

DTI 1.29	La sicurezza della comunicazione in rete: conoscenze di base
Presentazione	Le attività legate all'informatica, che richiedono comunicazioni sicure, sono in costante aumento. È sufficiente pensare all'odierna diffusione del commercio elettronico per rendersi conto dell'importanza di poter fare affidamento su transazioni sicure. Per poter giudicare l'efficacia dei metodi di sicurezza adottati dai produttori di software ed effettuare scelte corrette durante le installazioni e la gestione dei sistemi, è necessario capire i principi su cui si basano le tecniche di comunicazione sicura.
Obiettivi	Conoscere i principi della sicurezza informatica e le moderne tecniche di comunicazione sicura Applicare, attraverso studi di caso, le conoscenze acquisite
Programma	
Destinatari	Iscritti al MAS in Computer Science (MACS), ai corsi Specialista in sistemi e reti, Tecnologie software per Internet, Sicurezza informatica e Sviluppo di sistemi Wireless, informatici, ingegneri, interessati alla progettazione e alla gestione di reti telematiche, responsabili della sicurezza dei sistemi.
Requisiti	Sicurezza informatica - Introduzione - Definizioni, formulazione del problema, pericoli, attacchi, analisi e valutazione dei rischi, politica di sicurezza Nozioni di crittografia Crittosistemi simmetrici e asimmetrici Applicazioni della crittografia alla comunicazione in rete Distribuzione delle chiavi, firme digitali, autenticità di una firma, autenticità e integrità del messaggio, impronte di un messaggio, Smart card e E-commerce Sicurezza perimetrale Firewall e rivelazione di intrusi Tecniche di comunicazione sicura VPN, Internet e Intranet, autenticazione e servizi, standard (IPSEC, SSL, X.509, Kerberos); esempi pratici
Responsabile	Carlo Spinedi
Relatori	Andrea Graf, docente e ricercatore SUPSI Stefano Klett, Network & Security Engineer, ArgoNet, Lugano Silvano Marioni, docente SUPSI, CISSP, consulente informatico Altri specialisti del settore
Durata	24 ore-lezione
Date	14, 21, 28 settembre; 5, 12, 19 ottobre 2006
Orari	17.30-21.00
Costo	CHF 900 .-
Iscrizioni	Entro il 18 agosto 2006
Osservazioni	Questo è un modulo con indirizzo Sistemi e reti del MAS in Computer Science (MACS).
Certificato	Attestato di frequenza. 2 crediti di studio (ECTS) validi per il MAS in Computer Science (MACS) e per i corsi Specialista in sistemi e reti, Tecnologie software per Internet, Sicurezza informatica e Sviluppo di sistemi Wireless, subordinati al superamento dell'esame finale.