UNIVERSITÀ
DEGLI STUDI DI MILANO-BICOCCA

SYLLABUS DEL CORSO

Teoria dei Numeri e Crittografia

2223-1-F4001Q073

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, 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

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.

- Cenni sulla funzione zeta di Riemann e sulle funzioni L(?,s) fattorizzazione di Eulero; ipotesi di Riemann, 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).
- Cenni su isogenie di curve ellittiche e attacchi crittografici

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

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:
- discussione dello scritto;
- lo studente puo' scegliere se fare una classica prova orale in cui mostri la conoscenza e la padronanza degli argomenti trattati durante il corso, spiegando le motivazioni che hanno portato a trattare alcuni argomenti teorici, ma con risvolti applicativi, dando gli enunciati e le dimostrazioni dei teoremi, oppure dare un seminario in cui si approfondisca un argomento solo accennato durante il corso.

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