Insegnamento di:
Crittografia

Classe di laurea: LM-40 – Matematica		**Corso di Laurea in:** Matematica	**Anno accademico:** 2018/2019
Denominazione inglese insegnamento: Cryptography		**Tipo di insegnamento:** Obbligatorio/A scelta in dipendenza dell'orientamento	**Anno:** / **Semestre:** 2
Tipo attività formativa: b - Attività caratterizzante	**Ambito disciplinare:** Formazione Teorica	**Settore scientifico-disciplinare:** MAT/02	**CFU totali:** 7 di cui CFU lezioni: 6.5 CFU ese/lab/tutor: 0.5

Modalità di erogazione, ore di didattica assistita ed ore dedicate allo studio individuale
ore di lezione: 52
ore di esercitazione/laboratorio/tutorato: 8
totale ore didattica assistita: 60
totale ore di studio individuale: 90

Lingua di erogazione: Italiano	**Obbligo di frequenza:** no		
Docente: Roberto La Scala	**Tel:** +39 080 5442674 **e-mail:** roberto.lascala@uniba.it	**Ricevimento studenti:** Dip. Matematica piano 2, stanza 28	**Giorni e ore ricevimento:** Lunedì 11-13. In altri giorni e orari previo appuntamento.

Conoscenze preliminari:
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.

Obiettivi formativi: Acquisizione dei concetti e dei metodi della crittografia moderna.

Risultati di apprendimento previsti

Conoscenza e capacità di comprensione:
Acquisizione dei concetti fondamentali della crittografia moderna e dei metodi correlati.

Conoscenza e capacità di comprensione applicate:
Le conoscenze teoriche acquisite si utilizzano nelle tecnologie della sicurezza delle informazioni.

Autonomia di giudizio:
Capacità di valutare la correttezza dei metodi presentati. Capacità di individuare i giusti strumenti matematici e le giuste tecniche per affrontare problemi di sicurezza delle informazioni.

Abilità comunicative:
Acquisizione del linguaggio computazionale, necessario per la comprensione e la realizzazione dei metodi, l'analisi e la risoluzione dei problemi.

Capacità di apprendere:
Acquisizione di un metodo di studio adeguato, supportato dalla implementazione di algoritmi capaci di risolvere i problemi proposti periodicamente durante il corso.

Programma del corso
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.

Metodi di insegnamento:
Lezioni ed esercitazioni in aula.

Supporti alla didattica:
Implementazione di algoritmi nel linguaggio di programmazione di SageMath.

Controllo dell'apprendimento e modalità d'esame:
Prova orale.

Testi di riferimento principali:
D. Stinson, Cryptography: theory and practice, 3rd Edition, 2005
S. Vaudenay, A classical introduction to cryptography, Springer, 2006