

METODI MATEMATICI DELLA CRITTOGRAFIA

DAVIDE LOMBARDO

Anno accademico	2020/21
CdS	MATEMATICA
Codice	147AA
CFU	6

Moduli	Settore	Tipo	Ore	Docente/i
METODI MATEMATICI DELLA CRITTOGRAFIA/a	MAT/02	LEZIONI	42	PATRIZIA GIANNI DAVIDE LOMBARDO CARLO TRAVERSO

Obiettivi di apprendimento

Conoscenze

Verranno sviluppate alcune nozioni di base relative alla teoria delle curve ellittiche, con una particolare attenzione al caso in cui il campo di definizione sia un campo finito.

Gli studenti acquisiranno inoltre le conoscenze degli algoritmi e degli strumenti di base della crittografia, con particolare riferimento ai metodi basati sulla teoria delle curve ellittiche.

Modalità di verifica delle conoscenze

Si valuterà l'abilità dello studente di discutere con competenza e chiarezza i contenuti principali del corso.

Metodo:

* Esame orale finale

Capacità

Gli studenti acquisiranno le conoscenze necessarie per partecipare alla ricerca nel campo della crittografia matematica, specialmente in riferimento a metodi basati sulla conoscenza delle curve ellittiche. Sapranno anche collaborare all'implementazione di algoritmi in questo campo, compresi algoritmi di crittanalisi. Acquisiranno in particolare la capacità di utilizzare la teoria delle curve ellittiche come strumento per la risoluzione di problemi matematici e crittografici.

Modalità di verifica delle capacità

Verifica nel corso dell'esame orale finale, che comprenderà anche una breve relazione tecnica su un argomento a scelta

Comportamenti

Gli studenti sono consigliati a frequentare le lezioni e a studiare gli argomenti via via presentati.

Modalità di verifica dei comportamenti

Nessuna

Prerequisiti (conoscenze iniziali)

I prerequisiti di aritmetica, fondamenti di algebra, algebra polinomiale, campi finiti, algebra lineare sono insegnati nei corsi del primo anno, e saranno comunque ripresi a lezione.

I prerequisiti necessari di carattere crittografico e algebro-geometrico insegnati in altri corsi saranno richiamati e saranno date precise indicazioni bibliografiche.

Corequisiti

Il corso è indipendente da altri corsi, anche se sinergie sono possibili.

Prerequisiti per studi successivi

Indicazioni su studi utili per la continuazione delle ricerche illustrate nel corso saranno date a lezione o in documentazione resa disponibile.

Programma (contenuti dell'insegnamento)

CURVE ELLITTICHE

Richiami sulle varietà algebriche.

Curve ellittiche su un campo, equazioni di Weierstrass, legge di gruppo sui punti di una curva ellittica, differenziale invariante.

Isogenie: grado di un'isogenia, isogenia duale. L'isogenia di moltiplicazione per un intero. Anello degli endomorfismi di una curva ellittica.

Accoppiamento di Weil.

Punti di torsione e modulo di Tate di una curva ellittica.

Curve ellittiche su campi finiti: azione del Frobenius, teorema di Hasse-Weil.

CRITTOGRAFIA

I concetti e i protocolli crittografici base: crittografia simmetrica, crittografia a chiave pubblica: cifra, KEM (key establishment methods), firma.

hash, successioni pseudo casuali. Criteri di sicurezza, zero-knowledge proofs.

Protocolli a chiave pubblica "classici": RSA, Diffie Helman, El Gamal e corrispondenti problemi matematici (fattorizzazione, logaritmo discreto).

ARITMETICA

Calcolo della radice quadrata su un campo finito: algoritmi di Cipolla e Tonelli-Shanks. Equivalenza del calcolo della radice quadrata modulo N composto e della fattorizzazione di N .

Test di primalità: Test di Miller Rabin. Test di Pocklington-Lehmer. Algoritmo di Agrawal-Kayal-Saxena. Ricerca di numeri primi.

Fattorizzazione di interi: algoritmi $p-1$ e Rho di Pollard. Algoritmi di Fermat, di Dixon, quadratic sieve e algebraic number sieve.

Logaritmo discreto: Algoritmi Rho e Lambda (algoritmo del canguro) di Pollard. Algoritmo di Pohlig-Hellmann, algoritmi di Index Calculus.

Algoritmo di Shor (cenni). Calcolo quantistico dell'ordine di un elemento mod N , e tramite questa fattorizzazione e Logaritmo discreto.

ALGORITMI ARITMETICI CHE USANO CURVE ELLITTICHE

Fattorizzazione di Lenstra (generalizzazione dell'algoritmo $p-1$ di Pollard alle curve ellittiche) Algoritmo di Goldwasser-Kilian come generalizzazione del test di Pocklington-Lehmer.

ALGORITMI CRITTOGRAFICI SULLE CURVE ELLITTICHE

Logaritmo discreto sulle curve ellittiche. Attacchi e protocolli basati su accoppiamenti.

Algoritmi per calcolare il numero di punti di una curva ellittica: Baby-step-giant-step, Schoof, Schoof-Elkies-Atkin

Crittografia basata sulle curve ellittiche: protocolli, attacchi e problemi. Confronto con RSA, Diffie-Hellmann su campi finiti. Problemi di certificazione e trusted third party.

Cenni su altri protocolli crittografici basati su diversi problemi algebrici.

Bibliografia e materiale didattico

N. Koblitz A course in number theory and cryptography

S. Goldwasser and M. Bellare Lecture Notes on Cryptography (MIT notes) <https://cseweb.ucsd.edu/~mihir/papers/gb.html>

J. Silverman, The Arithmetic of Elliptic Curves

Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Handbook of Applied Cryptography, <http://cacr.uwaterloo.ca/hac/>

Modalità d'esame

Esame orale

Stage e tirocini

A richiesta, anche per conto di altri corsi.

Ultimo aggiornamento 20/09/2020 21:52