BIP Kreativitätsgymnasium Leipzig
Torgauer Straße 114
04347 Leipzig

Mathematisch-naturwissenschaftliches Symposium

Einführung in die Kryptologie und Datensicherheit

Mit Algorithmen in Python

und Übungsaufgaben

von: Matthias Richter
letzte Aktualisierung: 16. Januar 2018
erstellt mit: LaTeX 2ε

matthias.richter@gyl.bipschulen.de

Inhaltsverzeichnis

1 Begriff und Anliegen der Kryptologie **11**
- 1.1 Begriffserklärungen . . . 11
- 1.2 Anwendungsbereiche . . . 12
- 1.3 Anforderungen an kryptologische Algorithmen . . . 13
- 1.4 Funktionsweise . . . 13
- 1.5 Übungsaufgaben . . . 14

2 Monoalphabetische Verschlüsselungsverfahren **15**
- 2.1 Caesar-Verfahren . . . 15
- 2.2 Freimaurer–Alphabet . . . 16
- 2.3 Polybios–Code . . . 17
- 2.4 Freie Substitution . . . 19
- 2.5 Schlüsselwortchiffre . . . 20
- 2.6 Affine Chiffre . . . 21
- 2.7 ADFGX . . . 23
- 2.8 Das Prinzip von Kerckhoffs . . . 25
- 2.9 Kryptoanalyse monoalphabetischer Verschlüsselungen . . . 26
- 2.10 Übungsaufgaben . . . 32

3 Polyalphabetische Verschlüsselungsverfahren **37**
- 3.1 Motivation . . . 37
- 3.2 Verfahren von Alberti . . . 37
- 3.3 Trithemius-Tafel . . . 38
- 3.4 Vigenère-Verfahren . . . 40
- 3.5 Kryptoanalyse des Vigenère-Verfahrens . . . 43
  - 3.5.1 Kasiski-Test . . . 44
  - 3.5.2 Friedman-Test . . . 45
  - 3.5.3 Entschlüsselung des Beispieltextes . . . 48
- 3.6 Enigma . . . 49
  - 3.6.1 Geschichtliche Einordnung . . . 49
  - 3.6.2 Aufbau und Funktionsweise . . . 49
  - 3.6.3 Anzahl möglicher Schlüssel . . . 50
  - 3.6.4 Kryptoanalyse . . . 51
- 3.7 Übungsaufgaben . . . 51

4 Stromchiffren **53**
- 4.1 Strom- vs. Blockchiffren . . . 53
- 4.2 Funktionsweise von Stromchiffren . . . 53
- 4.3 One-Time Pad . . . 55
- 4.4 Exkurs: Zufallszahlen . . . 55
  - 4.4.1 Echte Zufallszahlengeneratoren (TRNG) . . . 55
  - 4.4.2 Pseudozufallszahlengenerator (PRNG) . . . 56
  - 4.4.3 Kryptographisch sichere Pseudozufallszahlengenerator (CPRNG) . . . 57
- 4.5 Auf Schieberegistern basierende Stromchiffren . . . 58
  - 4.5.1 Begriff & Funktionsweise . . . 58
  - 4.5.2 Mathematische Beschreibung eines allgemeinen LFSR . . . 59

4.5.3 Krytoanalyse eines LFSR . . . 61
4.5.4 Einsatz von Schieberegistern in der Kryptologie . . . 62
4.6 Übungsaufgaben . . . 63

5 Blockchiffren **65**
5.1 Funktionsweise . . . 65
5.2 Hill-Chiffre . . . 65
5.2.1 Mathematische Grundlagen der linearen Algebra . . . 65
5.2.1.1 Vektoren und Matrizen . . . 65
5.2.1.2 Matritzenmultiplikation . . . 67
5.2.1.3 Einheitsmatrix . . . 68
5.2.1.4 Inverse Matrix . . . 68
5.2.1.5 Rechnen in $\mathbb{Z}_n$ . . . 69
5.2.2 Verschlüsselung . . . 70
5.2.2.1 Codierung der Zeichen als Nummern . . . 70
5.2.2.2 Chiffriermatrix . . . 70
5.2.2.3 Klartextmatrix . . . 71
5.2.2.4 Verschlüsselungsalgorithmus . . . 71
5.2.3 Entschlüsselungsalgorithmus . . . 72
5.2.4 Zusammenfassung des Verfahrens . . . 73
5.2.5 Berechnung der inversen Matrix . . . 74
5.2.6 Kryptoanalyse . . . 74
5.2.7 Implementation in Python . . . 75
5.3 DES . . . 76
5.3.1 Geschichtliche Bemerkungen . . . 76
5.3.2 Kriterien für Blockchiffren . . . 76
5.3.3 Funktionsweise . . . 77
5.4 AES . . . 79
5.5 Betriebsmodi . . . 79
5.5.1 Motivation . . . 79
5.5.2 CBC-Modus . . . 79

6 Grundlagen der Public-Key-Kryptographie **81**
6.1 Grundprinzip symmetrische Verfahren . . . 81
6.2 Problem des Schlüsselaustauschs . . . 81
6.3 Grundidee asymmetrische (Public-Key) Verfahren . . . 82
6.4 Anforderung an asymmetrische Verschlüsselungsverfahren . . . 82
6.5 Mathematische Grundlagen . . . 83
6.5.1 Modulo-Arithmetik . . . 83
6.5.2 Kongruenzen . . . 84
6.5.3 Der euklidische Algorithmus . . . 84
6.5.4 Erweiterter euklidische Algorithmus . . . 86
6.5.5 Eulersche-Phi-Funktion . . . 87
6.5.6 Satz von Euler und kleiner Satz von Fermat . . . 88
6.6 Vergleich von Schlüssellängen und Sicherheitsniveau für symmetrische und asymmetrische Verfahren . . . 90
6.7 Übungsaufgaben . . . 90

7 Das RSA-Verfahren **93**
7.1 Schlüsselerzeugung von Alice . . . 93
7.2 Verschlüsselung . . . 93
7.3 Entschlüsselung . . . 94
7.4 Beispiel für den RSA-Algorithmus . . . 94
7.4.1 Schlüsselerzeugung von Alice . . . 94
7.4.2 Verschlüsselung . . . 95

7.4.3 Entschlüsselung . . . 95
7.5 Korrektheitsbeweis . . . 96
7.6 Folgerungen . . . 97
7.7 Bemerkungen zur Sicherheit . . . 97
7.8 Implementation . . . 98
7.9 Exkurs: Schnelles Exponentieren . . . 99
7.10 Exkurs: Primzahlen & Primzahltests . . . 101
7.10.1 Definition und erste Eigenschaften . . . 101
7.10.2 Primzahlverteilung . . . 102
7.10.3 Primzahltest durch Probedivision und das Sieb des Eratosthenes . . . 103
7.10.4 Fermat-Test . . . 104
7.10.5 Las-Vegas-Test . . . 105
7.10.6 Weitere Primzahltests . . . 106
7.11 Exkurs: Schnelles Entschlüsseln mit dem chinesischen Restesatz . . . 106
7.11.1 Chinesische Restesatz . . . 106
7.11.2 RSA und der chinesische Restesatz . . . 107
7.12 Übungsaufgaben . . . 109

8 Public-Key-Kryptographie auf der Basis von diskreten Logarithmen 112
8.1 Diffie-Hellman-Schlüsselaustausch . . . 112
8.1.1 Inititalisierungsphase . . . 112
8.1.2 Protokoll . . . 112
8.1.3 Beispiel . . . 112
8.1.4 Korrekteitsbeweis . . . 113
8.2 Diskreter Logarithmus . . . 113
8.3 ElGamal . . . 115
8.3.1 Grundidee ElGamal-Verfahren als Erweiterung des Diffie-Hellman-Schlüsselaustausch 115
8.3.2 Inititalisierungsphase . . . 115
8.3.3 Protokoll . . . 116
8.3.4 Beispiel . . . 116
8.3.5 Korrekheitsbeweis . . . 118
8.4 Übungsaufgaben . . . 118

9 Digitale Signaturen 120
9.1 Motivation . . . 120
9.2 Prinzip . . . 120
9.2.1 Naive Idee . . . 120
9.2.2 Verbesserung – Grundidee digitaler Signaturen . . . 121
9.2.3 Signaturprotokoll . . . 121
9.3 Sicherheitsziele . . . 122
9.4 Digitale Signaturen mit RSA . . . 122
9.4.1 Signaturprotokoll . . . 122
9.4.2 Beispiel . . . 122
9.4.3 Korrektheitsbeweis . . . 123
9.4.4 Exkurs: Schwächen/Angriffe . . . 123
9.4.4.1 Existenzielle Fälschung . . . 123
9.4.4.2 Verkettung von Signaturen . . . 124
9.5 Digitale Signaturen mit ElGamal . . . 126
9.5.1 Signaturprotokoll . . . 126
9.5.2 Beispiel . . . 127
9.5.3 Korrektheitsbeweis . . . 127
9.5.4 Schwächen/Angriffe . . . 128
9.5.4.1 Angriff auf den Sitzungsschlüssel . . . 128
9.5.4.2 Existentielle Fälschung . . . 128
9.6 Übungsaufgaben . . . 128

10 Hashfunktionen **129**
10.1 Motivation . . . 129
10.2 Anforderungen an Hashfunktionen . . . 129
10.3 Anwendung: Digitale Signaturen mit Hashfunktionen . . . 131
10.4 Anwendung: Anmeldung/Login an einem Computer . . . 131
10.5 Wichtige Hashfunktionen in der Praxis . . . 132
10.6 Übungsaufgaben . . . 132

11 Anwendungen in der Internetsicherheit **133**
11.1 SSL . . . 133
11.2 VPN . . . 133
11.3 PGP . . . 133

A Steganografie **134**
A.1 Motivation . . . 134
A.2 Klassische Verfahren . . . 134
A.3 Digitale Verfahren . . . 134
A.3.1 Versteckter Text in Office-Dokumenten . . . 134
A.3.2 Zusammenführung von Bild- und Textdatei . . . 135
A.3.3 Versteckter Text in einem Bild . . . 135

B Politisch-Gesellschaftliche-Bemerkungen **136**

C Perfekte Sicherheit **137**

D Mathematischer Hintergrund **138**
D.1 Affine Chiffre . . . 138
D.1.1 Beweis von Satz 1 . . . 138
D.1.2 Berechnung der Parameter für die Entschlüsselung . . . 138
D.2 Rechenregeln für Modulo-Arithmetik (Beweis von Satz 5) . . . 139
D.3 Beweis des Satzes von Euler (Satz 11) . . . 139

E Lösungsvorschläge der Übungsaufgaben **141**

Literaturverzeichnis **184**

Literaturverzeichnis

Bauer, Friedrich L. (2000): *Entzifferte Geheimnisse: Methoden und Maximen der Kryptologie*. 3. Auflage. Springer, Berlin.

Beckman, Bengt (2005): *Arne Beurling und Hitlers Geheimschreiber: Schwedische Entzifferungserfolge im 2. Weltkrieg*. Springer, Berlin.

Beutelspacher, Albrecht (2007): *Kryptologie: Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen*. 8. Auflage. Vieweg+Teubner.

Beutelspacher, Albrecht, Schwarzpaul, Thomas und Neumann, Heike B. (2005): *Kryptografie in Theorie und Praxis*. Vieweg+Teubner.

Buchmann, Johannes (2008): *Einführung in die Kryptographie*. 4. Auflage. Springer, Berlin.

Burton, David M. und Dalkowski, Heinz (2005): *Handbuch der elementaren Zahlentheorie*. Heldermann.

Corporation, PGP (2003): An Introduction to Cryptography. PGP Corporation.

Diffie, Whitfield und Hellman, Martin E. (1976): New Directions in Cryptography. IEEE Transactions on Information Theory, 22, 644–654.

Ertel, Wolfgang (2012): *Angewandte Kryptographie*. 4. Auflage. Hanser.

Gräbe, Hans-Gert (2012): *Algorithmen für Zahlen und Primzahlen*. Eagle.

Kahn, David (1996): *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. Scribner.

Klima, Richard E. und Sigmon, Neil P. (2012): *Cryptology: Classical and Modern with Maplets*. Chapman and Hall/CRC.

Massey, Kenneth (2011): *Hill Cipher Project*. 2011, http://massey.limfinity.com/207/hillcipher.pdf.

Menezes, Alfred, Oorschot, Paul van und Vanstone, Scott (1997): *Handbook of Applied Cryptography (Discrete Mathematics and Its Applications)*. Crc Press.

Paar, Christof und Pelzl, Jan (2011): *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer.

Paar, Christof und Pelzl, Jan (2016): *Kryptografie verstehen. Ein Lehrbuch für Studierende und Anwender*. Springer.

Ribenboim, Paulo (2006): *Die Welt der Primzahlen: Geheimnisse und Rekorde*. Springer.

Schmeh, Klaus (2004): *Die Welt der geheimen Zeichen. Die faszinierende Geschichte der Verschlüsselung*. W3L.

Schmeh, Klaus (2008): *Versteckte Botschaften. Die faszinierende Geschichte der Steganografie*. dpunkt.

Schmeh, Klaus (2016): *Kryptografie. Verfahren - Protokolle - Infrastrukturen*. dpunkt.

Singh, Simon (2001): *Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet*. Dtv.

Steinhausen, Detlef (1994): *Simulationstechniken*. Oldenbourg.

Trappe, Wade und Washington, Lawrence C. (2006): *Introduction to Cryptography with Coding Theory*. 2. Auflage. Prentice Hall.

Wätjen, Dietmar (2008): *Kryptographie: Grundlagen, Algorithmen, Protokolle*. 2. Auflage. Spektrum Akademischer Verlag.

Wobst, Reinhard (2001): *Abenteuer Kryptologie. Methoden, Risiken und Nutzen der Datenverschlüsselung*. 3. Auflage. Addison-Wesley.

Ziegenbalg, Jochen (2015): *Elementare Zahlentheorie. Beispiele, Geschichte, Algorithmen*. 2. Auflage. Springer.