

CRITTOGRAFIA

ANNA BERNASCONI

Anno accademico

2019/20

CdS

INFORMATICA

Codice

245AA

CFU

6

Moduli	Settore	Tipo	Ore	Docente/i
CRITTOGRAFIA	INF/01	LEZIONI	48	ANNA BERNASCONI

Obiettivi di apprendimento

Conoscenze

Lo studente che completa il corso con successo avrà acquisito una solida conoscenza delle primitive crittografiche fondamentali, della crittografia a chiave pubblica, delle firme digitali, della generazione di numeri pseudo-casuali e dei protocolli di base e dei loro requisiti di complessità computazionale.

Modalità di verifica delle conoscenze

Nell'esame scritto (2 ore), lo studente deve dimostrare la propria conoscenza del materiale didattico e della sua capacità di simulare protocolli di base crittografici.

Metodi:

Esame scritto finale

Capacità

Comprendere le nozioni elementari sottostanti il progetto dei sistemi di cifratura moderni.

Prerequisiti (conoscenze iniziali)

Nozioni di base di algebra, teoria della probabilità, algoritmi e strutture dati, sistemi operativi.

Indicazioni metodologiche

Attività didattiche:

lezioni frontali

esercitazioni in aula

studio individuale

Frequenza delle lezioni: consigliata

Metodi di insegnamento: lezioni

Programma (contenuti dell'insegnamento)

- Introduzione: definizione di crittografia e crittoanalisi
- Generatori di numeri pseudo-casuali
- Cifrari Storici
- Cifrari perfetti: definizione e proprietà, il One-time pad
- Cifrari a chiave simmetrica: DES, Triple-DES e AES
- Cifrari composti
- Cifrari a chiave pubblica: funzioni one-way trapdoor e RSA
- Crittografia su curve ellittiche
- Identificazione, Autenticazione e Firma digitale
- Il sistema SSL
- Protocolli "Zero Knowledge"
- La moneta elettronica e i protocolli bitcoin
- Elementi di crittografia quantistica

Bibliografia e materiale didattico

[BFL] Anna Bernasconi, Paolo Ferragina e Fabrizio Luccio. "Elementi di Crittografia", Pisa University Press 2015.

Modalità d'esame

Scritto e eventuale orale per spiegare lo scritto.

Ultimo aggiornamento 02/08/2019 17:35