Cryptography

Exercise 5.1 (🤝/📝/🏠)

1. Split into working groups of 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 *2 days before* the presentation a PDF export of the slides is uploaded on Moodle (once per group)
5. All groups present their topic to all their classmates who can ask questions afterwards

Presentation Format

- ~20-30 minutes presentation
  - *every* group member *has to* present for at least 5min
- ~5 minutes Q&A

ℹ️ *The presentation can be written and held in* 🇬🇧 *or* 🇩🇪 *based on each group's own preference. Just do not mix English and German slides. English slides but presentation held in German is fine.*

Topics

1. Cryptographic Hash Functions & Key derivation functions
2. Block Ciphers
3. Stream Ciphers
4. Asymetric-key Cryptography
5. Authenticated Encryption
6. Modern Protocols

Cryptographic Hash Functions & Key derivation functions

SHA-2, SHA-3, BLAKE2

scrypt, Argon2

- Introduction to the concept - what problems does it solve?
  - Disambiguation between hash functions and key derivation functions
- Description of the algorithm
- Known cryptographic issues
- Recommendations or related information

ℹ️ *Please provide a list of sources referred to in the presentation as the final slide.*

Block Ciphers

(**DES/3DES**), **AES/Rijndael**

- Introduction to concept of block ciphers
- Description of the algorithm
- Known cryptographic issues
- Recommendations or related information

ℹ️ *Please provide a list of sources referred to in the presentation as the final slide.*

ChCha20

- Introduction to concept of stream ciphers
- Description of the algorithm
- Known cryptographic issues
- Recommendations or related information

ℹ️ *Please provide a list of sources referred to in the presentation as the final slide.*

Asymetric-key Cryptography

RSA, Ed25519/X25519, ECDH

- Introduction to concept of asymetric-key cryptography
- Description of the algorithm
- Known cryptographic issues
- Recommendations or related information

Authenticated Encryption

ChaCha20-Poly1305, AES-[GCM, CCM, EAX]

- Introduction to concept of authenticated encryption
- Description of the algorithm
- Known cryptographic issues
- Recommendations or related information

ℹ️ *Please provide a list of sources referred to in the presentation as the final slide.*

Modern protocols

TLS [1.2, 1.3], Signal Protocol, Wireguard, Noise Protocol Framework

- Introduction to the protocol
  - Intended use
- Description of the used primitives
- Known cryptographic issues
- Recommendations or related information

ℹ️ *Please provide a list of sources referred to in the presentation as the final slide.*

Timeline

- Tue, 14.11.2023 *(today)*
  - Group building & topic assignment
- Sun, 03.12.2023 *(+3 weeks)*
  - All PDF-exported presentations uploaded on Moodle
- **Tue, 05.12.2023** and most likely **Tue, 19.12.2023** *(+2 days)*
  - **All groups present their topics** between 13:15 and 15:45