Vortragsseminar Kryptographie

Van Bang Le

Corona-Semester 2020

09–04–2020

Vortragsseminar: Kryptographie

Die Kryptographie beschäftigt sich mit Verschlüsselungsmethoden und ist eine der Grundvoraussetzungen für eine funktionierende digitale Gesellschaft (sichere Übermittlung von vertraulichen Informationen, überprüfbare Authentizität von Nachrichten etc.).

Die Seminarvorträge sollen die wichtigsten Verfahren sowie ihre mathematischen Grundlagen ausführlich behandeln.

In diesem Corona-Semester gehen wir nach folgenden zwei Büchern vor, die in Uni-Netz online (PDF, e-book) verfügbar sind:

- Olaf Manz, *Verschlüsseln, Signieren, Angreifen. Eine kompakte Einführung in die Kryptografie*, Springer Spektrum 2019.
- Johannes Buchmann, *Einführung in die Kryptographie*, Springer Spektrum 2016.

Vorgesehene Themen

1. Symmetrische Verfahren: DES (Manz § 2.1–§ 2.7, Buchmann Kap. 5)
2. Symmetrische Verfahren: AES (Manz § 2.8, § 2.9, Buchmann Kap. 6)
3. Public-Key-Kryptographie: Primzahlen und Faktorisierung (Buchmann Kap. 7, Kap. 9)
4. Public-Key-Kryptographie: Faktorisierung und RSA (Manz § 3.1–§ 3.4, Buchmann § 8.1–§ 8.3)
5. Public-Key-Kryptographie: Diskreter Logarithmus, Diffie-Hellman und ElGamal (Manz § 3.5–§ 3.8, Buchmann § 8.6, § 8.7, Kap. 10)
6. Public-Key-Kryptographie: Digitale Signatur I (Manz § 4.1–§ 4.5, Buchmann Kap. 11, 12)
7. Public-Key-Kryptographie: Digitale Signatur II (Manz § 4.6–§ 4.9, Buchmann Kap. 14)
8. Public-Key-Kryptographie: Elliptische Kurven (Buchmann Kap. 13)

Vorgehensweise (I)

- Beachten Sie, dass etwas Mathematik notwendig ist für ein echtes Verständnis über die Hintergründe und Arbeitsweise von kryptographischen Verfahren.
- Es ist vielleicht hilfreich für Ihre Entscheidung, etwas zur Geschichte der Kryptographie in [Manz, Kap. 1] zu erfahren und einen Blick auf die mathematische und algorithmische Grundlage der Kryptographie in [Buchmann, Kap. 1 und 2] zu werfen.
- Wenn Sie sich für die Teilnahme an diesem Seminar entscheiden, melden Sie sich bitte bis 22. April 2020 in Stud.IP an.
- Die erste Sitzung findet am 22. April um 17 Uhr statt. Wir werden die Plattform zoom oder BigBlueButton (via Stud.IP meetings) verwenden. Genaueres wird in Stud.IP rechtzeitig mitgeteilt.

Vorgehensweise (II)

- In der ersten Sitzung wird es u.a. eine Einführung geben, in der den Teilnehmern die Themen kurz vorgestellt werden und eine genaue Planung besprochen wird.
- In der zweiten Sitzung werden die Themen mit Vortragsterminen auf die Seminarteilnehmer verteilt. Beachten Sie: wir können nicht garantieren, dass Sie Ihr Wunschthema auch wirklich zugewiesen bekommen.
- Bis zum ersten Vortragstermin gibt es online-Betreuung/Konsulation zu den regulären Terminen.
- Die Vorträge richten sich in erster Linie an die anderen Seminarteilnehmer. Eine konstruktive, lebhafte Diskussion zu den behandelten Themen ist ausdrücklich erwünscht.
- Von den Teilnehmern wird erwartet, dass sie eigenständig weitere Literaturquellen hinzuziehen (und zitieren!).

Leistungsnachweis

Note besteht aus

- Vortrag (ca. 1 Stunde inkl. Zwischenfragen und anschliessende Diskussion),
- schriftlicher Ausarbeitung des Themas ($\pm$13 Seiten).

Bitte beachten:

- Der Vortrag muss in sich abgeschlossen sein!
- Vortragsfolien (pdf oder ppt) sind möglichst 2 Tage vor Vortragstermin einzureichen; sie werden in Stud.IP für alle Teilnehmer zur Verfügung bereitgestellt.
- Die schriftliche Ausarbeitung (pdf) ist spätestens bis 26. Juli 2020 (also 2 Wochen nach dem letzten Vorlesungstag) abzugeben.
- **Von allen Teilnehmern wird eine (aktive) Beteiligung an allen Vorträgen erwartet!**