UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

CONSIGLIO INTERCLASSE IN MATEMATICA

CORSO DI STUDIO LAUREA MAGISTRALE IN MATEMATICA (LM-40)

ANNO ACCADEMICO 2023-2024

INSEGNAMENTO CRITTOGRAFIA

Principali informazioni sull'insegnamento	
Anno di corso	Secondo
Periodo di erogazione	Secondo semestre (26 febbraio 2024 – 31 maggio 2024)
Crediti formativi universitari (CFU)	7
Settore scientifico disciplinare (SSD)	MAT/02 – Algebra
Lingua di erogazione	Italiano
Modalità di frequenza	Facoltativa

Docenti	
Nome e cognome	Roberto La Scala
Indirizzo mail	roberto.lascala@uniba.it
Telefono	+39 080 544 2674
Sede	Dipartimento di Matematica, stanza 28 secondo piano
Sede virtuale	Microsoft Teams: Crittografia, codice 8ge6u5g
Pagina web	https://www.dm.uniba.it/it/members/lascala
Ricevimento	Lun. Mer. Ven. 12:00 – 13:00, in presenza oppure online (previa prenotazione)

Organizzazione della didattica				
	Totali	Didattica frontale	Pratica	Studio individuale
Ore	175	56		119
CFU	7	7		

Obiettivi formativi	
	Acquisizione dei concetti e dei metodi della Crittografia moderna.

Prerequisiti	
	Le conoscenze che in genere vengono acquisite nei tre anni di una laurea della classe L-35. In particolare: aritmetica, strutture algebriche e probabilità discreta.

Syllabus	
Contenuti dell'insegnamento (Programma)	Crittografia classica, crittoanalisi. Teoria dell'informazione di Shannon, segretezza perfetta, entropia dell'informazione, key-equivocation. Cifrari prodotto, cifrari a blocchi, Data Encryption Standard, Advanced Encryption Standard. Crittografia a chiave pubblica, crittosistema RSA, test di primalità, radici quadrate modulo n, algoritmi di fattorizzazione. Logaritmi discreti, crittosistema di ElGamal, calcolo di logaritmi discreti. Applicazioni della crittografia alla firma digitale.
Testi di riferimento	D. Stinson, Cryptography: theory and practice, 3rd Edition, 2005 S. Vaudenay, A classical introduction to cryptography, Springer, 2006
Note ai testi di riferimento	Microsoft Teams
Materiali didattici	Implementazione di algoritmi nel linguaggio di programmazione di SageMath.

Risultati di apprendimento previsti (secondo i Descrittori di Dublino)	
DD1 Conoscenza e capacità di comprensione	Capacità di comprendere le idee che hanno permesso lo sviluppo dei maggiori cifrari in uso nella crittografia moderna e la loro crittoanalisi.
DD2 Conoscenza e capacità di comprensione applicate	Le conoscenze generali acquisite nel corso si utilizzano per l'implementazione e l'analisi dei cifrari presentati.
DD3-5 Competenze trasversali	*DD3 Autonomia di giudizio*: *Capacità di valutare la correttezza dei metodi presentati. Capacità di individuare strumenti adeguati per affrontare problemi di riservatezza delle informazioni.*
	DD4 Abilità comunicative: Acquisizione del linguaggio algoritmico, necessario per la comprensione, l'analisi e l'esposizione dei metodi inerenti la crittografia e la crittoanalisi.
	DD5 Capacità di apprendere: Acquisizione di un metodo di studio adeguato, supportato dalla implementazione degli algoritmi e dei cifrari proposti durante il corso.

Metodi didattici	
	Lezioni ed esercitazioni in aula.

Valutazione	
Modalità di verifica dell'apprendimento	Prova orale finale.
Criteri di valutazione	• *Conoscenza e capacità di comprensione*: • *Conoscenza e capacità di comprensione applicate*: • *Autonomia di giudizio*: • *Abilità comunicative*: • *Capacità di apprendere*:
Criteri di misurazione dell'apprendimento e di attribuzione del voto finale	Voto finale espresso in trentesimi con superamento dell'esame a partire da 18 trentesimi.

Ulteriori informazioni	
	La frequenza delle lezioni ed esercitazioni è fortemente consigliata.