Cryptography today

Program of the course

1. Introduction to cryptography
   a) confidentiality, authenticity, integrity
   b) principles and ingredients
   c) Caesar and One-Time-Pad ciphers
   d) Kerchoff's principle
   e) crypto-analysis
   f) algorithm types: symmetric, a-symmetric, hash
2. Symmetric algorithm
   a) blocks and stream
   b) principal symmetric algorithms
   c) DES
   d) AES
3. A-symmetric algorithms
   a) general principles
   b) introduction to RSA
   c) use of public and private keys
4. Hash algorithms
   a) principles of a cryptographic hash algorithm
   b) MAC and H-MAC
   c) from MD5 and SHA1 to SHA-256 etc.
5. Cryptographic protocols
   a) confidentiality
   b) authenticity
   c) integrity
   d) combined used of the algorithms

6. OpenPGP
   a) OpenPGP protocol
   b) web of trust
   c) key management
   d) format of the signed/encrypted documents
   e) use examples [practical demonstration]
   f) electronic mail and OpenPGP
7. Certification Authority and Openssl
   a) digital certificates
   b) create a CA with Openssl
   c) create certificates with Openssl
   d) use examples [practical demonstration]
   e) using a digital certificate for web navigation
   f) real security of web navigation protected by a PKI