Foundations of Cryptology – Basismechanismen der Kryptographie

Topics for the talks:

- Block Cipher Modes beyond ECB, CBC, CFB, OFB, CTR
  - Authenticated Encryption (CCM, GCM, …)
  - Drive Encryption Modes
- Padding Schemes beyond 01…1 and 10…0
- Signcryption
- The "new" Hash-Standard SHA-3
  - Keccak
  - The Finalists
- Conference Keying
- Stream ciphers
- One-time digital signatures
- Multi Party Computations
- AES-Finalists
- …
- Own Ideas are very welcome!

Teasers @ April 5, 2016

- 5 minutes
- Title + 2 x content + references

Language:

- Slides have to be in English
- The talk may be given in German as well (depends on the class)