ist ein umfangreiches Lernprogramm (Uni Siegen + Uni Darmstadt) zu Kryptographieverfahren und Zahlentheorie. Einige Beispiele
 - Einzelverfahren – Zahlentheorie interaktiv...– Lernprogramm Zahlentheorie
 - Einzelverfahren – Anwendung Chinesischer Restsatz – Astronomie
 - Besonders interessant ist auch das zu CrypTool gehörige Skript als PDF „Kryptographie, Mathematik und mehr“ (über 200 Seiten)
- [Teschl05, Bd. 1, S. 91ff] (erweiterter) Euklid-Algorithmus und diophantische Gleichungen, Chinesischer Restsatz
- [Teschl05, Bd. 1, S. 74ff] Hashfunktionen