# **Encryption**

## Exercise 5.1 ( ) ( )

- 1. Split into working groups of 3 or 4 students
- 2. Each group is assigned one of the topics (by consensus or randomization) described on the following slides
- 3. Every group prepares a digital presentation of 15-20min on their topic
- 4. At least 4 days before the presentation a PDF export of their slides is sent to bjoern.kimminich@nordakademie.de
- 5. All groups present their topic to all their classmates who can ask questions afterwards

### **Presentation Format**

- 15-20min presentation
  - o every group member has to present for at least 5min
- 5-10min Q&A
- ii The presentation can be written and held in  $\mathbb{H}$  or  $\blacksquare$  based on each group's own preference. Just do not mix English and German slides. English slides but presentation held in German is fine.

### **Presentation Topics**

- 1. WEP **FMS** & Chopchop
- 2. WPA2  $\neq$  KRACK
- 3. PGP  $\neq$  EFAIL
- 4. SSL/TLS ≠ POODLE & DROWN
- 5. BitLocker  $\neq$  TCG Opal
- The links provided are some documentation/specification (if publicly available) as well as vulnerability research papers. Each group is supposed to gather additional references as needed.

### **Presentation Structure**

- 1. Introduction of the protocol/system
- 2. Explanation of the attack(s)
- 3. Mitigation of the attack(s)
- 4. Recommendations or related information
- i Please provide a list of sources referred to in the presentation as the final slide.

### **Timeline**

- Thu, 17.10.2019 (today)
  - Group building & topic assignment
- Sun, 24.11.2019 (+5 weeks)
  - All PDF-exported presentations delivered to bjoern.kimminich@nordakademie.de
- Thu, 28.11.2019 (+4 days)
  - All groups present their topics between 09:15 and 11:45