FACOLTÀ	Ingegneria
ANNO ACCADEMICO	2011/12
CORSO DI LAUREA MAGISTRALE	Ingegneria delle telecomunicazioni (D.M.270/04)
INSEGNAMENTO	Crittografia e sicurezza delle reti
TIPO DI ATTIVITÀ	Caratterizzante
AMBITO DISCIPLINARE	Ingegneria delle telecomunicazioni
CODICE INSEGNAMENTO	10041
ARTICOLAZIONE IN MODULI	No
NUMERO MODULI	
SETTORI SCIENTIFICO DISCIPLINARI	ING-INF/03
DOCENTE RESPONSABILE	Luigi ALCURI Professore Associato Università degli Studi di Palermo
CFU	9
NUMERO DI ORE RISERVATE ALLO STUDIO PERSONALE	129
NUMERO DI ORE RISERVATE ALLE ATTIVITÀ DIDATTICHE ASSISTITE	96
PROPEDEUTICITÀ	Nessuna
ANNO DI CORSO	Primo
SEDE DI SVOLGIMENTO DELLE LEZIONI	Consultare l'orario delle lezioni: http://portale.unipa.it/Ingegneria/
ORGANIZZAZIONE DELLA DIDATTICA	Lezioni frontali, Esercitazioni in aula, Esercitazioni in laboratorio
MODALITÀ DI FREQUENZA	Facoltativa
METODI DI VALUTAZIONE	Prova Orale, Presentazione di una Tesina
TIPO DI VALUTAZIONE	Voto in trentesimi
PERIODO DELLE LEZIONI	Primo semester
CALENDARIO DELLE ATTIVITÀ DIDATTICHE	Consultare il calendario didattico: http://portale.unipa.it/Ingegneria/
ORARIO DI RICEVIMENTO DEGLI STUDENTI	Previo appuntamento via e-mail: luigi_alcuri@dieet.unipa.it

RISULTATI DI APPRENDIMENTO ATTESI

Conoscenza e capacità di comprensione

Lo studente, al termine del corso, avrà acquisito conoscenze e metodologie per affrontare e risolvere in maniera originale problematiche di criptografia e sicurezza delle reti. Lo studente sarà in grado di analizzare il comportamento delle reti, di formulare processi evolutivi originali ed innovativi e di valutare l'impatto dell'introduzione di nuovi componenti.

Capacità di applicare conoscenza e comprensione

Lo studente avrà acquisito conoscenze e metodologie per analizzare e risolvere problemi tipici della Network Security. Egli sarà in grado di formulare strategie di evoluzione, modellare l'effetto di

interdipendenza, individuare gli output in termini prestazionali e ROI e valutarne le conseguenze con riferimento a contesti di NGN e NGN2.

Autonomia di giudizio

Lo studente avrà acquisito una metodologia di analisi propria della Criptografia; attraverso tale metodologia egli sarà in grado di affrontare problemi e prendere le relative decisioni. Attraverso l'approccio metodologico acquisito durante il corso, egli potrà modellare problematiche complesse nell'ambito dei sistemi integrati di nuova generazione anche a supporto dell'e-commerce.

Abilità comunicative

Lo studente sarà in grado di comunicare con competenza e proprietà di linguaggio problematiche complesse riguardanti le architetture di sicurezza anche in contesti altamente specializzati.

Capacità d'apprendimento

Lo studente sarà in grado di affrontare in autonomia qualsiasi problematica relativa alla *secrecy*, *confidentiality*, *non repudiability*, *authentication*, *integrity* e *security* in generale. Sarà in grado di approfondire tematiche complesse quali l'interlavoro tra reti differenti, le politiche di protezione, etc.

OBIETTIVI FORMATIVI DEL MODULO

I principali obiettivi formativi del corso consistono nell'acquisizione da parte dello studente di nozioni, metodologie e tecniche per lo studio e l'analisi dei moderni sistemi criptografici su cui si basa la sicurezza nelle transazioni telematiche.

MODULO	**CRITTOGRAFIA E SICUREZZA DELLE RETI**
ORE FRONTALI	**LEZIONI FRONTALI**
1	Introduzione al Corso
4	Tecniche classiche di criptografia
5	Cifrari a blocco
3	Campi finiti
3	Advanced Encryption Standard
4	Altri sistemi simmetrici di criptografia
3	Confidenzialità e cifratura simmetrica
2	Cenni sulla teoria dei numeri
3	Criptografia a chiave pubblica ed RSA
4	Gestione delle chiavi
5	Algoritmi Hash e Mac
5	Applicazioni di autenticazione
3	Sicurezza di email
4	Sicurezza a livello IP
4	Intrusion detection
4	Sicurezza dei sistemi wireless
3	Uso e programmazione delle smartcards
	ESERCITAZIONI
30	Esercitazioni teoriche e pratiche sugli argomenti svolti

TESTI CONSIGLIATI	- Stallings: Cryptography and Network Security. Pearson - Schneier: Applied cryptography. Wiley - Materiale didattico disponibile on-line: http://www.tti.unipa.it