## SEMSTER PLAN

| SW | 1 | 2 | 3 | 4 | 5 | 6 | 7 | – | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Date | 20/02/26 | 27/02/26 | 06/03/26 | 13/03/26 | 20/03/26 | 27/03/26 | 03/04/26 | 10/04/26 | 17/04/26 | 24/04/26 | 01/05/26 | 08/05/26 | 15/05/26 | 22/05/26 | 29/05/26 | 05/06/26 | 12/06/26 |
| 8:20-11:55 | BTI4202 | BTI4202 | BTI4202 | BTI4202 | BTI4202 | BTI4202 | Karfreitag | UFZ | BTI4202 | BTI4202 | BTI4202 | BTI4202 | Auffahrt | BTI4201 | BTI4202 | BTI4202 | Finaltag |
| | Grothoff | Grothoff | Grothoff | Grothoff | Grothoff | Grothoff | | | Grothoff | Grothoff | Grothoff | Grothoff | | Haenni | Grothoff | Grothoff | |
| 12:45-16:00 | BTI4201 | BTI4201 | BTI4201 | BTI4201 | BTI4201 | BTI4201 | Karfreitag | UFZ | BTI4201 | BTI4201 | BTI4201 | BTI4201 | Auffahrt | BTI4201 | BTI4201 | BTI4201 | Finaltag |
| | Haenni | Haenni | Koenig | Haenni | Haenni | Haenni | | | Haenni | Koenig | Koenig | Koenig | | Koenig | Koenig | Koenig | |

## TOPICS

| SW | Dozent | Topic | Dozent | Topic |
|---|---|---|---|---|
| 1 | Grothoff | Introduction to Computer Security (Part I) | Haenni | Introduction Public-Key Cryptography |
| 2 | Grothoff | Introduction to Computer Security (Part II) | Haenni | Diffie-Hellman Key Exchange, Man-in-the-Middle |
| 3 | Grothoff | Distributed Systems | Koenig | Definitions and Terminology, Classical Ciphers |
| 4 | Grothoff | Availability & Key Management | Haenni | Mathematics for Public-Key Cryptography |
| 5 | Grothoff | Blockchains & Secure Integration | Haenni | Algorithms and Hardness Assumptions |
| 6 | Grothoff | Secure Channels | Haenni | Public-Key Encryption (RSA, ElGamal) |
| 7 | | | Karfreitag | |
| – | | | UFZ | |
| 8 | Grothoff | Certificates and Trust (X.509) | Haenni | Digital Signatures (RSA, DSA) |
| 9 | Grothoff | Centralized Public-Key Infrastructures | Koenig | Pseudo-Random Number Generators |
| 10 | Grothoff | Decentralized Public-Key Infrastructures | Koenig | True Random Number Generators |
| 11 | Grothoff | Anonymity | Koenig | Hash Algorithms and Keyed Hashing |
| 12 | | | Auffahrt | |
| 13 | Haenni | Elliptic Curves | Koenig | Symmetric Encryption |
| 14 | Grothoff | Blind Signatures | Koenig | Authenticated Encryption 1 |
| 15 | Grothoff | GNU Taler | Koenig | Authenticated Encryption 2 |
| 16 | | | Finaltag | |

x

## HOURS

| BTI4201 | Weeks | Hours | Prozent | ILV |
|---|---|---|---|---|
| Haenni | 7 | 28 | 50 | 104 |
| Koenig | 7 | 28 | 50 | 104 |
| Grothoff | 0 | 0 | 0 | 0 |
| **Total** | 14 | 56 | 100 | 208 |

| BTI4202 | Weeks | Hours | Prozent | ILV |
|---|---|---|---|---|
| Haenni | 0 | 0 | 0 | 0 |
| Koenig | 0 | 0 | 0 | 0 |
| Grothoff | 12 | 48 | 100 | 208 |
| **Total** | 12 | 48 | 100 | 208 |

**Version 1.3**