Seminar über Zahlentheorie und Kryptologie (Wintersemester 2019/2020)

Prof. Dr. Sander Zwegers, Christina Röhrig

Das Seminar umfasst 12 Vorträge, diese sollten jeweils ca. 60 Minuten dauern. Die untenstehenden Beschreibungen geben eine grobe Übersicht über die im Vortrag zu behandelnden Themen. Zusätzlich dazu sollten Sie ein bis zwei Aufgaben erstellen, in denen das Gelernte angewendet wird. Diese werden im Anschluss an den Vortrag von den anderen SeminarteilnehmerInnen bearbeitet und dann gemeinsam besprochen. Die Bearbeitungs- und Besprechungsphase sollte ca. 25 Minuten in Anspruch nehmen.

Vortrag 1. (07.10.)
Euklidischer Algorithmus und Primfaktorzerlegung
[1]: *Kurze Wiederholung zur Teilbarkeit (Abschnitt 1.1.4), Größter gemeinsamer Teiler (Abschnitt 1.1.6), Zerlegung in Primzahlen (Abschnitt 1.1.7), Euklidischer Algorithmus (Abschnitt 1.6.2), Erweiterter euklidischer Algorithmus (Abschnitt 1.6.3), Asymptotische Notation (Abschnitt 1.4.4), Effizienz (Abschnitt 1.6.4)*

Vortrag 2. (14.10.)
Restklassenringe und die Eulersche φ-Funktion
[1]: *Kongruenzen und Restklassenringe (Abschnitte 2.1 und 2.4), Division im Restklassenring (Abschnitt 2.6), Prime Restklassengruppen (Abschnitt 2.8)*

Vortrag 3. (21.10.)
Der Chinesische Restsatz und der kleine Satz von Fermat
[1]: *Der Chinesische Restsatz (Abschnitt 2.15), Zerlegung des Restklassenrings (Abschnitt 2.16), Bestimmung der Eulerschen φ-Funktion (Abschnitt 2.17), Der kleine Satz von Fermat (Abschnitt 2.11)*

Vortrag 4. (28.10.)
Primzahltests und Carmichael-Zahlen
[1]: *Der Fermat-Test (Abschnitt 7.2), Carmichael-Zahlen (Abschnitt 7.3), Der Miller–Rabin-Test (Abschnitt 7.4)*

Vortrag 5. (04.11.)
Symmetrische Verschlüsselungsverfahren
[1]: *Symmetrische und asymmetrische Verschlüsselungsverfahren (Abschnitte 3.1 und 3.3), Blockchiffren (Abschnitte 3.7 und 3.8), Affin lineare Funktionen (Abschnitt 3.16.7), Affin lineare Blockchiffren (Abschnitt 3.17), Beispiele (Abschnitt 3.18), Sicherheit (Abschnitt 3.19)*

Vortrag 6. (18.11.)
Wahrscheinlichkeit und perfekte Sicherheit
[1]: *Wahrscheinlichkeit und bedingte Wahrscheinlichkeit (Abschnitt 1.2), Das Geburtstagsparadox (Abschnitt 1.3.1), Perfekte Geheimhaltung (Abschnitt 4.1)*

Vortrag 7. (25.11.)
Public-Key Verschlüsselung und das RSA-Verfahren
[1]: *Public-Key Verschlüsselung (Abschnitte 8.1 und 8.2), Das RSA-Verfahren (Abschnitte 8.3.1-8.3.3)*

Vortrag 8. (02.12.)
Sicherheit des RSA-Verfahrens und Wahl der Parameter
[1]: *Sicherheit (Abschnitt 8.3.4), Wahl der Parameter (Abschnitte 8.3.5-8.3.7), Effizienz (Abschnitt 8.3.8)*
[2]: *Starke Primzahlen und der Gordon-Algorithmus (Abschnitt 5.5)*

Vortrag 9. (09.12.)
Das Rabin-Verschlüsselungsverfahren
[1]: *Beschreibung des Verfahrens, Schlüsselerzeugung, Ver- und Entschlüsselung, Sicherheit (Abschnitt 8.4)*

Vortrag 10. (16.12.)
Diffie–Hellman-Schlüsselaustausch und diskrete Logarithmen
[1]: *Diskrete Logarithmen (Abschnitt 8.6.1), Diffie–Hellman-Schlüsselaustausch, Wahl der Parameter, Sicherheit (Abschnitte 8.6.2-8.6.5), Berechnung diskreter Logarithmen (Abschnitt 10.3 oder 10.4 oder 10.5)*

Vortrag 11. (13.01.)
Elliptische Kurven und das ElGamal-Verfahren
[1]: *Elliptische Kurven (Abschnitt 13.2), Das ElGamal-Verfahren (Abschnitte 8.7.1-8.7.3)*
[2]: *Kryptosysteme mit elliptischen Kurven (Abschnitt 14.2)*

Vortrag 12. (20.01.)
Kryptographische Hashfunktionen
[1]: *Hashfunktionen und Kompressionsfunktionen (Abschnitte 11.1 und 11.4), Eine arithmetische Kompressionsfunktion (Abschnitt 11.6)*
[2]: *Hashfunktionen und Signaturen (Abschnitt 6.1)*

Literatur

[1] Johannes Buchmann: *Einführung in die Kryptographie*, Springer, 2016.

[2] Dietmar Wätjen: *Kryptographie*, Springer, 2018.