Module INF-42-55-M-6

Protocols and Algorithms for Network Security (M, 4.0 LP)

Module Identification

Module Number	Module Name	CP (Effort)
INF-42-55-M-6	*Protocols and Algorithms for Network Security*	4.0 CP (120 h)

Basedata

CP, Effort	4.0 CP = 120 h
Position of the semester	1 Sem. irreg. WiSe
Level	[6] Master (General)
Language	[DE/EN] German or English as required
Module Manager	Schmitt, Jens, Prof. Dr. (PROF | DEPT: INF) (/staff/502/)
Lecturers	Schmitt, Jens, Prof. Dr. (PROF | DEPT: INF) (/staff/502/)
Area of study	[INF-VVS] Distributed and Networked Systems
Reference course of study	[INF-88.79-SG] M.Sc. Computer Science (/mhb/FB-INF/cos-536/)
Livecycle-State	[NORM] Active

Notice

Special tutorials and exams at Bachelor level for the course of studies 'Sozioinformatik'.

Courses

Type/SWS	Course Number	Choice in Module-Part	SL	PL	CP	Sem.
2V+1U	**INF-42-55-K-6** (/mhb/courses/INF-42-55-K-6/)	P	U-Schein	PL1	4.0	irreg. WiSe

- About **[INF-42-55-K-6]** (/mhb/courses/INF-42-55-K-6/): Title: "Protocols and Algorithms for Network Security"; Presence-Time: 42 h; Self-Study: 78 h

- About **[INF-42-55-K-6]** (/mhb/courses/INF-42-55-K-6/): The study achievement **"[U-Schein] proof of successful participation in the exercise classes (ungraded)"** must be obtained.
  - It is a prerequisite for the examination for PL1.

Examination achievement PL1

- Form of examination: **oral examination (20-60 Min.)**
- Examination Frequency: Examination only within the course
- Examination number: 64255 ("Protocols and Algorithms for Network Security")

Evaluation of grades

The grade of the module examination is also the module grade.

Contents

From [INF-42-55-K-6] Protocols and Algorithms for Network Security (/mhb/courses/INF-42-55-K-6/)**:**

- History of secure communication systems
- Symmetric cryptography: DES, 3DES, AES
- Asymmetric cryptography: RSA, Diffie-Hellman, El Gamal
- Cryptographic protocols: Secret Sharing, Needham-Schroeder, Kerberos, X.509

Competencies / intended learning achievements

After successfully completing the module, students will be able to

- explain the essential features of important cryptographic procedures
- apply cryptographic procedures in wired as well as wireless and mobile systems,
- compare the specifics of the different security protocols
- select suitable procedures to secure IT systems
- justify the use of appropriate security measures and protocols at the different network layers

Literature

From [INF-42-55-K-6] Protocols and Algorithms for Network Security (/mhb/courses/INF-42-55-K-6/)**:**

- G. Schäfer: Netzsicherheit, dpunkt Verlag, 2003.
- B. Schneier: Applied Cryptography, John Wiley & Sons, 2nd Edition, 1996.
- J. Buchmann: Einführung in die Kryptographie, Springer-Verlag, 1999.

Requirements for attendance of the module (informal)

None

Requirements for attendance of the module (formal)

None

References to Module / Module Number [INF-42-55-M-6]

Course of Study	Section	Choice/Obligation
[INF-88.79-SG] M.Sc. Computer Science (/mhb/FB-INF/cos-536/)	[Specialisation] Specialization 1	[WP] Compulsory Elective