



Università degli Studi di Enna "Kore"

Facoltà di Ingegneria ed Architettura

Anno Accademico 2019 - 2020

SCHEDA DI TRASPARENZA PER LE ATTIVITA' DI DIDATTICA DIGITALE

A.A.	Settore Scientifico Disciplinare			CFU	Insegnamento	Ore in Ambiente Virtuale		Mutuazione	
2019/20	ING-INF/05			9	Sicurezza dei Sistemi Informatici e Laboratorio	56 (48 frontali + 8 di laboratorio)		No	
Classe	Corso di studi				Tipologia di insegnamento	Anno di corso e Periodo		Orario	
L8	Ingegneria Informatica				Caratterizzante	III Anno Secondo Semestre		Vedi Calendario	
N° Modulo	Nome Modulo	Tipologia lezioni	E-tivity	Ore Totali	Docente	SSD	Ruolo	Interno	Affidamento
No		DE/DI Video lezione interattiva	Problem solving	56	Vincenzo Conti vincenzo.conti@unikore.it	ING-INF/05	RTD	Si	Istituzionale

Contenuti e struttura del corso

N.	ARGOMENTO	TIPOLOGIA	DURATA
1	Concetti sulla Sicurezza Informatica: Attacchi, Servizi, Meccanismi	Frontale	2h
2	Cifratura Simmetrica Classica e Criptoanalisi	Frontale	4h
3	Introduzione Cifratura Simmetrica Moderna: Cifrari a Blocchi	Frontale	2h
4	Concetti di base sulla Teoria dei Numeri e sui Campi Finiti	Frontale	2h
5	Algoritmi di Crittografia: DES, Double DES, Triple DES, AES	Frontale	8h
6	Modi di Funzionamento dei Cifrari a Blocchi	Frontale	2h
7	Generatori di Numeri Pseudo-Casuali e Cifrari a Flusso	Frontale	2h
8	Introduzione Cifratura Asimmetrica: Chiave Pubblica e Chiave Privata	Frontale	2h
9	Algoritmi RSA e a Curva Ellittica	Frontale	4h



Università degli Studi di Enna "Kore"
Facoltà di Ingegneria e Architettura

10	Protocollo Scambio Chiave di Sessione: Diffie-Hellaman	Frontale	2h
11	Protocollo Scambio Chiave Pubblica e Certificati	Frontale	2h
12	Esercitazioni	Esercitazioni	16h
15	Laboratorio: Sviluppo di un Sistema di Sicurezza	Laboratorio	8h

Modalità di svolgimento del corso fino al 30 maggio 2020

A seguito delle disposizioni del DPCM dell'11.03.2020 e successivi il Corso di Sicurezza dei Sistemi Informatici e Laboratorio, fino al 30-05-2020, è organizzato in ambiente virtuale, utilizzando la piattaforma UNIKOREFAD e Google Meet, coadiuvate dall'utilizzo di qualsiasi supporto informatico che si renda necessario per garantire agli studenti il miglior grado di efficacia didattica e favorire la partecipazione attiva.

Il corso è articolato in DIDATTICA EROGATIVA (DE) e DIDATTICA INTERATTIVA (DI).

Nell'ambito della DIDATTICA EROGATIVA (DE) sono utilizzate le lezioni in web conference

Nell'ambito della DIDATTICA INTERATTIVA (DI) sono compresi:

- gli interventi didattici rivolti da parte del docente all'intera classe (o a un suo sottogruppo), tipicamente sotto forma di dimostrazioni o spiegazioni aggiuntive presenti in faq, mailing list o web forum (dimostrazione o suggerimenti operativi su come si risolve un esercizio e/o programma);
- gli interventi brevi effettuati dai corsisti (ad esempio in ambienti di discussione o di collaborazione: web forum);
- le forme tipiche di valutazione formativa, con il carattere di questionari o test in itinere e le E-tivity strutturate (individuali), sotto forma tipicamente di problem solving, effettuati dagli studenti con relativo feedback

Note. Per quanto non espressamente riportato, si rimanda alla scheda di trasparenza generale dell'insegnamento pubblicata nel sito del corso di laurea.