UNIVERSITÀ DEL SALENTO

SCHEDA INSEGNAMENTO

A005487 - CRITTOGRAFIA

Corso di studi di riferimento	LM39 - MATEMATICA
Dipartimento di riferimento	DIPARTIMENTO DI MATEMATICA E FISICA "ENNIO DE GIORGI"
Settore Scientifico Disciplinare	MAT/03
Crediti Formativi Universitari	9
Ore di attività frontale	LEZ:63
Ore di studio individuale	
Anno di corso	2°
Semestre	
Lingua di erogazione	Italiano
Percorso	022 - APPLICATIVO

Prerequisiti	Aver superato Geometria I e II, Algebra I e II. Si richiede, inoltre, la conoscenza della Teoria delle Probabilità discrete ed elementi di Teoria della complessità computazionale.
Contenuti	Il corso è dedicato l'acquisizione dei principi della crittografia classica e moderna. Particolare attenzione è dedicata alle tecniche matematiche utilizzate in ambito crittografico.
Obiettivi formativi	**Conoscenze e comprensione.** Acquisire un'ampia conoscenza dei principi e degli strumenti matematici su cui si fonda la sicurezza delle comunicazioni segrete. **Capacità di applicare conoscenze e comprensione.** Saper utilizzare diverse aree della matematica, come la teoria dei numeri, la teoria dei gruppi e dei campi, la teoria delle curve ellittiche e il calcolo delle probabilità discrete per la costruzione dei cifrari in uso per la sicurezza delle comunicazioni. Essere capaci di stabilire i punti di forza e di debolezza circa la sicurezza e la efficienza computazionali di un sistema crittografico. **Autonomia di giudizio.** Saper estrapolare e interpretare i dati ritenuti utili a determinare giudizi autonomi riguardanti sia problemi strettamente collegati alle tematiche sviluppate nel corso, sia problemi non necessariamente di ambito matematico ma collegate alla sicurezza delle comunicazioni. **Abilità comunicative.** Saper comunicare problematiche e soluzioni inerenti ad argomenti di Crittografia a interlocutori

	specialisti e non specialisti. **Capacità di apprendimento.** Essere consapevoli come diverse aree della matematica concorrano nella soluzione di problemi concreti, come, ad esempio, la mediazione tra sicurezza delle comunicazioni e l'efficienza computazionale dei sistemi crittografici. Essere in grado di comprendere autonomamente testi di livello avanzato ed articoli scientifici, anche a livello di ricerca.
Metodi didattici	Lezioni frontali ed esercitazioni.
Modalità d'esame	Gli studenti dovranno prenotarsi per sostenere l'esame finale utilizzando esclusivamente le modalità online previste dal sistema VOL.
Programma esteso	**Crittografia classica.** Fondamenti. Cifrario di Cesare, cifrario mediante sostituzione, cifrario affine, cifrario di Vigenère, cifrario di Hill, cifrario mediante permutazione. Crittosistemi a flusso. Principi della crittanalisi. Crittanalisi del cifrario affine, del cifrario mediante sostituzione, del cifrario di Hill. Crittanalisi dei cifrari a flusso LFSR. Elementi della Teoria di Shannon. Segeretezza perfetta. Caratterizzazione dei cifrari perfetti. Cifrario One-time Pad. Cifrari prodotto. **Cifrari a blocco. Advanced Encryption Standard.** Reti di sostituzione-permutazione (SPN). Crittanalisi lineare. Lemma Piling up. Approssimazione degli S-box. Attacchi lineari agli SPN. Crittanalisi differenziale. Data Encryption Standard: descrizione ed analisi. Advanced Encryption Standard: descrizione ed analisi. **Funzioni Hash Crittografiche.** Funzioni hash e integrità dei dati. Sicurezza delle funzioni hash. Il modello dell'oracolo random: algoritmi e confronto tra i sistemi di sicurezza. Funzioni hash iterate. La costruzione di Merkle-Damgård. L'algoritmo hash sicuro (SHA-1). Codici di autenticazione dei messaggi (MAC). MAC nidificati, HMAC, CBC-MAC. MAC incondizionatamente sicuri. Famiglie hash fortemente universali. Ottimalità della probabilità di inganno. **Il Crittosistema RSA e la fattorizzazione degli interi.** Introduzione alla crittografia a chiave pubblica. Il crittosistema RSA. Test di Primalità: Soloway-Strassen, Miller-Rabin. Radici quadrate modulo un intero. Algoritmi per la fattorizzazione: algoritmo di p-1 di Pollard, algorithmo rho di Pollard, algoritmo di Dixon sui quadrati casuali. Ulteriori attacchi al RSA: calcolo della funzione di Eulero, esponente di decifratura, attaco di Wiener all'esponente basso di cifratura. **Crittosistemi a chiave pubblica basati sul Problema del Logaritmo Discreto.** Crittosistema di El-Gamal. Algoritmi per il calcolo del problema del logaritmo discreto: algoritmo

	di Shank, algorithmo rho di Pollard per il problema del logaritmo discreto, Algoritmo di Pohlig-Hellmann. Curve ellittiche sui reali e sui campi finiti. Punti di compressione e sistemi di cifratura basati su curve ellittiche. Calcolo dei punti multipli su curve ellittiche. Sicurezza dei crittosistemi di El-Gamal. Crittosistema di Diffie-Hellmann. **Firma digitale.** Requisiti di sicurezza per uno schema di firma digitale. Firma digitale e funzioni hash. Schema di firma digitale di El-Gamal e relative varianti. Schema di firma di Schnorr. Algoritmo di firma digitale. schema di firma basato s curve ellittiche. Schemi di firma dimostrabilmente sicuri. Firme digitali one-time. Full domain hash. Firme digitali non ripudiabili. Firme Fail-stop.
Testi di riferimento	• O. Goldreich, Foundations of Cryptography, Cambridge University Press, 2001. • J. Katz, Y. Lindell, Introduction to Modern Cryptography, Second Edition, Chapman & Hall/CRC, 2014 • N. Koblitz, A course in Number Theory and Cryptography, Springer, 2nd edition, 1999. • D. R. Stinson, Cryptography Theory and Practice, Third Edition, Chapman & Hall/CRC 2005 • L. C. Washington, Elliptic curves. Number Theory and Cryptography, Chapman & Hall/Crc Florida, 2nd edition (2003) • Dispense del corso


UNIVERSITÀ
DEL SALENTO