



UNIVERSITÀ DEGLI STUDI DI PALERMO

DIPARTIMENTO	Ingegneria
ANNO ACCADEMICO OFFERTA	2015/2016
ANNO ACCADEMICO EROGAZIONE	2016/2017
CORSO DILAUREA MAGISTRALE	INGEGNERIA DELLE TELECOMUNICAZIONI
INSEGNAMENTO	SERVIZI E SICUREZZA SU INTERNET
TIPO DI ATTIVITA'	B
AMBITO	50362-Ingegneria delle telecomunicazioni
CODICE INSEGNAMENTO	16978
SETTORI SCIENTIFICO-DISCIPLINARI	ING-INF/03
DOCENTE RESPONSABILE	GALLO PIERLUIGI Professore Associato Univ. di PALERMO
ALTRI DOCENTI	
CFU	12
NUMERO DI ORE RISERVATE ALLO STUDIO PERSONALE	192
NUMERO DI ORE RISERVATE ALLA DIDATTICA ASSISTITA	108
PROPEDEUTICITA'	
MUTUAZIONI	
ANNO DI CORSO	2
PERIODO DELLE LEZIONI	2° semestre
MODALITA' DI FREQUENZA	Facoltativa
TIPO DI VALUTAZIONE	Voto in trentesimi
ORARIO DI RICEVIMENTO DEGLI STUDENTI	GALLO PIERLUIGI Venerdì 15:00 17:00 Ufficio del docente

DOCENTE: Prof. PIERLUIGI GALLO

PREREQUISITI	
RISULTATI DI APPRENDIMENTO ATTESI	Conoscenza e capacità di comprensione Al termine del corso l'allievo avrà acquisito le conoscenze sui servizi applicativi su Internet. In particolare conoscerà i servizi offerti in mobilità, sia di rete che di terminale, i servizi VoIP ed i protocolli relativi al web ed al trasferimento dei dati. I risultati attesi riguardano anche la capacità di valutare soluzioni architetturali per il WEB, il VoIP e per i servizi multimediali. Saranno inoltre forniti gli strumenti matematici e gli algoritmi più diffusi per la sicurezza, la segretezza e la confidenzialità. Gli allievi, oltre alla comprensione delle tematiche relative al corso, acquisiranno l'uso del linguaggio tecnico e la capacità di applicare in autonomia le metodologie e gli strumenti proposti. Capacità di applicare conoscenza e comprensione Le conoscenze spiegate durante le lezioni frontali verranno applicate in modo guidato durante le esercitazioni. Gli studenti applicheranno tali conoscenze in modo autonomo, durante la stesura della tesina o durante lo svolgimento della prova scritta. Autonomia di giudizio Gli allievi saranno in grado di affrontare in autonomia problemi riguardanti gli argomenti del corso e prendere le opportune decisioni per trovare le relative soluzioni. Lo svolgimento delle esercitazioni costituirà, per l'allievo, un rinforzo delle conoscenze e abilità acquisite e costituirà uno strumento con cui egli potrà compiere un'autovalutazione del livello raggiunto. Abilità comunicative L'allievo sarà capace di esporre con padronanza di linguaggio e con chiarezza le caratteristiche dei protocolli e delle architetture applicative. Egli saprà dunque interloquire con colleghi progettisti e con i tecnici per affrontare e risolvere problemi del settore. Capacità d'apprendimento La capacità di apprendimento degli allievi verrà stimolata con l'uso di tecniche quali il project work, il cooperative learning ed il brain-storming, utilizzate soprattutto durante le fasi di esercitazione. Lo studente sarà in grado di approfondire in modo autonomo gli argomenti affrontati.
VALUTAZIONE DELL'APPRENDIMENTO	La valutazione degli allievi sarà effettuata con differenti modalità: prova orale, tesina, discussione di un articolo scientifico. Tale molteplicità di strumenti consentirà di valutare i risultati attesi. In particolare, la conoscenza e la capacità di comprensione verranno valutate mediante la prova orale e la realizzazione di una tesina. L'autonomia di giudizio e le capacità comunicative saranno valutate mediante la discussione di un articolo scientifico. Le capacità di apprendimento e di applicare conoscenza e comprensione saranno oggetto di (i) autovalutazione da parte dell'allievo, durante le attività di esercitazione proposte dal docente; (ii) valutazione da parte del docente sulla base di una applicazione da progettare e realizzare secondo le richieste del docente.
OBIETTIVI FORMATIVI	Il corso, destinato agli studenti della laurea magistrale, ha lo scopo di formare gli allievi sulle architetture, i protocolli, gli strumenti per i servizi applicativi su Internet. Agli aspetti teorici verranno affiancati anche quelli tecnologici per la realizzazione di sistemi e di test-bed per la fornitura di tali servizi. Verranno inoltre trattati gli aspetti di integrazione tra la rete Internet ed il mondo delle reti cellulari introducendo l'IP Multimedia Subsystem.
ORGANIZZAZIONE DELLA DIDATTICA	Durante il corso saranno impartite lezioni frontali per stimolare la conoscenza e la capacità di comprensione ed esercitazioni teoriche per favorire la capacità d'apprendimento e di problem solving. Le attività di laboratorio, in parte svolte in gruppo, consentiranno agli allievi di esercitare la capacità di applicare conoscenza e comprensione, aumentare l'autonomia di giudizio e migliorare le abilità comunicative tra gli allievi.
TESTI CONSIGLIATI	Materiale fornito dal docente. William Stallings, "Crittografia e sicurezza delle reti"

PROGRAMMA

ORE	Lezioni
2	Sicurezza: attacchi, servizi, meccanismi, modelli.

PROGRAMMA

ORE	Lezioni
14	Applicazioni per la sicurezza delle reti (cenni) X.509 PGP S/MIME IPSec Secure Socket Layer (SSL) Transport Layer Security (TLS)
26	Il protocollo IPv6: Indirizzamento, formato del pacchetto e differenze con IPv4 Scenari d'uso in IPv6 I protocolli applicativi HTTP, FTP, Jabber Proxing e content filtering Architetture, protocolli e dispositivi per il VoIP SIP/SDP
14	La posta elettronica certificata Il video streaming Problematiche legate alle applicazioni real-time Localizzazione e geo-referenziazione Tecniche di programmazione di rete
19	Crittografia simmetrica Tecniche di sostituzione e trasposizione Cifratura a blocchi ed il Data Encryption Standard (DES) Richiami sui campi finiti Advanced Encryption Standard (AES) Cifrate simmetriche contemporanee
19	Crittografia a chiave pubblica Introduzione alla teoria dei numeri Algoritmo di Rivest, Shamir Adleman (RSA) La gestione delle chiavi Message Authentication Code (MAC)
8	Algoritmi hash Message Digest Algorithm (MD5) Secure Hash Algorithm (SHA) Firma digitale Digital Signature Algorithm (DSA)