UNIVERSITÀ
DEGLI STUDI DI MILANO-BICOCCA

SYLLABUS DEL CORSO

Teoria dei Numeri e Crittografia

2526-1-F4002Q032

Obiettivi

Coerentemente con gli obiettivi formativi del Corso di Studio, l'insegnamento si propone di fornire alcuni concetti e alcune tecniche di Teoria dei numeri, fondamentali per introdurre lo studente alla comprensione del funzionamento dei principali sistemi crittografici a chiave pubblica, che fanno uso dell'aritmetica modulo n e delle curve ellittiche su campi finiti.

I risultati di apprendimento attesi comprendono: la conoscenza di classici test di primalità di tipo probabilistico, e del test deterministico AKS; la conoscenza della struttura di gruppo di una curva ellittica su un campo finito e applicazioni al problema del logaritmo discreto e al problema della fattorizzazione di un numero intero; la capacità di analizzare e riproporre le dimostrazioni presentate durante le lezioni e di risolvere alcuni facili problemi facendo uso delle tecniche presentate; la capacità di approfondire, anche in maniera autonoma, alcuni dei risultati presentati durante il corso

Obiettivi formativi e risultati di apprendimento attesi, espressi secondo i cinque Descrittori di Dublino:

Conoscenza e capacità di comprensione (knowledge and understanding):
Lo studente acquisirà conoscenze avanzate di Teoria dei numeri con particolare riferimento all'aritmetica modulare, alla teoria delle curve ellittiche su campi finiti, ai test di primalità (probabilistici e deterministici), e ai fondamenti matematici di alcuni principali sistemi crittografici a chiave pubblica. Tali conoscenze saranno fondate su una solida preparazione matematica di base e intermeda e consentiranno di comprendere il ruolo delle strutture algebriche e aritmetiche in contesti applicativi.

Capacità di applicare conoscenza e comprensione (applying knowledge and understanding):
Lo studente sarà in grado di applicare le tecniche apprese per analizzare criticamente i principali algoritmi crittografici basati su problemi di Teoria dei numeri (come la fattorizzazione e il logaritmo discreto), e per risolvere problemi teorici ed esercizi, anche con elementi computazionali, connessi ai contenuti trattati.

Autonomia di giudizio (making judgements):
Lo studente svilupperà la capacità di valutare criticamente l'efficacia e la sicurezza di vari protocolli crittografici, e

di interpretare autonomamente risultati teorici e dimostrazioni, individuando ipotesi rilevanti e metodi di generalizzazione.

Abilità comunicative (communication skills):
Lo studente acquisirà la capacità di esporre con rigore e chiarezza i concetti teorici e le tecniche apprese, sia in forma scritta sia orale, utilizzando una terminologia matematica appropriata e adeguata al contesto scientifico e applicativo.

Capacità di apprendimento (learning skills):
Lo studente sarà in grado di approfondire autonomamente argomenti affini o complementari, consultando la letteratura matematica specialistica e comprendendo articoli e testi avanzati di Teoria dei numeri e crittografia matematica, anche in lingua inglese.

Contenuti sintetici

Il Corso presenta alcuni risultati di Teoria dei numeri, con particolare riguardo a test di primalità e metodi di fattorizzazione usando argomenti classici di Teoria dei numeri e le curve ellittiche.

Programma esteso

- Richiami sui numeri interi e sui campi finiti, aritmetica modulare, funzione di Eulero, teorema cinese del resto.
- Introduzione ai sistemi crittografici; chiave pubblica e chiave privata.
- Numeri primi: cenni sul Teorema di Dirichlet. Primalità e fattorizzazione:numeri pseudoprimi, alcuni test di primalità (Fermat, Jacobi, Miller-Rabin, AKS), metodo rho per la fattorizzazione; complessità computazionale di un algoritmo.
- Un'introduzione ai caratteri di Dirichlet.
- Cenni sulla funzione zeta di Riemann e sulle funzioni L(?,s); fattorizzazione di Eulero; cenni su ipotesi generalizzata di Riemann e ripercusssioni sui test di primalita
- Crittosistema di Diffie ed Hellman. Il problema del logaritmo discreto.
- Curve ellittiche: equazione di Weierstrass, gruppo dei punti di una curva ellittica, curve ellittiche su campi finiti.
- Endomorfismi di curve ellittiche.
- Teorema di Hasse (dimostrazione: cenni)
- Punti di torsione e Weil pairing
- Alcuni crittosistemi basati sulle curve ellittiche.
- Il problema del Logaritmo discreto. Attacco MOV. Baby step - Giant step.
- Firma digitale (DSA e ECDSA).
- Isogenie di curve ellittiche: definizione e cenni sul loro uso nel problema del logaritmo discreto

Prerequisiti

Conoscenze di base sulle strutture algebriche, generalmente acquisite nei corsi di Algebra di un corso di Laurea di Primo Livello, con particolare riguardo ai gruppi, gruppi abeliani finitamente generati e ai campi finiti.

Modalità didattica

Lezioni frontali (8 CFU), articolate in: lezioni teoriche in cui si fornisce la conoscenza di definizioni, risultati e teoremi rilevanti e altre in cui si intende fornire competenze e abilità necessarie per utilizzare tali nozioni nella risoluzione di esercizi e nell'analisi di problemi.

Per stimolare la partecipazione, sono proposti con regolarità agli studenti alcuni esercizi, la cui risoluzione viene da essi caricata sul sito e-learning.

In totale: 56 ore di lezione in presenza. Si utilizza un approccio didattico ibrido che combina didattica frontale (DE) e didattica interattiva (DI). La DE include la presentazione e spiegazione dettagliata dei contenuti teorici. La DI prevede interventi attivi degli studenti tramite esercizi e problemi, brevi interventi, discussioni collettive e lavori di gruppo o individuali. Non è possibile stabilire precisamente a priori il numero di ore dedicate alla DE e alla DI, poiché le modalità si intrecciano in modo dinamico per adattarsi alle esigenze del corso e favorire un apprendimento partecipativo e integrato, combinando teoria e pratica.

Materiale didattico

I principali testi di riferimento sono:

- N. Koblitz, A course in Number Theory and Cryptography, volume 114 of Graduate texts in Mathematics, Springer-Verlag, second edition, 1994.
- H.E. Rose, A course in Number Theory, II edizione, Oxford: Clarendon press, 1994
- Lawrence C. Washington, Elliptic Curves, Number Theory and Criptogtaphy CRCPress

Altri testi:

- Maria Welleda Baldoni, Ciro Ciliberto, Giulia Maria Piacentini Cattaneo, Elementary Number Theory, Cryptography and Codes, 2009 Springer-Verlag Berlin Heidelberg
- Graham Everest, Thomas Ward Introduction to Number Theory, Springer-Verlag London Limited 2005
- A. Languasco, A. Zaccagnini, Introduzione alla Crittografia, Hoepli Editore, 2004.

Periodo di erogazione dell'insegnamento

II semestre.

Modalità di verifica del profitto e valutazione

Esame scritto e orale

- La prova scritta consiste in alcuni esercizi da cui si evinca la capacita' dello studente a usare gli strumenti introdotti nelle lezioni
- Per quanto riguarda l'orale, obbligatorio per tutti, questo consiste in due parti:
  Prima parte: discussione dello scritto;
  Seconda parte: lo studente puo' scegliere se

1. fare una classica prova orale in cui mostri la conoscenza e la padronanza degli argomenti trattati durante il corso, spieghi le motivazioni che hanno portato a trattare alcuni argomenti teorici che hanno risvolti applicativi e
   dia gli enunciati e le dimostrazioni dei teoremi;
2. dare un seminario in cui si approfondisca un argomento solo accennato durante il corso.

entrambe le modalità dovranno permettere di verificare la conoscenza e padronanza dei contenuti del corso e la capacità di rielaborare i concetti appresi e di esporli in modo rigoroso.

Valutazione dell'esame: Voto in trentesimi 18-30/30

Lo studente è ammesso a sostenere la prova orale se raggiunge la votazione di 18/30 nello scritto

La discussione dello scritto e la prova orale concorrono alla valutazione finale, che è ottenuta dalla media tra la votazione ottenuta nello scritto+discussione (accorpati) e dalla seconda parte dell'orale.

Orario di ricevimento

Su appuntamento.

Sustainable Development Goals

ISTRUZIONE DI QUALITÁ