Titolo insegnamento (IT)	Reti e Sicurezza Informatica
Name of the course (EN)	Networks and Computer Security
Settore Scientifico Disciplinare (SSD) di Riferimento	Informatica - INF/01
Numero moduli / # of modules	2 (Part I, security basics; Part II practical network and computer security)
Numero ore di didattica assistita / Course duration	96h: 48 ore di didattica frontale + 48 ore di attività di laboratorio/48h lectures + 48h laboratory
Orario ricevimento studenti / Office hours	Lunedì/Monday h15:00 - 17:00
Email del docente / Teacher's e-mail	ianni@unical.it
Telefono/Phone	0984-496430

IT(Italiano)	**EN(English)**
Obiettivi formativi - Risultati di apprendimento attesi- Learning goals	
1. Capacità di mettere in sicurezza un sistema informatico (distribuito e non) a livello applicazione, trasporto, rete e link; 2. Conoscenza delle principali modalità di intrusione nei sistemi informatici e delle relative contromisure; 3. Conoscenze delle metodologie e dei sistemi di sicurezza basati su crittografia asimmetrica e simmetrica, con particolare attenzione ai requisiti di riservatezza e autenticità nella trasmissione dati;	1. Acquiring skills in securing a (distributed) computer system at the application, transport, network and link layers. 2. Understanding basic intrusion techniques against information systems and their related countermeasures. 3. Understanding methodologies and security systems based on asymmetric and symmetric cryptography techniques, especially focused on the requirements of confidentiality and authenticity of data transmission.

Prerequisiti / Skills required for attending the course	
Conoscenza delle architetture dei Sistemi Operativi, delle Reti di Calcolatori e dei Sistemi Informativi. Conoscenza dei paradigmi e dei linguaggi di programmazione di uso comune	Knowledge of Operating Systems and Computer Networks architectures. Knowledge of Information Systems Architectures. Computer Programming

Programma del corso - Course Programme	
Prima parte (Modulo I) Obiettivo del modulo è di introdurre alcune nozioni di base legate ai requisiti che un sistema informatico sicuro deve avere. Vengono inoltre illustrati i principali strumenti di crittografia oggi disponibili. • Requisiti di un sistema sicuro: autenticità, riservatezza, garanzia del servizio • Cenni agli algoritmi a chiave simmetrica: DES, 3DES, AES, RC4. Modalità di cifratura. Generazione di numeri casuali e pseudocasuali. • Cenni agli algoritmi a chiave asimmetrica: RSA • Algoritmi di handshake sicuro: Diffie-Helmann, RSA • Certificati digitali: cenni alle implicazioni legali, autorità di certificazione, PKI. • Funzioni MAC (Message Authentication Code) e Hash. • Cenni ai principali algoritmi MAC e Hash: MD5, SHA. • Firma digitale, Firma di un documento. • Metodologie di autenticazione: RADIUS, Kerberos. Laboratorio • Implementazione di conversazioni dati riservate • Installazione e messa in opera di un server SSL. • Installazione e messa in opera di una semplice Certification Authority • Generazione coppia chiavi pubblica/privata • Richiesta, Firma e Installazione di certificati digitali Seconda Parte (Modulo II) In questo modulo viene ripreso in esame lo stack ISO/OSI (con particolare riferimento allo stack TCP/IP), discutendo i problemi di sicurezza e riservatezza su ciascun livello. • Richiami alle principali modalità di intrusione e contraffazione: MAC/IP Spoofing, DNS spoofing. Sniffing, man-in-the-middle. Attacchi DOS. • Sicurezza a livello di rete - protocollo IPsec. Protocollo DNSSec. Proxy servers, NAT. • Sicurezza a livello di trasporto - protocollo SSL, Virtual Private Networks. • Sicurezza a livello applicazione - HTTPS, POP3/IMAP/SMTP over SSL. • Virus Informatici: Modalità di propagazione, allegati non sicuri, falle di sicurezza, buffer overflow, trojans, javascript, controlli activeX, modifica di	Part I The first module aims at introducing basic notions related to the security requirements for information systems. Moreover, the state of the art in encryption tools is presented. Lectures: Security requirements for informativon systems: authenticity, confidentiality, service assurance. Introduction on symmetric-key algorithms: DES, 3DES, AES, RC4. Methods of encryption. Random and pseudorandom number generators. Introduction on asymmetric-key algorithms: RSA Secure handshake algorithms: Diffie-Helmann, RSA I Digital certificates: outline on legal issues, certification authorities, PKI. MAC (Message Authentication Code) functions and cryptographic hash functions. The main MAC and Hash algorithms : MD5, SHA. Digital signature, signature of documents and messages. Authentication methods: RADIUS, Kerberos. Laboratory: Implementing a confidential data conversation. Installing and setting up an SSL server. Installing and setting up of a Certification Authority. Generating a public/private pair of keys. Requesting, Signing and installing digital certificates. Part II In Part II it is discussed the ISO/OSI stack (in particular the TCP/IP stack) focusing on the security problems and confidentiality issues related to each layer. Main intrusion and counterfeiting attacks: MAC/IP Spoofing, DNS spoofing. Sniffing with man-in-the-middle attacks. DOS attacks. Network and link layer Security - IPsec protocol. DNSSec protocol. Proxy servers, NAT and firewall traversal. Transport layer Security - SSL protocol, Virtual Private Networks. Application layer Security - HTTPS, POP3/IMAP/SMTP over SSL. Attacks to hosts and viruses: propagation

entry point in codice binario. Tipologie di payload: keyloggers, dialers, web server spoofing, spyware. • Social engineering, SQL injection e defacing.	mechanism, insecure attachments, security flaws, buffer overflow, trojans, javascript, activeX controls, entry point modification by means of binary code. Payloads: keyloggers, dialers, web server spoofing, spyware. Social engineering, SQL injection and defacing. Password storage and maintainance.

Testi di riferimento - Reference material	
Stallings & Brown. Computer Security: Principles and Practice, Prentice Hall. William Stallings, Cryptography and network security, 4th Ed., McGraw-Hill. Materiale didattico disponibile sul sito del corso.	Stallings & Brown. Computer Security: Principles and Practice, Prentice Hall. William Stallings, Cryptography and network security, 4th Ed., McGraw-Hill. Teaching notes and material available on the course web site.

Attività di apprendimento e metodologie didattiche - Teaching method	
Lezioni frontali interattive, esercitazioni guidate in laboratorio, esercitazioni autonome	Interactive front lectures, guided and self-learning laboratory sessions

Metodi e criteri di accertamento del profitto - Assessment method	
Preparazione di un seminario e di una dimostrazione funzionante; Esame Orale	Preparation of a talk and an operational demonstration; Oral exam