| | |
|---|---|
| **STRUTTURA** | Scuola Politecnica - DICGIM |
| **ANNO ACCADEMICO** | 2015/2016 |
| **CORSO DI LAUREA MAGISTRALE** | Ingegneria Informatica |
| **INSEGNAMENTO** | Sistemi di Elaborazione delle Informazioni |
| **TIPO DI ATTIVITÀ** | Caratterizzante |
| **AMBITO DISCIPLINARE** | Ingegneria Informatica |
| **CODICE INSEGNAMENTO** | 06461 |
| **ARTICOLAZIONE IN MODULI** | NO |
| **NUMERO MODULI** | 1 |
| **SETTORI SCIENTIFICO DISCIPLINARI** | ING-INF/05 |
| **DOCENTE RESPONSABILE** | Giuseppe Lo Re<br>Professore Associato<br>Università di Palermo |
| **CFU** | 12 |
| **NUMERO DI ORE RISERVATE ALLO STUDIO PERSONALE** | 192 |
| **NUMERO DI ORE RISERVATE ALLE ATTIVITÀ DIDATTICHE ASSISTITE** | 108 |
| **PROPEDEUTICITÀ** | Nessuna |
| **ANNO DI CORSO** | Secondo |
| **SEDE DI SVOLGIMENTO DELLE LEZIONI** | Consultare il sito politecnica.unipa.it |
| **ORGANIZZAZIONE DELLA DIDATTICA** | Lezioni frontali;<br>Analisi e discussione in aula di casi di studio;<br>Esercitazioni teoriche;<br>Esercitazioni di gruppo per progetti;<br>Presentazioni e discussioni in aula di progetti e implementazioni;<br>Dibattiti guidati in aula su temi di ricerca. |
| **MODALITÀ DI FREQUENZA** | Facoltativa |
| **METODI DI VALUTAZIONE** | Prova Scritta, Presentazione di una Tesina, Prova Orale, |
| **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** | Martedi 15-17 |

**RISULTATI DI APPRENDIMENTO ATTESI**

Conoscenza e capacità di comprensione (*knowledge and understanding*):

- Lo studente, al termine del corso, avrà acquisito conoscenze e metodologie per affrontare problematiche riguardanti temi di networking avanzato e sicurezza delle reti. Lo studente sarà in grado di analizzare reti di calcolatori wireless, reti per la distribuzione di contenuti multimediali, sistemi di gestione di rete e soprattutto tutti gli aspetti legati alla sicurezza delle informazioni trasferite in rete.

Conoscenza e capacità di comprensione applicate (*applying knowledge and understanding*):

- Lo studente avrà acquisito conoscenze e metodologie per collaudare, progettare e realizzare sistemi di trasmissione wireless, sistemi per la gestione e distribuzione di contenuti multimediali, sistemi per la gestione di reti complessi, apparati di sicurezza per la

trasmissione di informazione in rete.

Autonomia di giudizio (*making judgements*)

- Lo studente avrà acquisito una metodologia di analisi dei meccanismi che garantiscono la sicurezza di un sistema di trasmissone dei dati in Internet. Sarà inoltre in grado di giudicare la bontà di progetti di reti wireless e di reti per la distribuzione di contenuti multimediali.

Abilità comunicative (*communication skills*)

- Lo studente sarà in grado di comunicare con competenza e proprietà di linguaggio problematiche complesse di networking avanzato e di sicurezza delle trasmissioni di dati in Internet in contesti altamente specializzati.

Capacità di apprendere (learning skills)

- Lo studente sarà in grado di affrontare con autonomia qualsiasi problematica relativa alla sicurezza delle reti di calcolatori e agli argomenti avanzati di networking. Sarà in grado di indagare sulle tecniche di crittografia dei dati, di firma digitale, di autenticazione, di integrità e di non ripudiabilità.

**OBIETTIVI FORMATIVI**

Il corso si propone di fornire allo studente i concetti di base nell'ambito di sistemi distribuiti e e della sicurezza dei sistemi di elaborazione. Nella prima parte sono illustrate i concetti e le architetture generali. Nella seconda parte, relativa alla Sicurezza dei Sistemi di Elaborazione, sono illustrate le tecniche di crittografia e la loro applicazioni ai vari aspetti della sicurezza informatica.

| **ORE FRONTALI** | **LEZIONI FRONTALI** |
|---|---|
| 4 | Sicurezza delle Reti |
| 6 | Elementi di Crittografia |
| 6 | Cifratura a chiave simmetrica DES, AES |
| 3 | Generazione di numeri Pseudo-casuali |
| 6 | Cifratura a chiave pubblica, RSA. |
| 4 | Autenticazione dei messaggi e funzione SHA-1 |
| 4 | Codici di autenticazione dei Messaggi |
| 4 | Firma Digitale |
| 6 | Applicazioni di autenticazione: Kerberos. |
| 3 | Sicurezza della posta elettronica |
| 4 | Sicurezza a livello rete. |
| 3 | Sicurezza WEB |
| 3 | Firewall |
| 3 | Sicurezza dei sistemi Informatici |
| 4 | Sicurezza delle Reti Wireless |
| **63** | |
| | |
| | **ESERCITAZIONI** |
| 45 | Esercitazioni sugli argomenti del corso |
| | |
| **TESTI CONSIGLIATI** | William Stallings – Crittografia e Sicurezza nelle Reti, McGraw-Hill, 5 edizione<br>William Stallings, and Lawrie Brown - *Computer Security*: Principles and Practice , 1/e |