UNIVERSITÀ DI PISA

# TEORIA DEI CODICI E CRITTOGRAFIA

## CARLO TRAVERSO

| | |
|---|---|
| Anno accademico | 2018/19 |
| CdS | MATEMATICA |
| Codice | 079AA |
| CFU | 6 |

| Moduli | Settore/i | Tipo | Ore | Docente/i |
|---|---|---|---|---|
| TEORIA DEI CODICI E CRITTOGRAFIA | MAT/02 | LEZIONI | 48 | PATRIZIA GIANNI<br>CARLO TRAVERSO |

### Obiettivi di apprendimento

*Conoscenze*
Gli studenti avranno una conoscenza degli algoritmi e srumenti di base per i codici correttori e la crittografia, e una buoma base di partenza per ulteriori ricerche sul tema.

*Modalità di verifica delle conoscenze*
Gli studenti saranno valutati dalla loro dimostrazione di abilità nel discutere i contenuti principali del corso con l'uso della terminologia appropriata
Metodo:

- Esame orale finale

*Capacità*
Riconoscere gli algoritmi e i protocolli appropriati per la comunicazione e l'autenticazione di documenti con affidabilità e confidenzialità.

*Modalità di verifica delle capacità*
Verifica nel corso dell'esame orale finale, che comprenderà 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, e soprattutto in caso di impossibilità a frequentare tenersi aggiornati con colloqui coi docenti.

*Modalità di verifica dei comportamenti*
Tramite colloqui durante le lezioni e i ricevimenti

### 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.

### Corequisiti
Alcuni concetti utili sono insegnati nel corso di Algebra II, ma sono comunque ripresi a lezione.

### Prerequisiti per studi successivi
I temi di ricerca sulla crittografia post-quantistica sono critici per il futuro della crittografia (e i codici correttori ne sono un ingrediente essenziale) Parte del corso sarà dedicata ad una breve presentazione di alcuni di questi metodi.

### Indicazioni metodologiche
Esame: orale
Frequenza: consigliata

Attività di insegnamento:

- Frequenza alle lezioni frontali
- Preparazione di esposti orali
- Studio individuale

Metodologia di Insegnamento:

- Lezioni frontali

## Programma (contenuti dell'insegnamento)

ARITMETICA
Complessità delle operazioni sugli interi: somma, prodotto, divisione, GCD. Karatsuba.
Complessità delle operazioni modulari: esponenziale. Radice quadrata su un campo finito: algoritmi di Cipolli e Tonelli-Shanks.
Equivalenza di radice quadrata modulo n composto e fattorizzazione di n.
Simbolo di Legendre e di Jacobi, reciprocità quadratica.
Test di primalità: Solovay-Strassen, Miller-Rabin, ricerca di numeri primi.
Fattorizzazione di polinomi su campi finiti. Rialzamento P-adico.
CODICI CORRETTORI
Codici lineari e trasmissione. MLD (Maximum Likelihood Decoding). Errori e cancellature, soft decoding. Lunghezza, distanza, dimensione.
Codici a blocchi e di convoluzione.
Esempi di codici: parità, ripetizione, codice duale. Codici accorciati, bucati, estesi, contratti. Codici di Hamming.
Matrice generatrice e di parità. Codici sistematici.

Diseguaglianze sui codici: Hamming, Singleton, Gilbert-Varshamov.
Codici ciclici, Reed-Müller, Reed-Solomon, BCH, Goppa, codici di convoluzione.
Decodifica dei codici: polinomio locatore, equazione chiave, maggioranza, Viterbi.
Esempio di uso dei codici: CD audio.
CRITTOGRAFIA
Algoritmi e protocolli crittografici. Cifratura, firma, identificazione, scambio di chiavi. Cifratura simmetrica e a chiave pubblica. Hash crittografico.
Successioni pseudocasuali crittografiche.
Definizione di sicurezza crittografica: IND-CPA, IND-CCA, IND-CCA2. Zero-knowledge proof.
Protocolli crittografici: DES, AES. RSA, Diffie-Hellmann, El Gamal, DSS, Blum-Goldwasser, Merkle-Hellmann. Autenticazione: Fiat-Shamir, Fiat-Feige-Shamir.
ALGORITMI ARITMETICI E CRITTANALISI
Fattorizzazione degli interi: rho di Pollard, N-1, criterio di Fermat, crivelli, crivello quadratico.
Logaritmo discreto: baby step-giant step, rho, Pohlig-Hellmann, basi di fattori.
CURVE ELLITTICHE E CRITTOGRAFIA
Curve ellittiche, fattorizzazione tramite curve ellittiche.
Crittografia su curve ellittiche.
ALGEBRA LINEARE INTERA
Algebra lineare sugli interi, reticoli. Vettore più corto, vettore più vicino. Teorema di Minkowski. Basi ridotte. Algoritmi di Babai.
LLL, fattorizzazione dei polinomi a coefficianti interi tramite reticoli.
Crittanalisi tramite LLL.
CALCOLO QUANTISTICO E CRITTOGRAFIA POST QUANTISTICA (cenni)
Cenni sul Calcolo quantistico e sugli algoritmi di Shor e Grover.
Cenni di crittografia post-quantistica. Standardizzazione di protocolli post-quantistici del NIST.
Alcuni esempi: reticoli, LWE, NTRU, HFE, McEliece-Niederreiter e possibilmente altri.

## Bibliografia e materiale didattico

Letture consigliate di parti di:
D. G. Hoffman D. A. Leonard C. C. Lidner K. T. Phelps C. A. Rodger *Coding Theory: The Essentials*
H. J. van Lint *Introduction to Coding Theory*
N Koblitz *A course in number theory and cryptography*
N. Koblitz *Algebraic aspects of cryptography*
D Micciancio, S Goldwasser *Complexity of lattice problems: a cryptographic perspective*,
*Post-quantum cryptography* (D. Bernstein, J. Buchmann, E. Dahmen, eds.)
S. Goldwasser and M. Bellare *Lecture Notes on Cryptography* (MIT notes) https://cseweb.ucsd.edu/~mihir/papers/gb.html

## Indicazioni per non frequentanti

Gli studenti sono invitati a colloqui coi docenti anche su appuntamento.

## Modalità d'esame

Esame orale finale.

## Stage e tirocini

A richiesta, anche per conto di altri corsi.

### Pagina web del corso
http://barba.dm.unipi.it/CCC

### Altri riferimenti web
https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

*Ultimo aggiornamento 11/10/2018 06:27*