Module Description AKE for Bachelor Study Course EI

Course	
Encryption for Internet of Things As current content of the lecture *Selected Topics of Electrical Engineering*	EIoT *(AKE)*
Verantwortlicher / Responsible	
Prof. Dr. Martin Schubert, Prof. Dr. Wai-Kong Lee (UTAR, MY)	
Verpflichtende Voraussetzungen / Mandatory requirements	
Basic technical studies, knowing the C language	
Empfohlene Vorkenntnisse / Recommended previous knowledge	
C programming languagen.	
Lehrform / Teaching method	
50% theory & computer-aided simulation, 50% practical training in the lab	
Time required in hours for classroom study and for independent study (divided into preparation, follow-up and exam preparation)	
56h direct teaching time by the instructor, 62h preparation and follow-up, 32h exam preparation	
Inhalte / Contents	
Part A: Seminaristic Classroom Teaching with Computer-Based Simulation*) 1. Security Challenges for IoT Applications 2. Secret Key Cryptography 3. Public Key Cryptography 4. Montgomery Exponentiation 5. Privacy Preserving Computation in IoT 6. Implementing Security in IoT System 7. Mini Project 8. Case Studies Part B: Practical Training 1. Implementing AES Encryption on a Microcontroller (MCU) 2. Implementing SHA-3 Hash Function on a Microcontroller 3. Implement RSA on a Microcontroller 4. Implement NTT for lattice-based cryptosystems on a Microcontroller 5. Implement NTRU or Saber on a Microcontroller	
Lernziele: Fachkompetenz / Learning objectives: Professional competence	
After successfully completing this module, the students are able to … • Understand the role of cryptography works on IoT applications. • Implement basic cryptography algorithms on a microcontroller. • Optimize the performance of cryptography algorithms on a microcontroller. • Understand some advanced cryptography algorithms to protect the future IoT applications.	
Lernziele: Persönliche Kompetenz / Learning objectives: Personal competence	
See preamble	

Angebotene Lehrunterlagen / Teaching materials offered
Lecture notes, practical instructions, assignment-based learning, journal/conference papers.
Lehrmedien / Teaching media
STM32 B-L475-IOT01 board, projector, electronics laboratory equipment (S081)
Literature
[1] https://docs.zephyrproject.org/latest/boards/st/disco_l475_iot1/doc/index.html [2] https://www.st.com/resource/en/user_manual/um2153-discovery-kit-for-iot-node-multichannel-communication-with-stm32l4-stmicroelectronics.pdf [3] Handbook of Applied Cryptography, https://cacr.uwaterloo.ca/hac/