ITSecurity Public Encryption and Hashing: Agenda

Michael Claudius, Associate Professor, Roskilde

31.08.2024

Agenda of Today

- ***Introduction of todays hard work***

1. **Agenda of today and topics (5 min)**
2. **Lecture: Asymmetric Keys Principle (10 min)**
3. **Lecture: RSA (10 min)**
4. **Lecture: Diffie-Hellman (15 min)**
5. **Rehearsal of Homework 1 (15 min)**
6. **Wireshark (30 min)**
7. **Exercise: CrypTool No.2 (45 min)**
8. **LUNCH break**
9. **Lecture: Hash function and MAC (10 min)**
10. **Lecture: SHA512 (30 min)**
11. **Exercise: Certificates No. 1 (45 min)**
12. **Exercise: Certificates No. 2 (45 min)**

- ***A.O.B.: See you next week ☺***

Agenda done

- **So Agenda done, lets get started on the core lectures.**