Università di Catania

DIPARTIMENTO: INGEGNERIA ELETTRICA ELETTRONICA E INFORMATICA

Corso di laurea in Ingegneria informatica (LM-32) A.A. 2022/2023

Programmazione didattica

Primo anno

Primo semestre

Denominazione	Att. Form.	SSD	CFU	Ore	Tip. Att.	Lingua
1001224 - INGEGNERIA DEL SOFTWARE **Canale: A - Z** *TOMARCHIO Orazio*	B	ING-INF/05	9	79	AP	ITA
1001928 - TECNOLOGIA DEI SISTEMI DI CONTROLLO **Canale: A - Z** *GAMBUZZA LUCIA VALENTINA*	B, C	ING-INF/04	6	50	AP	ITA
1002043 - SICUREZZA DEI SISTEMI INFORMATIVI **Canale: A - Z** *MALGERI Michele Giuseppe*	B	ING-INF/05	6	50	AP	ITA
1001827 - INSEGNAMENTO A SCELTA	D		9	79	AP	ITA
1002682 - ALTRE CONOSCENZE UTILI PER L'INSERIMENTO NEL MONDO DEL LAVORO	F		3	18	I	ITA

Secondo semestre

Denominazione	Att. Form.	SSD	CFU	Ore	Tip. Att.	Lingua
1001628 - ARCHITETTURE E TECNOLOGIE DEI SISTEMI DI TELECOMUNICAZIONI **Canale: A - Z** *PANNO Daniela Giovanna Anna* *corso erogato presso - DESIGN OF COMMUNICATION NETWORKS AND SYSTEMS (9796796) - RIOLO SALVATORE*	C	ING-INF/03	9	79	AP	ITA
1002067 - RETI PER L'AUTOMAZIONE INDUSTRIALE **Canale: A - Z** *LO BELLO Lucia*	B	ING-INF/05	9	79	AP	ITA

Denominazione	Att. Form.	SSD	CFU	Ore	Tip. Att.	Lingua
1015336 - ADVANCED COMPUTER ARCHITECTURES **Canale: A - Z** *ASCIA Giuseppe*	B	ING-INF/05	6	50	AP	ITA

Secondo anno

Primo semestre

Denominazione	Att. Form.	SSD	CFU	Ore	Tip. Att.	Lingua
1015347 - ADVANCED PROGRAMMING LANGUAGES **Canale: A - Z** *CARCHIOLO Vincenza* *MANGIONI GIUSEPPE*	B	ING-INF/05	9	79	AP	ITA
1015340 - INTERNET OF THINGS BASED SMART SYSTEMS **Canale: A - Z** *CATANIA Vincenzo* *PALESI MAURIZIO*	B	ING-INF/05	9	79	AP	ITA
1016152 - DISTRIBUTED SYSTEMS AND BIG DATA **Canale: A - Z** *DI STEFANO Antonella* *MORANA GIOVANNI*	B	ING-INF/05	9	79	AP	ITA

Secondo semestre

Denominazione	Att. Form.	SSD	CFU	Ore	Tip. Att.	Lingua
1015361 - INDUSTRIAL INFORMATICS **Canale: A - Z** *CAVALIERI Salvatore*	B	ING-INF/05	9	79	AP	ITA
1015335 - COGNITIVE COMPUTING AND ARTIFICIAL INTELLIGENCE **Canale: A - Z** *GIORDANO Daniela*	B	ING-INF/05	9	79	AP	ENG
Gruppo opzionale: Gruppo Opzionale PROVA FINALE	E			450		

Dettaglio dei gruppi opzionali

Denominazione	Att. Form.	SSD	CFU	Ore	Tip. Att.	Lingua
Gruppo opzionale: Gruppo Opzionale PROVA FINALE						
1002356 - PROVA FINALE *(secondo semestre)*	E		18	450	AP	ITA
9794133 - PROVA FINALE IN AZIENDA *(secondo semestre)*			0	0	AP	ITA
MOD. ATTIVITA' DI RICERCA E/O PROGETTAZIONE IN AZIENDA *(secondo semestre)*	E		17	425		
MOD. ATTIVITA' DI REDAZIONE E DISCUSSIONE ELABORATO FINALE *(secondo semestre)*	E		1	25		
9794134 - PROVA FINALE ESTERO *(secondo semestre)*			0	0	AP	ITA
MOD. ATTIVITA' DI RICERCA E/O PROGETTAZIONE ALL'ESTERO *(secondo semestre)*	E		17	425		
MOD. ATTIVITA' DI REDAZIONE E DISCUSSIONE ELABORATO FINALE *(secondo semestre)*	E		1	25		

Legenda

Tip. Att. (Tipo di attestato): **AP** (Attestazione di profitto), **AF** (Attestazione di frequenza), **I** (Idoneità)

Att. Form. (Attività formativa): **A** Attività formative di base **B** Attività formative caratterizzanti **C** Attività formative affini ed integrative **D** Attività formative a scelta dello studente (art.10, comma 5, lettera a) **E** Per la prova finale e la lingua straniera (art.10, comma 5, lettera c) **F** Ulteriori attività formative (art.10, comma 5, lettera d) **R** Affini e ambito di sede classe LMG/01 **S** Per stages e tirocini presso imprese, enti pubblici o privati, ordini professionali (art.10, comma 5, lettera e)

Obiettivi formativi

SICUREZZA DEI SISTEMI INFORMATIVI

in - Primo anno - Primo semestre

Docente: ***MALGERI Michele Giuseppe***

Crittografia
Terminologia e concetti fondamentali: Algoritmi, principio di Kerckhoff, parametri e robustezza di un algoritmo di cifratura, violabilità di cifrario. Sistemi crittografici sicuri. (*)Principio di diffusione e confusione. Codici, rappresentazione dell'alfabeto.
Cenni sulle tecniche di cifratura classiche: Tecniche monoalfabetiche, (*)OTP (studio della complessità, della robustezza, limiti, crittoanalisi); (*)tecniche polialfabetiche: Vigenere, crittoanalisi; tecniche trasposizione: Rail fence, trasposizione per colonne; Macchine a rotazione: (*)enigma, dettagli costruttivi, meccanismo di funzionamento, (*)calcolo dello spazio delle chiavi
Cifratura a blocchi: caratteristiche generali. (*)Concetto di cifratura prodotto. Cifrario di Feistel. (*)DES, (*)doppio DES e (*)triplo DES, caratteristiche generali. Motivazione, (*)funzionamento, (*)robustezza,(*)progettazione della funzione F e del blocco S. (*)criteri SAC e BIC. Generazione delle chiavi. Crittoanalisi: elementi deboli noti, (*)chiavi, complementazione, differenziale, linerare. (*)AES, criteri di scelta, caratteristiche generali(*), (*)funzionamento, (*)robustezza, (*)generazione delle chiavi *cenni sul campo finito di Galois*
(*)Tecniche di Concatenazione per cifrari a blocchi, ECB, CBC, FCB, OFB, CTR (dettagli del funzionamento, debolezze e/o forza di ogni tecnica)
(*)Cifratura a Flusso: struttura della cifratura a flussi, cifrario RC4
Distribuzione delle chiavi: Tecniche di distribuzione delle chiavi, problemi di segretezza, durata.
Algoritmi a chiave pubblica: (*)Protocollo di Diffie-Hellmann. Requisiti della crittografia a chiave pubblica. (*)RSA
Meccanismi di base:
Message authentication code. (*)Hashing. Algoritmi di hashing, (*)SHA, MD5
(*)Firma Digitale
Certificati, (*)X509, gestione della revoca (OCSP), (*)Public Key Infrastructure
Autenticazione: password, salt, criteri, sistemi otp (*)Kerberos (funzionamento, problemi di distribuzione, possibili attacchi)
(*)PGP, storia, (*)algoritmi,certificati, (*)gestione del trust
Reti e Firewall
(*)Classificazione, Principali topologie. (*)Configurazione di un firewall. iptables
(*)IPSec , (*)architettura, (*)AH e ESP, gestione delle chiavi
(*)SSL, (*)protocolli, (*)architettura, transport Layer Security
SSH, funzionalità ed uso, protocollo, handshaking, tipi di autenticazione
Posta Elettronica, problemi della posta elettronica, (*)S/MIME, Posta Elettronica Certificata
Cenni sulle tecniche di analisi dei rischi, economicità.
Gli argomenti in cui è presente (*) rappresentano le competenze minime.