# 1. Grundlagen & historische Beispiele

1.1. Kryptosysteme

1.2. Alphabete & Wörter

1.3 Einschub: Die Gruppe $(\mathbb{Z}_n, +)$

1.4 Statistische Analyse

1.5 Blockchiffren

1.6 Typen von Attacken

1.7 Vignère - Chiffre

# 2. Komplexität & Zahlentheorie

2.1 (Binärentwicklung & Länge) Komplexität

2.2. Zahlentheorie

Der (erweiterte) euklidische Algorithmus

Bézout - Koeffizienten

Satz von Euler / Kleine Satz von Fermat

# 3. Sicherheit

3.1. Einschub aus der W-Theorie

3.2 Sicherheit

## 4. Symmetrische Verfahren

4.1. Die AES - Chiffrierung

## 5. Asymmetrische Verfahren

5.1. Einwegfunktionen

5.2. Die RSA - Verschlüsselung

5.3. Low Exponent attack

5.4 Verschlüsselung von Texten durch RSA

5.5 Effizienz

5.6 Die Wahl von p, q und e / der geheime Schlüssel d

## 6. Primzahltests

6.1 Probedivision

6.2 Fermat - Test

6.3 Der Miller - Rabin Test

6.4 Der AKS - Test

6.5 Der Solovay - Strassen - Test

## 7. Faktorisierung

7.1 Pollard's (p-1) - Methode

7.2 Faktorisierung mit Differenzen von Quadraten

7.3 Idee des quadratischen Siebs.

## 8 Das ElGamal-Verfahren & der Diffie-Hellman Schlüsselaustausch

8.1 Das ElGamal-Verfahren

8.2 Der Diffie-Hellman Schlüsselaustausch

## 9 Signaturen

9.1 Die RSA-Signatur

9.2 Einschub: Hashfunktionen

9.3 Signaturen mit RSA und Hashfunktionen

9.4 Die ElGamal Signatur

## 10. Der diskrete Logarithmus

10.1 Enumeration

10.2 Baby-Step-Giant-Step von Shanks

10.3 Pohlig-Hellman-Algorithmus