Einführung in die Kryptographie
Workshop SS18

Prof. Robert König & Stefan Huber

12. März 2018

1. Elementare Zahlentheorie (Stefan Betz)
   Restklassenringe, Endliche Körper, Chinesischer Restsatz. Kapitel 2 und 3 in [1].
2. Primzahlerzeugung, Primzahltests, Primzahlzerlegung (Hannes Burger)
   Euklid-Algorithmus, Kleiner Fermat, Fermat-Test, Miller-Rabin-Test, Faktorisierung (Quadratisches Sieb). Kapitel 8 und 10 in [1], auch Kapitel 3 in [2].
3. Diskrete Logarithmen (Philipp Naused)
   Eulersche φ-Funktion, Diskrete Logarithmen, Diffie-Hellmann-Schlüsselaustausch. Kapitel 9.5 und 11 in [1].
4. Private/Public-Key-Verfahren (Tobias Grasberger)
   Definitionen, RSA. Kapitel 9 in [1] und Kapitel 8 in [2].
5. Hashing und Signaturen (Jule Schindler)
   Kapitel 12 und 13 in [1], sowie Kapitel 9, 10, 11 in [2].
6. Interaktive Beweise und Zero-Knowledge-Protokolle (Julia Benirschke)
   Kapitel 1 in [3].
7. Secret Sharing / Two-Party Computation (Tobias Gerwald & Johann Protzmann)
   Kapitel 2 in [3].
8. Informationstheoretische Sicherheit (Julien Caselmann)
   Leftover Hash Lemma, Privacy Amplification, One-Time-Pad [5],[6].

Literatur

[1] J. Buchmann, *Einführung in die Kryptographie*, 5. Auflage, Springer (2010); http://link.springer.com/book/10.1007/978-3-540-74452-8, über OPAC (Universitätsbibliothek) verfügbar.

[2] A. Menezes, P. van Oorschot, S. Vanstone, *Handbook of Applied Cryptography*, CRC Press (1996); http://cacr.uwaterloo.ca/hac.

[3] M. Hirt, U. Maurer, *Kryptographische Protokolle*, Vorlesungsskript Frühjahr 2009, ETH Zürich; https://www.crypto.ethz.ch/teaching/lectures/KP18/script/CP09_script.pdf.

[4] A. Beutelspacher, J. Schwenk, K. Wolfenstetter, *Moderne Verfahren der Kryptographie*, 8. Auflage, Springer Spektrum (2015); http://link.springer.com/book/10.1007/978-3-8348-2322-9, über OPAC verfügbar.

[5] C. Bennett, G. Brassard, C. Crépeau, U. Maurer, *Generalized Privacy Amplification*, IEEE Transactions on Information Theory, Vol. 41, No. 6, November 1995; http://crypto.cs.mcgill.ca/∼crepeau/COMP649/04.00476316.pdf.

[6] L. Reyzin, *Extractors and the Leftover Hash Lemma*, Vorlesungsskript Frühjahr 2011, MIT & Boston University; http://www.cs.bu.edu/∼reyzin/teaching/s11cs937/notes-leo-1.pdf.

[7] M. Lehn, *Wie halte ich einen Seminarvortrag?*, http://www.alt.mathematik.uni-mainz.de/Members/lehn/le/seminarvortrag.