Eötvös Loránd University

SUBJECT

Title
Cryptographic protocols

Type of instruction
lecture + practical

Level
master

Faculty
Faculty of Informatics

Part of degree program
Credits
4

Recommended in
Semester 1/3

Typically offered in
Autumn semester

Course description
This course gives an overview of the basic building blocks used to engineer cryptographic protocols, and discusses in details the operation of mainstream cryptographic protocols used in wired and wireless computer networks. In particular, TLS and IPsec are covered, as well as security protocols in WiFi networks. We also study protocols used in emerging wireless networks, such as wireless sensor networks and RFID systems.

- Basic concepts and crypto primitives
- Block encryption modes
- Message authentication and authenticated encryption
- Key exchange protocols
- Random number generation
- Verification of key exchange protocols with ProVerif
- Public Key Infrastructres
- TLS
- WiFi security
- IPsec
- Security protocols for wireless sensor networks
- Secure routing and wormhole detection
- RFID security and privacy

Readings

- G. Schaefer, Security in Fixed and Wireless Networks, Wiley, 2004.
- J. Edney and W. A. Arbaugh, Real 802.11 Security: WiFi Protected Access and 802.11i, Addison-Wesley, 2003.
- L. Buttyán, JP. Hubaux, Security and Cooperation in Wireless Networks, Cambridge University Press, 2008.
- J. Lopez and Z-H. Zhou (eds), Wireless Sensor Network Security, IOS Press, 2008.
- A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.