UNIVERSITÀ
DEGLI STUDI DI MILANO-BICOCCA

SYLLABUS DEL CORSO

Teoria dei Numeri e Crittografia

2627-1-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, campin finiti, e vari strumenti di teoria dei numeri.

I risultati di apprendimento attesi comprendono: la conoscenza di classici test di primalità di tipo probabilistico; la conoscenza 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, ai 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..

Contenuti sintetici

Il corso presenta risultati di algebra e teoria dei numeri di interesse crittografico, e le loro applicazioni. Particolare attenzione sara rivolta ad aspetti algoritmici e di complessita computazionale. Gli argomenti includearanno test di primalità e metodi di fattorizzazione.

Programma esteso

- Richiami di vari argomenti sui numeri interi e l'aritmetica modulare, con attenzione ad aspetti di complessita` computazionale.
- Introduzione ai sistemi crittografici a chiave segreta e a chiave pubblica. Firme digitali.
- Numeri primi: cenni al Teorema di Dirichlet sui primi in progressione aritmetica, e al teorema dei numeri primi.
- I campi finiti e la legge di reciprocita` quadratica.
- Analisi dettagliata del crittosistema RSA: rischi e accortezze.
- Il logaritmo discreto in un campo finito, e sue applicazioni (incuso il crittosistema di Diffie-Hellmann).
- Primalità: test di primalità probabilistici (Fermat, Jacobi, Miller-Rabin), e test deterministici in certi casi.
- Metodi di fattorizzazione: metodo rho, metodo delle factor bases.
- A seconda del tempo e dell'interesse, cenni a qualche altro argomento di interesse o conseguenze crittografiche, quali: caratteri e serie di Dirichlet; stime di somme di caratteri; la funzione zeta di Riemann; fondamenti sulle curve ellittiche; il test di primalita` (deterministico) AKS.

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 esercizi da svolgere a casa. Le soluzioni saranno discusse a richiesta in classe, o a ricevimento.

Il corso comprende 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

Sono fornite delle note del corso, tratte in parte dal seguente testo, che si invita a consultare per approfondimenti:

- N. Koblitz, A course in Number Theory and Cryptography, volume 114 of Graduate texts in Mathematics, Springer-Verlag, second edition, 1994.

Si vedano le note per eventuali altre letture suggerite.

Periodo di erogazione dell'insegnamento

II semestre.

Modalità di verifica del profitto e valutazione

Esame scritto e orale

- La prova scritta richiedera` la risoluzione di alcuni esercizi, principalmente di carattere pratico.
- Nella prova orale si dovra` mostrare la conoscenza e la padronanza degli argomenti trattati durante il corso (inclusi enunciati e dimostrazioni dei teoremi).

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

Lo svolgimento dello scritto e la prova orale concorrono alla valutazione finale del corso.

Orario di ricevimento

Su appuntamento.

Sustainable Development Goals

ISTRUZIONE DI QUALITÁ