SEMINAR IM WINTERSEMESTER 2022/23: KRYPTOGRAPHIE

HEIKE MILDENBERGER

Vorbesprechung

am 18.7.2022 um 13:00 Uhr im Seminarraum 404
Für Online-Teilnahme BBB Raum
`https://bbb.uni-freiburg.de/b/hei-fw6-gm7-ijs`

Tutorat:

nn

Zeit und Ort

Blockseminar nach dem semester im Januar und im Februar oder in der vorlesungsfreien Zeit
WS 22/23
Hybrid in `https://bbb.uni-freiburg.de/b/hei-fw6-gm7-ijs` bei Bedarf.

Liste der Vortragsthemen, Quellenangaben

Wir folgen den Kapiteln von Buchmann [3], [2], die im Deutschen und im Englischen identisch sind.

Zur Vortragsvorbereitung kann man auch folgende Quellen benutzen:

(1) Simon Singh, The Code Book [5] (eher historisch),
(2) Beutelspacher, Neumann, Schwarzpaul Kryptographie in Theorie und Anwendung [1]. Ein ausführliches Lehrbuch mit viel motivierendem Text.
(3) Hoffstein, Pipher, Silvermann [4]. An introduction to mathematical cryptography. Ein sehr gutes mathematische ausgerichtetes Lehrbuch.

Date: 17.10.2022, HM.

(4) Von Buchmann sind die neueren Auflagen bis jetzt nur auf Deutsch erschienen: [3].

Es gibt das Buch von Buchmann in älteren Auflagen auch auf Englisch [2].

1. Vortrag 13.2.23 9:00 Uhr
Verschlüsselung Sektionen 4.1 bis 4.8
Vortragende:

2. Vortrag 13.2.23 11:30 Uhr
Verschlüsselung Sektionen 4.9 bis 4.15
Vortragender:

3. Vortrag 13.2.23 14:00 Uhr
Kapitel 5 Wahrscheinlichkeit und perfekte Geheimhaltung
Vortragender:

4. Vortrag
Kapitel 6 Der DES-Algorithmus
Vortragende(r):

5. Vortrag 14.2.2023 9:00 Uhr
Kapitel 7 Der AES-Algorithmus
Vortragender:

6. Vortrag.
Kapitel 8 Primzahlerzeugung
Vortragende(r):

7. Vortrag. 14.2.23 11:00 Uhr
Sektion 9.1 bis 9.3 Das RSA-Verfahren
Vortragende:

8. Vortrag. 14.2.23 14 Uhr
Sektion 9.4 bis 9.7 Der Rabin-Schlüsseltausch und das Diffie-Hellman-Verfahren
Vortragender:

9. Vortrag.
Sektion 9.8 Das ElGamal-Verschlüsselungsverfahren
Vortragende(r):

10. Vortrag. 15.2.23 9:00 Uhr
Kapitel 10, Faktorisierung
Vortragende(r):

11. Vortrag.
Kapitel 11, Diskrete Logarithmen
Vortragende(r):

12. Vortrag. 15.2.2023 11:00 Uhr
Kapitel 12, Hashfunktionen
Vortragende(r):

13. Vortrag.
Kapitel 13, Digitale Signaturen
Vortragende(r):

14. Vortrag.
Kapitel 14 Andere Gruppen, Veschlüsselung mit Hilfe elliptischer Kurven
Vortragende(r):

Literatur

[1] Albrecht Beutelspacher, Heike B. Neumann, and Thomas Schwarzpaul. *Kryptografie in Theorie und Praxis*. Vieweg + Teubner, Wiesbaden, revised edition, 2010. Mathematische Grundlagen für Internetsicherheit, Mobilfunk und elektronisches Geld. [Mathematical foundations for internet security, cellular phone networks and electronic money].

[2] Johannes Buchmann. *Introduction to cryptography*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, second edition, 2004.

[3] Johannes Buchmann. *Einführung in die Kryptographie*. Springer Spektrum Berlin, Heidelberg, 2016.

[4] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. *An introduction to mathematical cryptography*. Undergraduate Texts in Mathematics. Springer, New York, second edition, 2014.

[5] Simon Singh. *The Code Book*. Fouth Estate and Double Day, 1999.