

<b>SICUREZZA DEI SISTEMI INFORMATICI E LABORATORIO DI SICUREZZA DEI SISTEMI INFORMATICI</b>			
<b>NUMERO DI CREDITI (CFU):</b> 9			
<b>SETTORE SCIENTIFICO-DISCIPLINARE:</b> INF/01			
<b>TIPOLOGIA DELL'INSEGNAMENTO:</b> a scelta			
<b>DOCENTE:</b> Prof. Giovanni SCHMID			
<b>FINALITÀ DEL CORSO:</b> Il corso si prefigge di fornire una panoramica ed una serie di approfondimenti sui metodi e le tecniche per la protezione dei sistemi software.			
<b>ARTICOLAZIONE DIDATTICA:</b> Il corso si articola in 3 sezioni secondo lo schema seguente: Introduzione alla sicurezza in Internet (ca. 24 h) - Laboratorio tematico (ca. 24 h) - Crittografia (ca. 24 h)			
lezioni: 40 h	esercitazioni: 8 h	laboratorio: 24 h	seminari:
<b>PROGRAMMA DEL CORSO:</b> Parte introduttiva preposta all'introduzione dei concetti, metodiche e problemi principali del contesto di Internet e dei suoi più attuali scenari d'uso. Laboratorio in tema di sicurezza di sistema operativo, sicurezza di rete o sicurezza web. Elementi di crittografia: Elementi di teoria della calcolabilità, Complessità computazionale, Significato algoritmico di casualità e generatori pseudocasuali , Funzioni pseudo casuali e cifrari, Identificazione, autenticazione e firma digitale.			
<b>PRE-REQUISITI:</b> Nessuna propedeuticità. E' consigliabile comunque seguire o aver seguito i corsi di Algoritmi/Strutture Dati e Sistemi Operativi (laboratorio).			
<b>MODALITÀ DI ACCERTAMENTO DEL PROFITTO:</b> Prova scritta e Esame orale con la discussione di un elaborato (Tesina o Progetto operativo).			
<b>TESTI DI RIFERIMENTO:</b> Libri di testo ufficiali del corso. Appunti a cura del docente e articoli tratti dalla letteratura scientifica internazionale.			
<b>NOTE:</b> Alcune fonti potrebbero essere in lingua inglese.			