

---

# Sicurezza nelle reti di telecomunicazioni

## Finalità

The objective of this course is to analyze the main mechanisms and protocols for network security. It deals with the bases of modern cryptography, the various security protocols, possible network threats, and secure countermeasures.

## Programma

1) Introduction to modern cryptography

Symmetric cryptography (3DES, AES, etc) and asymmetric cryptography (RSA, Diffie-Hellman)

Hash functions and Message digest

Digital signature, digital certificates, certification authorities, X.509/ PKI (Public Key Infrastructure) and PGP (Pretty Good Privacy)

2) Protocols for network security

Authentication protocols (CHAP, EAP, RADIUS, Diameter)

Communication security at IP layer (IPSec), and transport/application layer (TLS, SSH)

Virtual Private Networks

Security in wireless local access (IEEE 802.1x, IEEE 802.11i)

3) TCP/IP vulnerabilities

Possible attacks and countermeasures (sniffing, network and port scanning, IP spoofing, flooding, buffer overflow, etc)

4) Network security

Firewalls (packet filtering, application level gateways, proxy, NAT, bastion host, DMZ), and

Intrusion Detection Systems (IDS)

## Attività d'esercitazione

Laboratory activities on vulnerability scanning, firewall configuration, digital certificate management, VPN/IPSec configuration, and other topics.

## Propedeuticità

Familiarity with TCP/IP stack and networking. One of these courses is suggested: Reti di Telecomunicazioni A, Telematica A, or Reti di Calcolatori A

## Testi consigliati

[1] W. Stallings, "Cryptography and Network Security: Principles and Practice" 3th Edition, Prentice Hall

[2] C. Kaufman, R. Perlman, M. Speciner, "Network Security: Private Communication in a Public World" 2nd Edition, Prentice Hall