

<b>Insegnamento di:</b> Crittografia			
<b>Classe di laurea:</b> LM-40 – Matematica		<b>Corso di Laurea in:</b> Matematica	
<b>Denominazione inglese insegnamento:</b> Cryptography		<b>Anno accademico:</b> 2017/2018	
<b>Tipo di insegnamento:</b> Obbligatorio/A scelta in dipendenza dell'orientamento		<b>Anno:</b>	<b>Semestre:</b> 2
<b>Tipo attività formativa:</b> b - Attività caratterizzante	<b>Ambito disciplinare:</b> Formazione Teorica	<b>Settore scientifico-disciplinare:</b> MAT/02	<b>CFU totali:</b> 7 di cui CFU lezioni: 6.5 CFU ese/lab/tutor: 0.5
<b>Modalità di erogazione, ore di didattica assistita ed ore dedicate allo studio individuale</b> ore di lezione: 52 ore di esercitazione/laboratorio/tutorato: 8 totale ore didattica assistita: 60 totale ore di studio individuale: 90			
<b>Lingua di erogazione:</b> Italiano	<b>Obbligo di frequenza:</b> no		
<b>Docente:</b> Roberto La Scala	<b>Tel:</b> +39 080 5442674 <b>e-mail:</b> roberto.lascala@uniba.it	<b>Ricevimento studenti:</b> Dip. Matematica piano 2, stanza 28	<b>Giorni e ore ricevimento:</b> Lunedì 11-13. In altri giorni e orari previo appuntamento.
<b>Conoscenze preliminari:</b> 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.			
<b>Obiettivi formativi:</b> Acquisizione dei concetti e dei metodi della crittografia moderna.			
<b>Risultati di apprendimento previsti</b>	<p><b>Conoscenza e capacità di comprensione:</b> Acquisizione dei concetti fondamentali della crittografia moderna e dei metodi correlati.</p> <p><b>Conoscenza e capacità di comprensione applicate:</b> Le conoscenze teoriche acquisite si utilizzano nelle tecnologie della sicurezza delle informazioni.</p> <p><b>Autonomia di giudizio:</b> 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.</p> <p><b>Abilità comunicative:</b> Acquisizione del linguaggio computazionale, necessario per la comprensione e la realizzazione dei metodi, l'analisi e la risoluzione dei problemi.</p> <p><b>Capacità di apprendere:</b> Acquisizione di un metodo di studio adeguato, supportato dalla implementazione di algoritmi capaci di risolvere i problemi proposti periodicamente durante il corso.</p>		
<b>Programma del corso</b> 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.			
<b>Metodi di insegnamento:</b> Lezioni ed esercitazioni in aula.			
<b>Supporti alla didattica:</b> Implementazione di algoritmi nel linguaggio di programmazione di SageMath.			
<b>Controllo dell'apprendimento e modalità d'esame:</b> Prova orale.			

**Testi di riferimento principali:**

D. Stinson, Cryptography: theory and practice, 3rd Edition, 2005

S. Vaudenay, A classical introduction to cryptography, Springer, 2006