



UNIVERSITÀ DEGLI STUDI DI PALERMO

| | |
|---|--|
| DIPARTIMENTO | Ingegneria |
| ANNO ACCADEMICO OFFERTA | 2016/2017 |
| ANNO ACCADEMICO EROGAZIONE | 2017/2018 |
| CORSO DILAUREA MAGISTRALE | INGEGNERIA INFORMATICA |
| INSEGNAMENTO | SICUREZZA DEI SISTEMI DI ELABORAZIONE DELL'INFORMAZIONE |
| TIPO DI ATTIVITA' | B |
| AMBITO | 50369-Ingegneria informatica |
| CODICE INSEGNAMENTO | 18539 |
| SETTORI SCIENTIFICO-DISCIPLINARI | ING-INF/05 |
| DOCENTE RESPONSABILE | LO RE GIUSEPPE Professore Ordinario 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 | Annuale |
| MODALITA' DI FREQUENZA | Facoltativa |
| TIPO DI VALUTAZIONE | Voto in trentesimi |
| ORARIO DI RICEVIMENTO DEGLI STUDENTI | LO RE GIUSEPPE Martedì 15:00 17:00 |

DOCENTE: Prof. GIUSEPPE LO RE

| | |
|--|--|
| PREREQUISITI | Reti di Calcolatori e Sistemi Operativi |
| RISULTATI DI APPRENDIMENTO ATTESI | <p>Conoscenza e capacita' di comprensione (knowledge and understanding): Lo studente, al termine del corso, avra' acquisito conoscenze e metodologie per affrontare problematiche legate alla sicurezza dei sistemi di elaborazione delle informazioni. Lo studente sara' in grado di analizzare algoritmi di cifratura a chiave simmetrica e pubblica, protocolli ed applicazioni di autenticazione, sicurezza della posta elettronica e del Web, e tutti gli aspetti legati alla sicurezza dei sistemi informatici.</p> <p>Conoscenza e capacita' di comprensione applicate (applying knowledge and understanding): Lo studente avra' acquisito conoscenze e metodologie per collaudare, progettare e realizzare sistemi informatici sicuri che facciano uso delle tecniche e degli strumenti analizzati durante il corso.</p> <p>Autonomia di giudizio (making judgements): Lo studente avra' acquisito una metodologia di analisi dei meccanismi che garantiscono la sicurezza di un sistema informatico e sara' in grado di giudicare la validita' di progetti di sistemi sicuri per l'elaborazione delle informazioni.</p> <p>Abilita' comunicative (communication skills): Lo studente sara' in grado di discutere con competenza e proprieta' di linguaggio problematiche complesse legate alla sicurezza dei sistemi informatici di elaborazione delle informazioni e delle reti.</p> <p>Capacita' di apprendere (learning skills): Lo studente sara' in grado di affrontare con autonomia qualsiasi problematica relativa alla sicurezza dei sistemi informatici e di networking. Sara' in grado di indagare sulle tecniche di crittografia dei dati, di firma digitale, di autenticazione, di integrita' e di non ripudiabilita'.</p> |
| VALUTAZIONE DELL'APPRENDIMENTO | Le conoscenze e le competenze acquisite dallo studente saranno verificate attraverso una prova scritta e un colloquio orale. La prova scritta sara' costituita da almeno tre esercizi volti a verificare le conoscenze dello studente degli argomenti affrontati durante il corso, e di applicare le capacita' e le conoscenze acquisite. Durante il colloquio orale lo studente dovra' essere in grado di discutere le soluzioni proposte durante la prova scritta; inoltre saranno proposte domande di diverso e crescente livello di complessita' al fine di valutare il raggiungimento degli obiettivi formativi e le abilita' comunicative dello studente. Infine, allo scopo di valutare l'autonomia di giudizio, sara' richiesto di analizzare le caratteristiche di specifici scenari applicativi e di proporre le soluzioni piu' adeguate ai problemi individuati. |
| OBIETTIVI FORMATIVI | Il corso si propone di fornire allo studente i concetti di base nell'ambito della sicurezza dei sistemi di elaborazione. Durante il corso sono affrontate le tecniche di crittografia e la loro applicazione ai vari aspetti della sicurezza informatica. Vengono inoltre analizzati i principali protocolli alla base della progettazione di sistemi distribuiti sicuri. |
| ORGANIZZAZIONE DELLA DIDATTICA | Lezioni frontali ed esercitazioni in aula |
| TESTI CONSIGLIATI | William Stallings – Crittografia e Sicurezza nelle Reti, McGraw-Hill, 5 edizione William Stallings, and Lawrie Brown - Computer Security: Principles and Practice , 1/e |

PROGRAMMA

| ORE | Lezioni |
|-----|--|
| 4 | Sicurezza delle Reti |
| 4 | Elementi di Crittografia |
| 8 | Cifratura a chiave simmetrica - DES, AES |
| 6 | Generazione di numeri Pseudo-casuali |
| 8 | 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 |
| 4 | Sicurezza della posta elettronica |
| 4 | Sicurezza a livello rete |
| 4 | Sicurezza WEB |
| 4 | Firewall |
| 4 | Sicurezza dei sistemi Informatici |

PROGRAMMA

| ORE | Lezioni |
|------------|-------------------------------|
| 4 | Sicurezza delle Reti Wireless |

| ORE | Esercitazioni |
|------------|--|
| 6 | Cifratura a chiave simmetrica - DES, AES |
| 6 | Cifratura a chiave pubblica, RSA |
| 6 | Protocolli di sicurezza |
| 6 | Teoria dei numeri e campi finiti |
| 6 | Funzioni Hash |
| 6 | Esercitazioni al computer |