| | |
|---|---|
| **STRUTTURA** | Scuola Politecnica - DEIM |
| **ANNO ACCADEMICO** | 2015/16 |
| **CORSO DI LAUREA MAGISTRALE** | Ingegneria delle Telecomunicazioni |
| **INSEGNAMENTO** | Servizi e sicurezza su internet |
| **TIPO DI ATTIVITÀ** | Caratterizzante |
| **AMBITO DISCIPLINARE** | Ingegneria delle Telecomunicazioni |
| **CODICE INSEGNAMENTO** | 16978 |
| **ARTICOLAZIONE IN MODULI** | No |
| **NUMERO MODULI** | |
| **SETTORI SCIENTIFICO DISCIPLINARI** | ING-INF/03 |
| **DOCENTE RESPONSABILE** | Pierluigi GALLO<br>Ricercatore Universitario<br>Università degli Studi di Palermo |
| **CFU** | 12 |
| **NUMERO DI ORE RISERVATE ALLO STUDIO PERSONALE** | 192 |
| **NUMERO DI ORE RISERVATE ALLE ATTIVITÀ DIDATTICHE ASSISTITE** | 108 |
| **PROPEDEUTICITÀ** | Reti di calcolatori e internet |
| **ANNO DI CORSO** | II |
| **SEDE DI SVOLGIMENTO DELLE LEZIONI** | Consultare il sito politecnica.unipa.it |
| **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.<br>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. |
| **MODALITÀ DI FREQUENZA** | Facoltativa |
| **METODI DI VALUTAZIONE** | 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.<br>**L'autonomia di giudizio e le capacità comunicative** saranno valutate mediante la discussione di un articolo scientifico.<br>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. |
| **TIPO DI VALUTAZIONE** | Voto in trentesimi |
| **PERIODO DELLE LEZIONI** | Consultare il sito politecnica.unipa.it |
| **CALENDARIO DELLE ATTIVITÀ DIDATTICHE** | Consultare il sito politecnica.unipa.it |
| **ORARIO DI RICEVIMENTO DEGLI STUDENTI** | Previo appuntamento concordato via e-mail |

**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 piú 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.

**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.

| | **SERVIZI E SICUREZZA SU INTERNET** |
|---|---|
| **ORE FRONTALI** | **LEZIONI FRONTALI** |
| 2 | Sicurezza: attacchi, servizi, meccanismi, modelli. |
| | **Crittografia simmetrica** |
| 2 | Tecniche di sostituzione e trasposizione |
| 2 | Cifratura a blocchi ed il Data Encryption Standard (DES) |
| 2 | Richiami sui campi finiti |
| 2 | Advanced Encryption Standard (AES) |
| 2 | Cifrature simmetriche contemporanee |
| | **Crittografia a chiave pubblica** |
| 3 | Introduzione alla teoria dei numeri |
| 3 | Algoritmo di Rivest, Shamir Adleman (RSA) |
| 3 | La gestione delle chiavi |
| 3 | Message Authentication Code (MAC) |
| | **Algoritmi hash** |
| 2 | Message Digest Algorithm (MD5) |
| 2 | Secure Hash Algorithm (SHA) |
| | **Firma digitale** |
| 2 | Digital Signature Algorithm (DSA) |
| | **Applicazioni per la sicurezza delle reti (cenni)** |
| 2 | X.509 |
| 1 | PGP |
| 1 | S/MIME |
| 1 | IPSec |
| 1 | Secure Socket Layer (SSL) |
| 1 | Transport Layer Security (TLS) |
| 2 | Richiami sulla pila OSI |
| 5 | Il protocollo IPv6: Indirizzamento, formato del pacchetto e differenze con IPv4 |
| 3 | Scenari d'uso in IPv6 |
| 4 | I protocolli applicativi HTTP, FTP, Jabber |
| 3 | Proxing e content filtering |
| 5 | Architetture, protocolli e dispositivi per il VoIP |
| 4 | SIP/SDP |
| 5 | Le reti peer-to-peer |
| 1 | La posta elettronica certificata |
| 3 | Il video streaming |
| 3 | Problematiche legate alle applicazioni real-time |
| 2 | Localizzazione e geo-referenziazione |
| 5 | Tecniche di programmazione di rete |
| | **ESERCITAZIONI** |
| 3 | La piattaforma Asterisk |
| 2 | Strumenti per lo sniffing di rete e per la visualizzazione dei pacchetti (wireshark, live http, ...) |
| 10 | Java nella programmazione di rete |
| 2 | Setup e configurazione di un server di streaming |
| | **SEMINARI E DIBATTITI GUIDATI** |
| 9 | Seminari e dibattiti guidati su temi di ricerca in robotica anche con la partecipazione di esperti del settore |
| | |
| **TESTI CONSIGLIATI** | [1] Materiale fornito dal docente.<br>[2] William Stallings, “Crtittografia e sicurezza delle reti” |