Principali informazioni sull'insegnamento	**A.A. 2019-2020**
Titolo insegnamento	Metodi Formali per la Sicurezza
Corso di studio	Sicurezza Informatica
Crediti formativi	6 (4 + 1 + 1)
Denominazione inglese	Formal Methods for Computer Security
Obbligo di frequenza	No
Lingua di erogazione	Italiano

Docente responsabile	Nome Cognome	Indirizzo Mail
	Gennaro Vessio Gianvito Pio	gennaro.vessio@uniba.it gianvito.pio@uniba.it
Luogo ed Orario di Ricevimento	Dip. Informatica 4° Piano	Previo accordo via mail

Dettaglio credi formativi	Ambito disciplinare	SSD	Crediti
	Informatico	INF/01 - Informatica	6 (4 + 1 + 1)

Modalità di erogazione	
Periodo di erogazione	Primo semestre
Anno di corso	Secondo anno
Modalità di erogazione	Lezioni frontali Esercitazioni guidate

Organizzazione della didattica	
Ore totali	150
Ore di corso	47
Ore di studio individuale	103

Calendario	
Inizio attività didattiche	Ottobre 2019
Fine attività didattiche	Dicembre 2019

Syllabus	
Prerequisiti	Conoscenze di base dell'Informatica, quali programmazione, linguaggi di programmazione, algoritmi e fondamenti. Conoscenze di base di Calcolo delle Probabilità e Statistica.
Risultati di apprendimento previsti	*Conoscenza e capacità di comprensione* Conoscenza dei principali formalismi per l'analisi critica di sistemi critici e complessi, con particolare riferimento a problemi di sicurezza. *Conoscenza e capacità di comprensione applicate* Conoscenza delle soluzioni esistenti in letteratura e capacità di analizzarle rispetto a problemi reali.

	Autonomia di giudizio Consapevolezza della necessità di trattare formalmente i sistemi informatici in generale e i problemi della sicurezza in particolare. *Abilità comunicative* Abilità comunicative nell'illustrare in modo adeguato problemi, rischi e soluzioni.
Contenuti di insegnamento	Parte teorica: Modelli simbolici e sub-simbolici per la progettazione e analisi di soluzioni software a problemi critici e complessi, con particolare riferimento ad aspetti legati alla sicurezza. Introduzione alla blockchain. Le blockchain di Bitcoin ed Ethereum. Problemi di sicurezza e possibili attacchi nelle blockchain. Parte applicativa: Applicazione di metodi simbolici all'analisi di protocolli di routing sicuri per reti mobili ad-hoc. Applicazione di metodi sub-simbolici alla progettazione di sistemi per la pubblica sicurezza. Programmazione di smart contract Ethereum nel linguaggio Solidity.

Programma	
Testi di riferimento	1. E. Börger, R. Stärk, *Abstract State Machine – A Method for High-Level System Design and Analysis*, Springer 2003 2. James, G., Witten, D., Hastie, T., & Tibshirani, R. (2013). *An introduction to statistical learning* (Vol. 112, p. 18). New York: Springer. 3. Chris Dannen, *Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners* (2017) 4. Richard Ma, Jan Gorzny, Edward Zulkoski, Kacper Bak, Olga V. Mack, *Fundamentals of Smart Contract Security* (2019)
Note ai testi di riferimento	I libri di testo sono integrati con le dispense dei docenti e con articoli scientifici di approfondimento.
Metodi didattici	Lezioni frontali, esercitazioni.
Metodi di valutazione	Caso di studio e prova orale.
Criteri di valutazione	Valutazione della capacità di analisi critica da parte dello studente.
Altro	