

## t.ISI - Internet-Sicherheit

---

**Person responsible for the course:** Marc Rennhard, rema  
**Responsible OU:**  
**ECTS:** 4  
**Valid for:** 2012/2013  
**Last saved:** 22.01.2013 16:12

---

### Expertise:

-

---

### Methodological skills:

-

---

### Social skills:

-

---

### Personal skills:

-

---

### Learning objectives:

Today, virtually every IT system has certain security requirements, in particular if the system is exposed and reachable over the network (e.g. the Internet). In this module, you'll learn the foundations of IT security, to secure IT systems and to analyse them with respect to security. In detail, the students will get the following competencies:

- You understand the basics of cryptology (algorithms, usage areas, resistance to attacks), which build the foundation for a large number of modern security technologies.
  - You master the modern protocols and methods to secure communications and access to systems and applications and can apply them adequately.
  - In particular, you understand the possibilities and limitations of these protocols and methods with respect to security they provide.
  - You master procedures to analyse systems and to attack systems by exploiting vulnerabilities and can apply such procedures on your own.
- 

### Course content:

Theorie Cryptology (10 lessons):

- Secret- and Public-Key Cryptography
- Authentication, Integrity, Digital Signatures
- Certificates, Public Key Infrastructure

Theorie Methods and Protocols (18 lessons):

- Layer 1 & 2 Security, Wireless LAN Security
-

- End-to-End Security (SSL/TLS, IPsec), Virtual Private Networks
- Authentication Protocols (NTLM, Kerberos, Shibboleth)
- Firewalls, Access Control Mechanisms (DAC, MAC, RBAC)
- E-Mail Security (S/MIME, PGP)

Lab Exercises:

- Secret-Key Cryptography
- Public-Key Cryptography and Hash Functions
- Network Attacks
- Firewalls & Portscans
- Intrusion Detection with Snort and Prelude
- Apache Web Server Hardening and Digital Certificates
- AUthorization in Linux

**Previous knowledge:**

KT1 (Kommunkationstechnik 1)

**Teaching method:**

Type of lesson:	Number of lessons per week:
Lecture	14*2
Tutorial/Practicum	14*2
Block instruction	

**Assessment:**

According to the table or as specified in writing by the lecture at the beginning of the semester!

description	type	form	scope	assessment	weighting
Performance records during school hours	Graded labs	Written and orally	All labs	Points that are added to the points achieved in the final exam	20%
Semester end exam	Test	Written	90 minutes	Grading	80%

**Language of instruction:**

Deutsch

**Instruction material:**

Slides with additional, elaborate comments

**Additional literature:**

For further education: Charlie Kaufmann, Radia Perlman, Mike Speciner, Network Security, Second Edition, Prentice Hall, ISBN 0130460192

**Comments:**

-