UNIVERSITÀ DEGLI STUDI DI PALERMO

DIPARTIMENTO	Ingegneria
ANNO ACCADEMICO OFFERTA	2019/2020
ANNO ACCADEMICO EROGAZIONE	2019/2020
CORSO DILAUREA MAGISTRALE	INGEGNERIA INFORMATICA
INSEGNAMENTO	CRITTOGRAFIA
TIPO DI ATTIVITA'	B
AMBITO	50369-Ingegneria informatica
CODICE INSEGNAMENTO	20612
SETTORI SCIENTIFICO-DISCIPLINARI	ING-INF/05
DOCENTE RESPONSABILE	LO RE GIUSEPPE Professore Ordinario Univ. di PALERMO
ALTRI DOCENTI	
CFU	6
NUMERO DI ORE RISERVATE ALLO STUDIO PERSONALE	108
NUMERO DI ORE RISERVATE ALLA DIDATTICA ASSISTITA	42
PROPEDEUTICITA'	
MUTUAZIONI	
ANNO DI CORSO	1
PERIODO DELLE LEZIONI	1° semestre
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	Conoscenza e capacita' di comprensione (knowledge and understanding): Lo studente, al termine del corso, avra' acquisito conoscenze e metodologie per affrontare problematiche legate agli algoritmi di cifratura adottati nei moderni sistemi di elaborazione delle informazioni. Lo studente sara' in grado di analizzare algoritmi di cifratura a chiave simmetrica e pubblica e gli algoritmi di generazione dei numeri casuali adottati nell'ambito della sicurezza dei sistemi di elaborazione delle informazioni. Conoscenza e capacita' di comprensione applicate (applying knowledge and understanding): Lo studente avra' acquisito conoscenze e metodologie per analizzare la validita' e la complessita' di diversi algoritmi di cifratura. Autonomia di giudizio (making judgements): Lo studente avra' acquisito una metodologia di analisi dei meccanismi alla base dei moderni algoritmi di crittografia, giudicando la loro adeguatezza nella progettazione di sistemi sicuri per l'elaborazione delle informazioni. Abilita' comunicative (communication skills): Lo studente sara' in grado di discutere con competenza e proprieta' di linguaggio problematiche complesse legate agli algoritmi di crittografia. Capacita' di apprendere (learning skills): Lo studente sara' in grado di affrontare con autonomia l'analisi di qualsiasi algoritmo di crittografia.
VALUTAZIONE DELL'APPRENDIMENTO	Le conoscenze e le competenze acquisite dallo studente saranno verificate attraverso una prova scritta (prova in itinere + prova finale o prova complessiva) e un colloquio orale. Valutazione della prova scritta Durante il corso, in accordo con il calendario accademico, sara' possibile sostenere una prova in itinere. Tale prova, a discrezione dell'allievo potra' essere completata con una prova finale da sostenere nel periodo compreso tra la fine delle lezioni ed il primo appello del corso. La media pesata della prova in itinere e di quella finale costituisce il voto della prova scritta. La prova scritta (in itinere + finale o complessiva) e' 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. Nello svolgimento assume fondamentale importanza il commento teorico dei risultati ottenuti. L'articolazione della soluzione consente di apprezzare tutti i livelli di preparazione. La valutazione e' espressa in trentesimi ed un minimo di 15 e' richiesto per accedere alla prova orale. Valutazione per la prova orale La prova orale consiste in un colloquio, volto ad accertare il possesso delle competenze e delle conoscenze disciplinari previste dal corso; la valutazione viene espressa in trentesimi. 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. La valutazione finale terra' conto sia del punteggio della prova scritta (50%) che di quello delle prova orale (50%). Eccellente 30-30 e lode. Durante entrambe le prove lo studente dovra' dimostrare padronanza completa degli argomenti del corso. Durante il colloquio orale l'allievo dovra' dimostrare la maturita' di saper collegare i diversi aspetti trattati e la capacita' di saper generalizzare. Dovra' mostrare autonomia nella soluzione dei quesiti e la capacita' di individuare le informazioni necessarie per la soluzione degli stessi. Molto buono 27-29 Buona padronanza degli argomenti, lo studente e' in grado di applicare le conoscenze per risolvere i problemi proposti. Buono 24-26 buona conoscenza dei principali, discreta padronanza e proprieta' di linguaggio, con capacita' di applicare autonomamente le conoscenze alla soluzione dei problemi proposti. Discreto 21-23 Piu' che sufficiente padronanza degli argomenti principali dell'insegnamento, limitata capacita' di applicare autonomamente le conoscenze acquisite. Sufficiente 18-20 conoscenza di base degli argomenti principali dell'insegnamento e del linguaggio tecnico. Insufficientenon possiede una conoscenza accettabile dei contenuti degli argomenti trattati nell'insegnamento.

OBIETTIVI FORMATIVI	Il corso si propone di fornire allo studente i concetti di base nell'ambito della crittografia. Durante il corso sono affrontate le tecniche di crittografia e la loro applicazione ai vari aspetti legati alle loro caratteristiche.
ORGANIZZAZIONE DELLA DIDATTICA	Lezioni frontali ed esercitazioni in aula
TESTI CONSIGLIATI	William Stallings – Cryptography And Network Security, 7th Edition

PROGRAMMA

ORE	Lezioni
6	Elementi di Crittografia
6	Cifratura a chiave simmetrica - DES, AES
4	Generazione di numeri Pseudo-casuali
6	Cifratura a chiave pubblica, RSA
4	Teoria dei numeri e campi finiti
2	Elliptic curve cryptography

ORE	Esercitazioni
6	Cifratura a chiave simmetrica - DES, AES
6	Cifratura a chiave pubblica, RSA
4	Teoria dei numeri e campi finiti
6	Cifratura simmetrica e asimmetrica
2	Esercitazioni su elliptic curve cryptography