UNIVERSITÀ
DEGLI STUDI DI MILANO-BICOCCA

COURSE SYLLABUS

Information Theory and Cryptography

2526-1-F1802Q139

Obiettivi

Conoscenza e capacità di comprensione
Gli studenti comprenderanno i principi di funzionamento dei codici per la correzione d'errore, e di alcune semplici tecniche di compressione dati lossless (senza perdita di informazione). Comprenderanno inoltre il funzionamento di un crittosistema o di un protocollo crittografico.

Conoscenza e capacità di comprensione applicate
Gli studenti saranno in grado di scegliere gli strumenti crittografici adatti per proteggere i dati durante la loro trasmissione e/o memorizzazione.

Autonomia di giudizio
Gli studenti acquisiranno la capacità di valutare se gli algoritmi proposti di correzione degli errori, di compressione dati, e di cifratura, sono adeguati.

Abilità comunicative
La grande attenzione posta sugli aspetti formali permetterà agli studenti di comprendere l'importanza di una comunicazione non ambigua, utilizzando la terminologia corretta per esprimere le nozioni e i concetti appresi.

Capacità di apprendere
La formalizzazione dei concetti faciliterà i meccanismi di apprendimento deduttivo. Inoltre, l'esposizione di esempi ed esercizi svolti alla lavagna, subito dopo aver spiegato una tecnica o un algoritmo, consentirà di chiarire eventuali dubbi e casi particolari.

Contenuti sintetici

Nozioni e concetti alla base della Teoria dell'Informazione, della Teoria dei Codici e della Crittografia moderna. Il

corso fornisce inoltre gli strumenti concettuali e teorici che consentono di comprendere le tecniche avanzate attualmente utilizzate per proteggere la trasmissione e la memorizzazione di informazioni in presenza di agenti ostili o di rumore nel canale.

Programma esteso

1. Codici per la correzione degli errori:

- Definizione di sorgente, canale, codifica
- Codici per il riconoscimento di errori. Controlli di parità
- Codici a correzione d'errore. Approccio geometrico e approccio algebrico. Codici di Hamming

2. Codifica di sorgente:

- Codici istantanei e loro costruzione
- Disuguaglianze di Kraft e di McMillan
- Codici di Huffman

3. L’entropia:

- Definizione e proprietà matematiche
- Codici di Shannon-Fano
- Primo teorema di Shannon

4. Il canale rumoroso:

- Definizione di canale, entropie di canale e mutua informazione
- Capacità di canale
- Il canale binario simmetrico
- Secondo teorema di Shannon

5. Introduzione alla Crittografia:

- Definizione di crittosistema
- Modelli di attacco
- Crittosistemi storici, e loro crittoanalisi

6. Crittosistemi simmetrici:

- Crittosistemi standard: DES, 3DES e AES
- Modi di funzionamento dei crittosistemi simmetrici

7. Fondamenti teorici dei crittosistemi simmetrici:

- Confusione e diffusione
- Reti di permutazione e sostituzione
- Struttura di Feistel

8. Crittosistemi a chiave pubblica:

- Funzioni one-way: logaritmi discreti e il problema della fattorizzazione
- Protocollo di Diffie-Hellman. Il crittosistema ElGamal. Crittosistemi ibridi

- Il crittosistema RSA. Alcuni semplici attacchi ad RSA. RSA randomizzato

9. Generatori di numeri pseudo-casuali
10. Schemi di firma digitale
11. Funzioni di hash crittografiche
12. Cenni alla crittografia post-quantum

Prerequisiti

Argomenti trattati nei corsi di matematica della laurea triennale in Informatica. È utile - ma non indispensabile - la conoscenza di alcune nozioni di base di informatica teorica (in particolare, macchine di Turing).

Modalità didattica

20 lezioni da 2 ore svolte in aula, in modalità erogativa, in presenza.
10 esercitazioni da 2 ore svolte in aula, in modalità erogativa, in presenza.

La lingua di erogazione prevista è l'Italiano. Tuttavia, lezioni ed esercitazioni potranno essere erogate in Inglese se si verifica almeno una delle seguenti condizioni:

- in aula c'è almeno uno studente straniero che non parla Italiano;
- gli studenti fanno richiesta di seguire lezioni ed esercitazioni erogate in Inglese.

Tutte le lezioni saranno videoregistrate, e le videoregistrazioni saranno disponibili nella pagina Web del corso.

Materiale didattico

Libri:

- R.W. Hamming. Coding and Information Theory. Second edition, Prentice-Hall, 1986
- D.R. Stinson. Cryptography: Theory and Practice. Fourth Edition, CRC Press, 2018

Appunti forniti dal docente.

Periodo di erogazione dell'insegnamento

Secondo semestre

Modalità di verifica del profitto e valutazione

La verifica dell'apprendimento è basata su un colloquio orale avente per oggetto gli argomenti svolti a lezione. Durante il colloquio verrà valutata la capacità dello studente di esporre gli argomenti del corso, e di effettuare brevi ragionamenti su di essi.

Non sono presenti prove in itinere.

Orario di ricevimento

Su appuntamento

Sustainable Development Goals

ISTRUZIONE DI QUALITÁ